Cryptographic Center of Excellence
PKI Discovery
Schedule

Service Overview

Entrust's Cryptographic Center of Excellence ("CryptoCoE") portfolio of Professional Services Offerings provides the Customer with the consulting services and expertise needed for the Customer to build its own CryptoCoE. Under the PKI Discovery Offering, Entrust will interview key Customer personnel to assess the current state and needs of Customer's PKI with respect to technology, use cases, operational practices, assurance and management. Entrust will deliver a report covering findings, a recommended high level solution design, deployment and, if relevant, a migration plan to address Customer requirements.

The Agreement for the PKI Discovery Offering is made up of this Schedule, Entrust General Terms and Conditions available at https://www.entrust.com/general-terms.pdf ("General Terms"), and an Order (as defined in the General Terms) for a PKI Discovery.

1. **Definitions.** Capitalized terms not defined herein have the meanings given to them in the General Terms.

   1.1. "Expert by Your Side hours" or "EBYS hours" means for the Offering Term, Entrust will provide remote consulting and technical support that is limited to the purchased number of hours in the form of telephone, email or virtual/remote meeting assistance (provided during normal business hours), to address general inquiries, questions, issues or changes related to PKI- and Identity-related services provided by Entrust.

   1.2. "PKI Governance" means the processes, the policy and organizational structure that the Customer has established to federate its PKI solution.

   1.3. "PKI System" means the technical environment used by the Customer for the PKI solution in place. It includes the servers (physical or virtual), certificate authority software, registration authority software, hardware security modules (HSMs) and associated configurations.

2. **Service Details.**

   2.1. Scope. An Entrust PKI Discovery engagement comprises of four key stages which commence with workshops/interviews with the key Customer stakeholders. The schedule of these and the requested attendees is agreed during project kick off as each organization is different, time zones need to be considered and it is sometimes better to run shorter workshops with smaller audiences to be the most efficient. Expert By Your Side hours may be purchased as a separate line item on an Order or under an additional Order and may be used for remediation of findings.

   2.2. Stages and Responsibilities. The table below sets out the four stages of a PKI Discovey engagement and the respective responsibilities of Entrust and Customer at each stage:

Stage	Entrust Responsibilities	Customer Responsibilities
1: Information Gathering—current state	• Collect details of any currently deployed PKI solutions and any existing Customer certificate lifecycle management issues. • Gather high-level business, functional and technical PKI requirements from key stakeholders. • Schedule and run workshop meetings with relevant staff. • Collect background and environmental information that may influence PKI requirements. • Endeavour to identify and assess known and potential future requirements, to ensure the PKI design will accommodate longer-term objectives.	• Assign a project manager to act as a single point of contact with Entrust. • Engage and manage the appropriate stakeholders within Customer's organization who are responsible for and/or have knowledge about the current state of the Customer PKI, current and future use cases and requirements of the PKI • Attend scheduled workshop meetings • Respond to Entrust's questions
2: Requirements Compilation – future state	Start to develop the detail needed to support the objectives of the project, based on the established current state and high-level requirements. Leverage Entrust's proprietary Assurance Framework to ensure that the information it has gathered is adequate to formulate proposed solutions based on best practices and relevant standards and approaches. Using this methodology, highlight information deficiencies and/or areas that need further investigation, in which case, a return to Stage 1 will be required.	• Engage and manage the appropriate stakeholders within Customer's organization who are responsible for and/or have knowledge about the current state of the Customer PKI, current and future use cases and requirements of the PKI • Respond to Entrust's questions
3: Requirements Collation – transitioning to future state	If the information gathered in Stages 1 & 2 is comprehensive and adequate, document the Customer's functional and non-functional requirements. Assess the organisation's priorities so that the target PKI design can accommodate phased implementation and migration (if relevant) from current state (if it is required). This is particularly important in more complex or multi-jurisdiction landscapes.	
4: PKI Discovery Report production and presentation	Production and presentation of the PKI Discovery Report, incorporating a target logical PKI architecture considering the requirements that have been gathered and collated alongside details of the Customer's IT estate and any other factors that influence the environment of the PKI and the applications it will need to support now and in the short/medium term, aiming to ensure the system design optimises key and certificate management.	• Engage and manage the appropriate stakeholders within Customer's organization who are responsible for and/or have knowledge about the current state of the Customer PKI, current and future use cases and requirements of the PKI to review the PKI Discovery Report, • Attend PKI Discovery Report presentation meeting

2.3. Out of Scope. The items below are outside the scope of the PKI Discovery Offering. Entrust has a rich portfolio of service offerings and could assist the Customer with some of the tasks below in a separate engagement:

- Provision of any content for policy, procedural or operational documentation
- Production of a detailed PKI architecture design document
- Formal project reporting (although informal status reporting will be provided);
- Remediation of the findings beyond use of the purchased EBYS hours
- PKI and/or Crypto Governance consulting beyond the Professional Services defined within this Schedule
- Except as expressly stated herein, travel or any work on Customer's premises
- Anything not explicitly listed in Scope

3. Deliverables.

3.1. On completion of the four key stages, Entrust will provide a written detailed report ("PKI Discovery Report") which would typically cover the following topics:

- Executive summary
- Identified Certificate Lifecycle Management issues
- Details of highest priority (core) use cases for PKI current and near future
- Summary of requirements for the future PKI solution to meet core requirements
    - Technical requirements
    - Availability requirements
    - Recommended policy document set
- Recommended high level logical PKI architecture for future state solution
- Indicative project schedule for deployment of future PKI solution
- High level migration plan from current to future state including identified migration considerations (e.g. trust anchor management, certificate reissuance process)
- Identified project stakeholders (customer and Entrust)
- Identified project risks

3.2. Entrust delivers all documents to its customers in Adobe Acrobat PDF format. This eliminates dependence on a common word processor, provides document integrity and reduces the possibility of transmitting macro viruses to our customers. Upon request, Entrust can also deliver documents in Microsoft Word format.

3.3. Entrust is committed to delivering high quality services and products to its customers. The PKI Discovery Report will be subject to peer review and require Entrust project manager approval before being delivered to Customer.

4. Assumptions and Limitations.

4.1. Workshop sessions are limited to a total of 5 maximum over the engagement.

4.2. Entrust will provide a maximum of two (2) revisions of the PKI Discovery Report based on Customer feedback under the scope of this Schedule.

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; in all cases, however, Entrust retains overall control and responsibility for the activities stated in this Schedule.

4.4. Entrust personnel shall not be available or on stand-by for non-Entrust tasks.

4.5. All work will be performed during regular business hours.

5. **Fees.** Customer will pay Entrust the costs and fees for the PKI Discovery Offering as set out in the applicable Order, which are payable in accordance with the Order and the General Terms.

6. **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.

7. **Term and Termination.**

7.1. The PKI Discovery Offering is sold as a one-time engagement. Unless otherwise specified on the Order, the Offering Term will commence on the date that the Order is accepted by Entrust and will continue in effect until the engagement is complete, unless terminated in accordance with the Agreement.

7.2. In addition to the termination rights in the General Terms, Entrust may terminate the Agreement with respect to the PKI Discovery Offering and refuse any additional Orders for the PKI Discovery Offering if Customer commits a material breach of this Schedule and fails to remedy such material breach within thirty (30) days after delivery of notice of the occurrence or existence of such breach or such longer period as may be agreed to in writing by Entrust.

Template version: December 14 2022