Entrust Managed Root CA
Schedule

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

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 SERVICE. THE CONTINUED RIGHT TO ACCESS AND USE THE HOSTED SERVICE 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 issued by the certification authority ("CA") 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, (e) contains a serial number and (f) is digitally signed by the CA.

   1.2. "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. **Service Details.** Subject to the Agreement, Entrust will provide the following as part of the Managed Root CA 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 Root CA experience.

   2.2. High level design document and build as detailed in Section 3 (Included Onboarding/Setup Services) below, including implementation and configuration for one high assurance Root CA for Customer's PKI.

   2.3. Customer's Root CA will have the following characteristics:

      2.3.1. standalone and offline (no external interfaces).

      2.3.2. hosted in Entrust's ISO 27001 compliant data centers on a FIPS 140-2 level 3 hardware security module (HSM).

      2.3.3. 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.

3. **Included Onboarding/Setup Services.** Subject to the Agreement, Entrust will provide the following Professional Services as part of the Managed Root CA Offering:

   3.1. Discovery & Design Review

      3.1.1. 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.

3.1.2. Review solution design and determine required configuration of the Root CA (with HSM-protected key store) to meet Customer's requirements.

3.2. Production Build

3.2.1. Installation and configuration of Root CA as detailed during the design review.

3.3. 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 the Root CA key is maintained and documented.

3.3.1. Root CA implementation key ceremony, including:

- creation of Root CA keys;
- signing of one subordinate CA(s) if required;
- creation of Root CA revocation list. The Offering includes one annual (1 time per year) support for the creation and signing of a revocation list.

3.3.2. During the key creation ceremony, Customer's HSM physical credentials will be issued and assigned to Entrust and Customer representatives as determined by their assigned roles as specified in the solution design. Each party is responsible for the secure storage and handling of the HSM credentials assigned to its representatives.

3.3.3. As the party who controls the quorum of HSM credentials, Customer is required to be present, either physically or virtually, during the key ceremonies to make up the quorum of HSM credentials. If Customer attends virtually, the physical credentials containing Customer keys will be securely transferred between the parties in a manner mutually agreed by the parties.

3.3.4. The key ceremonies will be undertaken in accordance with standard industry practices and Entrust's standard key ceremony policy.

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.

4. **Assumptions and Limitations.** The Managed Root CA Offering is subject to the following assumptions and limitations:

4.1. The Customer's Root CA is not initialized on hardware dedicated to the customer. All Root CAs managed by Entrust (i.e. for different customers) use the same shared hardware and HSM infrastructure. Root CA and CA keys are provided on dedicated virtual images which are initialized onto the shared hardware under audit, these are removed to back up after use and the HSM zeroized.

4.2. The Root CA is not subject to any specific regulatory or industry compliance requirements (e.g. public trust/WebTrust audit criteria).

4.3. Root CAs hosted anywhere other than in Entrust data centers are outside the scope of the Managed Root CA Offering.

4.4. Since access to the Root CA is limited to the physically secured CA, logical security will be implemented only at the system and application layers and not at a network layer.

4.5. All access to the operating system will be controlled through administrative accounts with access to these accounts limited to assigned individuals (role holders).

4.6. Any variations in policy and procedures to address customized requirements for Customer are outside the scope of the Managed Root CA Offering.

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

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

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

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

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

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

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

5.7. Ensuring that Customer's credentials are used in accordance with the detailed design.

5.8. Reporting actual and/or suspected loss or damage of credentials or any other factor that may threaten the HSM or Root CA security.

6. **Policy and Compliance.** Entrust will operate the Managed Root CA Offering in ISO 27001 compliant facilities according to the operational standards and procedures laid down in accordance with Entrust's corporate security policies and standard operational practices for PKI administration and management.

7. **Term.** The Managed Root CA Offering is offered on a subscription basis for the Offering Term set out on the Order.

8. **Warranty.** Entrust warrants that the Professional Services it provides in connection with the Managed Root CA Offering shall be performed in a professional manner in keeping with reasonable industry practice.

9. **Support.** Entrust provides the support commitments for the Managed Root CA Offering set out at https://www.entrust.com/certificatesolutions-identity/support-schedule.pdf.

10. **Fees.** Customer will pay the costs and fees for the Managed Root CA 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