Packaged services overview

DigiCert provides a variety of professional service plans to meet our customers' diverse needs. These packaged offerings can be used for new deployments, upgrades, PKI assessments or periodic reviews of your DigiCert® ONE solution.

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 or for a health-check listed below. If a customer desires to procure services for more than one DigiCert ONE manager or health-check, they must purchase a service package for each manager or health-check. The service packages are only available for platforms hosted and managed by DigiCert.

A Statement of Work (SOW) is not required with the service package if the customer/partner has accepted the DigiCert terms governing such services. This service is offered as a

Prerequisites for using the packaged services

- The customer/partner must have agreed to relevant terms with DigiCert to use the packaged services, such as DigiCert’s Master Service Agreement or Master Partner Agreement.

- The implementation will utilize qualified out-of-the-box product functionality for all packages except for Elite, where a service delivery scope is defined.

- The customer/partner has read this document and understands the scope and limitations of the selected package.

- Any product or service that is not defined above will require a Statement of Work. Examples of services that will require a Statement of Work include:

    - Document Trust Manager

    - Self-hosting the DigiCert ONE platform (on-premises or a cloud deployment).

    - Custom solutions.

    - Policy documentations or non-standard technical documentations.

Change control

- A change control is needed if a customer requires additional time, additional use cases, or a scope beyond what the service packages allotted time can cover.

- DigiCert will either recommend a package or prepare an amendment document detailing the required changes, including any additional hours and costs needed for the customer/partner, for approval.

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.

- The account has been configured with the required features.

- Cust

Customer requirements and DigiCert agreements for all managers

- Customer must have test machines/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, regarding third-party services, with priority given to delivering the qualified solution.
- 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 Administrator, Network engineer, Proxy Administrator, Third-Party Network/Load-Balancer/UEM 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 of the overall project.
    - DigiCert will provide project coordination and support to the customer/partner assigned project manager.
    - DigiCert will assign a project manager to oversee service delivery from the DigiCert side for the Elite package only.
- The project will be considered completed once one of the following conditions is met: the specified activities have been delivered, the maximum allocated hours for the package have been consumed, or the service package period of performance has expired—whichever occurs first.
- DigiCert reserves the right to amend the service offerings and the terms under which they are offered.
- The billing type is fixed fee. It is invoiced upon initial booking and is not dependent on the services being delivered.
- All documentation and textual output produced by DigiCert will be only in English.
- A lead time of up to 2 weeks from the time of booking is required to allocate a resource.
- The service will be provided by DigiCert Professional Services or by a certified DigiCert Service Delivery Partner based on resource availability.
- Services will be delivered remotely.
- Business Hours are between 8.30 AM - 6 PM where the DigiCert assigned resource is based, but working hours can be discussed and agreed to during the project kick-off to accommodate any time zone differences.
- The minimum consumption increment is 1-hour for remote calls and 0.5 hour for tasks.
- Requests for standby or work during extended hours on weekdays will be counted at a rate of 1.5 times the standard consumption rate, while requests during public holidays or weekends where the DigiCert assigned resource is based will be counted at a rate of 2 times the standard consumption rate.

Product	Lite	Essential	Essential Plus	Elite
DigiCert IoT Trust Manager	A single DigiCert ONE customer account on DigiCert's hosted and maintained cloud platform Coverage for up to two device PKI use cases CA key ceremony coordination CSR / Browser enrollment flow Certificate issuance using standards-based protocol such as SCEP/EST/CMPv2/ACME Guidance for REST API integration Informal Knowledge Transfer	A single DigiCert ONE customer account on DigiCert's hosted and maintained cloud platform CA key ceremony coordination Coverage for up to three device 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 Coverage for a total of four device PKI use cases Configuring and testing a qualified CA connector – DigiCert® 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 service packages rendered for this manager)	PKI assessment of any qualified product functionality for private and public trust use cases A well-defined and tailored scope of work covering services to be delivered Ongoing Cadence calls at preferred intervals Project management for DigiCert service delivery
Key Points	Coverage for up to two device PKI use cases Out-of-the-box product functionality only	Coverage for up to three device PKI use cases Out-of-the-box product functionality only	Coverage for up to four device PKI use cases Out-of-the-box product functionality only	The details will be covered in the scope of work, which is flexible. When the estimated level of effort exceeds the maximum allocated for this package, a change control process will be recommended Out-of-the-box product functionality only

Product	Lite	Essential	Essential Plus	Elite
DigiCert Software Trust Manager	A single DigiCert ONE customer account on DigiCert's hosted and maintained cloud platform CA key ceremony coordination Provide guidance to configure up to two basic qualified code signing use cases" (Authenticode and Java signing tools) On-boarding a development team and guidance for product use Informal Knowledge Transfer	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 Customer-subscribed Thales DPoD (cloud HSM) as a keystore One additional qualified basic and one advanced code signing use case Configuring Threat Detection Service Informal Knowledge Transfer Project summary documentation (consolidated for all service packages rendered for this manager)	PKI assessment of any qualified product functionality for private and public trust use cases A well-defined and tailored scope of work covering services to be delivered Ongoing Cadence calls at preferred intervals Project management for DigiCert service delivery
Key Points	Coverage for two qualified basic code signing use case Out-of-the-box product functionality only	Coverage for two qualified basic and one qualified advanced code signing use case Out-of-the-box product functionality only	Coverage for a total of three qualified basic and two qualified advanced use cases Out-of-the-box product functionality only	The details will be covered in the scope of work, which is flexible. When the estimated level of effort exceeds the maximum allocated for this package, a change control process will be recommended Out-of-the-box product functionality only

Product	Lite	Essential	Essential Plus	Elite
Health-check Service	Health-check for cloud-only use cases Applicable for a single DigiCert ONE customer account on DigiCert's hosted and maintained cloud platform Review the configuration of applicable DigiCert ONE Managers and usage of cloud services Deliver a summary report identifying gaps and proposing remediations If there are sufficient hours remaining after completing the health check, these can be utilized by DigiCert Professional Services to carry out any recommended remediation work; otherwise, DigiCert may recommend purchasing a package to ensure adequate hours for the necessary remediation.	Health-check for cloud-only and hybrid use-cases Applicable for a single DigiCert ONE customer account on DigiCert's hosted and maintained cloud platform Review the configuration of applicable DigiCert® ONE Managers and relevant software deployed at customer premises Deliver a report identifying gaps and proposing remediations If there are sufficient hours remaining after completing the health check, these can be utilized by DigiCert Professional Services to carry out any recommended remediation work; otherwise, DigiCert may recommend purchasing a package to ensure adequate hours for the necessary remediation.	Health-check for a DigiCert ONE on-premises setup. Review the architecture of the DigiCert ONE platform, the version of the software in use, the PKI operations processes, and the operational status. Review the configuration of applicable DigiCert ONE Managers and relevant	