DIGITAL CERTIFICATE(S) FOR CODE SIGNING

SUBSCRIBER AGREEMENT

Before downloading, installing, or using any Certificate for signing code, please carefully read these terms and conditions ("Agreement"). This Agreement is a binding legal agreement between the Subscriber of any Certificate and the CA that issues it, and governs all Applications for, access to, and use of Certificates, and defines the rights and responsibilities of individuals and legal entities who request or receive, or are otherwise involved in the verification and issuance of, such Certificates.

You, as the individual accepting this Agreement, represent and warrant that you are lawfully able to enter into contracts (e.g. you are not a minor). If you are accepting this Agreement on behalf of a legal entity, for example, your employer, you represent and warrant that you have legal authority to represent and bind such legal entity. If you are (or are acting as the authorized representative of) the Subscriber for the Certificate, this Agreement constitutes the 'subscriber agreement' as required and defined in the Industry Standards.

IF YOU DO NOT ACCEPT THIS AGREEMENT, OR IF YOU DO NOT HAVE THE LEGAL AUTHORITY TO ENTER INTO CONTRACTS OR TO BIND THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING SUCH ACCEPTANCE, YOU ARE PROHIBITED FROM DOWNLOADING, INSTALLING, OR USING ANY CERTIFICATE. THE CONTINUED RIGHT TO DOWNLOAD, INSTALL AND/OR USE CERTIFICATES IS CONTINGENT ON CONTINUED COMPLIANCE WITH THIS AGREEMENT.

WE RECOMMEND THAT YOU SAVE A COPY OF THIS AGREEMENT FOR YOUR FUTURE REFERENCE.

Capitalized words in this Agreement have the meanings set out in Section 15 (Definitions).

1. **Registration & Issuance**. The CA and/or one or more registration authorities appointed by the CA (each, an "RA") will provide the following services in accordance with Your Entitlement(s). You acknowledge and agree that:

   1.1. Upon receipt of an Application for a Certificate, the RA will perform the verification described in the CPS for the applicable type of Certificate. The RA may reject Applications for Certificates for the reasons set out in the CPS. You understand that issuance of a Certificate is conditional on the RA's completion of verification, which may include investigation and confirmation of information contained in or related to a Certificate Application, such as the identity and authority of the Subscriber and/or other individuals involved in the application and approval of Certificates, organizational/business name, street and mailing address, telephone number, line of business, year started, number of employees, CEO, business existence/status, and rights/control over or relationship with the relevant Subject(s) (collectively, "Verification Information").

   1.2. Verification requires the collection and processing of personal information. To the extent that a CA or RA collects or processes personal information, it will do so in accordance with the applicable product privacy notice and data processing agreement available at or through http://www.entrust.net/cps (or a similar agreement if agreed to by the CA or RA in writing). If You are an individual, You hereby consent to such collection and processing of Your personal information. If You are a legal entity, You represent and warrant that You have or will make any requisite disclosures to relevant individuals and obtain the requisite rights and consents, to enable the RA and CA to perform their obligations under this Agreement and the CPS.

   1.3. Verification may entail use of third-party databases which may result in some Verification Information being included in such databases (e.g. search history).

1.4. Some Verification Information will be included in Certificates. You acknowledge that Certificates, and any Verification Information included in a Certificate, are intended to be public.

1.5. Verification Information may be disclosed by and between a CA and RA and to third parties for the purpose of complying with, or demonstrating or facilitating compliance with, with Industry Standards.

1.6. If and when the Application passes verification, the CA will issue Certificates and make them available for retrieval and usage as set out in the CPS. Use of any Certificate constitutes Your acceptance of it. This Agreement applies to all Applications and Certificates, including initial and all subsequent certificate requests.

2. **Operation of the PKI.** Each CPS sets out the CA's practices for managing the public-key infrastructure for providing the types of Certificates identified in the CPS, including:

(a) Specification of the applicable Industry Standards and policies;
(b) Information for relying parties;
(c) Retention periods for event logs and other records concerning services;
(d) Procedures for complaints and dispute settlement;
(e) Specification of the applicable compliance audits and other assessments;
(f) Contact information for questions about Certificates;
(g) Any size limits on any subject naming attributes which are longer than stated in Industry Standards;
(h) Revocation reason options and explanations about when to choose each option;
(i) How revocation status information is provided and the period over which it is available.

3. **Revocation of Digital Certificates.** Certificates may be revoked by the CA if and when Your Entitlement ends (including if it is terminated for non-payment), or for any of the reasons set out in the CPS or Industry Standards. If the CA notifies You, or if You otherwise become aware, that any Certificate is required to be revoked under the CPS or the Industry Standards, You agree to revoke it or request revocation, and to otherwise cooperate with the CA to comply with all applicable revocation requirements and timelines. You acknowledge and agree that Certificates may need to be revoked within a matter of hours or days, depending on the circumstances. It is Your responsibility to ensure You are able to safely replace a Certificate in case it needs to be revoked within 24 hours. Revocation processes are as set out in the CPS.

4. **Grant of License.** Subject to Your compliance with this Agreement, the CA hereby grants to You a limited, personal, worldwide, non-exclusive, non-transferable, non-sublicensable license to access and use Your Certificate provided that at all times, Your use of the Certificate is in accordance with this Agreement, including the CPS which is incorporated herein, and Your Entitlement. If You are issued any Certificates for the purposes of an evaluation of the CA's services ("Trial Certificates"), Your right to use such Trial Certificates is limited to short-term evaluation only, revocable at the CA's discretion, and may only be used in a test environment. You will revoke any Trial Certificates prior to the end of the evaluation period, and if You fail to do so You authorize the CA to revoke any outstanding Trial Certificates upon termination of Your evaluation rights.

5. **Subscriber Obligations.** You, as the Subscriber of the Certificate(s) to be issued or on the Subscriber's behalf, understand and agree that as a condition of having any Certificate issued to or for the Subscriber, Subscriber makes, on its own behalf and if applicable on behalf of Subscriber's principal or agent under a subcontractor or hosting service relationship, the following representations, commitments, affirmations and warranties for the benefit of Certificate Beneficiaries, the CA, the RA, any Signing Service (defined below), and any of the CA's or RA's Affiliates that will be involved in provision of Certificates to or for Subscriber:

5.1. Subscriber will use one of the following options to generate and protect its Certificate private keys:

5.1.1. Subscriber uses 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) ("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+ ("Specified Requirements");

5.1.2. Subscriber uses 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.

5.1.3. Subscriber uses an organization that generates a key pair and securely manages the private key associated with a Certificate on behalf of Subscriber ("Signing Service"), which Signing Service meets the requirements of the applicable Industry Standards.

5.2. If Subscriber uses a Signing Service, Subscriber will:

5.2.1. Use such Signing Service solely for authorized purposes that comply with this Agreement, the Industry Standards, and all applicable laws;

5.2.2. Not knowingly submit software for code signature that contains Suspect Code, and

5.2.3. Inform the Signing Service if it is discovered (by whatever means) that code submitted to the Signing Service for code signature contained Suspect Code.

5.3. Subscriber will provide accurate and complete information at all times in connection with the issuance of a Certificate, particularly in the Certificate request and verification processes and as otherwise requested by the CA or RA. This includes keeping information up to date at all times.

5.4. Where the key is available outside a Signing Service, Subscriber will, at all times, maintain sole control of, keep confidential, properly protect the private key (and any associated access or activation data or device, e.g., password or token), in accordance with the "Subscriber Private Key Protection" provisions of the Industry Standards. Subscriber will use commercially reasonable efforts to employ the code signing practices set out in the Code Signing Best Practices document available at https://www.entrust.com/-/media/documentation/whitepapers/code-signing-best-practices-v2.pdf or by contacting the CA ("**Code Signing Best Practices**"). Subscriber will generate and operate any device storing private keys in a secure manner, as described in the Code Signing Best Practices, and will use passwords that are randomly generated with at least 16 characters containing uppercase letters, lowercase letters, numbers, and symbols to transport private keys.

5.5. Subscriber will not request a Certificate as defined in this Agreement (i.e. a code signing Certificate) containing a public key that is, or will be used with any non-code signing certificate.

5.6. The Certificate and the private key corresponding to the public key in such Certificate will only be used for authorized and legal purposes, will not be used to digitally sign Suspect Code, and will be used solely in compliance with all applicable laws and in accordance with this Agreement, including the applicable CPS, and for the purposes designated in the key usage field in the Certificate.

5.7. Subscriber acknowledges and agrees that the CA is entitled to modify this Agreement when necessary to comply with any changes in Industry Standards.

5.8. Subscriber will provide an adequate network and other security controls to protect against misuse of the private key corresponding to the public key in the Certificate, and acknowledges and agrees that the CA will revoke the Certificate without requiring prior notification if there is unauthorized access to the private keys.

5.9. Subscriber will not use a Certificate until after Subscriber or its agent has reviewed and verified the Certificate contents for accuracy.

5.10. Subscriber will promptly request the revocation of the Certificate and cease using it and its associated private key if Subscriber believes that:

5.10.1. any information in the Certificate or the Application for a Certificate is or becomes incorrect or inaccurate;

5.10.2. the private key associated with the public key included in the Certificate was misused or compromised, including if the value of the private key has been disclosed to an unauthorized person or an unauthorized person has had access to it, even if it is not known whether there was an actual unauthorized use or disclosure resulting from the access or compromise (collectively, "**Key Compromise**"); or

5.10.3. there is evidence that the Certificate was used to sign Suspect Code.

5.11. Subscriber acknowledges and agrees that the CA and RA are authorized to share information about the Subscriber, signed application, Certificate, and surrounding circumstances with other certification authorities or industry groups, including the CA/Browser Forum, if:

5.11.1. the Certificate or Subscriber is identified as a source of Suspect Code,

5.11.2. the authority to request the Certificate cannot be verified, or

5.11.3. the Certificate is revoked for reasons other than at Subscriber's request (e.g. as a result of private key compromise, discovery of malware, etc.).

5.12. Subscriber will promptly cease all use of the private key corresponding to the public key in a Certificate upon revocation or expiration of the Certificate.

5.13. Subscriber will immediately respond to the CA's instructions concerning any Key Compromise or misuse of a Certificate. This response may include the provision of requested information in connection with the Key Compromise or misuse, and Subscriber must be prepared to respond within 24 hours, including during non-business hours.

5.14. Subscriber acknowledges and accepts that the CA is entitled to revoke a Certificate immediately (including during non-business hours) if Subscriber breaches this Agreement, or if revocation is required under the CPS or the Industry Standards.

6. **No High-Risk Use.** Certificates may not be used 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.

7. **Confidentiality.** Any confidential information shared in connection with Certificates and associated services is subject to the confidentiality provisions in the Commercial Agreement and in the Confidentiality of Business Information section of the CPS.

8. **Export.** The Certificate and related information is subject to export restrictions. You agree to comply

in all respects with any and all applicable laws, rules and regulations and obtain all permits, licenses and authorizations or certificates that may be required in connection with Your use of the Certificate and related information.

9. **Disclaimer of Warranty.** You may be the beneficiary of certain limited warranties with respect to Certificates and/or related services in a Commercial Agreement and in the CPS. **Subject to the foregoing sentence, the Certificate and all related services provided to You by the CA or RA, and each of their respective Affiliates, suppliers, licensors, resellers, distributors, subcontractors, employees, officers, directors and representatives (collectively the "CA Group") are provided "as is", and the CA Group disclaims any and all representations, conditions or warranties of any kind, express or implied. The CA Group disclaims any implied or statutory warranties, such as any implied warranty of non-infringement, merchantability or fitness for a purpose, or any warranties implied by course of dealing, usage or trade. The CA Group makes no warranty under this Agreement that Your Certificate will be error free, timely, uninterrupted, completely secure, or will be recognized or trusted by any particular third party or third party product or service. You acknowledge that ASVs may independently determine that a Certificate is malicious or compromised and that ASVs and ASV products may have the ability to modify customer experiences or "blacklist" a Certificate without notice to Subscriber or the CA and without regard to the revocation status of the Certificate.**

10. **Liability. This Agreement incorporates by reference the limitations and exclusions of liability set out in the CPS with respect to the CA, and, if You are a party to a Commercial Agreement, the limitations and exclusions of liability set out in the Commercial Agreement. If You are not a party to a Commercial Agreement the following applies:**

    In no event will: (A) the CA Group be liable for any consequential, indirect, special, incidental, punitive or exemplary damages, or for any loss of business, opportunities, revenues, profit, savings, goodwill, or reputation, or costs of reprocurement or business interruption, or any damages, losses or costs to the extent arising from Your negligence or misuse; and (B) the CA Group's liability arising out of or related to this Agreement exceed the amount paid for all Certificates covered by Your Entitlement, which in the case of extended validation Certificates will be no less than US$2000.00 per Certificate, up to a total aggregate maximum of US$10,000.00. These limits and exclusions apply regardless of the form of action, whether in contract, tort including negligence, warranty, indemnity, breach of statutory duty, strict liability or otherwise, even if the possibility of excluded or limited damages was known in advance and even if a limited remedy fails of its essential purpose. You acknowledge that the CA has set its prices and entered into this Agreement in reliance on the limitations and exclusions in this section, which form an essential basis of this Agreement. Notwithstanding anything to the contrary, each member of the CA Group neither excludes nor limits its liability for death or bodily injury caused by its own negligence; its own fraud or fraudulent misrepresentation; or other matters for which liability cannot be excluded or limited under applicable law.

11. **Term & Termination.**

    11.1. Term. The term of this Agreement shall begin on the date that You have agreed to this Agreement and shall terminate immediately upon the earlier of (a) the expiry or termination of Your Entitlement; and (b) the rejection of the Application to have one or more Certificates issued to You. The Sections entitled "Disclaimer of Warranty", "Liability", "Governing Law", "Severability", and "Miscellaneous" shall survive any termination or expiry of this Agreement.

    11.2. Early Termination of Your Entitlement. The CA may terminate Your Entitlement early: (a) if You fail to comply with any of the material terms or conditions of this Agreement or the CPS; or (b) in the CA's discretion with notice to You in order to comply with any third party licensing or other contractual or legal obligation (including any Industry Standard) to which the CA is subject.

12. **Governing Law.** If You are a party to a Commercial Agreement, this Agreement incorporates by reference the governing law and dispute resolution provisions set out in the Commercial Agreement. If You are not a party to a Commercial Agreement, any disputes related to a Certificate, as well as the construction, validity, interpretation, enforceability and performance of this Agreement, and all claims arising out of or related to this Agreement, including tort claims, shall, (i) if You are located in Canada, be governed by the laws of the Province of Ontario, Canada, and shall be brought in the provincial or federal courts sitting in Ottawa, Ontario; (ii) if You are located in Europe, be governed by the laws of England and Wales and shall be brought in the courts sitting in London, England; and (iii) if You are located anywhere else in the world, be governed by the laws of the State of Minnesota, United States, and shall be brought in the federal and state courts located in Hennepin County, Minnesota. Each party hereby agrees that the applicable courts identified in this Section (Governing Law) shall have personal and exclusive jurisdiction over such disputes. In the event that any matter is brought in a provincial, state or federal court each party waives any right that such party may have to a jury trial. To the maximum extent permitted by applicable law, the parties agree that the provisions of the United Nations Convention on Contracts for the International Sale of Goods, as amended, shall not apply to this Agreement.

13. **Severability.** To the extent permitted by applicable law, the parties hereby waive any provision of law that would render any provision of this Agreement invalid or otherwise unenforceable in any respect. In the event that a provision of this Agreement is held to be invalid or otherwise unenforceable in application to particular facts or circumstances: (a) such provision will be interpreted and amended to the extent necessary to fulfill its intended purpose to the maximum extent permitted by applicable law and its validity and enforceability as applied to any other facts or circumstances will not be affected or impaired; and (b) the remaining provisions of this Agreement will continue in full force and effect. **FOR GREATER CERTAINTY, IT IS EXPRESSLY UNDERSTOOD AND INTENDED THAT EACH PROVISION THAT DEALS WITH LIMITATIONS AND EXCLUSIONS OF LIABILITY, DISCLAIMERS OF REPRESENTATIONS, WARRANTIES AND CONDITIONS, OR INDEMNIFICATION IS SEVERABLE FROM ANY OTHER PROVISIONS**.

14. **Miscellaneous.** This Agreement may be amended by the written consent of each party at the time of such amendment. Additionally, this Agreement may be amended by the CA at any time with notice to You; such amendment to be effective immediately in the case of changes required to comply with law or Industry Standards. This Agreement shall not be assigned by You without prior written consent of the CA, and any attempt to assign any rights, duties, or obligations, which arise under this Agreement without such consent will be void. The CA may assign this Agreement (including all of its rights and obligations) at any time. The CA may use one or more Affiliate(s) or subcontractors to perform its obligations under this Agreement, provided that such use will not affect the CA's obligations under the Agreement. The CA is not Your agent, fiduciary, trustee, or other representative and the relationship between the CA and You is not that of an agent and a principal. Except for the rights granted expressly in this Agreement, no other right is or will be deemed to be granted, whether by implication, estoppel, inference or otherwise, by or as a result of this Agreement or any conduct of either party. The CA and its licensors expressly retain all ownership rights, title, and interest in the products and services provided by the CA (including any modifications, enhancements and derivative works thereof). In the event of a conflict between a Commercial Agreement between You and the CA, the CPS and this Agreement, the following order of precedence shall apply: (1) the CPS, (2) this Agreement and 3) the Commercial Agreement. You expressly acknowledge that each Application Software Vendor and each member of the CA Group are express third party beneficiaries, may rely on and enforce this Agreement and the CPS against You. The definitive version of this Agreement is written in English. If Agreement are translated into another language and there is a conflict between the English version and the translated version, the English language version controls.

15. **Definitions.** In this Agreement capitalized words shall have the following meanings:

    15.1. "**Affiliate**" of a company shall mean any entity that directly or indirectly controls, is controlled by, or is under common control with such company, where control means ownership of fifty percent (50%) or more of the voting rights for the board of directors or other mechanism of

control.

15.2. "**Application**" means the submission of information and/or a certificate signing request to the CA or its appointed RA to support the issuance of a Certificate, using a process and form defined by the CA or RA for this purpose.

15.3. "**Application Software Vendor**" or "**ASV**" means a developer of software that displays or uses Certificates, including but not limited to Adobe, Apple, Google, Intel, Microsoft, Mozilla, and Oracle.

15.4. "**CA**" means the certification authority who operates the system that issues and signs Certificates, and who is identified as the CA in the applicable CPS.

15.5. "**Certificate**" means a digital document that at a minimum: (a) identifies the certification authority issuing it; (b) names or otherwise identifies a Subject; (c) contains a public key of a key pair; (d) identifies the operational period; (e) contains a serial number; and (f) is digitally signed by the certification authority. There are various types of Certificate(s) that may be issued to Subscriber by the CA. This Agreement applies to code signing Certificates, i.e. Certificates with code signing indicated in the extended key usage field, which may be extended validation (EV) code signing Certificates or non-EV code signing Certificates.

15.6. "**Certificate Beneficiaries**" means, collectively, all Application Software Vendors with whom the CA has entered into a contract to include the CA's root Certificate(s) in such ASV's software, and all individuals or entities who actually rely on such Certificate during the period when it is valid (i.e., not expired and not revoked).

15.7. "**Commercial Agreement**" means a separate legal agreement with Entrust Corporation or one of its Affiliates for the provision of services relating to publicly trusted Certificates.

15.8. "**CPS**" means the most recent version of the certification practice statement, as amended from time to time by the CA, that is applicable to a Certificate issued by the CA, and which is incorporated by reference into this Agreement. The CPS applicable to a specific Certificate depends on the type of Certificate and can be found at or through http://www.entrust.net/cps or by contacting the CA.

15.9. **"Entitlement"** means a right to enroll to receive one or more specific types of Certificates procured by or for You through a purchasing mechanism authorized by the CA, such as an order made through an online store, under a Commercial Agreement.

15.10. "**Industry Standards**" means, collectively, the most up-to-date versions of each of the following, in each case, that are applicable to the various types of publicly-trusted Certificates issued by the CA (as stated in the CPS), and to which the CA is subject and bound as an issuer of such Certificates:

a) the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates.

15.11. "**Subject**" means the entity identified in the "Subject" field in a Certificate.

15.12. "**Subscriber**" means the natural or legal person who applies for a Certificate.

15.13. "**Suspect Code**" means 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.

15.14. “**You**” **or** “**Your**” means the Subscriber who has accepted this Agreement.

This document is considered public and available to all viewers.

Version	Date	Changes
1	September 25 2024	Adopted.