Entrust Managed PKI EMEA Schedule

Service Overview

Entrust is in the business of building, operating and supplying PKIs and related products and services to enable end-to-end provision of a PKI trust service.

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

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.

"Certificate Policy": The named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements.

"EMEA": The territory coverage for Entrust Managed PKI EMEA, more specifically including Europe, Middle East and Africa.

"Entrust Managed PKI EMEA Offering": means the hosting, operation, maintenance and support of Customer's PKI and provision of related customer services within EMEA.

"Relying Party": means the person that relies on the identity (of a Subscriber) to undertake specified business actions such as accepting and processing a payment request.

"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, to protect against compromise and assure the trust of the entire PKI hierarchy which is bound to the Root CA.

"Registration Authority" or "RA": means the entity that manages the registration and certificate lifecycle processes for subscribers.

"Setup Services": means Services covered in Section 3 below.

"Validation Authority": means a function of a CA, whereby the status of a Certificate is determined and made available to a parties that rely on that Certificate.

2. Entrust Managed PKI EMEA Offering Details

Subject to the Agreement, Entrust will provide the following as part of the Entrust Managed PKI EMEA Offering:

a. PKI design and build, as detailed in Section 3 below, including implementation and configuration of the PKI Managed Service.

b. Preparation of Certificate Policy documentation applicable to Customer's PKI as detailed in Section 3 below.

c. Professional operational management of all PKI components, under the applicable Certificate Policies and procedures, including :
   i. Critical component and performance monitoring;
   ii. CA & HSM log analysis;
   iii. Routine maintenance and PKI operations; and
   iv. Compliance supporting procedures.

3. Included Onboarding/Setup Services

Subject to the Agreement, Entrust will provide the following Professional Services as part of the Onboarding/ Setup Services for the Entrust Managed PKI EMEA 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 or Issuing CA (HSM-protected key store) signed by the Root CA; and
   - Registration Authority and Validation Authority software components.

b. Production Build

   i. Installation and configuration of the PKI components as detailed during the design and based on the Entrust standard Managed PKI Service design.

c. Certificate policy (CP) documentation for the Customer 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. Customer will have the role of the "Policy Authority" for the CP and be considered the owner of those documents, all changes to the Customer CP must be approved by both the Customer and Entrust representative.

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; and
   - creation of Root CA Authority Revocation List (ARL)/Certificate Revocation List (CRL). The standard 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 keys; and
   - 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 credentials will be issued and assigned to Entrust and Customer representatives as determined by their assigned roles as specified in the CP (each, a "Custodian").Each Custodian is responsible for the secure storage and handling of its assigned credentials.

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

   v. The key ceremony 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 may be provided pursuant to a separate statement of work agreed by the Parties.

4. Assumptions and Limitations

The Managed PKI Service 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. CA/RA components, the Root CA and HSMs are hosted in Entrust's secure data center facilities.

c. 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.

d. Any development or customization of software to meet Customer requirements is outside the scope of Managed PKI Service.

e. Professional Services shall be deemed accepted by the Customer at the expiry of the 10 (ten) business days from the completion of Professional Services by Entrust.

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. Reporting loss or damage of credentials or any other factor that may threaten PKI security.

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

i. Connectivity Requirements: Customer, in connecting external systems to Entrust information systems via VPN, shall comply with the following connectivity requirements:

   i) all network connections are monitored and activity is logged for the purpose of security, compliance, and crime prevention and detection;

   ii) all hosts on the connected system are protected with anti-malware software that is update not less than weekly;
   iii) all hosts are fully patched with the latest security updates applied;
   iv) all hosts are securely configured with unnecessary ports and protocols disabled;
   v) all users and system activity can be uniquely identified from system logs;
   vi) all users are authorized by the system owner with the principle of least privilege required to operate;
   vii) all users are suitably vetted, trained and qualified on the system;
   viii) connected infrastructure is supported by a single time source of which all hosts and devices are synchronized with;
   ix) Customer shall comply, as applicable, to ISMS security requirements;
   x) VPN connections as agreed with Entrust shall not be changed without further written agreement and;
   xi) all security incidents associated with the connected system are to be reported to Entrust at the earliest opportunity.
   xii) Customer shall not to make use of the Entrust VPN connection for any purpose other than the agreed purpose as defined in this Service Schedule;
   xiii) Customer shall not conduct security testing, penetration testing or vulnerability scans on Entrust information systems.

6. Policy and Compliance

Entrust will operate the Managed PKI Service 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 CP.

7. Warranty

Entrust warrants that the services it provides in connection with the Managed PKI Service shall be performed in a professional manner in keeping with reasonable industry practice.

8. Service Levels and Support

Entrust provides the service level and support commitments for the Managed PKI Service set out in the Entrust Managed PKI EMEA Offerings Service Levels and Support. Notwithstanding the foregoing, where the Offering 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 PKI Service 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.

9. Price

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

Exhibit 1:

1. Software Subscription

A. If and to the extent that Entrust provisions any Software for use with the Managed PKI Service, this Exhibit 1 shall apply.

B. For the purposes of this Exhibit 1, "Software" means, any software provided by Entrust Datcard to Customer in machine readable format and any upgrades or other modification thereto supplied by Entrust, except software covered by subsection 1.F below.

C. Software License. Subject to the Agreement, Entrust hereby grants to Customer a non-exclusive, non-transferable, non-sublicensable license to use such Software strictly for internal business use for the Term to receive the Certificate services, subject to any quantity limitations stipulated in the Order. If no quantity limitations are stipulated in the Order, then the quantity will be deemed to be one (1). Any such distribution shall be pursuant to the terms of the click-through license agreement accompanying the products for the sole purpose of conducting business with the Customer.

D. License Conditions. Customer may make additional copies of the Software (to the extent that any such Software has been delivered), but only for archival or back-up purposes. Each permitted copy of the Software must include all copyright notices, restricted rights legends, proprietary markings and the like exactly as they appear on the copy delivered by Entrust. Customer may not rent, lease, sell, sublicense, assign, distribute or otherwise transfer the Software, except as provided in the Agreement. The Software, including any related copyright, trade-mark, trade secret, and patent rights are owned by Entrust or its third-party licensors and will remain the sole and exclusive property of Entrust and its third-party licensors. Customer will not copy, modify, adapt or merge copies of the Software except as provided in the Agreement. Customer will not decompile, disassemble, disclose, reverse engineer, or in any other manner attempt to determine any source code of or trade secret related to any Software provided by Entrust except to the extent expressly permitted by applicable law, notwithstanding a contractual obligation to the contrary. Any third party software or hardware supplied in connection with the Software may only be used with the Software. All licenses to the Software terminate upon expiry or termination of the related Managed PKI Service. You will destroy all copies of such Software.

E. Free Software. "Free Software" means any software that is distributed together with the Software as freeware, shareware, open source software or under or pursuant to similar licensing or distribution models. Free Software which is licensed and distributed pursuant to the associated license that accompanies it may be distributed with Hardware and/or Software. If any Free Software licenses require that Entrust provide rights to use, copy or modify Free Software that are broader than the rights granted in this Exhibit 1, then such rights will take precedence over any rights and restrictions in this Schedule.

F. If a third-party hardware or software product is sold or licensed by Entrust as a standalone product, then such hardware or software will be sold or licensed pursuant to the applicable manufacturer's shrink wrap agreement.