



**TERMS OF USE
DIGITAL CERTIFICATE(S)
FOR ELECTRONIC SIGNATURES, ELECTRONIC SEALS, EMAIL, AND MOBILE DEVICES**

Before downloading, installing, or using any Certificate issued by Entrust, please carefully read these terms of use (“Terms of Use”), which govern access to and use of Certificates issued by Entrust for electronic signatures, electronic seals, emails and mobile devices, and define 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 the Terms of Use, represent and warrant that you are lawfully able to enter into contracts (e.g. you are not a minor). If you are accepting the Terms of Use on behalf of a legal entity, for example, the company or organization you work for, you represent and warrant that you have legal authority to bind such legal entity. If you are (or are acting as the authorized representative of) the Subscriber for the Certificate, these Terms of Use constitute the ‘subscriber agreement’ as required and defined in the Industry Standards.

IF YOU DO NOT ACCEPT THESE TERMS OF USE, 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 ISSUED BY ENTRUST. THE CONTINUED RIGHT TO DOWNLOAD, INSTALL AND/OR USE ENTRUST CERTIFICATES IS CONTINGENT ON CONTINUED COMPLIANCE WITH THESE TERMS OF USE.

WE RECOMMEND THAT YOU SAVE A COPY OF THESE TERMS OF USE FOR YOUR FUTURE REFERENCE.

Capitalized words in these Terms of Use have the meanings set out in Section 18.

1. **Verification & Issuance.** Entrust will provide the following services in accordance with Your Entitlement(s).

1.1. Verification. Upon receipt of an application for a Certificate, Entrust will perform the verification described in the CPS for the applicable type of Certificate. Entrust may reject applications for Certificates for the reasons set out in the CPS. You understand that issuance of a Certificate is conditional on Entrust’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, Subject 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, rights/control over domain name(s) and trademarks (collectively, “Verification Information”). You acknowledge and agree that:

1.1.1. Verification requires the collection and processing of personal information. To the extent that Entrust is a ‘processor’ of personal information, it will process the information in accordance with the product privacy notice and Entrust customer data processing agreement available at <https://www.entrust.com/legal-compliance/data-privacy> (or a similar agreement mutually agreed by Entrust and the Subscriber). 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 Entrust to perform its obligations under these Terms of Use and the CPS.

- 1.1.2. Some types of verification for certain Certificates require that You use a smartphone or tablet mobile device with specified operating systems to be valid, as set out in the applicable CPS. You are responsible for ensuring that You comply with any requirements to use the specified type of device when undergoing verification.
 - 1.1.3. Verification may entail use of third-party databases which may result in some Verification Information being included in such databases.
 - 1.1.4. 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.
 - 1.1.5. Entrust may disclose Verification Information to third parties for the purpose of complying with Industry Standards.
- 1.2. If and when the application passes verification, Entrust will issue Certificates and make them available for retrieval and usage as set out in the CPS and Documentation. Use of any Certificate constitutes Your acceptance of it.
2. **Operation of the PKI.** Each CPS and TPS sets out Entrust'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 regarding 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) How revocation status information is provided and the period over which it is available;
3. **Revocation of Digital Certificates.** Certificates may be revoked by Entrust 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. Revocation processes are as set out in the CPS.
4. **Grant of License.** Subject to Your compliance with these Terms of Use, Entrust 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 these Terms of Use, including the CPS which is incorporated herein, and Your Entitlement. If the Certificate that You are issued is designated as a document signing certificate (including a Qualified Signature Certificate), mobile device certificate or a secure email enterprise certificate and has been purchased on Your behalf by a legal entity, then You may only use the Certificate to conduct business with or for that legal entity. If You are issued any Certificates for the purposes of an evaluation of Entrust's services ("Trial Certificates"), your right to use such Trial Certificates is limited to short-term evaluation only 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 Entrust to revoke any outstanding Trial Certificates upon termination of your evaluation rights. You agree to supply any information reasonably requested by Entrust to ensure Your compliance with the terms hereof.
5. **Subscriber Obligations.** If You are the Subject for the Certificate to be issued but not the Subscriber, this section does not apply to You: skip down to Section 6 below (with the heading Subject Obligations). If You are the Subscriber for the Certificates to be issued, you understand and agree that as a condition of having any Certificate issued to or for You, You make, on Your own behalf and if applicable on behalf of Your principal or agent under a subcontractor or hosting service relationship, the following representations, commitments, affirmations and warranties for the benefit of Certificate Beneficiaries, Entrust and any of Entrust's Affiliates that will issue Certificates to or for You:

- 5.1. With respect to document signing Certificates, qualified seal Certificate(s) (eIDAS QSealCs and PSD2 QSealCs), and eIDAS Qualified Signature Certificate(s) (eIDAS QSigCs):
 - 5.1.1. If Subscriber is applying for a Certificate to be issued to or for another individual or legal entity (each, a "Person"), such Person has authorized Subscriber to act on its behalf, including to request Certificates on behalf of such Person, and to make the representations, commitments, affirmations and warranties in this Section on behalf of such Person as well as on Subscriber's own behalf.
 - 5.1.2. Subscriber will provide true, accurate and complete information in accordance with the Industry Standards in relation to any Certificate, particularly in the Certificate request and verification processes, and hereby confirms that all information to be held in the Certificate is correct.
 - 5.1.3. Subscriber will comply with any requirements in the CPS for it to use a specific type of cryptographic device (including a secure cryptographic device or a qualified electronic signature/seal creation device "QSCD", which, for clarity, is required for creating qualified digital signatures and seals), and if so required:
 - 5.1.3.1. the Subject's private key(s) will only be used for cryptographic functions within the specified cryptographic device.
 - 5.1.3.2. if the Subject's keys are generated under control of the Subscriber or Subject, the Subject's keys will be generated within the specified cryptographic device.
 - 5.1.4. The unauthorized use of the Subject's private key will be prohibited.
 - 5.1.5. Subscriber consents to Entrust's keeping of a record of information used in registration, subject device provision, including whether this is to the Subscriber or to the Subject where they differ, and any subsequent revocation, the identity and any specific attributes placed in the Certificate, and the passing of this information to third parties under the same conditions as required by Industry Standards in the case of Entrust terminating its services.
 - 5.1.6. Subscriber requires the publication of the Certificate in the manner and in accordance with the conditions set out in the CPS and will obtain, where applicable, the Subject's consent to such publication.
 - 5.1.7. The private key and corresponding public key associated with the Certificate will only be used in accordance with the limitations notified to the Subscriber, including in the CPS.
 - 5.1.8. If the Subscriber or Subject generates the Subject's keys:
 - (a) the Subject keys will be generated using an algorithm as specified in the Industry Standards for the uses of the certified key as identified in the CPS.
 - (b) the key length and algorithm will be as specified in the Industry Standards for the uses of the certified key as identified in the CPS during the validity time of the Certificate.
 - (c) and if the Subject is an individual, the Subject's private key must be kept under the Subject's sole control.
 - (d) and if the Subject is a legal entity, the Subject's private key must be kept under the Subject's control.
 - 5.1.9. If the Subject is an individual, the Subject's private key will be maintained (or, if Entrust is managing the keys for the Subject, the private key will be used) under the Subject's sole control.

- 5.1.10. If the Subject is a legal entity, the Subject's private key will be maintained (or, if Entrust is managing the keys for the Subject, the private key will be used) under the Subject's control.
 - 5.1.11. Upon being informed that the Subject's Certificate has been revoked, or that the issuing CA has been compromised, Subscriber will ensure that the private key corresponding to the public key in the Certificate is no longer used by the Subject.
 - 5.1.12. Key pairs associated with eIDAS QSigCs will only be used for electronic signatures.
 - 5.1.13. Key pairs associated with eIDAS QSealC and PSD2 QSealC will only be used for electronic seals.
 - 5.1.14. Subscriber will notify Entrust without unreasonable delay if any of the following occur up to the end of the validity period indicated in the Certificate: (a) there is any actual or suspected loss, theft, or potential compromise of the Subject's private key; (b) control over the Subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons; or (c) any information included in the Certificate or the application for a Certificate changes, is or becomes incorrect or inaccurate, or if any change in any circumstances would make the information in the Certificate misleading.
 - 5.1.15. Subscriber will immediately and permanently discontinue the use of the Subject's private key, except for key decipherment, if it becomes compromised.
- 5.2. With respect to S/MIME (email) and mobile device Certificates:
- 5.2.1. Subscriber will provide accurate and complete information at all times in relation to any Certificate, both in the Certificate request and as otherwise requested by Entrust in connection with the verification processes and issuance of the Certificate.
 - 5.2.2. All reasonable measures have been taken to, at all times, assure control of, keep confidential, and properly protect the private key corresponding to the public key submitted to Entrust with the Certificate request (and any associated access or activation data or device, e.g., password or token).
 - 5.2.3. Subscriber will review and verify the Certificate contents for accuracy.
 - 5.2.4. the Certificate will only be used in compliance with all applicable laws and solely in accordance with these Terms of Use, and, in the case of SMIME Certificates, the Certificate will only be used on email addresses listed in the Certificate.
 - 5.2.5. Subscriber will promptly request the revocation of the Certificate and cease using it:
 - (a) if any information included in the Certificate or the application for a Certificate changes, is or becomes incorrect or inaccurate, or if any change in any circumstances would make the information in the Certificate misleading.
 - (b) if there is any actual or suspected misuse or compromise of the private key corresponding to the public key in the Certificate, including if the value of the private key has been disclosed to an unauthorized person or an unauthorized person has had access to it (collectively, "**Key Compromise**").
 - 5.2.6. Subscriber will promptly cease all use of the Certificate and the private key corresponding to the public key in such Certificate, upon any Key Compromise, and in any event, upon revocation of the Certificate for reasons of Key Compromise.
 - 5.2.7. Subscriber will immediately respond to Entrust's instructions concerning any Key Compromise or misuse of a Certificate.

- 5.2.8. Subscriber acknowledges and agrees that Entrust is entitled to revoke a Certificate immediately if:
- (a) Subscriber breaches these Terms of Use.
 - (b) Entrust discovers that there has been a Key Compromise of the Certificate's private key.
 - (c) Revocation is required under the CPS or the Industry Standards.
- 5.2.9. Where the Subject named in the Certificate(s) is a separate entity from the Subscriber, the Subject has authorized the inclusion of the Subject's information in the Certificate.
- 5.2.10. In the case of SMIME Certificates, Subscriber owns, controls, or has the exclusive right to use the email address listed in Certificate.
6. **Subject Obligations.** If You are the Subject for the Certificate to be issued but You are not the Subscriber, You accept the following obligations:
- 6.1. Subject will comply with any requirements in the CPS for Subject to use a specific type of cryptographic device (including a secure cryptographic device or a qualified electronic signature/seal creation device), and if so required, Subject's private key(s) will only be used for cryptographic functions with the specified cryptographic device;
- 6.2. Subject consents to Entrust's keeping of a record of information used in registration, subject device provision, including whether this is to Subject or, if different, to the Subscriber, and any subsequent revocation, the identity and any specific attributes placed in the Certificate, and the passing of this information to third parties under the same conditions as required by applicable law or Industry Standards in the case of Entrust terminating its services.
- 6.3. The unauthorized use of the Subject's private key will be prohibited.
- 6.4. The private key and corresponding public key associated with the Certificate will only be used in accordance with the limitations notified to the Subject, including in the CPS.
- 6.5. Subject will notify Entrust without unreasonable delay if any of the following occur up to the end of the validity period indicated in the Certificate: (a) there is any actual or suspected loss, theft, or potential compromise of the Subject's private key; (b) control over the Subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons; or (c) any information included in the Certificate or the application for a Certificate changes, is or becomes incorrect or inaccurate, or if any change in any circumstances would make the information in the Certificate misleading.
- 6.6. Upon being informed that the Subject's Certificate has been revoked, or that the issuing CA has been compromised, Subject will no longer use the private key corresponding to the public key in the Certificate.
- 6.7. Subject will immediately and permanently discontinue the use of the Subject's private key, except for key decipherment, if it becomes compromised.
7. **Protect Access Credentials.** You will take reasonable measures to protect the access credentials that You use for accessing and/or using the Certificate, and will not share such access credentials with any other person.
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. You also represent and warrant that You: (a) are not located in, under the

control of, or a national or resident of any country to which the export of the Certificate or related information would be prohibited by the applicable laws, rules or regulations of the United States (U.S.), Canada, United Kingdom (U.K.), European Union (E.U.), or other applicable jurisdiction; (b) are not an individual to whom the export of the Certificate or related information would be prohibited by the laws of the U.S., Canada, U.K., E.U., or other applicable jurisdiction; (c) have complied and will comply with applicable laws, rules and regulations of the U.S., Canada, U.K., E.U., or other applicable jurisdiction(s) and of any state, province, or locality or applicable jurisdiction governing exports of any product or service provided by or through Entrust; and (d) will not use the Certificate for any purposes prohibited by applicable laws, rules or regulations on trade controls, including related to nuclear, chemical, or biological weapons proliferation, arms trading, or in furtherance of terrorist financing; (e) are not (i) an individual listed on, or directly or indirectly owned or controlled by, a person (whether legal or natural) listed on, or acting on behalf of a person listed on, any U.S., Canadian, E.U., U.K., or U.N. sanctions list, including the list of Specially Designated Nationals of the Office of Foreign Assets Control or the Department of Commerce Entities List, or (ii) located in, incorporated under the laws of, or owned (meaning 50% or greater ownership interest) or otherwise, directly or indirectly, controlled by, or acting on behalf of, a person located in, residing in, or organized under the laws of any of the countries listed at <https://www.entrust.com/legal-compliance/denied-parties>. In the event any of the above representations and warranties is incorrect or You engage in any conduct that is contrary to sanctions or trade controls or other applicable laws, regulations, or rules, then any agreements, purchase orders, performance of services, or other contractual obligations of Entrust are immediately terminated. You understand and agree that Entrust is not responsible for service interruptions that may be experienced by anyone using third party devices (e.g. Huawei mobile phones) that may interoperate with an Entrust Certificate, to the extent that trade compliance restrictions, legal obligations, or information security requirements applicable to Entrust do not allow for compliance with third party device requirements.

9. **AI Notice.** You acknowledge and agree that, in the provision of Certificates and related services under these Terms of Use, Entrust may use AI technology. Entrust will employ AI in a manner informed by evolving industry standards and best practices, striving to ensure the accuracy, reliability, and security of the AI systems it employs, and will from time to time, to the extent required by laws and regulations applicable to Entrust and otherwise in its discretion, make available details of its AI use on www.entrust.com. While Entrust is committed to the responsible and ethical use of AI, You acknowledge that AI-driven decisions are fallible. Therefore, where Entrust has identified an Entrust offering (or component thereof) as incorporating AI, You agree to exercise reasonable judgment when relying on AI-generated information and to use human intervention where feasible for decisions made by AI that may negatively impact data subjects, taking into account the particular uses for which and contexts in which You are considering using AI-generated outputs of the applicable Entrust offering. Entrust will comply with all relevant data protection and privacy laws concerning the collection, processing, and storage of personal information used in conjunction with AI as further outlined in Section 1.1 (Verification) of these Terms of Use. You will not, and will not allow third parties to, use Entrust Certificates or services (or any content, data, output, or other information received or derived therefrom) to directly or indirectly create, train, test, or otherwise improve any machine learning algorithms, automated decision-making processes, or AI systems, or input or upload any Entrust confidential information to an AI system or application.
10. **Disclaimer of Warranty.** Entrust may provide certain limited warranties in a separate written agreement with the Subscriber or in the CPS. **Subject to the foregoing sentence, the Certificate and all related services provided to You by Entrust or any its Affiliates, and each of their respective suppliers, licensors, resellers, distributors, subcontractors, employees, officers, directors and representatives (collectively the “Entrust Group”) are provided “as is”, and the Entrust Group disclaim any and all representations, conditions or warranties of any kind, express or implied, including warranties of non-infringement, title, merchantability or fitness for a purpose, satisfactory quality, or any representations, conditions or warranties implied by statute, course of dealing, course of performance, or usage or trade. Entrust makes no representations, conditions or warranties regarding any third party product or service, including any third party product with which a Certificate may interoperate. Entrust makes no representations or warranties that any Certificate or digital signature created using a Certificate**

will be recognized or trusted by any particular third party or third party product or service. Entrust further disclaims and makes no representation, warranty or condition of any kind, whether express or implied, either in fact or by operation of law, to You or any person that (A) any person to whom a Certificate is issued is in fact person, entity or organization it claims to have been; (B) any person is in fact the person, entity or organization listed in the Certificate; or (C) that the information contained in the Certificate is accurate, authentic, complete or reliable. In no event does the Entrust Group make any representations, or provide any warranties, or conditions to You or any person with respect to (i) the techniques used by any party other than Entrust in the generation and storage of the private key corresponding to the public key in a Certificate, including whether such private key has been compromised or was generated using sound cryptographic techniques, (ii) the reliability of any cryptographic techniques or methods used in conducting any act, transaction, or process involving or utilizing a Certificate, or (iii) non-repudiation of any Certificate or any transaction facilitated through the use of a Certificate, since such determination is a matter of applicable law.

11. **Your Indemnification of Entrust.** Except as expressly otherwise set out in a separate written agreement between You and Entrust, You shall, at Your expense, indemnify, hold harmless, and, at Entrust's request, defend the Entrust Group from and against all claims, demands, suits or proceedings, fines, costs, damages, losses, settlement fees, and expenses (including investigation costs and attorney fees and disbursements) arising out of or related to: (1) any breach by You of Your obligations under Section 5 (Subscriber Obligations), Section 6 (Subject Obligations), or the CPS; and (2) claims (including, without limitation, infringement claims) pertaining to content or other data supplied or required to be supplied by You in connection with a Certificate. Notwithstanding the foregoing, You shall not be obligated to provide any indemnification to a member of the Entrust Group in respect to any losses, costs, damages or fees to the extent that such losses, costs, damages and fees arise out of or relate to any willful misconduct by such member of the Entrust Group.

12. **Liability.**

12.1. IN NO EVENT WILL ENTRUST GROUP BE LIABLE FOR, AND YOU WAIVE ANY RIGHT YOU MAY HAVE TO, ANY CONSEQUENTIAL, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR EXEMPLARY DAMAGES OR FOR ANY LOSS OF BUSINESS, OPPORTUNITIES, REVENUES, PROFITS, SAVINGS, GOODWILL, REPUTATION, CUSTOMERS, USE, OR DATA, OR COSTS OF REPROCUREMENT OR BUSINESS INTERRUPTION, OR ANY DAMAGES, LOSSES OR COSTS (I) ARISING OUT OF ANY ALLEGATION THAT THE CONTENT OF A CERTIFICATE (INCLUDING ANY MARKS IN A VMC) INFRINGES, MISAPPROPRIATES, DILUTES, UNFAIRLY COMPETES WITH, OR OTHERWISE VIOLATES ANY PATENT, TRADEMARK, COPYRIGHT, TRADE SECRET, OR ANY OTHER INTELLECTUAL PROPERTY RIGHT OR OTHER RIGHT OF ANY PERSON IN ANY JURISDICTION; (II) THAT ARE NOT DIRECTLY ATTRIBUTABLE TO THE USE OR RELIANCE ON A CERTIFICATE, INCLUDING ANY LOSS OR DAMAGE RESULTING FROM THE COMBINATION OR INTEGRATION OF THE CERTIFICATE WITH ANY SOFTWARE OR HARDWARE NOT PROVIDED BY ENTRUST IF THE LOSS OR DAMAGE WOULD NOT HAVE OCCURRED AS A RESULT OF USE OF THE CERTIFICATE ALONE; OR (III) ARISING FROM THE TECHNOLOGY THAT ISSUED THE CERTIFICATE SIGNING REQUEST (CSR) OR ANY INFORMATION CONTAINED IN THE CSR, UNLESS THE CSR WAS GENERATED BY ENTRUST GROUP.

12.2. IN NO EVENT WILL ENTRUST GROUP BE LIABLE FOR, AND YOU WAIVE ANY RIGHT YOU MAY HAVE TO, ANY CLAIMS, DAMAGES, LOSSES OR COSTS ARISING OUT OF OR RELATING TO USE OR MISUSE OF, OR RELIANCE ON ANY CERTIFICATE THAT (I) HAS EXPIRED OR BEEN REVOKED; (II) HAS BEEN USED FOR ANY PURPOSE OTHER THAN AS SET FORTH IN THESE TERMS OF USE OR THE CPS; (III) HAS BEEN TAMPERED WITH; (IV) WITH RESPECT TO WHICH THE UNDERLYING KEY PAIR, OR THE CRYPTOGRAPHY ALGORITHM USED TO GENERATE SUCH CERTIFICATE'S KEY



PAIR, HAS BEEN COMPROMISED BY THE ACTION OF ANY PARTY OTHER THAN ENTRUST GROUP (INCLUDING WITHOUT LIMITATION YOU); OR (V) IS THE SUBJECT OF MISREPRESENTATIONS OR OTHER MISLEADING ACTS OR OMISSIONS OF ANY OTHER PARTY, INCLUDING BUT NOT LIMITED TO YOU.

12.3. EXCEPT AS EXPRESSLY OTHERWISE SET OUT IN A SEPARATE WRITTEN AGREEMENT BETWEEN YOU AND ENTRUST, IN NO EVENT WILL ENTRUST GROUP'S LIABILITY ARISING OUT OF OR RELATED TO THESE TERMS OF USE, THE CPS AND THE USE AND PERFORMANCE OF ANY PRODUCTS OR SERVICES PROVIDED HEREUNDER EXCEED (I) IN THE CASE OF EXTENDED VALIDATION SSL/TLS CERTIFICATES AND CODE SIGNING CERTIFICATES, TWO THOUSAND UNITED STATES DOLLARS (\$2000.00 U.S.) PER CERTIFICATE, AND (II) IN THE CASE OF ALL OTHER CERTIFICATES, ONE THOUSAND UNITED STATES DOLLARS (\$1000.00 U.S.) PER CERTIFICATE, IN EACH CASE UP TO A TOTAL AGGREGATE MAXIMUM OF ONE HUNDRED THOUSAND U.S. DOLLARS (US\$100,000.00).

12.4. THE EXCLUSIONS AND LIMITS IN THIS SECTION (LIABILITY) APPLY: (I) REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT (INCLUDING FUNDAMENTAL BREACH), TORT (INCLUDING NEGLIGENCE), WARRANTY, INDEMNITY, BREACH OF STATUTORY DUTY, MISREPRESENTATION, STRICT LIABILITY, STRICT PRODUCT LIABILITY, OR OTHERWISE; (II) ON AN AGGREGATE BASIS, REGARDLESS OF THE NUMBER OF CLAIMS, TRANSACTIONS, DIGITAL SIGNATURES OR CERTIFICATES; (III) EVEN IF THE POSSIBILITY OF THE DAMAGES IN QUESTION WAS KNOWN OR COMMUNICATED IN ADVANCE AND EVEN IF SUCH DAMAGES WERE FORESEEABLE; AND (IV) EVEN IF THE REMEDIES FAIL OF THEIR ESSENTIAL PURPOSE. YOU ACKNOWLEDGE THAT ENTRUST HAS AGREED TO PROVIDE CERTIFICATES AND RELATED SERVICES IN RELIANCE ON THE LIMITATIONS AND EXCLUSIONS IN THIS SECTION (LIABILITY), WHICH FORM AN ESSENTIAL BASIS OF THESE TERMS OF USE.

12.5. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS SECTION (LIABILITY) OR ELSEWHERE IN THESE TERMS OF USE, TO THE EXTENT REQUIRED BY APPLICABLE LAW ENTRUST 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.

13. **Term & Termination.**

13.1. Term. The term of these Terms of Use shall begin on the date that You have agreed to these Terms of Use and shall terminate immediately upon the earlier of (a) the expiry or termination of Your Entitlement; (b) if you are only issued one Certificate hereunder, the revocation of Your Certificate, or, if you are issued more than one Certificate hereunder, the revocation of all Your Certificates; (c) the rejection of the application to have one or more Certificates issued to You. The Sections entitled "Your Indemnification of Entrust", "Disclaimer of Warranty", "Liability", "Governing Law", "Severability", "Dispute Settlement", and "Miscellaneous" shall survive any termination or expiry of these Terms of Use.

13.2. Early Termination of Your Entitlement. Entrust may terminate Your Entitlement early: (a) if You fail to comply with any of the material terms or conditions of these Terms of Use, the CPS or TPS; or (b) in Entrust'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 Entrust is subject.

14. **Governing Law.** Except as expressly otherwise set out in a separate written agreement between You and Entrust, any disputes related to a Certificate or related services, as well as the construction, validity,



interpretation, enforceability and performance of these Terms of Use, and all claims arising out of or related to these Terms of Use, 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 these Terms of Use.

15. **Severability.** To the extent permitted by applicable law, the parties hereby waive any provision of law that would render any provision of these Terms of Use invalid or otherwise unenforceable in any respect. In the event that a provision of these Terms of Use 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 these Terms of Use 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.**
16. **U.S. Government End Users.** Your Certificate is a commercial item as that term is defined at 48 CFR 2.101, consisting of commercial computer software and commercial computer software documentation as those terms are used in 48 CFR 12.212. If a Certificate is acquired by or on behalf of the U.S. government or by a U.S. government contractor (including without limitation prime contractors and subcontractors at any tier), then in accordance with 48 CFR 227.7202-4 (for Department of Defense licenses only) and 48 CFR 12.212 (for licenses with all federal government agencies), the government's rights to such Certificate are limited to the commercial rights specifically granted in these Terms of Use, as restricted by these Terms of Use. The rights limited by the preceding sentence include any rights to reproduce, modify, perform, display, disclose, release, or otherwise use the Certificate. This Section (U.S. Government End-Users) does not grant You or the government any rights not specifically set forth in these Terms of Use.
17. **Miscellaneous.** These Terms of Use may be amended by the written consent of each party at the time of such amendment. Additionally, these Terms of Use may be amended by Entrust at any time with notice to You; such amendment to be effective immediately in the case of changes required to comply with Industry Standards. These Terms of Use shall not be assigned by You without prior written consent of Entrust, and any attempt to assign any rights, duties, or obligations, which arise under these Terms of Use without such consent will be void. Entrust may assign these Terms of Use (including all of its rights and obligations) at any time. Entrust may use one or more Affiliate(s) or subcontractors to perform its obligations under these Terms of Use. Entrust is not your agent, fiduciary, trustee, or other representative and the relationship between Entrust and You is not that of an agent and a principal. Except for the rights granted expressly in these Terms of Use, no other rights is or will be deemed to be granted, whether by implication, estoppel, inference or otherwise, by or as a result of these Terms of Use or any conduct of either party. Entrust and its licensors expressly retain all ownership rights, title, and interest in the products and services provided by Entrust (including any modifications, enhancements and derivative works thereof). In the event of a conflict between an Entitlement or other agreement between You and Entrust, the CPS and these Terms of Use, the following order of precedence shall apply: (1) the CPS, (2) these Terms of Use and (3) the Entitlement or other agreement. You expressly acknowledge that each Application Software Vendor and each member of the Entrust Group are express third party beneficiaries, may rely on and enforce these Terms of Use and the CPS against You. The definitive version of these Terms of Use is



written in English. If Terms of Use are translated into another language and there is a conflict between the English version and the translated version, the English language version controls.

18. **Definitions.** In these Terms of Use capitalized words shall have the following meanings:

- 18.1. “**Affiliates**” of Entrust shall mean any subsidiary of Entrust Corporation.
- 18.2. “**AI**” (Artificial Intelligence) means computer algorithms and machine learning systems that can analyze, process, and make decisions based on data inputs, without the need for direct human intervention.
- 18.3. “**Application Software Vendor**” or “**ASV**” means a developer of email software or other software that displays or uses Certificates, including but not limited to Adobe, Apple, Google, Intel, Microsoft, Mozilla, and Oracle.
- 18.4. “**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 Subject/Subscriber by Entrust. These Terms of Use apply to document signing Certificates, mobile device Certificates, SMIME Certificates, eIDAS qualified seal certificate(s) (“**eIDAS QSealCs**”), PSD2 qualified Seal Certificate(s) (“**PSD2 QSealCs**”), and eIDAS Qualified Signature Certificate(s) (“**eIDAS QSigCs**”).
- 18.5. “**Certificate Beneficiaries**” means, collectively, all Application Software Vendors with whom Entrust has entered into a contract to include Entrust’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).
- 18.6. “**CPS**” means the most recent version of the certification practice statement, as amended from time to time by Entrust, that is applicable to a Certificate issued by Entrust, and which is incorporated by reference into these Terms of Use. The CPS applicable to a specific Certificate depends on the type of Certificate and can be found on the Internet at <http://www.entrust.net/cps> or by contacting Entrust. For example, eIDAS QSealCs and eIDAS QSigCs are governed by the most recent version of the document titled “Certification Practice Statement For Qualified Certificates”, and other Certificates are generally governed by the most recent version of the document titled “Certification Practice Statement”.
- 18.7. “**Documentation**” means the user guide, manual, technical specifications or release notes for the applicable Certificate provided by Entrust, all as may be updated from time to time.
- 18.8. “**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 Entrust, such as an online store or separate legal agreement. If You are an individual who is enrolling to receive a Certificate without having purchased it, Your Entitlement may have been purchased for you by a legal entity such as Your employer or a legal entity with which You are transacting (e.g. Your bank).
- 18.9. “**Entrust**” means the Entrust Corporation subsidiary(ies) identified in the applicable CPS.
- 18.10. “**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 Entrust, and to which Entrust 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 Certificates,



- b) the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates (“S/MIME BRs”),
 - c) European Standards produced by the ETSI Technical Committee Electronic Signatures and Infrastructures, and
 - d) laws and regulations.
- 18.11. “**Subject**” means the natural or legal person or device identified in the “Subject” field in a Certificate.
- 18.12. “**Subscriber**” means the natural or legal person who applies for a Certificate.
- 18.13. “**You**” or “**Your**” means the Subject or Subscriber who has accepted these Terms of Use.