Managed Microsoft PKI
Schedule

The Agreement for Entrust's Managed Microsoft PKI Offering is made up of this Schedule ("Managed MS Schedule"), the Entrust General Terms and Conditions at https://www.entrust.com/general-terms.pdf ("General Terms"), and an Order for Managed Microsoft PKI.

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.**

   Capitalized terms not defined in this Schedule have the meanings given to them in the General Terms.

   1.1. "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 its operational period, and (e) contains a serial number and (f) is digitally signed by the CA.

   1.2. "Certification Authority" or "CA" means the signing authority consisting of people, processes, systems, and devices which creates, issues, manages and revokes Certificates. The CA will certify the public keys and associated data including subscriber or end entity information, creating a trust relationship between the CA and those subscribers.

   1.3. "Root CA" means the CA that acts as the trust anchor at the top of a particular public key infrastructure (PKI) certification hierarchy. Standard PKI practice is that the Root CA be kept offline while not in use, to protect against compromise and assure the trust of the entire PKI hierarchy which is bound to the Root CA.

2. **Hosted Service Details.** Subject to the Agreement, Entrust will provide the following as part of the Managed Microsoft PKI Offering:

   2.1. One of Entrust's technical experts to serve as the overall primary contact for Customer in order to ensure a successful Managed Microsoft PKI experience.

   2.2. PKI design and build as detailed in Section 4 (Included Onboarding/Setup Services) below, including implementation and configuration of Microsoft Certificate Services in its Enterprise configuration and integration with Customer-provided, existing Microsoft Active Directory identity source.

   2.3. Preparation of Certificate policy documentation applicable to Customer's PKI as detailed in Section 4 (Included Onboarding/Setup Services) below.

   2.4. One Root CA with the following characteristics:

      2.4.1. standalone and offline (no external interfaces).

      2.4.2. FIPS 140-2 level 3 hardware security module (HSM) protection for Root CA keys configured to meet service level requirements (see Subsection 2.8 (Service Levels) below).

   2.5. HSM credentials will be issued during the key ceremony and provided to the designated Entrust and Customer custodians such that controlling quorum of credentials remains in Customer's possession. Physical credentials (e.g. tokens, smartcards) are provided subject to the Hardware and Supplies Schedule to the General Terms.

   2.6. FIPS 140-2 level 3 HSM protection for subordinate CA (Microsoft CA) Certificates, hosted and run by

Entrust from its secure facilities and separated from the Root CA HSM.

2.7. Professional operational management of all PKI components, including Customer's instance of Microsoft Certificate Services provided in a dedicated Customer Azure tenant, under the applicable Certificate policies and procedures.

2.8. Service Levels. Entrust's service level commitments for the Managed Microsoft PKI Offering are available at https://www.entrust.com/mPKI-uptime-service-levels.pdf.

3. **Third Party Vendor Products.** Customer is responsible for procuring its own instance of the Microsoft Certificate Services provided in a dedicated Customer Azure tenant and all applicable licenses. Customer is responsible for assigning to Entrust or otherwise ensuring that Entrust has the required permissions and rights under such licenses to perform the tasks described in this Schedule.

4. **Included Onboarding/Setup Services.** Subject to the Agreement, Entrust will provide the following Professional Services as part of the Managed Microsoft PKI Offering:

4.1. Discovery & Design Review

4.1.1. Collaborative discovery process with Entrust technical staff and Customer's technical point of contact and other representatives as appropriate to determine and document Customer's business and technical requirements.

4.1.2. Review solution design and determine required configuration to meet Customer requirements based on Entrust's standard two-tier PKI hierarchy design composed of:

- One Root CA with (HSM-protected key store)
- One subordinate CA (HSM-protected key store) signed by the Root CA
- Microsoft Active Directory Certificate Services implementation in Customer's AD Forest in coordination with Customer's technical point of contact

4.2. Production Build. Installation and configuration of Microsoft PKI components as detailed during the design review and based on the Entrust standard Microsoft CA service design.

4.3. Customization of Entrust Certificate policy (CP) and Certificate practice statement (CPS) documentation in line with RFC 3647. The CP details what Certificates can be used, by whom, and how, as well as minimum standards for the usage and protection of Certificates. The CPS details the operations practices around the administration and management of the CA(s). Customer will have the role of the "Policy Authority" for the CP and CPS and be considered the owner of those documents, but all changes to the Entrust CP/CPS standard documentation must be approved by both the Customer and Entrust representatives.

4.4. Formal key ceremonies as detailed below, including documented processes and procedures to perform signing operations for Certificates and revocation lists. The key ceremonies are designed to ensure that the chain of custody for CA keys is maintained and documented.

4.4.1. Root CA implementation key ceremony, including:

- creation of Root CA keys;
- creation of subordinate CA (MSCA) keys; and
- creation of Root CA Authority Revocation List (ARL)/Certificate Revocation List (CRL). The Offering includes one annual (1 time per year) support for the creation and signing of an ARL/CRL.

4.4.2. Subordinate CA implementation key ceremony, including:

- creation of subordinate CA (MSCA) keys.
- creation of subordinate CA Authority Revocation List (ARL)/Certificate Revocation List (CRL). Offering includes one annual (1 time per year) support for the creation and signing of an ARL/CRL.

4.4.3. During the key creation process, Customer's HSM credentials will be issued and assigned to Entrust and Customer representatives as determined by their assigned roles as specified in the CP and CPS. Each party is responsible for the secure storage and handling of the HSM credentials

assigned to its representatives.

4.4.4. As the party who controls the quorum of HSM credentials, Customer is required to be physically present during the key ceremonies with the quorum of HSM credentials.

4.4.5. The key ceremonies will be undertaken under the accreditation and compliance requirements as set out in the applicable CP.

No travel by Entrust or per diems are required or included for the above Professional Services.

Any other Professional Services beyond the scope of this Section (Included Onboarding/Setup Services) may be provided pursuant to a separate statement of work agreed by the parties.

5. **Assumptions and Limitations.** The Managed Microsoft PKI Offering is subject to the following assumptions and limitations:

   5.1. Customer's PKI is not subject to any specific regulatory or industry compliance requirements (e.g. public trust/WebTrust audit criteria).

   5.2. Microsoft CA will be hosted in Azure; the Root CA and HSMs are hosted in Entrust's secure data center facilities.

   5.3. Microsoft CA interface is limited to NDES and MS native enrollment interface.

   5.4. Networking-based assumptions and limitations:

   5.4.1. Customer will have facilities to terminate VPN tunnels as specified by Entrust.

   5.4.2. Customer will perform support, troubleshooting or monitoring of its communications infrastructure and components, network (LAN or WAN) for the purposes of problem resolution.

   5.4.3. Network accessibility from Customer sites to external networks or the Internet is outside the scope of the Managed Microsoft PKI Offering.

   5.5. Any development or customization of software to meet Customer requirements is outside the scope of the Managed Microsoft PKI Offering.

6. **Customer Roles and Responsibilities**. Customer will be responsible for the following:

   6.1. Identifying a primary technical point of contact within Customers' organization with respect to the Offering.

   6.2. Procuring all required Microsoft products and services, including payment of the applicable Azure subscription fee.

   6.3. Providing assistance in identifying representatives from Customer's various internal and external stakeholders who have an interest or are affected by the Offering.

   6.4. Facilitating scheduling of stakeholder representatives to participate in the exchange of information with Entrust.

   6.5. Responding in a timely fashion to questions posed by Entrust regarding the Offering.

   6.6. Attendance at all key ceremonies, with quorum of credentials.

   6.7. Ensuring that Customer's credentials are stored in a secure location and protected from environmental threats.

   6.8. Reporting actual and/or suspected loss or damage of credentials or any other factor that may threaten PKI security.

   6.9. Comply with the requirements applicable to Customer's roles (including Policy Authority) under the CP.

7. **Policy and Compliance.** Entrust will operate the Managed Microsoft PKI Offering 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 CPS.

8. **Term.** The Managed Microsoft PKI Offering is offered on a subscription basis for the Offering Term set out on the Order.
9. **Warranty.** Entrust warrants that the Professional Services it provides in connection with the Managed Microsoft PKI Offering shall be performed in a professional manner in keeping with reasonable industry practice.
10. **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. Support for the Managed Microsoft PKI Offering includes troubleshooting and facilitation of repair or replacement in case of CA and HSM hardware or software failure but excludes any obligation to resolve issues identified with third party products that rely on action by the applicable third party vendor (e.g. Microsoft).
11. **Fees.** Customer will pay the costs and fees for the Managed Microsoft PKI Offering as set out in the applicable Order, which are payable in accordance with the Order and the General Terms.

Template version: December 14 2022