Entrust Managed PKI
Managed Microsoft PKI Schedule

Service Overview

Entrust's Managed Microsoft PKI Offering provides management by public key infrastructure (PKI) experts of Customer's Microsoft CA(s) in Azure, with a hosted high assurance offline Root CA to serve as the root of trust for Customer's PKI, built to exacting standards and operated by Entrust experts in a specialized root hosting environment. Experienced, knowledgeable staff advise on digital certificates, and manage the rules, policies and procedures required for an effective PKI.

The Agreement for Entrust's Managed Microsoft PKI Offering is made up of this Schedule, the Entrust Products and Services General Terms and Conditions ("General Terms"), and an Order for Managed Microsoft PKI .

1. Definitions

"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 Microsoft PKI Offering:

a. 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.

b. 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.

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

d. One Root CA with the following characteristics:

   i. standalone and offline (no external interfaces).

   ii. FIPS 140-2 level 3 hardware security module (HSM) protection for Root CA keys configured to meet service level requirements (see Section 10 (Service Levels and Support) below).

   iii. 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.

e. 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.

f. 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.

3. Third Party 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, all of which are Third Party Products as defined in the General Terms. Customer is responsible for assigning to Entrust or otherwise ensuring that Entrust has the required permissions and rights under such Third Party Products 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:

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 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

b. Production Build

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

c. 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.

d. 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;
      - 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.

   ii. 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.

   iii. 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.

iv. 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.

v. 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:

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

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

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

d. Networking-based assumptions and limitations:

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

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

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

e. 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:

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

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

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

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

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

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

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

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

i. 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 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.

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. Service Levels and Support

Entrust provides the service level and support commitments for the Managed Microsoft PKI 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).

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.

11. Price

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.