

CERTIFICATE SERVICES AGREEMENT

This is a **binding legal agreement** between SSL Corp., a Nevada corporation doing business as SSL.com ("SSL.com"), and the person who establishes a Certificate Services account with SSL.com ("you").

- By submitting an Application, you are making legal representations and warranties to SSL.com and third parties who rely on your Certificate.
- SSL.com may revoke your Certificate if you violate this Agreement, and on other grounds described below.
- An individual who submits an Application for Certificate Services on behalf of a company or other legal entity represents and warrants to SSL.com that he or she has the legal authority to submit the Application and bind that entity to this Agreement.

Capitalized terms used in this document have special meanings as stated in Section 1 (Definitions).

This Agreement includes a binding arbitration clause and class action waiver provision. **This means that you are required to use arbitration on an individual basis to resolve disputes rather than a court action with a jury, or a class action.**

1. Definitions

Capitalized Terms are as defined in this section.

Agreement means, collectively:

1. this SSL.com Certificate Services Agreement, and
2. the online terms for each Certificate Services Product that you select, whether for purchase or to use without charge on a free or trial basis.

Application means, collectively, your submission of information to SSL.com to: (i) open a Certificate Services account, (ii) make a Certificate Signing Request, and (iii) enable SSL.com to verify your Certificate information.

Backdated Revocation means to revoke a Certificate and use a date/time entry in the past. This mainly applies to Certificates used to sign data objects (e.g., Code Signing and Document Signing Certificates). When a certificate is revoked with a certain revocation date/time entry, any signature created after that revocation date/time entry will effectively be

nullified.

Certificate means a digital certificate that has been signed by SSL.com.

Certificate Services means SSL.com's validation and certificate signing process, and related support and services included with the applicable Certificate Services Product.

Certificate Services Product means the SSL.com bundle of services offered as part of a single subscription as described in SSL.com's online materials, such as the Basic, Wildcard, SAN/UCC, and EV products.

Certificate Signing Request or **CSR** means your submission of a certificate signing request via an SSL.com defined process and form.

Code is a contiguous set of bits that has been or can be digitally signed with a Private Key that corresponds to a Code Signing Certificate.

Code Signing Certificate is a digital certificate issued by a CA that contains a Code Signing Extended Key Usage.

Code Signing Subscriber means a Subscriber that controls a Private Key associated with a Code Signing Certificate capable of signing code.

Confidential Information means:

1. for SSL.com, SSL.com's business continuity plans, including incident response, contingency and disaster recovery plans, SSL.com's security documentation, including security practices and methodology, audit logs and archive records related to any part of the SSL.com PKI; SSL.com's transaction records, financial audit records and external or internal audit trail records related to SSL.com; external auditor reports related to SSL.com (but not including any auditor's letter or document designed for public release that confirms the result of an external audit); and
2. for both parties,
 1. private keys, any data regarding your access to or activation of private keys, and any data utilized to access the SSL.com PKI infrastructure,
 2. information regarding a party's assets, liabilities, financial results, financing plans, business strategies, pricing, product development plans, marketing strategies, operations, source code, technology, know-how, trade secrets, customers, distributors, sales channels, contractors, suppliers, employees, other personnel, and
 3. all other information disclosed by a party that the other party should reasonably understand to be confidential, due to the nature of the information or the circumstances of its disclosure, regardless of the form or manner in which it is disclosed, and regardless of whether the information is marked or designated as confidential. Confidential Information does not include information that becomes publicly known through no fault of the Receiving Party. **Confidential Information**

does not include Certificate Signing Requests, Certificates, Certificate status information, and other information that SSL.com publishes as part of providing the Certificate Services or information.

CP/CPS means the SSL.com Certification Practices Statement published at [https://www.ssl.com/repository/ https://legal.ssl.com/documents/SSLcom-CP-CPS.pdf](https://www.ssl.com/repository/https://legal.ssl.com/documents/SSLcom-CP-CPS.pdf) as it may be modified from time to time in accordance with its terms.

Hardware Crypto Module is a tamper-resistant device, with a cryptography processor, used for the specific purpose of protecting the lifecycle of cryptographic keys (generating, managing, processing, and storing).

Key Pair means the Private Key and its associated Public Key.

Online Certificate Status Protocol (OCSP) means the online certificate status protocol (OCSP) which is one of the two protocols aside from certificate revocation lists (CRL) for providing the status of a certain X.509 certificate.

Personal Data means information that can be used to identify you as an individual, such as your name, business name, email address, telephone number, and photograph.

Public Key Infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

Privacy Policy means the current SSL.com Privacy Policy, available at https://www.ssl.com/privacy_policy/.

Private Key means the private key corresponding to the public key included in a Certificate.

Public Key means the corresponding cryptographic key to the Private Key included in a Certificate.

Relying Party is an entity that relies upon the information contained within the Certificate.

Representative means an individual appointed by you as described in Section 2 (*Certificate Services*) to make Certificate Signing Requests

Revocation means an action by SSL.com to its certificate status services such that a Certificate is marked to no longer be trusted.

Revoke means to perform Revocation on an issued Certificate such that no new signatures or trust may be generated using the revoked certificate.

Signing Service means an organization that generates the Key Pair and securely manages the

Private Key associated with a Code Signing Certificate, on behalf of a Subscriber.

Subscriber means the entity that has been issued a Certificate.

Suspect Code: Code that contains malicious functionality or serious vulnerabilities, including spyware, malware, and other code that installs without the user's consent and/or resists its own removal, code that compromises user security, and/or code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes.

2. Application for Certificate Services, Certificate Signing Requests

On your submission of all information required to establish an account for Certificate Services and each Certificate Signing Request, and payment of the applicable fee, SSL.com will process your Application. SSL.com will use commercially reasonable efforts to verify the information provided by you in your Application. SSL.com has no obligation to accept your Application and may refuse to do so on any reasonable basis.

3. Certificate Services

If SSL.com accepts your Application, it will provide the Certificate Services you purchased subject to the terms, conditions, and restrictions stated in the Agreement. This Agreement applies to all Certificate Signing Requests and Certificates, including the initial and all subsequent multiple requests that you may make. The Certificate Services are provided on a subscription basis for a limited term. SSL.com has no obligation to provide the Certificate Services following the expiration of the initial term or any renewal term unless you have renewed the Certificate Services prior to expiration as provided in this Agreement. Your right to use any Certificates issued during the term of your Certificate Services expires on the expiration of the Certificate Services. SSL.com may terminate the Certificate Services, and revoke any Certificates prior to the expiration of your subscription term for your violation of this Agreement and other grounds as provided in Section 7 (*Term and Termination*) below.

SSL.com may test its pre-production systems by creating concurrent versions of your Certificate. **These test certificates are for test purposes only and may not be used by you or SSL.com in a production environment.** At your request, we will provide you with a copy of any test certificate we create, provided you acknowledge this limitation in writing.

You must identify at least one individual (natural person) as your authorized employee or agent to submit a Certificate Signing Request on your behalf (each a "**Representative**"). The Representative(s) must be named using SSL.com's online dashboard, or other SSL.com approved process. SSL.com may rely on the information and instructions submitted by your

Representative(s) until it receives your written notice of revocation of authority. You must notify SSL.com and update your Representative information if any Representative is no longer authorized to act on your behalf.

Your Certificate Signing Requests must be submitted on SSL.com's certificate request form, either electronically via your dashboard, or via other SSL.com approved means.

4. Your Obligations and Restrictions on Use

4.1. You must review your Certificate for accuracy

You must review each Certificate for accuracy. If a Certificate is inaccurate you may not use it, even if the inaccuracy is due to an error by SSL.com. You must notify SSL.com of any inaccuracy and cooperate in the correction of the inaccuracy.

4.2. You must comply with the law

You must use the Certificate Services and your Certificates in compliance with applicable local, State, national and international law and regulations. You may not export your Certificate or permit the use of the Certificate Services in violation of United States export law.

4.3. You must protect your Private Key

You must take all reasonable measures to protect your Certificate Services account, your Private Key(s), and any associated activation data or device (such as a password, pass phrase, or token) from unauthorized use and disclosure. You may not create a Private Key that is substantially similar to an SSL.com or third party's Private Key.

For Code Signing Subscribers, you agree that you will use one of the following options to generate and protect your Code Signing Certificate Private Keys in a Hardware Crypto Module with a unit design form factor certified as conforming to at least FIPS 140-2 Level 2 or Common Criteria EAL 4+:

1. A Hardware Crypto Module meeting the specified requirement;
2. A cloud-base key generation and protection solution with the following requirements: a. Key creation, storage, and usage of Private Key must remain within the security boundaries of the cloud solution's Hardware Crypto Module that conforms to the specified requirements; b. Subscription at the level that manages the Private Key must be configured to log all access, operations, and configuration changes on the resources securing the Private Key; or
3. A Signing Service which meets the requirements of section 6.2.7.3 of the SSL.com CP/

CPS.

4.4. You must request revocation of your Certificate if information changes

You must immediately stop using your Certificate(s) and request a revocation of your Certificate(s) if you discover, or have a reasonable basis to believe, that the representations and warranties stated in Section 5 (*Your Representations and Warranties*) below were not true and complete when made, or have become untrue or incomplete.

4.5. You must request revocation of your Certificate if you discover or suspect that your Private Key was compromised

You must immediately stop using your Certificate(s) and request revocation of your Certificate(s) if you learn or reasonably suspect that any Private Key has been, or may have been, compromised, even if you do not know whether there was an actual unauthorized use or disclosure resulting from the compromise.

4.6. You must notify SSL.com if you discover or suspect that your Certificate Services account has been compromised

You must immediately notify SSL.com if you learn or reasonably suspect that your Certificate Services account has been compromised, even if you do not know whether there was an actual unauthorized use or disclosure resulting from the compromise.

4.7. You must cooperate with SSL.com concerning any compromise

You must provide the information we request in connection with a known or suspected compromise of your Private Key (s) or Certificate Services, and you must respond to our instructions concerning any Private Key(s) or Certificate Services account compromise within 24 hours, including during non-business hours.

4.8. You must keep your account information up to date

You must keep your Certificate Services account information up-to-date at all times. You may update your account information using your account dashboard, or via written authorization from a verified account administrator.

4.9. You must comply with other published requirements

You must use your Certificate in compliance with the CP/CPS (and for EV Certificates see the [EV Subscriber Agreement](#)).

4.10. You may not install your Certificate(s) on a server that is not accessible at the domain name listed.

You may not install your Certificates on a server unless it is accessible at the domain name shown on the Certificate.

4.11. You may not use your Certificate for any purpose other than the purpose designated in the Certificate

You may not use your Certificate for any purpose other than the purpose designated in the Certificate Key Usage field, or for any business other than your authorized business. You may not use the Certificate in a way that misrepresents the identity of the Certificate holder or could reasonably create confusion about the identity of the Certificate holder.

4.12. No High-Risk Use

You may not use the Certificate Services or your Certificate in connection with any information technology where the failure of the technology might result in death, personal injury, or severe physical or environmental damage, such as controlling aircraft or other modes of human mass transportation, nuclear or chemical facilities, life support systems, implantable medical equipment, motor vehicles, and weaponry systems.

4.13. Resellers must comply with our Reseller Terms

If you resell the Certificate Services, you must do so in compliance with our Reseller Terms. Your resale of the Certificate Services constitutes your agreement to the Reseller Terms, including the additional indemnification and other obligations stated in the Reseller Terms.

4.14. You may use the SiteSeaL logo only as expressly authorized

If SSL.com authorizes you to place the SiteSeaL logo on your Website, the authorization is a limited term, non-exclusive, revocable license to use the logo only on the Website published at the domain identified in your Certificate, for the term of the Certificate. You may not modify the SiteSeaL logo or combine it with any other image. You may not use the logo in a way that states or implies that SSL.com endorses your Website or any goods or services offered on your Website. You must comply with SSL.com's trademark usage guidelines provided to you and with SSL.com's detailed supervision of the use of the logo, including the placement, graphic quality, size, and other display elements. If SSL.com creates a new SiteSeaL logo, you must substitute the new logo for the old one on SSL.com's request. Your right to use the logo on a Website is automatically revoked on expiration or earlier termination of the Certificate for the Website's domain.

4.15. You must not knowingly sign the Suspect Code.

For Code Signing and EV Code Signing Certificates, the Subscriber must not knowingly sign software that contains a Suspect Code.

4.16. You are hereby informed, and acknowledge understanding, of the reasons for revoking a Certificate

You are hereby informed and acknowledge understanding, of the reasons for revoking a Certificate, including those stated in Section 4.9.1.1 (Reasons for Revoking a Subscriber Certificate) of the SSL.com CP/CPS, which is incorporated herein by reference and made a part of this Agreement.

5. Your Representations and Warranties

You make the following representation and warranties to SSL.com as of the date of your submission of your initial Application, the date of each Certificate Signing Request, and the date of each renewal of your Certificate Services.

1. The information stated in your Application (including each Certificate Signing Request) is true and correct and there is no additional information that is necessary to make the information submitted materially accurate and complete;
2. You exclusively control the domain(s) listed in your Certificate Signing Request, or, for SSL.com's validation services not tied to a domain (such as a Code Signing Certificate), you are the sole owner of or otherwise have the full legal right and authority to obtain a Certificate for the information to be validated.
3. The Private Key associated with your Certificate Signing Request(s) is protected and secured and conforms to Section 4.5.1 of the SSL.com CP/CPS.
4. The information stated in your Application does not infringe the intellectual property rights of any third party;
5. You are at least 18 years old, and are lawfully able to enter into legal agreements;
6. Your Representative submitting the Certificate Signing Request is authorized to submit the Certificate Signing Request;
7. You have all authorizations and licenses necessary to use the Certificate for the purpose designed in the Certificate; and
8. You have full power and authority to enter into the Agreement and perform your obligations under this Agreement.

In addition to the representations and warranties you make to SSL.com in this Certificate Services Agreement, **you make the representations and warranties stated in the CP/CPS to the Relying Parties and other Certificate Beneficiaries.**

5.1 NAESB Certificates

Subscribers for NAESB Certificates acknowledge their understanding of, and agreement with, all obligations of the NAESB Wholesale Electric Quadrant Business Practice Standards WEQ-012 (the "WEQ PKI Standards").

Subscribers and/or any NAESB end entity or organization applying in association with or on behalf of a Subscriber certifies to SSL.com that it has reviewed and acknowledges the following WEQ PKI Standards:

1. Subscriber acknowledges the electric industry's need for secure private electronic communications for the following purposes:
 - **Privacy:** The assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended;
 - **Authentication:** The assurance to one entity that another entity is who he/she/it claims to be;
 - **Integrity:** The assurance to an entity that data has not been altered (intentionally or unintentionally) between "there" and "here," or between "then" and "now"; and
 - **Non-Repudiation:** A party cannot deny having engaged in the transaction or having sent the electronic message.
2. Subscriber acknowledges the industry's endorsement of Public Key cryptography which utilizes Certificates to bind a person's or computer system's Public Key to its entity and to support symmetric encryption key exchange.
3. Subscriber has reviewed the WEQ PKI Standards with respect to industry guidelines for establishing a trusted PKI.
4. Subscriber has evaluated SSL.com's CP/CPS in light of those industry standards and agrees to adhere to all applicable controls therein.
5. Subscribers participating in the WEQ PKI Standards for WEQ-012 applications shall be required to be registered in the NAESB Electric Industry Registry ("EIR") and furnish proof that they are an entity authorized to engage in the wholesale electricity industry. Entities or organizations that may require access to applications using authentication specified under the WEQ PKI Standards, but do not qualify as a wholesale electricity market participant (e.g., regulatory agencies, universities, consulting firms, etc.) must register in the EIR.

Registered NAESB end entities and any Subscribers they represent shall be required to meet to all end entity obligations in the WEQ PKI Standards.

If applicable, Subscribers shall be obligated to register their legal business identification and

secure an "Entity Code" which must be published in the EIR and shall be used in all Subscriber applications submitted by, and Certificates issued to that end entity.

In cases where SSL.com receives requests for Certificates for use within the energy industry for other than WEQ-012 applications, SSL.com shall comply with the provisions of the WEQ PKI Standards, except any provisions that require or control end entity registration within the EIR.

NAESB end entities representing Subscribers shall also be required to comply with the following requirements:

- Protect their Private Keys from access by other parties
- If applicable, identify, through the EIR, that they have selected SSL.com to use as their ACA
- Execute all agreements and contracts with SSL.com necessary for SSL.com to issue Certificates to the end entity for use in securing electronic communications
- Comply with all obligations required and stipulated by SSL.com's CP/CPS
- Identify the type of Subscriber (i.e., individual, role, device, or application) and provide complete and accurate information for each Certificate Request
- Confirm that it has a Certificate management program, has trained all affected employees in that program, and has established controls to ensure compliance with that program. This program shall include, but is not limited to, policies addressing a) Certificate Private Key security and handling, and b) Certificate revocation.

6. SSL.com's Service Warranty and Disclaimers

SSL.com warrants that the Certificate Services will be provided in a professional manner consistent with industry standards and its commitments stated in the CP/CPS. If SSL.com fails to provide the Certificate Services as stated in the prior sentence, and you give SSL.com notice of this failure during the term of your subscription, SSL.com shall use commercially reasonable efforts to cure the failure. If SSL.com is unable through the use of commercially reasonable efforts to cure the failure, then, as your **sole and exclusive remedy** for the failure you may terminate the non-conforming Certificate Services and receive a refund of prepaid fees for the unused remaining term of the Certificate Services.

Except as expressly stated in this Agreement, the Certificate Services and any other SSL.com service is provided "AS IS" and "AS Available" and SSL.com makes no other representation or warranty whatsoever. **SSL.com disclaims any implied or statutory warranties, such as any implied warranty of merchantability or fitness for a particular purpose, non-infringement, and any warranties that may arise through trade usage or a course of dealing. SSL.com does not warrant that your Certificates Services will be error free, timely, uninterrupted, or completely secure.** If applicable law prohibits the disclaimer of any warranty disclaimed in this Section, then the warranty period for that warranty is 30 days.

SSL.com has no fiduciary or special duty to you arising from this Agreement or the Certificate Services. SSL.com has no obligation to provide you with any hardware, software, or network arrangements necessary for your use of the Certificate.

SSL.com's CP/CPS states certain representations and warranties for the benefit of "Certificate Beneficiaries" as defined in the CP/CPS. Those representations and warranties are solely for the benefit of Certificate Beneficiaries and are not made to you as a Certificate Services subscriber under this Agreement.

7. Term and Termination

7.1. Initial Term

The initial term of your Certificate Service is stated in the online product description for the product you select. The initial term begins on the date SSL.com issues your initial Certificate. On expiration of the initial term, the Certificate Service will expire unless you have renewed the Certificate Services as provided below. Please refer to the SSL.com [Purchasing Policy](#) (PP) for further details.

7.2. Renewals

To renew your Certificate Services, you must submit a new Certificate Signing Request and pay any applicable charges. SSL.com may discontinue its offer of any Certificate Services product at any time in its sole discretion.

7.3. Termination

7.3.1. Termination by You for Convenience

If the product description for your Certificate Services includes a "30-day unconditional refund" or like term, then you may terminate your Certificate Services and receive a full refund by giving notice via email from your administrator email address no later than 45 days from the date of purchase or 30 days from the date of Certificate issuance (whichever comes first).

7.3.2. Termination by SSL.com for Breach

SSL.com may terminate your Certificate Services for your breach of this Agreement, including the untruth of any representation or warranty. SSL.com may elect, in its sole discretion, to suspend your Certificate Services if you are in breach of the Agreement in a way that does not create an imminent or un-curable risk to SSL.com or Relying Parties, and SSL.com elects to give you time to cure the breach. You may not use the Certificate Services

to issue any new Certificates during a suspension. If you fail to cure the breach within the time permitted by SSL.com, then SSL.com may terminate your Certificate Services and revoke your Certificate(s) without further notice.

7.3.3. Termination by SSL.com for Non-payment, Dispute/Chargeback of Payment, or other Breach of Financial Obligation

SSL.com may terminate your Certificate Services for non-payment, dispute, or chargeback of payment via credit card or merchant account services, or other breach of financial obligation on your part. SSL.com may elect, in its sole discretion, to revoke any and all issued certificates related to the financial dispute. Complete lack of payment or dispute/chargeback of previous payment may result in backdated revocations to nullify any trust applied to subscriber code or written documents that were signed using the disputed certificates. You acknowledge that SSL.com is in no way responsible for any disruption to services or software that you or your clients may face when those items are no longer trusted and you agree to be responsible for any, and all, fiscal, physical, or emotional damages related to the backdated revocation.

7.3.4. Termination by SSL.com for Unacceptable Use

SSL.com may suspend or terminate your Certificate Services and revoke any Certificate(s) if it discovers or reasonably suspects that the Certificate Services or Certificate (or any element of the Certificate):

1. has been compromised,
2. is being used in connection with any illegal activities, such as phishing attacks, fraud, or the distribution of Suspect Code,
3. is being used in connection with activities that violate industry norms for acceptable network use, such as hate speech, defamation, intellectual property infringement, non-consensual sex acts or child pornography, network abuse, bulk correspondence (spam), etc.,
4. the continued use of the Certificate Services or Certificate presents a risk to the security or integrity of SSL.com's PKI or presents any other risk to its business or its reputation, or the Relying Parties or other users,
5. you or your Affiliates are added to an export restriction list, or
6. you or your Affiliates are engaged in conduct that is illegal or would be grounds for revocation of your Certificate under this Section if the conduct was associate with your Certificate, and
7. other grounds stated in the CP/CPS.

Backdate Revocation may be applied to such certificates to prevent Relying Parties from executing Suspect Code, to protect Internet users and the SSL.com PKI. If SSL.com terminates your Certificate Services or Certificate under this subsection for reasons other than

your breach of this Agreement then, on your request, and as your **sole and exclusive remedy**, it will refund the prepaid fees for the remaining unused portion of your Certificate Services or Certificate, as applicable. SSL.com has no liability for a decision to suspend or terminate in excess of this refund, even if there is an alternative reasonable explanation of the facts and circumstances, and even if facts come to light after SSL.com's decision that, if known at the time, would have resulted in a different decision.

7.4. Other termination reasons

Your Certificates may be revoked if SSL.com ceases doing business or is no longer allowed to issue Certificates and no other certificate provider is willing to provide revocation support.

7.5. Automatic Revocation of Certificates on Termination

Any Certificate issued as part of your Certificate Services may be revoked without further notice on termination of your Certificate Services account.

7.6. Expired and Revoked Certificates

You may not use any revoked or expired Certificate. You may not use any Private Key associated with your revoked or expired Certificates except to decrypt previously encrypted data associated with your Private Key.

8. Fees and Payments

8.1. Fees

Fees for each Certificate Services Product are stated on SSL.com's website. Fees are exclusive of sales, use, value-added, and like transaction taxes ("**Sales Tax**"). Unless otherwise expressly agreed in writing, Fees and applicable Sales Tax are due in advance for the entire term of the Certificate Services and, except as expressly provided below, are non-refundable. You must establish a means of payment satisfactory to SSL.com.

If you authorize SSL.com to charge your payment card, SSL.com may charge the card on the date of your initial purchase and each subsequent purchase, such as an upgrade. You must make sure that your payment card information is up to date at all times. SSL.com may suspend or terminate your Certificate Services if your account information is out of date, is invalid, or if SSL.com's charge to your payment card is refused on any basis. If SSL.com agrees to invoice you, then unless otherwise agreed, invoices are due on receipt and are overdue if not paid within thirty (30) days of the invoice date.

If you reasonably dispute an SSL.com invoice amount, and give SSL.com written notice

describing the dispute in reasonable detail prior to the overdue date, then SSL.com shall suspend the overdue date for up to three (3) days. You must work in good faith with SSL.com to resolve the dispute during the 3-day period.

8.2. Refunds

If the product description for your Certificate Services includes a "30-day unconditional refund" or like the term, then you may terminate your Certificate Services and receive a full refund by giving notice via email from your administrator email address no later than 45 days from the date of purchase or 30 days from the date of issuance (whichever comes first).

8.3. Backdated Revocation for Refunds

You accept that SSL.com may perform, at its sole discretion, Backdated Revocation of your Document or Code Signing product due to non-payment, including refunds and chargebacks, so that any trust extended to signed items will be removed and those items will no longer be trusted. Partial or pro-rated refunds of Document or Code Signing products may result in a Backdated Revocation to match, proportionally, the amount of the refund. SSL.com will not perform a full Backdated Revocation of a certificate if only a portion of the fees is refunded. You acknowledge that SSL.com is in no way responsible for any disruption to services or software that you or your clients may face when refunded certificates are backdate revoked. You agree to be responsible for any, and all, fiscal, physical, or emotional damages related to the Backdated Revocation.

8.4. Other Services

We may charge you additional fees if you use the SSL.com OCSP and time-stamping services in a manner that is excessive relative to your Certificate Services. If you ask SSL.com to provide services other than the Certificate Services, SSL.com may charge you additional fees for those services, provided that you give your advance written acknowledgment of the services to be performed and our related fees.

9. Confidentiality

Confidential Information of a party that is disclosed by that party (the "Discloser") to the other party (the "Recipient") is subject to the terms of this Confidentiality clause. Your Confidential Information which is Personal Data is also subject to the SSL.com Privacy Policy. Except as expressly permitted in this clause or the SSL.com Privacy Policy neither of us may disclose the other's Confidential Information except to our employees, and to third parties who need to know the information to represent or advise the Recipient with respect to the subject matter of this Agreement, provided that all employees and third party recipients must be bound by written confidentiality obligations covering the Confidential Information

that are at least as stringent as those stated in this Agreement.

Neither party shall use the other party's Confidential Information except in connection with the performance of its obligations or exercise of its rights under this Agreement. However, the Recipient shall not be in violation of this Section if it discloses or uses Discloser's Confidential Information to comply with a legal requirement, such as a subpoena or preservation order, or to bring or defend a claim in an adjudicatory proceeding, provided that Recipient has limited its disclosure to only that Confidential Information reasonably necessary in light of circumstances. Each Party agrees to use reasonable care to protect the other party's Confidential Information from unauthorized use and disclosure.

Each party agrees not to reverse engineer, decompile, or disassemble the other party's Confidential Information, except as permitted by applicable law and then on advance written notice of at least thirty (30) days to the other party. Each party shall return or destroy the other party's Confidential Information on expiration or termination of this Agreement or earlier on request of the other party, provided that a party may retain the other party's Confidential Information to the extent reasonably necessary to maintain reasonable and customary business records and as required for legal or regulatory compliance consistent with Recipient's reasonable and customary practices, provided that the use of the archived records is limited to legal or regulatory compliance. On request of a party, the other party shall sign a certificate stating that it has complied with the requirement to return or destroy the other party's Confidential Information as required by this Section. If you are an entity, the certificate must be signed by your officer having the authority of a corporate vice president or greater.

Retained Confidential Information remains subject to the requirements of this Section and the SSL.com Privacy Policy. Each party is responsible for a breach of this Section by its agents or representatives or any other person to whom it discloses the Discloser's Confidential Information.

10. Indemnification

You agree to indemnify and hold harmless SSL.com and each cross-signing entity, and their affiliates, and each of their respective employees, personnel, contractors, agents, officers, and directors from and against any claim, loss, damage or expense, including reasonable attorney fees, arising from or related to any of the following:

1. your misrepresentation of, or omission, of any material fact in your Application or otherwise submitted to SSL.com for purposes of the Certificate Services, regardless of whether such misrepresentation or omission was intentional or unintentional;
2. your breach of this Agreement, including a breach of your representations and warranties,
3. your violation of law,

4. the compromise or unauthorized use or disclosure of a Certificate or a Private Key, and
5. your misuse of a Certificate or Private Key.

Unless SSL.com asks you to defend an indemnified claim, SSL.com will control the defense and settlement of the claim, including choice of counsel, and you will pay SSL.com's reasonable defense costs (including attorney fees) as incurred. If SSL.com asks you to defend the claim, you shall select counsel reasonably acceptable to SSL.com, and you may not settle the claim without SSL.com's consent, not to be unreasonably withheld or delayed.

11. Limitation of Liability

To the maximum extent permitted by applicable law, (A) in no event shall SSL.com or its licensors, suppliers or affiliates have any liability for any consequential, exemplary, special, indirect, incidental or punitive damages, including any lost profit, lost revenue, lost business opportunity, or lost savings, even if it has been advised of the possibility of such damages; and (B) in any event and notwithstanding any other provision in this Agreement to the contrary, except for claims based on SSL.com's willful misconduct, the aggregate liability of SSL.com and any of its licensors, suppliers, or affiliates to you for any reason and upon any cause of action is limited to the amount you paid for the Certificate Services giving rise to the claim for the term during which the claim arose.

You acknowledge that SSL.com has set its prices and entered into this Agreement in reliance on the limitations of remedies and liability stated in this Agreement and that these limitations reflect an agreed allocation of risk between the parties. The limitations stated in this Section shall apply to any liability arising from any cause of action whatsoever, whether in contract, tort, commercial code, strict liability, or otherwise, **even if a limited remedy fails of its essential purpose**. Nothing in this Subsection precludes a party from seeking specific enforcement, injunctive relief, or other equitable remedy. If these limitations as written are not permitted by applicable law, they shall apply to the extent permitted by applicable law.

12. Governing Law, Dispute Resolution

The Agreement is governed by the laws of the State of Texas, excluding any law that would require the application of the law of a different jurisdiction. Any dispute or claim relating in any way to your use of the Certificate Services or any other product or service of SSL.com will be resolved by binding arbitration, rather than in court, except that a party may bring suit in court to enjoin infringement or other misuse of intellectual property rights or Confidential Information. The arbitration will be conducted by the American Arbitration Association (AAA) under its rules, which are available at www.adr.org or by calling 1-800-778-7879.

Payment of filing, administration, and arbitrator fees will be governed by the AAA's rules. The parties agree that they will not seek attorney's fees and costs in arbitration unless the

arbitrator determines the claims are frivolous. You may choose to have the arbitration conducted by telephone, based on written submissions, or at a mutually agreed location.

The parties agree that any dispute resolution proceedings will be conducted only on an individual basis and not in a class, consolidated, or representative action. If for any reason a claim proceeds in court rather than in arbitration the parties waive any right to a jury trial.

13. Miscellaneous

13.1. Force Majeure

A party's failure to perform an obligation under this Agreement shall be excused to the extent the failure is due to an event that is beyond the party's reasonable control, such as a failure of the power grid or Internet, natural disaster, war, riot, insurrection, epidemic, organized labor action, terrorism, or other event of a magnitude or type for which precautions are not generally taken in the industry (a "**force majeure event**"). A party shall be excused under this Section only to the extent that there is no reasonable alternative means of performance or effective mitigation. Nothing in this Section excuses a party from liability arising from its failure to implement or maintain any reasonably prudent preventative or recovery measure (such as back-up power generators, fire suppression system, and data backups) or any measure described in a business continuity, disaster recovery, security, or other plan required by this Agreement.

13.2. Notices

Each party shall give notices required or permitted under this Agreement in the manner specified in the CP/CPS or other means made available via the Certificate Service. Requests to revoke a certificate may be made by submission of SSL.com's revocation request form published on its Website or via the SSL.com portal.

13.3. No Assignment

Neither party may assign this Agreement without the other party's prior written consent, except that:

1. SSL.com may assign this Agreement as part of a transaction by which it transfers all or substantially all its operating assets to a third party, or
2. as part of a merger or like transaction resulting in a change of control of SSL.com.

13.4. Publicity

Use of Marks. Neither party may issue any press release or other publicity regarding this Agreement or the relationship or transactions contemplated by this Agreement without the prior written consent of the other party. Neither party may use the other party's trade or service marks without the other party's prior consent, and then only to the limited extent expressly authorized, and subject to the other party's reasonable trademark usage guidelines that are communicated to the party from time to time.

13.5. Computation of Time

In calculating any period of time under this Agreement, the day of the act, event or default from which the designated period of time begins to run shall not be included.

13.6. Ownership of Certificates and Related Information

SSL.com retains ownership of all Certificates issued through the SSL.com PKI and associated status information. You are licensed to reproduce and distribute your Certificate(s) on a non-exclusive, revocable, royalty free basis, on the conditions and subject to the restrictions stated in this Agreement, and provided that the Certificate(s) are reproduced and distributed in full. You may not modify or create derivative works of the Certificate(s).

You own Public Keys and Private Keys that you generated in accordance with this Agreement. SSL.com CA Private Keys are the property of SSL.com.

13.7. Reservation of Rights

Except for the rights expressly granted under this Agreement, each party shall retain all right, title and interest in and to its intellectual property, worldwide. Neither Party shall remove, efface or obscure any copyright notices or other proprietary notices or legends from any technology or materials provided under this Agreement and owned by the other party. You may not reverse engineer, disassemble, or decompile any part of SSL.com's Public Key Infrastructure or other technology without SSL.com's prior written consent, unless such activity is permitted notwithstanding this limitation, and then on at least thirty (30) days advance written notice to SSL.com.

No rights in intellectual property may arise by implication or estoppel.

13.8. Independent Contractors

The parties are independent contractors. This Agreement is not intended to create a partnership, joint venture, or employment relationship. Neither party is the agent of the other, and neither party is authorized to make any representations, contract, or commitment on behalf of the other.

13.9. Interpretation of Certain Words

- The use of the words "partner" or "partnership" in this Agreement or otherwise refers only to a business relationship, and does not create or reflect any legal partnership, joint venture, or other fiduciary or other special relationship between the persons described as partners.
- The term "person" refers to any legal person, and may mean a natural person (individual), a legally created person (such as an entity, trustee, or executor), or an entity (such as a corporation, partnership, or limited liability company).
- The word "including" means "including, without limitation."
- The words "will" and "shall" are words of obligation, not expressions of intent or expectation.
- The term "parties," either in lower- or upper-case form, refers to the signatories to this Agreement.
- Unless otherwise defined, the words "business day," "business hours," or the like shall mean Monday – Friday, 9:00 a.m. – 5:00 p.m., United States Central Time, excluding federal public holidays in the United States.
- A reference to "day" shall mean a calendar day, unless expressly designated as a "business" day.
- The term "personnel" shall refer to employees of the person referred to and individual contractors of the person referred to if the individuals are under the direct supervision of the person referred to.
- The word "affiliate" refers to an individual or entity that controls, is controlled by, or is under common control with the person referred to, where control means ownership of the majority of voting interests of an entity or the right to control the policies of the entity by means of a controlling number of seats on the entity's governing body.
- A reference to the "law" or "laws" includes laws, regulations, ordinances, codes, and other government mandates, all as they may be amended from time to time.
- Any requirement in this Agreement that a statement be written, in writing, or a like requirement is satisfied by an email or other digital form of writing unless expressly stated otherwise.
- Nouns stated in the singular shall imply the plural as indicated by the context, and pronouns that are gender specific shall be read to refer to either gender.

The Section captions in this Agreement are for convenience only; they are not part of this Agreement and may not be used to interpret the terms of this Agreement.

13.10. Severability

In the event one or more of the terms of this Agreement are adjudicated invalid, illegal, or unenforceable, the adjudicating body may either interpret this Agreement as if such terms had not been included, or may reform such terms to the limited extent necessary to make them

valid, legal or enforceable, consistent with the economic and legal incentives underlying the Agreement.

13.11. Amendments

This Agreement may be modified only by a written document that expressly refers to this Agreement by name and date and is signed by the parties.

13.12 Waiver

No right or remedy arising in connection with this Agreement shall be waived by a course of dealing between the parties, or a party's delay in exercising the right or remedy. A party may waive a right or remedy only by signing a written document that expressly identifies the right or remedy waived. Unless expressly stated in the waiver, a waiver of any right or remedy on one occasion will not be deemed a waiver of that right or remedy on any other occasion, or a waiver of any other right or remedy.

13.13. Pre-Printed Terms on Business Forms, Click Wraps

The pre-printed terms on the party's purchase orders or other business forms shall have no effect whatsoever. Unless and to the extent specifically stated otherwise in another part of this Agreement, an electronic "agree" or "accept" entered by a party's personnel as part of the installation or activation process for any software or services provided under this Agreement shall be of no force or effect whatsoever.

13.14. Counterparts, Signatures

This Agreement may be signed in multiple counterparts, which taken together shall be read as one Agreement. A signed agreement transmitted by facsimile, email attachment, or other electronic means shall be considered an original. The parties agree that electronic or digital signatures shall be given the same effect as a manual signature.

This Agreement is the complete and exclusive agreement between the parties regarding its subject matter and supersedes and replaces in its entirety any prior or contemporaneous agreement or understanding regarding the subject matter of this Agreement, written or oral.

About this document

This document is Version 1.7 of the SSL.com Subscriber Agreement. This document shall be updated to accurately reflect any changes, which shall be displayed in the version table below.

This document is created, approved and amended by the SSL.com Policy Management Authority (PMA). Any questions about this document or information contained within it can be directed to: pma@ssl.com.

This document is considered public and available to all viewers.

VERSION	DATE	CHANGES
1.0	June 24, 2016	Adopted
1.1	Sept. 6, 2016	Revised for EV Code Signing
1.2	Feb. 20, 2018	Formatting correction; test certificate notification
1.3	July 3, 2018	3.3.1 added for Code Signing Subscribers
1.4	Aug. 31, 2018	4.1 added for NAESB Subscribers
1.5	Oct. 20, 2022	3.16 added for TLS certificate revocation reasons (MRSP v2.8)
1.6	Dec. 19, 2022	Added backdate revocation rules and fair use of time-stamping services
1.7	Feb. 05, 2024	Formatting improvements, reorganizing sections, updated Subscriber Private Key Protection rules based on CSBRs