



## Entrust Cryptographic Security Platform Deployment of PKI Professional Services Schedule

The Agreement for Professional Services for the deployment of Public Key Infrastructure (PKI) for the Entrust Cryptographic Security Platform (CSP) is made up of this Schedule, the Entrust General Terms and Conditions available at <https://www.entrust.com/general-terms.pdf> (“General Terms”), and an applicable Order. Capitalized terms not defined herein have the meanings given to them in the General Terms.

### 1. **Scope of Services.**

1.1. Scope. The table below sets out the scope and stages of the Professional Services and the respective responsibilities of Entrust and Customer at each stage. These steps will be completed for each engagement. If additional work is determined to be required, this will be addressed as set out in Section 7.2 (*Changes*) below.

Entrust will assign a project manager (“PM”) who will have overall responsibility for ensuring delivery of the Professional Services to the Customer. The PM is the Customer’s single point of contact with Entrust for the duration of the engagement, providing co-ordination of resources, tracking and closure of action items, and schedule, requirements, and financial management.

Customer will assign a PM to act as a single point of contact for Entrust, to ensure suitably qualified technical and business resources are available to fulfill the Customer’s responsibilities at the required times indicated in the table below.

<b>Stage 1: Kickoff</b>
<p>Entrust Responsibilities:</p> <ul style="list-style-type: none"><li>• Assign a project manager</li><li>• Contact Customer’s project manager to schedule the project kickoff meeting, confirm attendee roles, and identify key participants.</li><li>• Schedule and facilitate the project kickoff meeting including the following agenda<ul style="list-style-type: none"><li>○ Review scope of the Professional Services purchased</li><li>○ Review Customer requirements for deploying CSP PKI, including enrolment protocol required</li><li>○ Confirm which environment will be deployed (either a Production or Non-Production environment)</li><li>○ Review of prerequisites</li><li>○ Schedule the subsequent engagement steps and explain dependencies</li><li>○ Identify required attendees for future sessions</li></ul></li></ul> <p>Customer Responsibilities:</p> <ul style="list-style-type: none"><li>• Assign a project manager</li><li>• Engage and manage Customer resources, as identified in kickoff planning discussions, and ensure their attendance at kickoff meeting</li><li>• Gather information requested during the kick-off meeting</li></ul>

**Stage 2: Review High-level design(s)**

**Entrust Responsibilities:**

- Customize the high-level design shown in Section 2 of this Schedule to meet the high-level Customer use case based on information provided during and following the kickoff meeting.
- Answer Customer questions and feedback on the high-level design provided, making minor adjustments as needed – within the overall project scope
- Produce a final draft of the high-level design document for Customer approval

**Customer Responsibilities:**

- Engage Customer technical points of contact(s) responsible for the CSP PKI solution and environment, as identified in the kickoff meeting
- Review and comment on Entrust proposed design
- Complete review and final sign-off the high-level design document prior to commencement of the deployment activities

**Stage 3: Follow up to validate prerequisites are in place and schedule the solution deployment**

**Entrust Responsibilities:**

- Confirm completion of prerequisites as outlined in the high-level design document
- Coordinate Entrust resources to assist with deployment activities
- Schedule solution deployment activities with Customer

**Customer Responsibilities:**

- Complete the initial and appropriate setup of the infrastructure, including hardware procurement, operating system installation and verification, non-Entrust software installation and configuration, client machines with network connectivity. Ensure CSP Compliance Manager is installed.
- Complete pre-requisites as outlined in the high-level design document
- Plan and coordinate (in advance of scheduled deployment activities) for required service window(s)

**Stage 4: Deployment Activities**

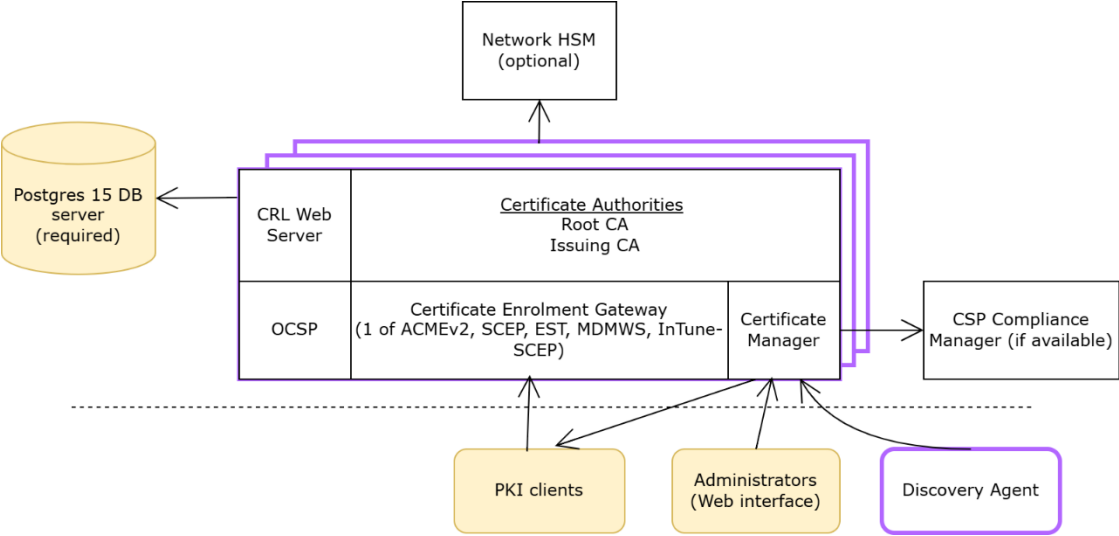
**Entrust Responsibilities:**

- Deploy and configure a single cluster of 3 nodes of CSP PKI and configure the following features and functionalities:
  - Certificate Authorities:
    - Configure a Root Certificate Authority within CSP PKI connected to a Customer supplied and compatible database. Root CA may store keys on an HSM if available (HSM configuration out of scope).
    - Configure an Issuing Certificate Authority within CSP PKI connected to Customer supplied and compatible database. Issuing CA may store keys on an HSM if available (HSM configuration out of scope).
  - Certificate Enrolment Gateway:
    - Configure Certificate Enrolment Gateway for certificate issuance from the Issuing CA with a single enrolment protocol from the below list and validate that a test client is able to enroll a certificate successfully:
      - ACME, SCEP, EST, InTune, MDM

- **Certificate Manager:**
    - Configure Certificate Manager against a Customer supplied database and connect to Issuing CA and CSP Compliance Manager
    - Configure a single report within Certificate Manager
    - Configure a single supported certificate destination and validate that a certificate can be issued to a test end point successfully.
    - Configure a single network scanner to discover certificates on a single network segment.
- Customer Responsibilities:
- Respond to Entrust questions
  - Shadow deployment and assist with questions, access requests, and/or third-party tools

**2. Deployment High-Level Design**

The CSP PKI will be configured according to the following diagram, with actual services deployed and configuration of services tailored as per Customer requirements and as agreed during the review of the high-level design. Entrust will deploy and configure the components outlined in purple, other components are outside the scope of these Professional Services. The diagram below shows a typical design targeted at common use cases.



**Certificate Authorities**

The Root Certificate Authority acts as the root of trust for the CSP PKI. The Root CA certificate should be propagated to all subscribers and relying parties consuming PKI services. The Root CA will sign the Issuing CA, which will issue certificates to PKI subscribers using the configured Certificate Enrolment protocol.

**Certificate Manager**

Certificate Manager has some or all of the following capabilities depending upon your licensed entitlements, as set out in the applicable Order:

- The **discovery capabilities** inventory certificates through the network discovery scanner and automated certificate import (from the Issuing CA).

- The **control capabilities** centrally manage policy, issuance & revocation. Perform manual operations as necessary to issue, renew, and revoke certificates.
- The **automation capabilities** push keys and certificates to endpoints, with fully managed rotation and certificate profile management.

In addition, Certificate Manager can produce and disseminate management notifications and reports to remind certificate owners of actions they need to take.

### 3. **Deliverables**

For each engagement, a tailored high-level design document, substantially conforming with the design set out in Section 3 above, will be produced, including the following details:

- Target use cases
- Solution diagram
- Components description
- Installation pre-requisites and dependencies
- Details of how customized parameters are configured for customer deployment

Entrust will provide one draft version and one final version of the deliverable.

### 4. **Dependencies and Assumptions.**

Customer acknowledges and agrees that performance of Professional Services by Entrust will be subject to the dependencies and assumptions noted below.

- 4.1. All work is to be performed during regular business hours.
- 4.2. All work is to be performed remotely.
- 4.3. Entrust reserves the right to fulfill delivery of Professional Services using Entrust employed staff, contractors or sub-contractors with appropriate experience and skills.
- 4.4. Any Entrust products provided to or used by Customer in relation to the engagement shall be subject to Entrust standard terms and conditions for such products (unless otherwise agreed to between Entrust and Customer).
- 4.5. All third-party products/components shall be supported by Entrust integrations as set out in the current Entrust product related documentation.
- 4.6. Entrust personnel shall not be made available or placed on stand-by for non-Entrust tasks or tasks unrelated to the Professional Services.
- 4.7. All Entrust products will be deployed on platforms supported by the Entrust products.

### 5. **Customer Obligations.**

Customer shall be responsible for the timely performance of its obligations under this Schedule, including, without limitation, the obligations below. Customer acknowledges that any delay on its part in the performance of its obligations may affect Entrust provision of the Professional Services. Customer must:

- 5.1. Provide Entrust with remote access as well as such information and materials as Entrust may



reasonably require to perform the Professional Services and ensure that such information is complete and accurate in all material respects.

- 5.2. Obtain (before the date on which the Professional Services are to start being performed) and maintain all necessary licenses, permissions and consents which may be required for Customer to provide the Professional Services before the date on which the Professional Services are to start.
- 5.3. Maintain in place a current subscription for CSP, including a current support plan.
6. **Out of Scope.** The following activities/tasks fall outside the scope of the Professional Services. Entrust does offer customized Professional Services and may be able to assist the Customer with some of the tasks below subject to a separate engagement under a separate statement of work:
  - 6.1. Provision of any content for policy, procedural or operational documentation.
  - 6.2. Formal project reporting (although informal status reporting will be provided).
  - 6.3. Formal Key Signing Ceremony
  - 6.4. Installation and configuration of Entrust software in any environments not specifically identified during the kick-off meeting.
  - 6.5. Provision, installation or configuration of Entrust or third party hardware, software (except as specifically set out herein), operating systems or supporting network components.
  - 6.6. Development of custom code, including development or customization of any component or application.
  - 6.7. Development and/or execution of a formal test plan.
  - 6.8. Installation or configuration of a database or directory.
  - 6.9. Detailed build or customized documentation (i.e. operations guides).
  - 6.10. On-call/stand-by availability.
  - 6.11. Travel or any work on Customer's premises.
  - 6.12. All Professional Services not specifically identified in this Schedule.
7. **Acceptance and Changes.**
  - 7.1. Acceptance. Any deliverable specified in this Schedule as requiring Customer sign-off or acceptance shall be considered complete and accepted when it has been provided and reviewed by the Customer in accordance with the specified timelines, or if no timelines are specified, within ten (10) business days, and Customer has not provided Entrust with a written notice of rejection. Customer may only reject a deliverable if it materially deviates from its specifications and the requirement in this Schedule. In the event of such a rejection Entrust shall correct the deviation and redeliver the deliverable. After redelivery pursuant to the previous sentence, the parties shall again follow the acceptance procedures set forth in this Section 8.1 (*Acceptance*). This Section, in conjunction with Customer's right to terminate for material breach where applicable, sets forth Customer's only remedy and Entrust's only liability for failure of a deliverable.
  - 7.2. Changes. The Professional Services covered in this Schedule represent a defined-scope package with a fixed price and are therefore not subject to a change management process. No changes to the high-level design or requirements are permitted at any point after Customer's sign-off at Stage 2 in Section 1.1 above. In the event that Customer requires additional



professional services beyond the scope of this Schedule, including if any Entrust work or deliverables need to be revised or repeated due to Customer's failure or errors in performing its obligations, these additional professional services may be provided pursuant to a separate statement of work agreed by the parties. In the absence of any agreement on a separate statement of work, Entrust shall have no obligation to provide additional or modified professional services or deliverables.

8. **Fees.** Customer will pay Entrust the costs and fees for the Professional Services as set out in the applicable Order, which are payable in accordance with the Order and the General Terms.
9. **Warranty.** Entrust warrants that the Professional Services it provides as described in this Schedule shall be performed in a professional manner in keeping with reasonable industry standards.

**10. Term; Customer Default; Cancellation/Rescheduling.**

10.1. Term. The Professional Services are sold on a one-time engagement basis. The Offering Term will commence on the date that the Order is accepted by Entrust and will continue in effect until the work identified in Stages 1 through 4 in Section 1.1 above is complete, or six months has elapsed, whichever occurs earlier. Any Professional Services that remain unused at the expiry of the Offering Term will be forfeited.

10.2. Customer Default. If Entrust performance of any of its obligations under this Schedule is prevented or delayed by any act or omission by the Customer or failure by the Customer to perform any relevant obligation ("Customer Default"):

10.2.1. without limiting or affecting any other right or remedy available to it, Entrust shall have the right to suspend performance of the Professional Services until the Customer remedies the Customer Default, and to rely on the Customer Default to relieve it from the performance of any of its obligations in each case to the extent the Customer Default prevents or delays Entrust performance of any of its obligations;

10.2.2. Entrust shall not be liable for any costs or losses sustained or incurred by the Customer to the extent such costs or losses arise from Customer's failure or delay to perform any of its obligations as set out herein; and,

10.2.3. the Customer shall reimburse Entrust for any costs or losses sustained or incurred by Entrust to the extent these arise from the Customer Default.

10.3. Cancellation/Rescheduling by Customer.

10.3.1. Requests by Customer to cancel or reschedule Professional Services engagement must be submitted in writing only via email to the assigned Entrust engagement manager, who is assigned when the engagement is scheduled. Requests by phone or voicemail will not be accepted by Entrust.

10.3.2. Remote service cancellation/rescheduling. If Customer cancels or reschedules a remote engagement within three (3) business days of the scheduled engagement start date, Entrust reserves the right to charge a cancellation fee, equal to the value of one (1) day of Entrust consulting fees as set forth in the Entrust price list in effect at that time. Customer will reimburse Entrust for the costs incurred by Entrust due to Customer's cancellation or rescheduling. New engagement date requests shall be established by mutual agreement only, up to a maximum of two (2) rescheduling dates. Subsequent requests shall be subject to a cancellation fee per request.

10.4. Cancellation/Rescheduling By Entrust. In the event of an engagement cancellation by Entrust, Entrust shall extend the Offering Term by the duration of the delay caused by the engagement cancellation.