LET'S ENCRYPT

SUBSCRIBER AGREEMENT

This Subscriber Agreement **("Agreement")** is a legally binding contract between you and, if applicable, the company, organization or other entity on behalf of which you are acting (collectively, **"You" or "Your"**) and Internet Security Research Group **("ISRG," "We," or "Our")** regarding Your and Our rights and duties relating to Your acquisition and use of SSL/TLS digital certificates issued by ISRG.

If you are acting on behalf of a company, organization or other entity, You represent that you have the authority to bind such entity to this Agreement.

1. Definitions and Terms

"ACME Client Software" — A software application that uses the Automated Certificate Management Environment (ACME) protocol to request, accept, use or manage Let's Encrypt Certificates.

"Certificate" — A computer-based record or electronic message issued by an entity that associates a Public Key with an Internet domain name or other technical identifiers and is Digitally Signed by the issuing entity.

"Digital Signature/Digitally Sign" — The transformation of an electronic record by one person, using a Private Key and Public Key Cryptography, so that another person having the transformed record and the corresponding Public Key can accurately determine (i) whether the transformation was created using the Private Key that corresponds to the Public Key, and (ii) whether the record has been altered since the transformation was made. A Digital Signature need not incorporate a handwritten signature.

"Key Pair" — Two mathematically-related keys (a Private Key and its corresponding Public Key), having the properties that (i) one key can be used to encrypt a message (i.e., create a Digital Signature) that can only be decrypted using the other key (i.e., verify the Digital Signature), and (ii) even while knowing or possessing one key (e.g., the Public Key), it is computationally difficult or infeasible to discover the other key (e.g., the Private Key).

"Let's Encrypt Certificate" — A Certificate issued by ISRG under the Let's Encrypt name.

"Private Key" — A key kept secret by its holder and which is used in Public Key Cryptography to create Digital Signatures and to decrypt messages or files that were encrypted with the corresponding Public Key.

"Public Key" — In Public Key Cryptography, this is the publicly-disclosed key that is used by the recipient to (i) validate Digital Signatures created with the corresponding Private Key and (ii) encrypt messages or files to be decrypted with the corresponding Private Key.

"Key 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.

"Public Key Cryptography" — A type of cryptography that uses a Key Pair to securely encrypt and decrypt messages. One key encrypts a message, and the other key decrypts the message. One key is kept secret (the Private Key), and one is made available to others (the Public Key). These keys are, in essence, large mathematically-related numbers that form a unique pair. Either key may be used to encrypt a message, but only the other corresponding key may be used to decrypt the message.

"Validity Period" — The intended term of validity of a Certificate, beginning with the date of issuance ("Valid From" or "Activation" date), and ending on the expiration date indicated in such Certificate ("Valid To" or "Expiry" date).

"Your Certificate" — A Let's Encrypt Certificate issued to You.

2. Effective Date, Term, and Survival

2.1 Effective Date of Agreement

This Agreement is effective once You request that ISRG issue a Let's Encrypt Certificate to You.

2.2 Term

Each of Your Certificates will be valid for the Validity Period indicated in such Certificate unless revoked earlier. This Agreement will remain in force during the entire period during which any of Your Certificates are valid, continuously so as to include any renewal periods (including automatic renewals). Once You no longer possess any valid Let's Encrypt Certificate, this Agreement will terminate.

2.3 Survival

Sections in this Agreement concerning privacy, indemnification, disclaimer of warranties, limitations of liability, governing law, choice of forum, limitations on claims against ISRG, and prohibitions on the use of fraudulently-obtained Certificates and expired Certificates shall survive any termination or expiration of this Agreement.

3. Your Warranties and Responsibilities

3.1 Warranties

By requesting, accepting, or using a Let's Encrypt Certificate:

- **You warrant** to ISRG and the public-at-large that You are the legitimate registrant of the Internet domain name that is, or is going to be, the subject of Your Certificate, or that You are the duly authorized agent of such registrant.
- **You warrant** to ISRG and the public-at-large that either (1) You did not obtain control of such domain name as the result of a seizure of such domain name, or (2) such domain name had no ongoing lawful uses at the time of such seizure.
- **You warrant** to ISRG and the public-at-large that all information in Your Certificate regarding You or Your domain name is accurate, current, reliable, complete, and not misleading.
- **You warrant** to ISRG and the public-at-large that all information You have provided to ISRG is, and **You agree** that all information you will provide to ISRG at any time will be, accurate, current, complete, reliable, and not misleading.
- **You warrant** to ISRG and the public-at-large that You rightfully hold the Private Key corresponding to the Public Key listed in Your Certificate.
- **You warrant** to ISRG and the public-at-large that You have taken, and **You agree** that at all times You will take, all appropriate, reasonable, and necessary steps to assure control of, secure, properly protect, and keep secret and confidential the Private Key corresponding to the Public Key in Your Certificate (and any associated activation data or device, e.g. password or token).

3.2 Changes in Certificate Information

If at any time You no longer control the Internet domain names associated with one or more of Your Certificates, or if any of the warranties in Section 3.1 above are no longer true with respect to one or more of Your Certificates in any other way, You will immediately request that ISRG revoke the affected Certificates. You may request replacement Let's Encrypt Certificates before revoking the affected

Certificates, provided that the warranties in Section 3.1 above are true with respect to the replacement Certificates.

3.3 Certificate Issuance

The contents of Your Certificates will be based on the information You or Your ACME Client Software sends to ISRG.

If ISRG accepts your request for a Let's Encrypt Certificate, ISRG will create Your Certificate and it will be provided to You through the ACME protocol. If ISRG is unable to confirm your identity or authorization, Your request may be denied.

ISRG may, in its sole discretion, refuse to grant Your request for a Let's Encrypt Certificate, including for any lawful reason stated or not stated in this Agreement.

3.4 Key Pair Generation

Your Key Pair (Public and Private Keys) will be generated by You or Your ACME Client Software on Your systems. You will submit the corresponding Public Key to ISRG and it will be incorporated into Your Certificate. ISRG will not have access to Your Private Key. Your Private and Public Keys will remain Your property.

We will use technical methods and protocols to verify that You have control over the subject Internet domain name. This verification is done solely to assist ISRG in determining whether to issue a Let's Encrypt Certificate and is not a service being performed for Your benefit or on Your behalf.

3.5 Inspection and Acceptance of Certificates

You warrant to ISRG and the public-at-large, and You agree, that You will immediately inspect the contents of Your Certificate ("Initial Inspection") and will immediately request revocation if you become aware of any inaccuracies, errors, defects, or other problems with Your Certificate. Your ACME Client Software may perform this task for You. You agree that You will have accepted Your Certificate when You first use Your Certificate or the corresponding Private Key after obtaining Your Certificate, or if You fail to request revocation of Your Certificate immediately following Initial Inspection.

3.6 Installation and Use of Your Certificate

You may reproduce and distribute Your Certificate on a nonexclusive and royalty-free basis, provided that it is reproduced and distributed in full and in compliance with this Agreement. You warrant to ISRG and the public-at-large, and You agree, that You will install Your Certificate only on servers that are accessible at the subjectAltName(s) listed in Your Certificate, and that you will use Your Certificate solely in compliance with all applicable laws and solely in accordance with this Agreement. Your Certificate will remain the property of ISRG, subject to Your right to use it as set forth in this Agreement.

The purpose of Your Certificate is to authenticate and encrypt Internet communications. ISRG is not responsible for any legal or other consequences resulting from or associated with the use of Your Certificate. You agree that You will not use Your Certificate for:

(a) any purpose requiring fail-safe performance, such as the operation of public utilities or power facilities, air traffic control or navigation systems, weapons systems, or any other systems, the failure of which would reasonably be expected to lead to bodily injury, death, or property or environmental damage; or

(b) software or hardware architectures that provide facilities for interference with encrypted communications, including but not limited to:

(1) active eavesdropping (e.g., monster-in-the-middle attacks); or

(2) traffic management of domain names or internet protocol addresses that You do not own or control.

Note that these restrictions apply regardless of whether a relying party communicating through the software or hardware architecture has knowledge of its providing facilities for interference with encrypted communications.

3.7. Revoking Your Certificate

You warrant to ISRG and the public-at-large, and You agree, that You will immediately request that Your Certificate be revoked if: (i) there is any actual or suspected misuse or Key Compromise of the Private Key associated with the Public Key included in Your Certificate, or (ii) any information in Your Certificate is, or becomes, misleading, incorrect or inaccurate. You may make a revocation request to ISRG using ACME Client Software. You should also notify anyone who may have relied upon Your use of Your Certificate that Your encrypted communications may have been subject to compromise.

You warrant to ISRG and the public-at-large, and You agree, that before providing a reason for revoking Your Certificate, you will have reviewed the revocation guidelines found in the "Revoking Certificates" section of the Let's Encrypt documentation available at https://letsencrypt.org/docs/, and that you will provide Your corresponding revocation reason code with awareness of such guidelines.

You acknowledge and accept that ISRG may modify any revocation reason code provided by You if ISRG determines, in its sole discretion, that a different reason code for revocation is more appropriate or is required by industry standards.

3.8 When to Cease Using Your Certificate

You warrant to ISRG and the public-at-large, and You agree, that You will promptly cease using Your Certificate (i) if any information in Your Certificate is, or becomes, misleading, incorrect or inaccurate, or (ii) upon the revocation or expiration of Your Certificate.

3.9 When to Cease Using Your Private Key

You warrant to ISRG and the public-at-large, and You agree, that You will promptly cease all use of the Private Key corresponding to the Public Key included in Your Certificate upon revocation of Your Certificate for reasons of known or suspected Key Compromise.

3.10 Indemnification

You agree to indemnify and hold harmless ISRG and its directors, officers, employees, agents, and affiliates from any and all liabilities, claims, demands, damages, losses, costs, and expenses, including attorneys' fees, arising out of or related to: (i) any misrepresentation or omission of material fact by You to ISRG, irrespective of whether such misrepresentation or omission was intentional, (ii) your violation of this Agreement, (iii) any compromise or unauthorized use of Your Certificate or corresponding Private Key, or (iv) Your misuse of Your Certificate. If applicable law prohibits a party from providing indemnification for another party's negligence or acts, such restriction, or any other restriction required by law for this indemnification provision to be enforceable, shall be deemed to be part of this indemnification provision.

4. ISRG's Rights and Responsibilities

4.1 Privacy

Because others may rely on your use of Your Certificates to encrypt Internet communications, the information You send to ISRG, as well as Your Certificates, may be published by ISRG and become a

matter of public record. ISRG's collection, storage, use and disclosure of such information are governed by the Let's Encrypt Privacy Policy at: https://letsencrypt.org/privacy/.

4.2 Revocation

You acknowledge and accept that ISRG may immediately revoke Your Certificate if any party notifies ISRG that Your Certificate is invalid or has been compromised. ISRG will determine, in its sole discretion, whether to revoke Your Certificate. If You or Your agent requests that Your Certificate be revoked, ISRG will revoke Your Certificate as soon as practical. If a request for revocation is signed by your Private Key, then ISRG will automatically deem the request to be valid. You also acknowledge and accept that ISRG may, without advance notice, immediately revoke Your Certificate if ISRG determines, in its sole discretion, that: (i) Your Certificate was not properly issued or was obtained through misrepresentation, concealment, or fraud; (ii) Your Certificate has become, or appears to have become, unreliable; (iii) the security of the Private Key corresponding to Your Certificate has been or may be stolen, lost, or otherwise compromised, or subject to unauthorized use; (iv) any information in Your registration with ISRG or Your request for a Let's Encrypt Certificate has changed or has become misleading, incorrect or inaccurate; (v) You have violated any applicable law, agreement (including this Agreement), or other obligation; (vi) Your Certificate is being used, or has been used, to enable any criminal activity (such as phishing attacks, fraud or the distribution of malware); (vii) Your Certificate is being used, or has been used, to intercept the traffic of others; (viii) You request revocation; (ix) ISRG is legally required to revoke Your Certificate pursuant to a valid court order issued by a court of competent jurisdiction; (x) this Agreement has expired or been terminated; or (xi) there are other reasonable and lawful grounds for revocation. ISRG may provide notice of revocation via email to the email address of record.

4.3 Important Disclaimer of Warranties and Limitation of Liability

Except as expressly set forth in ISRG's Certificate Policy and Certification Practice Statement, Let's Encrypt Certificates and any services provided by or on behalf of ISRG are provided "as-is" and ISRG disclaims any and all warranties of any type, whether express or implied, including without limitation any implied warranty of title, non-infringement, merchantability, or fitness for a particular purpose, in connection with any such Certificates or services.

Because Let's Encrypt Certificates are issued free-of-charge as a public service, ISRG cannot accept any liability for any loss, harm, claims, or attorney's fees in connection with such Certificates. Accordingly, you agree that ISRG will not be liable for any damages, attorney's fees, or recovery, regardless of whether such damages are direct, consequential, indirect, incidental, special, exemplary, punitive, or compensatory, even if ISRG has been advised of the possibility of such damages. This limitation on liability applies irrespective of the theory of liability, i.e., whether the theory of liability is based upon contract, warranty, indemnification, contribution, tort, equity, statute or regulation, common law, or any other source of law, standard of care, category of claim, notion of fault or responsibility, or theory of recovery. The parties agree that this disclaimer is intended to be construed to the fullest extent allowed by applicable law.

By way of further explanation regarding the scope of the disclaimer, and without waiving or limiting the foregoing in any way, ISRG does not make, and ISRG expressly disclaims, any warranty regarding its right to use any technology, invention, technical design, process, or business method used in either issuing Let's Encrypt Certificates or providing any of ISRG's services. You affirmatively and expressly waive the right to hold ISRG responsible in any way, or seek indemnification against ISRG, for any infringement of intellectual property rights, including patent, trademark, trade secret, or copyright.

5. Additional Terms

5.1 Governing Law

The parties agree that the laws of the State of California govern this Agreement, irrespective of California's choice of law and conflicts of law principles.

5.2. Choice of Forum

Any claim, suit or proceeding arising out of this Agreement must be brought in a state or federal court located in San Jose, California.

5.3 Limitation on Claims against ISRG

Any claim, suit or proceeding against ISRG arising out of this Agreement must be commenced within one year of any alleged harm, loss, or wrongful act having occurred.

5.4 No Third-Party Beneficiary

This Agreement does not create rights in favor of any third parties. Furthermore, it is the express intent of the parties that this Agreement shall not be construed to confer any rights on any third party.

5.5 Entire Agreement

This Agreement, together with any documents incorporated by reference herein, constitutes the entire Agreement between You and ISRG concerning the subject matter hereof.

5.6 Amendment

ISRG may modify this Agreement from time to time. Each modified version of this Agreement will be posted to ISRG's Let's Encrypt website (letsencrypt.org) at least fourteen (14) days before it becomes effective. If such new version contains material changes and You have provided ISRG with an email address, ISRG will send an email to such address notifying You of such new version at least fourteen (14) days before it becomes effective. In addition, major changes will be flagged with a new Subscriber Agreement version number in the ACME protocol, so You may be able to configure Your ACME Client Software to notify You of such changes.

5.7 Severability

If any provision of this Agreement is found to be invalid, unenforceable, or contrary to law, then the Agreement will be deemed amended by modifying such provision to the extent necessary to make it valid and enforceable while preserving its intent or, if that is not possible, by striking the provision and enforcing the remainder of this Agreement.

5.8 Authorization of ISRG to Send Emails

By requesting, accepting or using a Let's Encrypt Certificate, You authorize ISRG to send You emails relating to the renewal or revocation of Your Certificates, or to Your request, acceptance, or use of Let's Encrypt Certificates.

ISRG may send You such emails using any email address You provide to ISRG or any commonly-accepted contact email address for the domain names associated with Your Certificates, such as WHOIS domain contacts or common administrative email addresses.