Managed PKI Services
Managed Root CA Schedule

Service Overview

Entrust’s Managed Root CA Offering provides a hosted, high assurance, offline Root CA to serve as the root of trust for Customer’s public key infrastructure (PKI). The hosting infrastructure and CA are built to meet standards for high assurance to ensure Customer’s PKI can be trusted and can act as the root of trust for other high assurance CAs or for lower assurance CAs. Experienced, knowledgeable staff maintain and operate the Offering from established, secure and ISO 27001 certified facilities, which facilitates demonstration of compliance with industry standards and of chain of custody for Customer’s Root CA.

The Agreement for Entrust’s Managed Root CA Offering is made up of this Schedule, the Entrust Products and Services General Terms and Conditions (“General Terms”), and an Order for the Managed Root CA Offering.

1. Definitions

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

“Certificate”: The signed public key and associated electronic data of an entity (user, service, device) which is cryptographically derived and bound to a private key. The certificate is signed by the private key of the Certificate Authority that issued it and bound to the Certificate policy under which the CA is operated. The certificate format is in accordance with ITU-T recommendation X.509.

“Certification Authority” or “CA”: 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.

“Root CA”: 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:

a. 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.

b. 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.

c. Provision of Entrust’s standard Root CA 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 Root CA. Modification of the CP and CPS documentation is out of scope of the Managed Root CA Offering.

d. Customer’s Root CA will have the following characteristics:

   i. standalone and offline (no external interfaces).

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

   iii. the HSM for the Root CA will include any PIN Entry Device (PED) or card reader required by the HSM.

   iv. 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 provision of the General Terms.

3. Included Onboarding/Setup Services

Subject to the Agreement, Entrust will provide the following Professional Services as part of the Managed Root CA Offering:

a. Discovery & Design Review

   i. 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.

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

b. Production Build

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

c. 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.

   i. Root CA implementation key ceremony, including:

      - creation of Root CA keys;
      - signing of one subordinate CA(s) if required;
      - 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.

   ii. 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.

   iii. 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.

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

4. Assumptions and Limitations

The Managed Root CA Offering is subject to the following assumptions and limitations:

a. The Customer's Root CA does not reside on dedicated hardware. All Root CAs managed by Entrust (i.e. for different customers) use the same hardware and HSM but are isolated from each other due to having their own operating model and credentials.

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

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

d. 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.

e. All access to the operating system will be controlled through administrative accounts with access to these accounts limited to assigned individuals (role holders), as per the CP.

f. Any variations in policy and procedures (including any changes to Entrust's standard Root CA CP and CPS) 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:

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

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

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

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

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

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

g. Ensuring that Customer's credentials are used in accordance with the CP.

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

i. Comply with the requirements applicable to Customer's roles under the CP.

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 the CPS.

7. Term

The Managed Root CA Offering is offered on a 3-year subscription term ("Term"). The Term can be extended by renewal as set out in the General Terms. All subscriptions are non-cancellable and non-refundable.

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 here. Notwithstanding the foregoing, where support is purchased through an authorized reseller and the Order indicates that the reseller will provide support, then such support will be provided by the authorized reseller (and not Entrust).

10. Price

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.