Administering DigiCert ONE Software Trust Manager (STM)

Fast Facts

Virtual Instructor Led Training

7.5 hours lecture

7.5 hours hands-on labs

90 minute proctored exam

DigiCert Solutions Architect Certification

About this course

Welcome to the Administering DigiCert Software Trust Manager(STM) certification course. This course provides a technical overview of the DigiCert ONE code signing solution. The course covers initial configuration of the service including license management, account setup and certificate authority (CA) configuration. You will learn to use and modify built-in certificate templates, automated certificate enrollment methods, and configure certificate issuance workflows. You will also learn how to configure CI/CD integration, key management and policy enforcement.

The hands-on labs provide the opportunity to put theory into practice. The instruction and lab will take approximately 16 hours to complete.

Course Outline

Planning an STM Deployment	System Account Configuration	Signing Fundamentals	Releases	Continuous Integration/ Continuous Delivery	Reporting and Logging
• Describe the STM value proposition • List and describe the supported STM deployment models (Cloud / on premises / hybrid) • Describe the STM system architecture (Components, software layers, key stores) • List and describe the STM deployment requirements • Perform initial system setup • Install STM license and create Admin Keys	• Describe the benefits of test and production signing • List and configure code signing certificate profiles • Describe and configure account security controls • Configure user access controls using user types and group memberships • Describe and configure access policy controls • Integrate STM with CertCentral for public code singing certificates • Describe keypair profiles • List and configure key models (dynamic, static, rotation) • Create certificate profiles, configure user access, and configure system access policies	• Describe basic code signing methods and characteristics • Describe and install the STM client tools • Describe and install the STM software development kit • Describe the benefits of the SMCTL CLI • Generate keypairs and certificates for specific code signing use cases • Sign MS, Java and Docker Files • Describe and perform certificate revocation (backdating, implications, controlling impact) • Install client tools and SDK, sign files and perform a revocation	• Describe test, online production and offline production keypair types • Describe and create and manage releases using the GUI and SMCTL • Describe and configure offline production approvals • Describe and configure baselines and production release with a baseline • Create a baseline and manual approvals to prevent malware injection	• Create a script to automate a build (generate keypair, create window, sign) • List and describe STM integration capabilities • Describe STM integration with Azure • Describe and configure STM to integrate with Jenkins • Describe STM integration with other development platforms • Configure release window automation with Jenkins • Configure code singing automation using the CLI with Jenkins	• Describe the STM logging capabilities (client, server) • List and describe STM audit and signature logs • List and describe STM client logs • Export logs to CSV and XLSX files • Perform basic system troubleshooting tasks • Examine and export system log files

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

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

Partners seeking to qualify for DigiCert partner program benefits may be required to complete technical certification training depending on their partner tier. Please check with your DigiCert Channel Account manager for details.

Hands-On Experience

The Administering DigiCert ONE Software Trust Manager (STM) course is augmented by a virtual lab environment. Using a supported, modern browser, participants can access a virtual lab that simulates an enterprise PKI environment. Step-by-step lab instructions guide you through the process of installing and configuring the infrastructure services and then the DigiCert ONE on-premise install.

Complete the Digital Trust Associate certification, as well as Deploying DCONE Core Services, Administering DigiCert Trust Lifecycle Manager, and 2 additional Technical Certification Courses to achieve your Solutions Engineer certification.

Course Registration

Anyone wishing to register for a DigiCert University account and to enroll in sales and technical certification training should email:

DCU_Help@Digicert.com

DigiCert partners can enroll for courses in DCU via 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 sales and technical certification requirements for DigiCert partners.

DigiCert Software Trust Manager Technical Professional

Earners of the Software Trust Manager Technical Professional certification have developed specialized skills in gathering requirements and planning the deployment of a Software Trust Manager implementation. They can perform initial configuration of the service including license management, account setup, and certificate authority (CA) configuration. Badge earners are able to modify built-in certificate templates, automate certificate enrollment methods, and configure cert issuance workflows.