# Entrust Managed PKI
# Cryptography as a Service Schedule

## Service Overview

Entrust's Cryptography-as-a-Service ("CaaS") Offering provides a secure, hosted solution for storing, managing, and using cryptographic keys via multi-tenant hardware security modules (HSMs). Experienced, knowledgeable staff maintain and operate the HSM from established, secure and ISO 27001 certified facilities, which facilitates demonstration of compliance with industry standards and chain of custody of critical key materials. The Entrust hosted model is designed to be straightforward and simplifies the implementation of cryptographic services by isolating Customer involvement with HSM management to client software and credentials. All other elements of the Offering will be controlled and managed by Entrust for the Customer.

The Agreement for Entrust's CaaS is made up of this Schedule, the Entrust Products and Services General Terms and Conditions ("General Terms"), and an Order for CaaS. Capitalized terms not defined in this Schedule have the meanings given to them in the General Terms.

## 1. Service Details

Subject to the Agreement, Entrust will provide the following as part of the CaaS Offering:

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

b. Access to and use of one (1) dedicated cryptographic partition on an HSM cluster, hosted on a FIPS 140-2 level 3 HSM, including a dedicated/single tenant secure client.

   i. Dedicated, Customer-specific credentials per cryptographic partition.

   ii. Secure creation and storage of cryptographic keys.

   iii. Dedicated cryptographic processing power for the encryption and decryption of such cryptographic keys.

   iv. HSM cluster will include any PIN Entry Device (PED) or card reader required by the HSM.

c. Implementation and configuration of the HSM partition.

d. Professional operational management of the HSM under high assurance security policies and procedures (see "Policies and Compliance" below) including:

   i. Dual Control for HSM administration

   ii. Role separation with assigned roles for HSM administrators and Customer cryptographic uses.

e. Secure handling and storage of all HSM components and administration keys according to Entrust and CaaS policies and procedures.

## 2. Third Party Client Software

All network HSMs require 3rd party client software written by the HSM manufacturer to securely communicate with the HSM. Gemalto's SafeNet Luna Network HSMs use client based software ("Client Software"), which is configured to securely authenticate and communicate with the HSM using unique asymmetric keys defined in the HSM and client. This Client Software, distributed to Customers by Entrust as part of the CaaS Offering, is a Third Party Product licensed by Gemalto, and Customer's use will be subject to the end user license agreement or other terms included in the Client Software or otherwise made available by Gemalto. All installation, maintenance, and operation of the Client Software is the sole responsibility of the Customer. Entrust will provide assistance with installation, troubleshooting or connection issues, but Customer is ultimately responsible for the HSM Client Software and its installation on the client system(s).

## 3. Assumptions and Limitations

The CaaS Offering is subject to the following assumptions and limitations:

a. Currently the CaaS Offering will implement and operate only using the SafeNet Luna Network HSMs owned and managed by Entrust in an authorized Entrust data center facility.

b. Networking-based assumptions and limitations:

   i. Customer will provide its own means of network connectivity via dedicated network connection or Internet Service Provider for access to the Entrust data center and service environment. For clarity, Entrust will provide the termination to its environment.

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

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

   iv. Network accessibility from Customer sites to external networks or the Internet is outside the scope of CaaS.

c. Support and maintenance of the Client Software is outside the scope of the CaaS Offering.

d. Any custom software required for this engagement is outside the scope of the CaaS Offering.

e. Any variations in policy and procedures to address customized requirements for Customer are outside the scope of the CaaS Offering.

## 4. 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.

## 5. Policy and Compliance

Entrust will operate the CaaS Offering in ISO 27001 compliant facilities according to the operational standards and procedures laid down in Entrust's HSM Management Policy, and in accordance with Entrust's corporate security policies.

Under the HSM Management policy, Entrust administrators may act as a partition owner on behalf of the Customer for the purpose of activating or deactivating a Customer cryptographic partition or in troubleshooting an HSM or a partition. Under dual control and role separation requirements, any partition data will require that at least two (2) Entrust personnel be present for any direct operation with the HSM or a partition. It should be noted that even if a key can be seen in a partition, it cannot be exported from the HSM.

## 6. Term

The CaaS Offering is provided 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.

## 7. Warranty

Entrust warrants that any Professional Services it provides in connection with the CaaS Offering 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 CaaS 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 CaaS Offering includes troubleshooting and facilitation of repair or replacement in case of HSM hardware or software failure. Customer is responsible for troubleshooting Client Software issues, which may involve engaging both HSM vendor support and Entrust support.

## 9. Price

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