



Entrust Professional Services Deployment of Offline Root CA Schedule

The Agreement for Entrust's Professional Services for the deployment of an offline root certification authority ("CA") 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/stages indicated in the table below.

Stage 1: Kickoff	
Entrust Responsibilities:	
• Assign a project manager, contact Customer's project manager to schedule the project kickoff meeting, confirm attendee roles, and identify key participants • Schedule and facilitate the project kickoff meeting including the following agenda: ○ Provide an overview of the scope of the Professional Services purchased ○ Review Customer's requirements for deployment of an offline root CA, including any applicable certificate policy, certification practices statement, internal security policy, governance requirement, operational procedure, or other Customer-provided requirement applicable to the root CA ○ Confirm whether the deployment will be performed in a production or non-production environment and identify any environment-specific requirements, constraints, dependencies, or assumptions ○ Provide an overview of the prerequisites for next steps, e.g. server availability, supported OS, HSM availability, network/firewall readiness, DNS/time sync, access requirements, licenses/support contracts, customer resources, and required approvals ○ Schedule the subsequent engagement steps and explain dependencies ○ Identify required attendees for future sessions • Following the kickoff meeting, deliver the kickoff meeting minutes (as detailed in Section 3)	
Customer Responsibilities:	
• Assign a project manager • Engage and manage Customer resources, as identified in kickoff planning discussions, and ensure their attendance at kickoff meeting • Gather and provide complete and accurate information reasonably requested by Entrust during or following the kickoff meeting to support planning, design, scheduling, and delivery of the Professional Services • Review and provide feedback/sign-off on the kickoff meeting minutes	

Stage 2: High-level Design and Key Ceremony Script

Entrust Responsibilities:

- Customize the high-level design shown in Section 2 of this Schedule to meet the required configuration based on information provided during and following the kickoff meeting
- Review the Customer's existing Certificate Policy and Certification Practice Statement, if available
- Customize the key ceremony script according to Customer's required configuration
- Answer Customer questions and feedback on the high-level design provided, making minor adjustments as needed – within the overall project scope
- Produce final drafts of the high-level design document, key ceremony script, and high-level timeline of next steps ("Project Timeline") for Customer approval

Customer Responsibilities:

- Engage Customer technical points of contact(s) responsible for the offline root CA 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, key ceremony script, and Project Timeline prior to commencement of the deployment activities

Stage 3: Key Ceremony Rehearsal

Entrust Responsibilities:

- Confirm completion of the applicable prerequisites identified in the high-level design document, based on Customer-provided information
- Coordinate the required Entrust resources to support the deployment activities
- Schedule the root CA deployment activities with Customer, subject to Customer readiness and mutually agreed service windows in accordance with the Project Timeline
- Perform the deployment activities required to prepare the root CA server and HSM for the key ceremony. This may include:
 - Configure the root CA HSM. Entrust is able to configure current supported HSMs manufactured by Entrust (nShield) or Thales (Luna)
 - Install HSM client software on offline root CA server
 - Configure LDAP software in preparation to be used with the CA software
 - Install and configure CA software
- Conduct a key ceremony rehearsal to validate the key ceremony script, confirm participant roles and responsibilities, verify applicable prerequisites and evidence requirements, and identify any outstanding dependencies prior to the formal key ceremony
- Update the key ceremony script to capture the rehearsal results and submit the updated script to the Customer for review and acknowledgment
- After completion of rehearsal, erase the keys and format HSM

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 of an offline client machine
- Complete all prerequisites specified in the high-level design document prior to the scheduled deployment, rehearsal, or key ceremony activities
- Plan and coordinate the required service window(s) in advance of the scheduled deployment activities
- Ensure attendance and participation of all Customer-side participants in the key ceremony rehearsal, to ensure their ability to fulfill their roles in the final key ceremony
- Review and acknowledge the key ceremony rehearsal results

Stage 4: Final Key Ceremony Execution

Entrust Responsibilities:

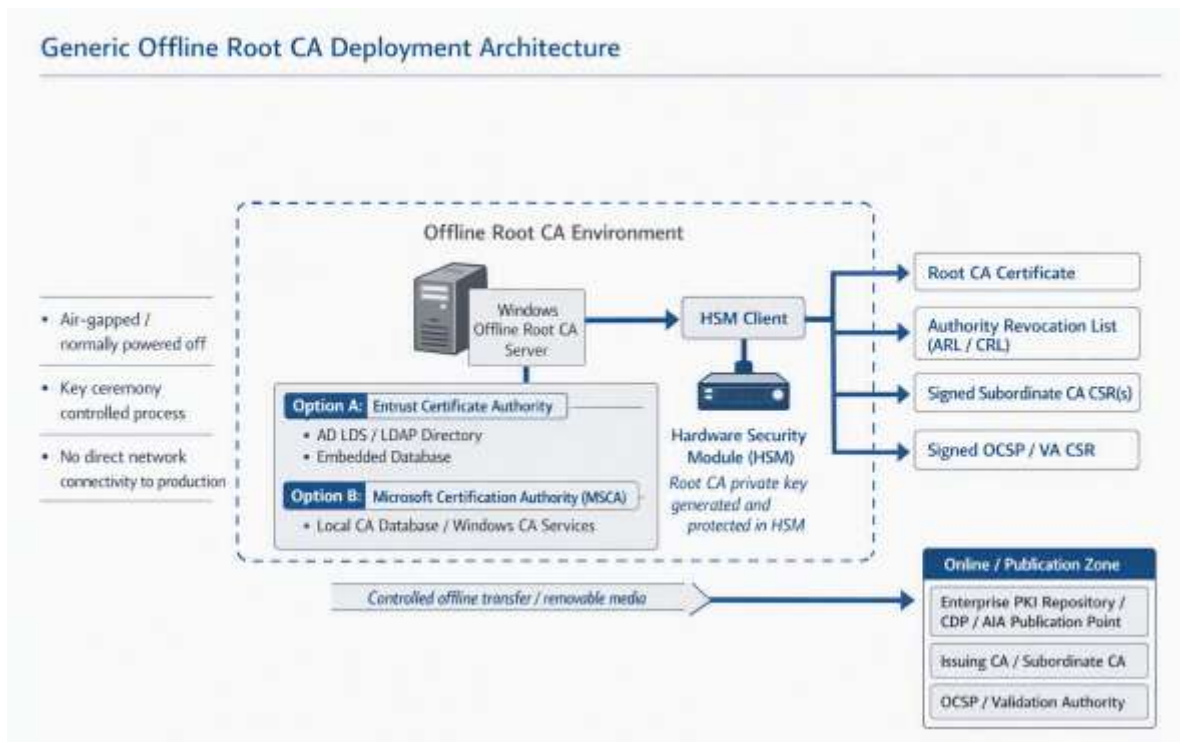
- Execute the key ceremony in accordance with the approved key ceremony script. The purpose of the key ceremony is to formally witness and document the creation of the root CA private signing key and to support the integrity, evidentiary record, and non-repudiation of the CA signing key pair. The key ceremony activities may include the following:
 - HSM:
 - HSM initialization or Security World creation
 - Create HSM keys and activation data (e.g. OCS cards, partitions, etc.) as required by the agreed key ceremony script
- Initialize the root CA, generate the root CA certificate, and validate the root CA certificate for correctness
- Validate root CA health by issuing revocation lists and validate database integrity
- Sign up to two (2) subordinate CA certificate signing requests and one (1) OCSP validation authority certificate signing request, if such requests are available during the key ceremony
- Back up the root CA and shut down
- Update key ceremony script with results

Customer Responsibilities:

- Respond to Entrust questions
- Fulfill required roles during the key ceremony
- Engage an auditor and coordinate their attendance at the key ceremony if required
- Enter any required passwords or configuration information as specified by the key ceremony script
- Acknowledge key ceremony script with results

2. Deployment High-Level Design

2.1. The following diagram and descriptions provide a high-level overview of the deployment architecture and components.



Offline Root CA Server

The offline root CA server runs on Windows and hosts the core PKI components required to support root CA operations, including the CA software and supporting directory services.

Certificate Authority Software

The certificate authority software supports root certificate issuance, authority revocation list publication, and certificate signing for subordinate CA and validation authority requests, using local data storage as applicable.

PKI Directory Service

The directory service provides LDAP-based support for publishing and retrieving PKI objects, including CA certificates and revocation information, within the offline root CA environment.

HSM Client and Hardware Security Module

HSM client on the Windows server interfaces with an external HSM that secures private keys and performs cryptographic operations.

3. Deliverables

3.1. Entrust will provide the following deliverables:

- **Kickoff meeting minutes** confirming completion of the kickoff meeting and documenting the parties' initial alignment on project contacts, deployment environment, Customer requirements, prerequisites, dependencies, and subsequent engagement activities.
- **Customized high level design document** including the following details:
 - Software components and versions
 - Root CA certificate profiles and certificate definitions
 - Installation pre-requirements
 - Up to two versions of the high level design document will be produced: an initial draft and a final version following Customer review.
- **Project Timeline** including high-level dates, date ranges, and/or deadlines for activities and requirements in Stages 3 and 4, based on information provided in Stage 1 and the high level design agreed in Stage 2.
- **Key ceremony script** describing the configuration of the offline root CA and generation of the root CA certificate, including the technical steps to support an audited process and provide evidence of key ceremony execution.
 - Up to four versions of the key ceremony script will be produced: an initial draft, updates following Customer review and key ceremony rehearsal, and a final update following key ceremony execution, if required.

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. The root CA HSM must be either an Entrust nShield or a Thales Luna device.
 - 4.2. All work is to be performed during regular business hours.
 - 4.3. All work is to be performed remotely other than key ceremony which can be performed on-site if requested. If the key ceremony is performed on-site at Customer's request, Entrust will provide a single Entrust resource for up to three days for such work, for no extra cost. For any other/additional on-site work: (a) it will be billed on a time and materials basis; (b) Entrust incurred travel and living expenses are billed at cost and paid by Customer; and (c) travel time is billable to Customer at fifty percent (50%) of Entrust's then-current per diem rates.
 - 4.4. Entrust reserves the right to fulfill delivery of Professional Services using Entrust employed staff, contractors or sub-contractors with appropriate experience and skills.
 - 4.5. 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).
 - 4.6. All third party products/components shall be supported by Entrust integrations as set out in the current Entrust product related documentation.
 - 4.7. Entrust personnel shall not be made available or placed on stand-by for non-Entrust tasks or tasks unrelated to the Professional Services.
 - 4.8. All Entrust products will be deployed on platforms supported by the Entrust products.
 - 4.9. No changes will be made to the agreed design, certificate profiles, cryptographic parameters, HSM selection, directory service selection, deployment environment, or key ceremony requirements after Customer approval of the applicable element in accordance with the stages set out in Section 1.
5. **Customer Obligations.** Customer shall be responsible for the timely (e.g. adhering to the Project Timeline) performance of its obligations under this Schedule, including the obligations below. Customer acknowledges that any delay on its part in the performance of its obligations may affect Entrust provision of Professional Services.
 - 5.1. Customer must provide Entrust with 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. Customer must obtain and maintain valid licenses and support contracts for all products used as part of the Professional Services, and any other necessary permissions and consents which may be required for Entrust to provide the Professional Services before the date on which the Professional Services are to start.
 - 5.3. Customer must ensure that all prerequisite infrastructure, operating systems, security controls, firewall rules, DNS configuration, time synchronization, and supporting services are available, correctly configured, and ready before any scheduled deployment, rehearsal, or key ceremony activity.
 - 5.4. Customer must make suitably qualified Customer stakeholders, technical resources, administrators, security officers, key ceremony participants, approvers, and any required auditors available for workshops, reviews, deployment windows, rehearsals, and key ceremony activities.



- 5.5. Customer must, prior to or on the scheduled key ceremony date, generate, validate, secure, and provide any subordinate CA, OCSP validation authority, or other certificate signing requests that are to be signed during the key ceremony.
 - 5.6. Customer must maintain responsibility for Customer-managed infrastructure, operating systems, third-party components, security controls, backup storage, audit record retention, evidence retention, and secure handling of key ceremony materials following handover.
 - 5.7. Customer must secure and protect offline root CA media, credentials, tokens, smart cards, activation data, HSM materials, backup media, and related key ceremony evidence in accordance with Customer's applicable security policies and procedures.
 - 5.8. If the parties agree that any on-site work will be performed by Entrust, Customer will provide on-site working space for the Entrust Professional Services team. Customer shall take all steps reasonably necessary to ensure the health and safety of the employees and subcontractors of Entrust and its Affiliates when such personnel are on Customer sites and Customer shall advise such personnel of the rules and regulations governing their conduct at Customer sites.
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. Installing network HSM in server room racks and/or installing PCIe cards in target server.
 - 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. Detailed build or customized documentation (i.e. operations guides).
 - 6.9. On-call/stand-by availability.
 - 6.10. Travel or any work on Customer's premises other than to support key ceremony as described above.
 - 6.11. Any key ceremonies or rehearsals other than the one rehearsal and one formal key ceremony described herein.
 - 6.12. Activities relating to issuing CAs or OCSP servers, including generation of CSRs and the import of the certificates and associated configurations (except for signing CSRs during the scheduled key ceremony as described herein).
 - 6.13. Any Professional Services not expressly identified in this Schedule.



7. **Scheduling.**

- 7.1. The actual start and completion dates of the Professional Services are dependent upon Entrust resource availability and Customer resource availability.
- 7.2. Cancellation/Rescheduling by Customer. Requests by Customer to cancel or reschedule a Professional Services engagement must be submitted in writing only via email to the assigned Entrust PM. Requests by phone or voicemail will not be accepted by Entrust. If Customer cancels or reschedules the Professional Services within five (5) 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 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 engagements dates requests shall be established by mutual agreement only up to a maximum of two (2) rescheduling dates. Subsequent requests shall be subject a cancellation fee per request.
- 7.3. Cancellation/Rescheduling By Entrust. In the event of an engagement cancellation by Entrust, Entrust shall provide a prorated credit for the unperformed Professional Services to be applied towards alternative engagement dates.

8. **Acceptance and Changes.**

- 8.1. 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 requirements 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.
 - 8.2. 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.
9. **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. For any on-site Professional Services to be provided on a time and materials basis (i.e. on-site key ceremonies), an Order may set out, if and as applicable, the number of hours in a working day, the specialists, their per diem rates, their estimated level of effort and their estimated fees. Fees are calculated to the nearest hour. Overtime work on Saturdays and beyond the number of hours in a working day will be charged at 1.5 times the regular per diem rate. Overtime work on Sundays and statutory holidays will be charged at 2 times the regular per diem rate. Work on Saturday, Sunday and statutory holidays is subject to a minimum charge of one (1) day.
10. **Warranty.** Entrust warrants that Professional Services it provides as described in this Schedule shall be performed in a professional manner in keeping with reasonable industry standards.



11. Term and Termination.

- 11.1. Term. The Professional Services covered in this Schedule are sold on a one-time engagement basis. The Offering Term will commence on the date that the Order is accepted 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.
- 11.2. Customer Default. If Entrust's 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"):
- 11.2.1. 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's performance of any of its obligations;
- 11.2.2. 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,
- 11.2.3. the Customer shall reimburse Entrust for any costs or losses sustained or incurred by Entrust to the extent these arise from the Customer Default.

Template version: September 14 2026