

Subscriber Agreement

This Subscriber Agreement (the "Agreement") is made between Google Trust Services ("GTS") and the party requesting a Certificate or Certificate Services from GTS ("Subscriber").

Subscriber must read and accept this Agreement before applying for, accepting, or using any Certificates, Certificate Services, or information, content, or materials that GTS provides in connection with this Agreement, including accessing or using any public key infrastructure or online database of Certificate information provided by or on behalf of GTS (all of the foregoing, together with GTS's hardware, software, networking, and communications infrastructure used to provide the foregoing, the "GTS PKI").

Subscriber agrees to the terms of this Agreement upon making a Certificate Request for a given Certificate, or if earlier, upon accessing or using the GTS PKI ("Effective Date").

In addition to this Agreement, Subscriber must also read and understand the applicable GTS Certificate Policy and Certification Practice Statement ("CP/CPS") , which is available in the Repository at pki.goog (<https://pki.goog/>) and which also applies to Subscriber's use of GTS-issued Certificates.

1. Definitions.

Capitalized terms used but not defined in this Agreement have the meaning given to them in the CP/CPS Appendix A (Definitions, Acronyms and References) available in the Repository at pki.goog (<https://pki.goog/>).

Certificate Request: An application for a new Certificate or a renewal of a Certificate.

Certificate Services: All services provided by or on behalf of GTS in connection with this Agreement or the issuance of any Certificate, including providing access to and use of the Repository, OCSP, Certificate information, and other features of the GTS PKI.

Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value. A Private Key is also considered compromised if methods have been developed that can easily calculate it based on the Public Key or if there is clear evidence that the specific method used to generate the Private Key was flawed.

Intellectual Property Rights: Patent rights, copyrights, trademark rights, rights in trade secrets (if any), design rights, database rights, domain name rights, moral rights, and any other intellectual property rights (registered or unregistered) throughout the world.

Key Usage Extension: An attribute included in a Certificate that determines the purposes for which the Certificate may be used.

Subject Alternative Name: An attribute included in the Certificate, which repeats the Common Name, as well as any other names that may apply to the subject.

2. Certificate Processing and Review.

After GTS receives Subscriber's Certificate Request, applicable payment, and any information and materials required for GTS to complete the Certificate validation procedures described in the CP/CPS, Google will process Subscriber's Certificate Request. GTS may reject Subscriber's Certificate Request for any reason, including the reasons stated in the CP/CPS. If GTS issues a Certificate to Subscriber, Subscriber must promptly review and verify the information in the Certificate before installing and using the Certificate. Subscriber must notify GTS by using the contact form at <https://pki.goog> within seven (7) days of receipt of any errors in the Certificate, in which case GTS may revoke the Certificate and issue Subscriber a corrected Certificate.

3. Use and Restrictions.

Subject to the restrictions and obligations in this Section 3 (Use and Restrictions) and Sections 4 (Reporting Obligations), 5 (Revocation), 6 (Subscriber's Warranties), and 8 (Term and Termination), Subscriber may use the Certificate in conjunction with Private Key and Public Key operations until the Certificate expires or is revoked. Subscriber will:

- (a) generate key pairs only on trustworthy systems and protect Subscriber's Private Key with levels of protection appropriate for sensitive data such as encryption or other means;
- (b) use the Certificate only in connection with properly licensed cryptographic software;
- (c) use the Certificate only for use cases that are consistent with the Key Usage Extensions in the Certificate;
- (d) not use, or provide access to, any Certificate for use in circumstances or applications in which the failure or compromise of any Certificate, Certificate Services, or any other aspect of the Google PKI could lead to death, personal injury, or severe physical or environmental damage;
- (e) not monitor, interfere with, or reverse engineer the technical implementation of the GTS PKI, or otherwise compromise the security of the GTS PKI;

- (f) use the OCSP in a manner that is reasonable with respect to the Certificate Services;
and
- (g) where the Certificate is used for any other party, ensure that such other party complies with the foregoing and the Subscriber is authorized by such other party to obtain the Certificate on its behalf.

4. Reporting Obligations.

If Subscriber believes its Certificate's Private Key has been Compromised or if the information in its Certificate is no longer accurate, Subscriber must immediately notify GTS by using the contact form at <https://pki.goog>. If GTS contacts Subscriber regarding Compromise or Certificate misuse, Subscriber must respond to GTS's inquiries or instructions or both within 48 hours of GTS's communication. In cases of abuse or other concern for security or the integrity of the Certificate, Google may revoke Subscriber's Certificate before Subscriber responds to GTS.

5. Revocation.

5.1. GTS will revoke Subscriber's Certificate for the reasons and within the applicable timeframes stated in the section of the CP/CPS referring to reasons for Revoking a Subscriber Certificate. GTS may revoke Subscriber's Certificate immediately if Subscriber violates the terms of this Agreement or GTS discovers that the Certificate is being used to enable criminal or other malicious activities, such as phishing attacks, fraud, or the distribution of malware. GTS may also revoke Subscriber's Certificate within a commercially reasonable period under the following circumstances: (a) Subscriber requests revocation of the Certificate; (b) Subscriber is added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of GTS's jurisdiction of operation; (c) GTS determines that use of the Certificate may compromise the security, reputation or trust status of the GTS PKI or GTS; (d) GTS reissues a Certificate (in which case, GTS may revoke the previously issued Certificate); (e) a licensing agreement affecting the Certificate terminates or expires; or (f) GTS determines that use of the Certificate is otherwise harmful to the business or reputation of GTS or third parties, considering, among other things: (i) the nature and number of complaints received; (ii) the identity of the complainant; (iii) relevant legislation in force; and, (iv) Subscriber's response to the alleged harmful use.

5.2. Acknowledgment of CA Obligations

Subscriber acknowledges that GTS is subject to applicable policies and standards relevant to its Certificates and Certificate Services. Subscriber will timely cooperate with GTS and will employ systems that are sufficient in order to meet all applicable Certificate revocation timelines, including consistent with the CP/CPS and any such policies or standards of relevant industry stakeholders. Subscriber acknowledges that it has been explicitly warned against using

publicly-trusted TLS server certificates on systems that cannot comply with timely revocation requirements.

6. Subscriber's Warranties.

Subscriber represents and warrants, for the benefit of GTS and the Certificate Beneficiaries, that it will:

- (a) provide accurate, complete and truthful information at all times to GTS, both in the Certificate Request and as otherwise requested by GTS in connection with the issuance of a Certificate;
- (b) take all reasonable measures to ensure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate (and any associated activation data or device, e.g., password or token);
- (c) review and verify the Certificate contents for accuracy;
- (d) install the Certificate only on servers that are accessible at the Subject Alternative Name(s) in the case of TLS Certificates, and MailBox Addresses in the case of S/MIME Certificates, listed in the Certificate, and use the Certificate solely in compliance with all applicable laws and solely in accordance with this Agreement;
- (e) promptly request revocation of the Certificate, and cease using it and Subscriber's associated Private Key if: (i) there is any actual or suspected misuse or Compromise of Subscriber's Private Key or, (ii) any information in the Certificate is or becomes incorrect or inaccurate;
- (f) review and select the appropriate revocation reason code as defined and explained in Section 4.9.1.1 of the CP/CPS; and
- (g) promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Compromise.

7. Consent to Publish Information.

By providing personal information, including name and e-mail address, in a Certificate Request, Subscriber consents to GTS's disclosure of this information publicly by: (a) embedding the information in the issued Certificate, and (b) submitting the issued Certificate to a publicly accessible Certificate Transparency (CT) log for publication.

8. Term and Termination.

This Agreement is effective as of the Effective Date until the earlier of Subscriber's Certificate expiring or being revoked, or termination by either party. Upon any termination of this Agreement, all of Subscriber's rights under this Agreement immediately terminate and Subscriber will cease using the Certificates issued under this Agreement and the Certificate Services. Sections 7 (Consent to Publish Information), 9 (Indemnification), 11 (Limitation of Liability), 12 (Intellectual Property Rights), and 14 (Miscellaneous) of this Agreement will survive termination of this Agreement.

9. Indemnification.

Subscriber will defend and indemnify GTS and its affiliates, directors, officers, and employees against all liabilities, damages, losses, costs, fees (including legal fees), and expenses relating to any allegation or third-party legal proceeding to the extent arising from: (a) Subscriber's breach of this Agreement or its representations or warranties under this Agreement; (b) Subscriber's intentional or unintentional misrepresentations or omissions in connection with this Agreement; or (c) claims that any content or information provided by Subscriber in connection with the Agreement violates or infringes a third party's rights, including Intellectual Property Rights. GTS has the right to approve controlling counsel, such approval not to be unreasonably withheld (and which approval may be withheld or withdrawn if there is a conflict of interest) and may appoint its own non-controlling counsel, at its own expense. Any settlement requiring GTS to admit liability, pay money, or take (or refrain from taking) any action, will require GTS's prior written consent, not to be unreasonably withheld, conditioned, or delayed.

10. GTS Disclaimer.

EXCEPT AS STATED IN THE CP/CPS, THE CERTIFICATE SERVICES IN CONNECTION WITH THIS AGREEMENT ARE PROVIDED "AS IS." GTS AND ITS AFFILIATES AND LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE CERTIFICATE SERVICES, INCLUDING ANY WARRANTY THAT THE CERTIFICATE SERVICES WILL BE UNINTERRUPTED, ERROR FREE, OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. EXCEPT TO THE EXTENT PROHIBITED BY LAW, GTS AND ITS AFFILIATES AND LICENSORS DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR QUIET ENJOYMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE.

11. Limitation of Liability.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, GTS AND ITS AFFILIATES WILL NOT HAVE ANY LIABILITY ARISING OUT OF OR RELATING TO THE AGREEMENT, CERTIFICATES, CERTIFICATE SERVICES, OR THE GTS PKI FOR ANY: (I) LOST PROFITS, REVENUES, GOODWILL, OR SAVINGS; OR (II) INDIRECT, CONSEQUENTIAL, SPECIAL, INCIDENTAL, OR PUNITIVE DAMAGES. TO THE EXTENT PERMITTED BY APPLICABLE LAW, GTS AND ITS AFFILIATES' TOTAL LIABILITY FOR DAMAGES ARISING OUT OF OR RELATING TO THE AGREEMENT, CERTIFICATES, CERTIFICATE SERVICES, OR THE GTS PKI WILL NOT UNDER ANY CIRCUMSTANCES, EXCEED THE LESSER OF THE AMOUNT PAID BY SUBSCRIBER FOR THE CERTIFICATE(S) AT ISSUE OR THE AMOUNTS PAID FOR THE CERTIFICATE SERVICES FOR THE CERTIFICATE(S) AT ISSUE IN THE LAST TWELVE (12) MONTHS BEFORE THE CLAIM AROSE. THIS LIABILITY LIMITATION WILL BE THE SAME REGARDLESS OF THE NUMBER OF DIGITAL SIGNATURES, TRANSACTIONS, OR CLAIMS RELATED TO SUCH CERTIFICATE.

12. Intellectual Property Rights.

Except as expressly described in the Agreement, the Agreement does not grant either party any rights, implied or otherwise, to the other's Intellectual Property Rights. As between the parties, GTS retains all Intellectual Property Rights in the Certificates, all documentation provided by GTS in connection with the Certificates, the Certificate Services, the GTS PKI and derivative works of any of the foregoing.

13. Export Compliance.

Subscriber will comply with all applicable export control and sanctions laws and regulations, including (a) the Export Administration Regulations maintained by the U.S. Department of Commerce, (b) trade and economic sanctions maintained by the U.S. Treasury Department's Office of Foreign Assets Control, and (c) the International Traffic in Arms Regulations maintained by the U.S. Department of State.

14. Miscellaneous.

14.1 Modifications.

GTS may modify this Agreement at any time by posting a revised version in the Repository (<https://pki.goog/>). The modified terms will become effective upon posting. By continuing to use the Certificate Services after the effective date of any modifications to this Agreement, Subscriber agrees to be bound by the modified terms. It is Subscriber's responsibility to check the Repository regularly for modifications to this Agreement.

14.2 Governing Law.

ALL CLAIMS ARISING OUT OF OR RELATING TO THIS AGREEMENT WILL BE GOVERNED BY CALIFORNIA LAW, EXCLUDING CALIFORNIA'S CONFLICT OF LAWS RULES, AND WILL BE LITIGATED EXCLUSIVELY IN THE FEDERAL OR STATE COURTS OF SANTA CLARA COUNTY, CALIFORNIA, USA. THE PARTIES CONSENT TO PERSONAL JURISDICTION IN THOSE COURTS.

14.3 **Force Majeure.**

Neither party will be liable for failure or delay in performance to the extent caused by circumstances beyond its reasonable control.

14.4 **U.S. Government Users.**

The Certificates, Certificate Services, and GTS PKI were developed solely at private expense and are commercial computer software and related documentation within the meaning of the applicable Federal Acquisition Regulations and their agency supplements. If Subscriber is using the Certificate Services on behalf of the U.S. Government and these terms fail to meet the U.S. Government's needs or are inconsistent in any respect with federal law, Subscriber will immediately discontinue its use of the Certificate Services.

14.5 **Assignment.**

Neither party may assign any part of this Agreement without the written consent of the other, except to an affiliate where: (a) the assignee has agreed in writing to be bound by the terms of this Agreement; (b) the assigning party remains liable for obligations under this Agreement if the assignee defaults on them; and (c) the assigning party has notified the other party of the assignment. Any other attempt to assign is void.

14.6 **Change of Control.**

During the Agreement's term, if a party experiences a change of control (for example, through a stock purchase or sale, merger, or other form of corporate transaction): (a) that party will give written notice to the other party within 30 days after the change of control; and (b) the other party may immediately terminate this Agreement any time between the change of control and 30 days after it receives that written notice.

14.7 **No Waiver.**

Neither party will be treated as having waived any rights by not exercising (or delaying the exercise of) any rights under this Agreement.

14.8 **Independent Contractors; No Agency.**

The parties are independent contractors. This Agreement does not create any agency, partnership, joint venture, or employment relationship.

14.9 No Third-Party Beneficiaries.

This Agreement does not confer any benefits on any third party unless it expressly states that it does.

14.10 Severability.

If any part of this Agreement is invalid, illegal, or unenforceable, the rest of this Agreement will remain in effect.

14.11 Notices.

All notices of termination or breach must be in English, in writing, and addressed to the other party's Legal Department. The address for notices to GTS's Legal Department is legal-notices@google.com. All other notices must be in English, in writing and addressed to the other party's primary contact. Emails are written notices. Notice will be treated as given on receipt, as verified by written or automated receipt or by electronic log (as applicable).

14.12 Privacy.

Google's general privacy policy (<http://www.google.com/privacypolicy.html>) explains how GTS treats Subscriber's personal data and protects Subscriber's privacy when Subscriber uses the Certificate Services. By using the Certificate Services, Subscriber agrees that GTS can use that data in accordance with these policies.. Google may amend the privacy policy at any time by posting the amended privacy policy on its website. By providing personal information when applying for a Certificate, Subscriber consents to Google's processing, disclosure and transfer of this information on a global basis to its affiliates, agents and subcontractors as necessary to validate and issue a Certificate, including processing, disclosure and transfer to countries that may have data protection laws that are less protective than those in the country where Subscriber is located.

14.13 Conflicting Terms.

To the extent this Agreement conflicts with the CP/CPS, this Agreement will govern.

14.14 Conflicting Languages.

If this Agreement is translated into any other language, and there is a discrepancy between the English text and the translated text, the English text will govern.

14.15 Entire Agreement.

This Agreement, including the CP/CPS and Google's Privacy Policy, states all terms agreed between the parties and supersedes all other agreements between the parties relating to its subject matter. In entering into this Agreement neither party has relied on, and neither party will have any right or remedy based on, any statement, representation or warranty (whether made negligently or innocently), except those expressly stated in this Agreement.