Cryptography as a Service
Schedule

The Agreement for Entrust's Cryptography as a Service (CaaS) 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 CaaS.

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

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. **Hosted Service Details.** Subject to the Agreement, Entrust will provide the following as part of the CaaS Offering:
   - 1.1. One of Entrust's technical experts to serve as the overall primary contact for Customer in order to ensure a successful CaaS experience.
   - 1.2. 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.
     - 1.2.1. Dedicated, Customer-specific credentials per cryptographic partition.
     - 1.2.2. Secure creation and storage of cryptographic keys.
     - 1.2.3. Dedicated cryptographic processing power for the encryption and decryption of such cryptographic keys.
     - 1.2.4. HSM cluster will include any PIN Entry Device (PED) or card reader required by the HSM.
   - 1.3. Implementation and configuration of the HSM partition.
   - 1.4. Professional operational management of the HSM under high assurance security policies and procedures (see "Policies and Compliance" below) including:
     - 1.4.1. Dual Control for HSM administration
     - 1.4.2. Role separation with assigned roles for HSM administrators and Customer cryptographic uses.
   - 1.5. Secure handling and storage of all HSM components and administration keys according to Entrust and CaaS policies and procedures.
   - 1.6. Entrust's service level commitments for the CaaS Offering are available at https://www.entrust.com/mPKI-uptime-service-levels.pdf.
2. **Third Party Products and Services.** Certain third-party hardware, software and services may be resold, distributed, provided or otherwise made available by Entrust through or in connection with the Hosted Services ("**Third Party Vendor Products**"). Except as expressly stated in this Schedule, Entrust has no obligation and excludes all liability with respect to Third Party Vendor Products, the use of which shall be exclusively subject to the third party vendor's terms, conditions and policy documents ("**Vendor Terms**") accompanying, embedded in, or delivered with the Third Party Vendor Products, or otherwise made available by the third party vendor. In particular, **a**ll 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 Vendor 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:

   3.1. 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.

   3.2. Networking-based assumptions and limitations:

      3.2.1. 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.

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

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

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

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

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

   3.5. 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:

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

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

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

   4.4. 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 offered on a subscription basis for the Offering Term set out on the Order.

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. **Support.** Entrust provides the support commitments set out in the Support Schedule available at https://www.entrust.com/certificatesolutions-identity/support-schedule.pdf for the CaaS Offering. 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. **Fees.** 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.