Public Key Infrastructure as a Service
Terms of Use

The Agreement for Entrust's Public Key Infrastructure as a Service Offering is made up of these terms of use ("Hosted Services Schedule"), the Entrust General Terms and Conditions ("General Terms") available at https://www.entrust.com/general-terms.pdf, and an applicable Order for the Hosted Services. Capitalized terms not defined herein have the meanings given to them in the General Terms.

You, as the individual accepting the Agreement (as defined in the General Terms), represent and warrant that you are lawfully able to enter into contracts (e.g. you are not a minor). If you are entering into the Agreement on behalf of a legal entity, for example, the company or organization you work for, you represent to us that you have legal authority to bind such legal entity. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THE AGREEMENT (OR 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 SHALL NOT ACCESS OR USE THE HOSTED SERVICES. THE CONTINUED RIGHT TO ACCESS AND USE THE HOSTED SERVICES IS CONTINGENT ON CONTINUED COMPLIANCE WITH THE TERMS AND CONDITIONS OF THE AGREEMENT BY YOU (OR BY THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING ACCEPTANCE).

In consideration of the commitments set forth below, the adequacy of which consideration the parties hereby acknowledge, the parties agree as follows.

1. **Definitions**.

1.1. "**Administration Information**" means information in and related to Customer's Management Account and information generated by Customer's usage of the Hosted Services, such as Customer's access credentials, contact information for Administrators, license entitlements, and consumption.

1.2. "**CA**" means the certification authority system that issues and signs Certificates and, when applicable to an entity, means the entity that operates such system.

1.3. "**Certificate**" means a digital document that at a minimum: (a) identifies the CA issuing it, (b) names or otherwise identifies a Subject, (c) contains a public key of a key pair, (d) identifies its operational period, and (e) contains a serial number and (f) is digitally signed by the CA. Certificates issued by a root CA to an issuing CA are "CA Certificates".

1.4. "**Customer Content**" means any data, text or other content that Customer or any User transfers to Entrust for processing, storage or hosting by the Hosted Services and any computational results that Customer or any User derives from the foregoing through its use of the Hosted Services, and includes Administration Information.

1.5. "**Device**" means an electronic endpoint in a network, system, or application, such as a computer, laptop, terminal, workstation, server, pager, telephone, smartphone, tablet, virtual workload, or other physical object enabled through embedded technology to execute functions and collect and exchange data.

1.6. "**Documentation**" has the meaning set out in the General Terms, and in this Schedule, includes the PKI Policy and Practices Documentation.

1.7. "**Hosted Services**" means, in this Schedule, the specific public key infrastructure elements (such as CAs) and related services and processes managed or operated by Entrust that Customer has purchased as specified in an Order, and may include a Management Account if provided by Entrust.

1.8. "**Management Account**" means one or more self-service consoles, portals, platforms, or other such administration and management tools that identify Customer by its organization name, track Customer's entitlements with respect to the Hosted Services and enable Customer, as applicable in accordance with its entitlements, to administer Hosted Services components and functions, including to appoint and grant permissions to Users and to request and manage Certificates.

1.9. "**Order**" has the meaning set out in the General Terms, and in this Schedule, if the Management Account provides the ability to order more or different inventory or features, or to renew a subscription for the Hosted Services, includes such an order placed through Customer's Management Account.

1.10. "**PKI Participant**" is a Person who has or plays a role identified in the applicable PKI Policy and Practices Documentation, and includes CAs, registration authorities, operational authorities, policy authorities,

Relying Parties, Subjects, and Subscribers.

1.11. "**PKI Policy and Practices Documentation**" means, collectively, the most recent versions of the policy/ies, requirements, and rules applicable to a Certificate issued by Entrust-operated public key infrastructure (PKI) and the practices statements and guidelines applicable to that PKI, PKI Participant, or components of the PKI operated as part of the Hosted Services, all as may be amended from time to time. The PKI Policy and Practices Documentation applicable to a specific Certificate, PKI, and/or PKI Participant depends on the type and nature of the Certificate and of the PKI, and the role of the PKI Participant.

1.12. "**Relying Party**" means a Person that relies on a Certificate and/or any digital signatures verified using that Certificate.

1.13. "**Subject**" means the Person or Device identified in the "Subject" field in a Certificate.

1.14. "**Subscriber**" means the Person who applies for or is issued a Certificate.

1.15. "**User**" has the meaning set out in the General Terms, and in this Schedule, includes Customer's Affiliates and any Administrator (as defined below), or a Subscriber or Subject of any Certificates issued or managed by the Hosted Services.

2. **Hosted Services Details**.

2.1. Professional Services. Entrust may provide set-up, onboarding and/or other Professional Services for some deployments of the Hosted Services, as specified in an Order, in which case the Professional Services will be provided in accordance with the applicable Order, the General Terms, and, if applicable, a Schedule describing the particular package of Professional Services purchased. Following deployment of the Hosted Services, any Customer request for changes to the Customer's deployment (i) may require Customer to complete a change request form or process; and (ii) shall be subject to mutual written agreement between the parties and may involve additional fees.

2.2. Hosted Service Provision. Following the completion of the set-up and onboarding of the Hosted Services, Entrust will provide and operate the Hosted Services in accordance with the Documentation and Customer's Order(s) for the Hosted Services. For clarity, with respect to the PKI Policy and Practices Documentation, Entrust's obligation is limited to the responsibilities applicable to its own role(s) as a PKI Participant as identified in the applicable PKI Policy and Practices Documentation; Entrust does not assume responsibility for the obligations of other PKI Participants.

2.3. Service Levels. If Entrust offers any service level commitments for the Hosted Services, they will be made available at https://www.entrust.com/legal-compliance/terms-conditions/entrust-pki.

2.4. Hosted Services Revisions. Entrust may modify Hosted Services features and functionality at any time. Additionally, Entrust may add, reduce, eliminate or revise service levels at any time where a third-party service level agreement applicable to the Hosted Services has been changed. Where any such change will cause a material detrimental impact on Customer, Entrust will take commercially reasonable efforts to provide Customer sixty (60) days prior written notice (email or posting notice on Entrust's website constitutes written notice). It will be Customer's responsibility to notify its Users of any such changes.

3. **Grant of Rights**. Customer receives no rights to the Hosted Services other than those specifically granted in this Section 3 (Grant of Rights).

3.1. General. Subject to Customer's (and Users') compliance with the Agreement, Entrust grants Customer, during the Offering Term, a personal, worldwide, non-exclusive, non-transferable, non-sub-licensable right to access and use the Hosted Services, and to grant its Users the ability to access and use the Hosted Services, in each case (a) in accordance with this Schedule; (b) in accordance with the Documentation; (c) in accordance with any specifications or limitations set out in the Order or imposed by technological means (such as a license code provided by Entrust) of the capabilities of the Hosted Services that Customer is permitted to use, such as limits associated with subscription levels, on numbers or types of Certificates, identities, Users, signatures or Devices, and on types of deployment (e.g. high availability, test or disaster recovery); and (d) subject to the restrictions set out in the General Terms (Section 6, Customer Responsibilities).

3.2. Evaluation/Trial. At Entrust's discretion, it may provide Customer with access to and right to use the Hosted

Services for trial or evaluation purposes, in which case, notwithstanding anything to the contrary in the Agreement, either this Subsection (Evaluation/Trial) or a separate evaluation agreement executed by the parties will apply. Subject to Customer's compliance with all restrictions, conditions and obligations in the General Terms, this Schedule, and an applicable Order (if any), for the period specified by Entrust at its discretion Customer may, solely as necessary for Customer's evaluation or trial of the Hosted Services, access and use the Hosted Services exclusively in and from a test (non-production) environment and using only fictitious non-production data. Entrust may extend the evaluation period in writing at its discretion. Evaluation purposes exclude any purpose from which Customer (or any of its Users) generates revenue. Sections 3.1 (General), 9 (Support), and 14.1 (Term) do not apply to any evaluation of the Hosted Services. Entrust may in its sole discretion suspend or terminate any and all evaluation access and other evaluation rights to the Hosted Services at any time, for any or no reason, without advance notice.

3.3. Not-for-Resale (NFR). At Entrust's discretion, it may provide Customer with access to and right to use the Hosted Services for not-for-resale purposes, in which case, notwithstanding anything to the contrary in the Agreement, either this Subsection (Not-for-Resale) or a separate not-for-resale license agreement executed by the parties will apply. NFR rights are granted to Customers that are Entrust authorized distributors, resellers, or indirect resellers (for the purposes of this Section, "Authorized Resellers"). Subject to Authorized Reseller's compliance with all restrictions, conditions and obligations in the General Terms, this Schedule, and an applicable Order (if any), for the period specified by Entrust at its discretion Authorized Reseller may access and use the Hosted Services for purposes of development, testing, support, integration, proofs of concept and demonstrations, in each case, in and from a test (non-production) environment and using only either fictitious non-production data, or data owned by Authorized Reseller or its own personnel (i.e. in no event may it use data of prospective clients or other third parties). Entrust may extend the NFR period in writing at its discretion. Sections 3.1 (General), 9 (Support), and 14.1 (Term) do not apply to any NFR use of the Hosted Services. Entrust may in its sole discretion suspend or terminate any and all NFR access and other NFR rights to the Hosted Services at any time, for any or no reason, without advance notice.

4. **Customer Roles and Responsibilities**.

4.1. Users. Customer exercises its rights and obligations with respect to the Hosted Services through individuals that the Customer appoints at its discretion ("Administrators"). The names and contact information of Administrator(s) initially appointed by Customer will be those provided to Entrust during enrollment. The initial Administrator(s) will have the ability to appoint and set permissions for additional Administrators. Customer agrees that Entrust is entitled to rely on instructions provided by the Administrators with respect to the Hosted Services as if such instructions were provided by the Customer itself.

4.2. PKI Participants. Where Customer or any of its Administrators or other Users is a PKI Participant, Customer is responsible for ensuring that it or such User fulfills the responsibilities and functions of such PKI Participant as set out in the applicable PKI Policy and Practices Documentation, including, if applicable, the verification and administration of Subscribers and Subjects, the provision of compliance artifacts, and the provision of the representations and warranties applicable to that PKI Participant. If a separate agreement with a PKI Participant is required under the applicable PKI Policy and Practices Documentation, then Customer will be responsible for meeting such requirements itself if it is a PKI Participant, and for ensuring that the Users it appoints as PKI Participants meet such requirements. Customer will exercise appropriate due diligence in appointing Users as Administrators and PKI Participants, and in the supervision of all its Users. Customer represents and warrants that it has or will obtain sufficient authority over, or authorization from, its Users to accept and comply with its commitments under this subsection.

4.3. No Representations. Customer will make no representations or warranties regarding the Hosted Services or any other matter, to Users, Relying Parties and/or any other third party, for or on behalf of Entrust, and Customer will not create or purport to create any obligations or liabilities on or for Entrust regarding the Hosted Services or any other matter. Entrust may direct any requests or other communications by Users or Relying Parties to Customer.

4.4. Customer-hosted Components. If Customer's Order for the Hosted Services includes on-premise Software components, or if Customer uses any third party products or services in connection with the Hosted Services (collectively, "Customer-hosted Products") Customer will be responsible for the lifecycle management

(patching, upgrades, etc.) of such Customer-hosted Products and the security of the environment where it installs and uses such Customer-hosted Products. Customer will implement commercially reasonable security measures with respect to the Customer-hosted Products and the environment where they are installed. Without limiting the foregoing, Customer will: (i) operate the Customer-hosted Products in an environment with appropriate physical, personnel, and electronic security measures; and (ii) for any Customer-hosted Products that are or include software, always use the current version of such software and promptly install any security patches and any upgrades/updates required for proper functioning of all features of the Hosted Services. Customer understands if it fails to comply with this Section it could create a security risk and/or otherwise negatively impact the operation of the Hosted Services and Entrust may have the right to suspend the Hosted Services in accordance with Section 15 (Suspension) to mitigate such risks or impacts. In addition, Customer may not be able to access new features or functions of the Hosted Services if it does not comply with this Section.

4.5. Network Requirements. Customer is responsible for procuring, maintaining, monitoring and supporting its communications infrastructure, network (LAN or WAN), and all components that connect to the Hosted Services, including facilities to terminate VPN tunnels as specified by Entrust, and any components identified as being on Customer's site or environment in the Documentation. Entrust assumes no responsibility for the reliability or performance of any connections as described in this paragraph for any such external infrastructure, nor for any service degradation or failures caused by network connectivity of such external infrastructure.

4.6. Certificates. Certificates issued by CAs operated by Entrust as part of the Hosted Services have the characteristics and features, and are subject to the rules, restrictions and processes, including regarding revocation, set out in the applicable PKI Policy and Practices Documentation. Customer is responsible for ensuring (i) that it can safely replace a Certificate should it need to be revoked; (ii) for Certificates issued to Devices, that the relevant Devices support and are interoperable with the Certificates; and (iii) for Certificates issued to Persons, that the relevant Persons understand, accept and comply with their responsibilities as Subscribers and/or Subjects.

4.7. Unauthorized Access. Customer will take reasonable steps to prevent unauthorized access to the Hosted Services, including by securing, protecting and maintaining the confidentiality of its access credentials and any access credentials issued to its Users. Customer is responsible for any access and use of the Hosted Services via Customer's Management Account and for all activity that occurs in Customer's Management Account. Customer will notify Entrust immediately of any known or suspected unauthorized use of the Hosted Services or breach of its security and will use best efforts to stop such breach or unauthorized use. The foregoing shall not reduce Customer's liability for all its Users.

5. **Customer Content**.

5.1. Customer Content and Administration Information. Entrust agrees to access, use and disclose the Customer Content only to the extent necessary to provide the Hosted Services, or as necessary to comply with law or a binding order of a government body. Notwithstanding the foregoing, Administration Information may be processed for the purposes of billing, providing Support and to investigate fraud, abuse or violations of this Agreement in the United States, Canada and other locations where Entrust maintains its support and investigation personnel.

5.2. Consents. Customer represents and warrants that Customer (and/or Users) will have obtained any requisite rights and consents, and made any requisite disclosures to relevant Users or other third parties, in accordance with all applicable laws, rules or regulations, to enable Customer and its Users to transfer the Customer Content to Entrust. Customer hereby grants Entrust and each PKI Participant (including any of its applicable Affiliates, subcontractors or hosting service providers) all rights and consents required for the collection, use, and disclosure of the Customer Content in accordance with the Agreement and the Documentation. Customer shall be responsible for the accuracy, quality and legality of Customer Content and the means by which Customer acquired them.

5.3. Non-Disclosure. For the purposes of this Schedule, the definition of "Confidential Information" in the General Terms excludes any Customer Content. Except as otherwise provided in this Section (Customer Content) or in the Agreement, Entrust shall not disclose to any third party any Customer Content that Entrust obtains in its provision of the Hosted Services. However, Entrust may make such information available (i) to courts, law enforcement agencies or other third parties (including release in response to civil discovery) upon

receipt of a court order or subpoena or upon the advice of Entrust's legal counsel, (ii) to law enforcement officials and others for the purpose of investigating suspected fraud, misrepresentation, unauthorized access, or potential illegal activity by Customer in the opinion of Entrust and (iii) to third parties as may be necessary for Entrust to fulfill its responsibilities under this Agreement.

6. **Software.** If Entrust provides any Software in connection with the Hosted Services, the Schedule provided with the Software will apply (and not this Schedule, with the exception of Section 4.4 (Customer-hosted Components)). If no more specific Schedule is provided with the Software, the Schedule for the Software is the end user license available at https://www.entrust.com/end-user-license.pdf.

7. **Open Source**. Versions of certain third-party open source software (including libraries and redistributable files) may be embedded in, delivered with or automatically downloaded as part of any Software ("Ancillary Software"). The Ancillary Software is subject to the applicable separate open source license agreement(s) pertaining to the Ancillary Software, which shall be provided with the Software or otherwise made available by Entrust. The complete list of Ancillary Software (not the Ancillary Software itself) shall be deemed Entrust Confidential Information.

8. **Interoperability.** Third parties may make available plugins, agents, or other tools that enable the Hosted Services to interoperate with third party products or services (each, an "Interoperation Tool"). Customer acknowledges and agrees that such Interoperation Tools are not part of the Hosted Services, and that Entrust grants no rights, warranties or support for any Interoperation Tools or for the interoperability of the Hosted Services with such Interoperation Tools. If Customer uses any Interoperation Tool, Customer has exclusive responsibility to ensure that it has any and all requisite rights to use the Interoperation Tool, including using it to transfer any data from or to the Hosted Services, and to use the product or service with which it connects. The use of an Interoperation Tool does not create any data subprocessor relationship between Entrust and any third party.

9. **Support.** Entrust provides the support commitments set out in the Support Schedule available at https://www.entrust.com/certificatesolutions-identity/support-schedule.pdf for the Hosted Services and any Software provided in connection with the Hosted Services. The "Silver Support Plan", as described in the Support Schedule, is included at no additional charge with a subscription to the Hosted Services. Other levels of Support may be available for purchase for an additional fee.

10. **Acknowledgement**. Customer understands that the Hosted Services are commercial off-the-shelf services and are not custom-built for Customer. Further, Customer understands that some or all of the Hosted Services are cloud-hosted, and there are inherent risks in storing, transferring and otherwise processing data in the cloud. The Hosted Services may offer different configuration options, encryption algorithms, and other security or compliance features. Customer is solely responsible for determining whether the Hosted Services offer appropriate safeguards, permissions, configurability, encryption, characteristics, and functions for Customer's intended use and any of its particular needs, and for selecting, configuring, and otherwise using the Hosted Services in a manner that it deems appropriate and sufficient to meet its requirements. Entrust will have no liability to Customer for the performance, security, or availability of the Hosted Services except as expressly provided in this Schedule, or for any damage, theft, unauthorized access, compromise, alteration, or loss occurring to Customer Content or any data stored in, transferred to or from, or otherwise processed by the Hosted Services, including in transit.

11. **DISCLAIMER OF WARRANTY**. For the purposes of this Schedule, the following is added to the disclaimer of warranties in the General Terms: **Except as expressly stated in this Schedule or in the Documentation, Entrust makes no representations or warranties that the Hosted Service or any digital artifact generated by the Hosted Service will be recognized or trusted by any particular third party or third party product or service, or will meet any particular legislative, regulatory, industry, or security standard or compliance requirement.**

12. **Indemnification**. In addition to the indemnification obligations in the General Terms, Customer shall defend, indemnify and hold harmless Entrust and its licensors against any damages, settlements, costs and expenses, including court costs and reasonable attorney's fees awarded against Entrust, arising out of or related to any third party claims, demands, suits, proceedings concerning any of the following (each, a "Claim"): (i) Customer's breach of, or errors in providing, the representations and warranties set out in Section 5 (Customer Content); (ii) a violation of applicable law by Customer, Users, or Customer Content; (iii) an allegation that the Customer Content infringes or misappropriates a third party's intellectual property rights; (iv) a dispute between Customer and any User or Relying Party; and (v) the use or reliance of a Relying Party on a Certificate issued through Customer's

Hosted Services.

13. **Fees.** Customer will pay the costs and fees for the Hosted Services as set out in the applicable Order, which are payable in accordance with the Order and the General Terms.

14. **Term & Termination**.

    14.1. Term. The Hosted Services are sold on a subscription basis for the Offering Term set out in the applicable Order.

    14.2. Termination. In addition to the termination rights in the General Terms, Entrust may terminate the Agreement for the Hosted Services for any reason by providing Customer advance notice of at least 1 year, unless Entrust discontinues the general commercial availability of the Hosted Services, in which case Entrust may terminate the Agreement upon 180 days' notice to Customer.

    14.3. Effects of Termination. Without limiting the generality of the effects of termination set out in the General Terms, upon termination of the Hosted Services, the CAs forming part of the Hosted Services will be inaccessible, any CAs dedicated to Customer may be decommissioned, Entrust will cease provide status reporting and may revoke CA Certificates, and Customer's rights to use or access the Hosted Services, including the ability to use the Hosted Services to revoke Certificates, will cease. If required by the PKI Policy and Practices Documentation, Entrust may revoke end entity Certificates issued by the Hosted Services upon termination of the Agreement. Customer understands that any use or reliance on unrevoked Certificates is entirely at Customer's own risk.

15. **Suspension**. In the event that Entrust suspects any breach of the Agreement by Customer and/or Users, Entrust may suspend Customer's, and/or such Users' access to and use of the Hosted Service without advance notice, in addition to such other remedies as Entrust may have pursuant to the Agreement. Nothing in the Agreement requires that Entrust take any action against any Customer, User or other third party for violating the Agreement, but Entrust is free to take any such action at its sole discretion.

16. **Third Party Products and Services**. Certain third-party hardware, software and services may be resold, distributed, provided or otherwise made available by Entrust through or in connection with the Hosted Services ("**Third Party Vendor Products**"). Entrust has no obligation and excludes all liability with respect to Third Party Vendor Products, the use of which shall be exclusively subject to the third party vendor's terms, conditions and policy documents accompanying, embedded in, or delivered with the Third Party Vendor Products, or otherwise made available by the third party vendor.

17. **Feedback**. The Hosted Services may provide the opportunity to provide Feedback. The provision and receipt of Feedback is not part of the Hosted Services, is provided on a voluntary basis, and is governed Section 23 (Feedback) of the General Terms. Feedback may be used by Entrust in its discretion. Any Personal Information received or collected in connection with Feedback will be treated in accordance with Entrust's data privacy policies available at https://www.entrust.com/legal-compliance/data-privacy.