

About this certification program

Delivered by expert trainers and accompanied by hands-on lab activities, the DigiCert Solutions Engineer certification program provides practical knowledge and experience with PKI deployment, configuration, maintenance, and support for a broad range of use cases in any industry. Discover how cloud services are shaping modern PKI and learn to deploy PKI for enterprise user and device security, IoT device encryption and secure management, modern development operations and code signing, or remote and mass digital document signing.

Fast facts

Format	Virtual instructor-led training
Estimated time	15 hours lecture 5 Hours of assessment
Requirement	Complete 4 Technical Professional courses to be certified as a DigiCert Solutions Engineer
Certification validity	2 years
Credential	DigiCert Solutions Engineer Certification

Certification courses

Select and complete four from the five Technical Professional courses available in DigiCert University:

Managing DigiCert CertCentral TLS Manager	Deploying DigiCert Private On-Premises CA	Administering DigiCert Trust Lifecycle Manager	Administering DigiCert Software Trust Manager	Administering DigiCert Device Trust Manager
Describe the importance of public trust and the role of TLS in Digital Trust Explain Transport Layer Security (TLS) and how it works Navigate the CertCentral Dashboard and interpret certificate activity and industry updates Manage sub-accounts, user roles, and divisions for flexible oversight and permissions Submit, review, and approve certificate requests with customized workflows Design and customize email notifications Automate certificate issuance using ACME and REST APIs Generate and analyse reports to monitor certificate performance and compliance Track account finances, orders, and lifecycle notifications Pre-validate organizations and domains for efficient certificate issuance Access audit logs and configure account security settings Utilize support resources and help documentation effectively managing DigiCert CertCentral TLS Manager	Explain the DigiCert On-prem CA Architecture & Infrastructure Services Describe the benefits of Deployment Models & Database Requirements Explain the full installation and components involved in a DigiCert Private On-prem CA Configure the newly installed DigiCert On-prem CA and creation of the initial Root & ICA Certificate Authority Explain the ongoing system management tasks. Outline some troubleshooting techniques and describe the backup-and-restore strategy	Deploy Trust Lifecycle Manager, manage administrator roles, permissions, and access structures Discover and monitor certificates using TLM agents and sensors Configure certificate profiles, enrollment/authentication, and self-service portal access Integrate PKI operations using REST API, SCEP, EST, and CMP protocols Leverage DigiCert Trust Assistant for issuance, renewal, and key security Implement automation with ACME and configure integration with F5, Citrix, AWS, A10, and Load Balancers	Describe Software Trust Manager architecture and deployment models (cloud, on-premises, or hybrid) Perform initial system configuration: configure credentials, roles, security policies, and system accounts Apply code signing fundamentals: test and production signing, secure hashing, and automated signing workflows Manage releases: create, update, approve releases, and integrate security/compliance tools (ReversingLabs, FOSSA) Automate CI/CD integration across platforms such as GitHub and Azure Monitor, report, and audit: access client logs, audit trails, and signature logs to maintain traceability	Plan a Device Trust Manager deployment, define roles, and identify success factors Describe system architecture and core operational concepts within DigiCert ONE Register devices, assign certificates, manage divisions, and automate issuance processes Create, manage, and enforce device trust policies, including automated updates Integrate DTM with third-party tools using APIs and automation workflows Utilize reporting tools, troubleshoot issues, and access documentation for operational support



What is DigiCert University?

DigiCert University is a non-degree granting, online learning portal that offers short online, self-paced and virtual instructor-led training covering a variety of digital trust-related topics and solutions. DCU offers training for both sales and technical professionals in the security industry.

Who should attend?

The certification includes the Digital Trust Professional prerequisite and six solution-focused sales courses. Each Solutions Engineer course is designed to help sellers understand the customer challenge, recognize qualified opportunities, and explain the value of the related DigiCert solution.

This program will benefit anyone responsible for sales engineering pre-sales support, service deployment planning and implementation, and technical support of public key infrastructure (PKI) solutions.

Anyone seeking to complete the DigiCert Solution Architect certification is also required to complete both the Digital Trust Associate and Solutions Engineer certifications.

Participants should have experience performing Microsoft domain administration tasks, basic networking configuration, and have a foundational knowledge of PKI concepts such as cryptography and encryption. Familiarity with the Unix/Linux command line and experience running simple commands is an asset.

Hands-on experience

All of the Technical Professional courses are instructor-led and delivered virtually via live meeting. Each course offers hands-on labs, providing the opportunity to put theory into practice. Using a supported, modern browser, participants can access a virtual lab that simulates an enterprise PKI environment. Detailed lab instructions guide you through the steps to configuring the DigiCert® ONE Trust Managers to issue and manage certificates for a broad range of PKI use cases.

Course registration

If you want to register for a DigiCert University account and enroll in any of the DigiCert certification training, simply email: DCU_Help@digicert.com

If you're a DigiCert partner, you can enroll courses in DigiCert University courses in the DigiCert Partner Portal. Depending on your role, you will be enrolled in sales and technical certification courses. Please contact your DigiCert channel account manager for further information regarding course enrollment or certification requirements for DigiCert partners.

DigiCert Solutions Engineer

Earners of the Solutions Engineer Certification have developed practical knowledge and expertise in PKI deployment, configuration, maintenance, and support for diverse use cases in any industry. They have gained skills in deploying PKI for enterprise user and device security, IoT device encryption and secure management, modern development operations and code signing, as well as remote and mass digital document signing. DigiCert Solution Engineers are equipped to support customers across various industries, establishing themselves as trusted professionals in the field of PKI.

About DigiCert

DigiCert is a global leader in intelligent trust, securing people, data, and devices with AI-powered solutions built to stop threats today and prepare for a quantum-safe future.

© 2026 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere. All other trademarks and registered trademarks are the property of their respective owners.