Managed PKI
Terms of Use

The Agreement for Entrust's Managed PKI Offering is made up of these terms of use (the "mPKI Schedule"), the Entrust General Terms and Conditions ("General Terms") available at https://www.entrust.com/general-terms.pdf, and an Order for mPKI. 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. "Certificate" means a digital document that, at a minimum: (a) identifies the certification authority ("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".

1.2. "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 Service and any computational results that Customer or any User derives from the foregoing through its use of the Hosted Service.

1.3. "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.

1.4. "Hosted Service" means, in this mPKI Schedule, the specific mPKI and associated elements and services, that Customer has purchased as specified in the Order.

1.5. "mPKI" means a public key infrastructure consisting of software and processes hosted and managed by Entrust.

1.6. "Management Account" means a self-service administration tool hosted by Entrust that identifies Customer by its full legal name in the "Customer Name" field, tracks Customer's entitlements with respect to the Hosted Service and enables Customer, as applicable in accordance with its entitlements, to administer Hosted Service components and functions.

1.7. "PKI Policy and Practices Documentation" means, collectively, the most recent versions of the policy/ies setting out the requirements and rules applicable to a Certificate issued by an mPKI, the practices statements applicable to an mPKI or components thereof, and any guides issued by Entrust detailing the roles and responsibilities of different participants in an mPKI. The PKI Policy and Practices Documentation applicable to a specific Certificate and/or mPKI depends on the type and nature of the Certificate and of the mPKI.

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

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

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

1.11. "User" has the meaning set out in the General Terms, and in this mPKI Schedule, includes Customer's Affiliates and any Person who holds a role under applicable PKI Policy and Practices Documentation, an

mPKI Administrator (as defined below), or a Subscriber or Subject of any Certificates issued or managed by the Hosted Service.

2. **Hosted Service Details**.

2.1. Professional Services. Entrust may provide set-up, onboarding and/or other Professional Services for some deployments of the Hosted Service, 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 bundle of Professional Services purchased.

2.2. Hosted Service Provision. Following the completion of the set-up and onboarding of the Hosted Service, Entrust will provide and operate the Hosted Service in accordance with the Documentation, Customer's Order(s) for the Hosted Service, and in accordance with the applicable PKI Policy and Practices Documentation.

2.3. Compliance and Security Measures. Entrust will implement and maintain commercially reasonable physical and procedural security controls for the Hosted Service. Entrust will operate the Hosted Service in ISO 27001 compliant facilities according to the operational standards and procedures laid down in accordance with Entrust's corporate security policies and the applicable PKI Policy and Practices Documentation.

2.4. Service Levels. Entrust's service level commitments for the Hosted Service are available at https://www.entrust.com/mPKI-uptime-service-levels.pdf.

3. **Grant of Rights**. Customer receives no rights to the Hosted Service 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 Service, and to grant its Users the ability to access and use the Hosted Service, and to distribute Certificates issued by the Hosted Service in each case (a) in accordance with this mPKI Schedule, and, if and as applicable, the PKI Policy and Practices Documentation; (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 Service 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 general restrictions set out in Section 3 of the General Terms (Restrictions).

3.2. Evaluation. At Entrust's discretion, it may provide Customer with access to and right to use the Hosted Service for evaluation purposes, in which case, notwithstanding anything to the contrary in the Agreement, either this Section 3.2 (Evaluation) 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 mPKI 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 of the Hosted Service, access and use the Hosted Service exclusively in and from a test (non-production) environment (and which environment contains, for clarity, 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 2.1 (Professional Services), 2.2 (Hosted Service Provision), 3.1 (General), 6 (Support), 11.1 (Term) and 13 (Publicity) do not apply to any evaluation of the Hosted Service. Entrust may in its sole discretion suspend or terminate any and all evaluation access and other evaluation rights to the Hosted Service at any time, for any or no reason, without advance notice.

4. **Customer Roles and Responsibilities**.

4.1. mPKI Participants and Roles. Customer will have one or more roles in the Hosted Service, and will fulfill the responsibilities and functions of such roles as set out in the applicable PKI Policy and Practices Documentation. In addition, Customer will appoint trusted Users into additional roles ("mPKI Administrators"), and will be responsible for ensuring that such mPKI Administrators fulfill the responsibilities

and functions of their roles as set out in the applicable PKI Policy and Practices Documentation, including in the verification of Certificate applications and the administration of Subscribers. Customer agrees that Entrust is entitled to rely on instructions provided by the mPKI Administrators with respect to the Hosted Service as if such instructions were provided by the Customer itself.

4.2. Users and Other Third Parties. Customer will make no representations or warranties regarding the Hosted Service 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 Service or any other matter. Entrust may direct any requests or other communications by Relying Parties or Users to Customer.

4.3. On-premise Components. If Customer's Order for the Hosted Service includes on-premise Software components, or if Customer uses any third party products or services in connection with the Hosted Service (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 at a minimum such security measures with respect to the Customer-hosted Products and the environment where it is installed as set out in the applicable PKI Policy and Practices Documentation. Without limiting the foregoing, Customer will: (i) operate the Customer-hosted Products in an environment with appropriate physical, personnel, and electronic security measures, including maintaining the communication workstation(s) in a physically-secure room with access restricted to a limited number of named persons; (ii) ensure that persons employed by or contracted to work with the Customer-hosted Products on behalf of Customer have appropriate skills, knowledge, and backgrounds (including any security clearance requirements imposed by law or Government policy) to operate in a trusted and secure environment; and (iii)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 Service. Customer understands if it fails to comply with this Section it would create a security risk and/or otherwise negatively impact the operation of the Hosted Service and Entrust will have the right to suspend the Hosted Service in accordance with Section 12 (Suspension). In addition, Customer may not be able to access new features or functions of the Hosted Service if it does not comply with this Section.

4.4. 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 Service(s), including facilities to terminate VPN tunnels as specified by Entrust. 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.

4.5. Devices. For Certificates issued to Devices, Customer is responsible for ensuring that the relevant Devices support and are interoperable with the Certificates.

4.6. Unauthorized Access. Customer will take reasonable steps to prevent unauthorized access to the Hosted Service, including, without limitation, 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 Service 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 Service 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.

4.7. Data Safeguards. Customer is responsible for determining whether the Hosted Service offers appropriate safeguards for Customer's intended use of the Hosted Service, including any safeguards required by applicable laws, prior to transmitting or processing, or prior to permitting Users to transmit or process, any data or communications via the Hosted Service.

5. **Software.** If Entrust provides any Software in connection with the Hosted Service, the Schedule provided with the Software will apply (and not this mPKI Schedule, with the exception of Section 4.3 (On-premise 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.

6. **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 Service and any Software provided in connection with the Hosted Service. The "Silver Support Plan", as described in the Support Schedule, is included at no additional charge with a subscription to a Hosted Service. Other levels of Support may be available for purchase for an additional fee.

7. **Interoperability.** Entrust or third parties may make available plugins, agents, or other tools that enable the Hosted Service 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 Service, are licensed separately, and that Entrust grants no rights, warranties or support for any Interoperation Tools or for the interoperability of the Hosted Service with such Interoperation Tools under this mPKI Schedule. 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 Service, 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.

8. **Hardware.** If the Order specifies any Hardware and Supplies to be delivered to Customer by Entrust or one of its suppliers in connection with the Hosted Service, the Hardware and Supplies Schedule available at https://www.entrust.com/hardware-supplies-schedule.pdf will apply, unless the Hardware and Supplies are Third Party Vendor Products, in which case Section 15.1 of the General Terms (Third Party Vendor Products) will apply.

9. **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, or proceedings concerning the use or reliance of a Relying Party on a Certificate issued for Customer.

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

11. **Term & Termination**.

    11.1. Term. The Hosted Service is sold on a subscription basis for the Offering Term set out in the applicable Order. All subscriptions are non-cancellable and non-refundable.

    11.2. Termination. In addition to the termination rights in the General Terms, Entrust may terminate the Agreement for the Hosted Service if Customer commits a material breach of this mPKI Schedule and fails to remedy such material breach within 30 days (or such longer period as Entrust may approve in writing) after delivery of the breach notice.

    11.3. Effects of Termination. Without limiting the generality of the effects of termination set out in the General Terms, upon termination of the Hosted Service, the CAs forming part of the Hosted Service will be inaccessible, Entrust will cease providing status reporting and may revoke the CA Certificates, and Customer's rights to use or access the Hosted Service, including the ability to use the Hosted Service to revoke Certificates, will cease. Customer understands that any use or reliance on unrevoked Certificates is entirely at Customer's own risk.

12. **Suspension**. In the event that Entrust suspects any breach of the Agreement or the PKI Policy and Practices Documentation by Customer and/or Users, Entrust may suspend Customer's, and/or such Users' access to and use of the Hosted Service without advanced notice, in addition to such other remedies as Entrust may have pursuant to the Agreement.

13. **Publicity**. Customer agrees to participate in Entrust's press announcements, case studies, trade shows, or other marketing reasonably requested by Entrust. During the Term and for thirty (30) days thereafter, Customer

grants Entrust the right, free of charge, to use Customer's name and/or logo, worldwide, to identify Customer as such on Entrust's website or other marketing or advertising materials.