digicert®

PROFESSIONAL SERVICE ESSENTIAL PACKAGE OVERVIEW

Below are the service descriptions for the packages. By procuring the service package at this level, a customer can use it to obtain services for any one of the DigiCert® ONE managers listed below. If a customer desires to procure essential services for more than one DigiCert ONE manager, they must purchase a services package for each manager. The service packages are only available for platforms hosted and managed by DigiCert, including those on DigiCert's cloud partner, Oracle Cloud Infrastructure (OCI).

A Statement of Work (SOW) is not required with this service package if the customer/partner has accepted the DigiCert terms governing such services. This service is offered as a flat fee and must be consumed within six months of the project kick-off date. DigiCert requires a lead time of two weeks from the time of booking to kick off a project.

The Essential package will provide a customer with a maximum of 24 normal working hours for professional services, while the Essential Plus package will offer a maximum of 40 normal working hours. Project completion is based on the utilization of allocated hours within six months of the the project kick-off and is not contingent upon specific project deliverables. DigiCert reserves the right to amend the service offerings and the terms under which they are offered.

The following table displays a list of the DigiCert ONE managers covered by these service packages, along with a list of included tasks and their coverage limitations. If the requirements do not align with these service packages, we can create a custom Statement of Work. Additionally, should a customer need additional hours or have additional use cases beyond what the service package covers post-purchase, a change control will be initiated to extend the scope of work.

Product	Essential	Essential Plus	Services that will require a SOW
DigiCert® Trust Lifecycle Manager	• A single DigiCert® ONE customer account on DigiCert's hosted and maintained cloud platform • CA key ceremony coordination • Coverage for up to three PKI use cases for one or more seat types • CSR / Browser / SAML enrollment flow • Qualified or supported UEM integrations • Auto-Enrollment for a single Active Directory Forest • Guidance for REST API integration • Informal Knowledge Transfer • DigiCert Professional Services Delivery Report	• Tasks listed in the Essential Package • Discovery services: Network scanning with up to two sensors • Automation: Demonstration of certificate automation in up to five servers and two appliances • One qualified out-of-the-box third-party integration, such as Azure Key Vault, Qualys, Tenable, MSCA, SNOW, AWS CA, for a single business unit. • Guidance for TLS inspection use case • Informal Knowledge Transfer • Project summary documentation (consolidated for all services packages rendered for this manager)	• PKI assessment • DigiCert ONE on-premises deployment • Tasks that are not explicitly listed in the service description • Custom solutions • Policy documentations or non-standard technical documentations • Note: Health Check of DigiCert ONE hosted and hosted hybrid is available as SKUs to order. These SKUs will require an SOW for now.

Product	Essential	Essential Plus	Services that will require a SOW
DigiCert® IoT Trust Manager	• A single DigiCert® ONE customer account on DigiCert's hosted and maintained cloud platform • CA key ceremony coordination · • Coverage for up to two PKI use cases • CSR / Browser enrollment flow • Certificate issuance using standards-based protocol such as SCEP/EST/CMPv2/ACME • Batch certificate requests (configuration and demonstration) • Guidance for REST API integration • Informal Knowledge Transfer • DigiCert Professional Services Delivery Report	• Tasks listed in the Essential Package • Configuring and testing a qualified CA connector – CertCentral or EJBCA • Configuring an unmanaged CA • Configuring and testing applicable use cases via DigiCert Gateway • Informal Knowledge Transfer • Project summary documentation (consolidated for all services packages rendered for this manager)	• PKI assessment • DigiCert ONE on-premises deployment • Tasks that are not explicitly listed in the service description • Custom solutions • Policy documentations or non-standard technical documentations • Note: Health Check of DigiCert ONE hosted and hosted hybrid is available as SKUs to order. These SKUs will require an SOW for now.
DigiCert® Software Trust Manager	• A single DigiCert® ONE customer account on DigiCert's hosted and maintained cloud platform • CA key ceremony coordination • Up to two basic qualified code signing use cases (Authenticode and Java signing tools) and one advanced qualified code signing use case (CI/CD pipeline, GPG, Apple/Android signing, Docker signing, or third-party signing tools) • On-boarding for up to two dev teams and guidance for product use • Informal Knowledge Transfer • DigiCert Professional Services Delivery Report	• Tasks listed in the Essential Package • Thales DPoD (cloud) HSM as a keystore • One additional qualified basic or advanced code signing use case • Configuring Threat Detection Service • Informal Knowledge Transfer • Project summary documentation (consolidated for all services packages rendered for this manager)	• PKI assessment • DigiCert ONE on-premises deployment • Tasks that are not explicitly listed in the service description • Custom solutions • Policy documentations or non-standard technical documentations • Note: Health Check of DigiCert ONE hosted and hosted hybrid is available as SKUs to order. These SKUs will require an SOW for now.
DigiCert® Document Trust Manager	Not available at this moment	Not available at this moment	A Statement of Work will be required
DigiCert® Embedded Trust Manager	Not available at this moment	Not available at this moment	A Statement of Work will be required
Hours Allocated	24 hours (fixed)	40 hours (fixed)	

PRODUCT 1

DigiCert® Trust Lifecycle Manager

Essential

- Review customer PKI use-case requirements
- Provide guidance for preparing public and private CA (Certification Authority) naming documents and coordinate the CA key ceremony
- Provide guidance to configure the DigiCert® ONE production account for identified use cases
- Provide guidance for configuring SCEP integration for Unified Endpoint Manager/Mobile Device Manager (UEM/MDM) products
- Provide guidance for configuring and testing certificate lifecycles using any of the following enrollment methods:
  - CSR
  - Browser PKCS12
  - DigiCert Trust Assistant
- And with supported authentication methods:
  - Manual approval
  - Enrollment Code
  - SAML IdP
- Provide guidance for installing, configuring, and testing Auto-enrollment Server software on up to two qualified Windows member servers within a single Active Directory Forest for the identified use cases
- Provide guidance on REST API integration by identifying a list of APIs along with request and response details
- Offer informal knowledge transfer sessions for the DigiCert® ONE manager product, covering troubleshooting, maintenance, and effective collaboration with DigiCert technical support
- Write and deliver a post-engagement summary document
- Provide project coordination and administrative support

Essential Plus

- All tasks defined in the Essential package for Trust Lifecycle Manager
- Guidance on deploying up to two sensors on the customer's network, including private cloud, for certificate discovery
- Guidance on performing certificate lifecycle automation using private or public TLS certificates on up to five qualified server platforms and two qualified appliances
- Guidance on integrating with one of the qualified third-party software or services
- Guidance for TLS inspection, including creating necessary CA hierarchies and configuring certificate profiles needed to issue online CAs for TLS inspection
- Informal knowledge transfer covering troubleshooting, maintenance, and effective collaboration with DigiCert technical support for the configured use cases
- Writing and delivering a post-engagement summary document covering all services rendered for this manager
- Project coordination and administrative support

PRODUCT 2

DigiCert® IoT Trust Manager

Essential

- Participate in technical discussions with the customer to review IoT use cases requiring PKI
- Provide guidance for preparing private CA (Certification Authority) naming documents and coordinate the CA key ceremony
- Provide guidance to configure DigiCert IoT Trust Manager with appropriate profiles
- Test and demonstrate certificate issuance using any of the following issuance methods:
  - Portal based manual issuance
  - Batch requests
  - Standards based protocols (SCEP, EST, CMPv2, ACME)
  - REST API integration
- Provide guidance to the customer's IoT team on integration and testing for manufacturing and operational lifecycle processes with DigiCert IoT Trust Manager
- Provide an informal knowledge transfer of DigiCert IoT Trust Manager, including troubleshooting, maintenance, and effectively working with DigiCert technical support
- Write and deliver a post-engagement summary document
- Project coordination and administrative support

Essential Plus

- All tasks defined in the Essential package for DigiCert IoT Trust Manager
- Provide guidance for configuring and testing the issuance of certificates from a qualified CA connector, such as DigiCert® CertCentral or EJBCA
- Provide guidance for configuring an unmanaged CA
- Provide guidance for deploying and testing the issuance of certificates via the DigiCert Gateway
- Informal knowledge transfer covering troubleshooting, maintenance, and effective collaboration with DigiCert technical support for the configured use cases
- Writing and delivering a post-engagement summary document covering all services rendered for this manager
- Project coordination and administrative support

PRODUCT 3

DigiCert® Software Trust Manager

Essential

- Participate in technical discussions with the customer to review code signing use cases
  - This package will cover any two basic qualified code signing use cases and any one qualified advanced use case:
    - Basic use cases: Authenticode and Java signing
    - Advanced use cases: CI/CD pipeline, GPG, OpenSSL, Apple, Android, Docker, or other third-party signing tools
- Provide guidance for preparing private CA (Certification Authority) naming documents and coordinate the CA key ceremony
- Review and confirm a successful DigiCert CertCentral® integration to issue public code signing certificates
- Support up to two development teams for on-boarding to DigiCert Software Trust Manager for code signing
  - Work with development groups to test and validate that code signing works via DigiCert Software Trust Manager from their environment(s)
  - Provide guidance to the development groups to migrate to DigiCert Software Trust Manager based code signing process
- Provide an informal knowledge transfer of the DigiCert ONE manager product, including troubleshooting, maintenance, and effectively working with DigiCert technical support
- Write and deliver a post-engagement summary document
- Project coordination and administrative support

Essential Plus

- All tasks defined in the Essential package for DigiCert Software Trust Manager
- Provide guidance to configure, demonstrate and test one additional qualified basic or advanced use case
- Provide guidance to configure, integrate, and use a customer subscribed Thales Data Protection on Demand (DPoD) as HSM for DigiCert Software Trust Manager to generate and host code signing keys
- Provide guidance to configure and test Threat Detection service
- Informal knowledge transfer covering troubleshooting, maintenance, and effective collaboration with DigiCert technical support for the configured use cases
- Write and deliver a post-engagement summary document covering all services rendered for this manager
- Project coordination and administrative support

Assumptions and Key dependencies

DigiCert Trust Lifecycle Manager

- A maximum of three PKI use cases are covered in the Essential package. The most common PKI use cases relevant to Trust Lifecycle Manager include user authentication, device authentication, server authentication, secure email signing and/or encryption, and document and code signing using a private CA issued certificate.
- The Essential Plus package covers certificate discovery, automation, TLS inspection, and one qualified out-of-the-box third-party integration in addition to up to three PKI use cases included in the Essential package.

DigiCert IoT Trust Manager

- A maximum of two PKI use cases are covered. The most common PKI use cases are device and server authentication.

DigiCert Software Trust Manager

- The essential package covers two qualified basic and one qualified advanced code signing use case while the essential plus covers one additional qualified basic or qualified advanced use case.

Applicable for all managers

- DigiCert® ONE account has been created and is active on a DigiCert-managed platform
- Account has been configured with correct number of seats and CA count
- Customer contact has been on-boarded and has access to the DigiCert ONE portal
- The project will be performed remotely during the normal working hours of the assigned consultant

Customer requirements and DigiCert agreements for all managers

- Customer must have test machine/devices and test accounts that can be utilized during the DigiCert engagement for testing
- If the Customer makes use of a third-party product/service that needs to provision or consume end-entity certificates issued by the DigiCert PKI solution, then the Customer must provide access to the subject-matter experts for the third-party product/service
    - DigiCert will provide advice, as appropriate, and put forth our best effort regarding third-party services, with priority given to delivering the scope of services mentioned above
- Customer must provide timely access to any individuals/systems that DigiCert is dependent on during the engagement
    - This may include, but is not an exhaustive list: DigiCert ONE Administrator, Web Server Administrator, Firewall administrators, Network engineer, Proxy Administrator, etc.
- Customer must ensure that the technical resource assigned to work with the consultant has access to the DigiCert ONE administrator portal
- The customer/partner will be responsible for project management
    - DigiCert will provide project coordination and support to the customer/partner assigned project manager
- The project will be considered completed once the specified activities have been delivered, or when the maximum allocated hours for the package (24 hours for Essential, 40 hours for Essential Plus) have been consumed, or when the service package validity period has expired, whichever is the earliest
- DigiCert reserves the right to invoice the customer at any time, and invoicing is not dependent on the services being delivered
- All documentation and textual output produced by DigiCert will be in English only