Administering DigiCert ONE Trust Lifecycle Manager

Fast Facts

- Virtual Instructor Led Training
- 6 hours lecture
- 6 hours hands-on labs
- 90 minute proctored exam
- DigiCert Solutions Architect Certification

About this course

This course provides a technical overview of the Trust Lifecycle Manager solution. The course covers initial configuration of the service including deployment models and requirements, system setup and Private CA/ICA set up. You will learn to use Certificate profiles and the new DigiCert Trust Assistant. You will also take a closer look at the capabilities of REST API, Protocols and other clients.

The hands-on labs provide the opportunity to put theory into practice. The instruction and lab will take approximately 12 hours to complete.

Course Outline

Planning a TLM Deployment	TLM Overview	Certificate Profiles	Use Cases	API, Protocols, and Clients	Automation via ACME and Sensors
• Brief overview of the multiple ways DC1 may be deployed and how it affects TLM	• Explain how to navigate the TLM dashboard	• Discuss the different enrollment methods available	• Explain use cases for authenticating users via certificates	• Discuss the REST API and the various resources available	• Explain the ACME Service standard
• Explain how DC1 is built, with specifics pertaining to TLM	• Discuss seat management	• Explain the different authentication methods and their use cases	• Explain use cases for Smart Card login	• Discuss SCEP and the resources available for using it	• Discuss how Certbot may be configured to access the ACME Service
• Discuss the resource requirements of DC1 and TLM	• Discuss certificate management	• Explain autoenrollment implementations and use cases	• Explain use cases for Mobile Device Management certificates	• Explain what EST is and how to use it	• Discuss how Kubernetes may be configured to access the ACME Service
• Discuss any special instructions needed to get TLM running	• Explain enrollments	• Discuss where we may obtain data from for profiles	• Explain use cases for a secure intranet website	• Discuss PKI Client and how it is used to manage certificates	• Explain what sensors are and how they work
• Explain the differences between administrator types	• Explain certificate templates and how the differ from certificate profiles	• Explain what the profile matrix is and why we provide default templates	• Discuss use cases for TLS Inspection and how to implement it	• Discuss the DigiCert Desktop Client and how it is used to manage certificates	• Discuss integrations with F5
• Explain the differences between public/private roots and how TLM uses each	• Discuss business units (sub-accounts)	• Explain what email templates are and how to use them	• Explain use cases for secure email communication	• Discuss the DigiCert Trust Assisstant and how it is used to manage certificates	• Discuss integrations with Citrix
• Discuss why and how to configure a Private CA/ICA	• Finish configuring DC1 and setting up administrators specific to TLM	• Explain how to brand enrollments/ certificates to provide a uniform experience	• Explain how to adapt a profile to other use cases that may emerge	• Configure an S/MIME Profile and install certificates to Outlook	• Discuss integrations with Amazon Web Services
• Setup and update an existing DC1 deployment and apply license		• Configure and enroll for a web-based certificate profile & Installing the DDC	• Download, Install, and Configure the Autoenrollment Server		• Discuss integrations with A10
					• Lab #6: Configuring and using sensors for automation

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 digital trust 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 Trust Lifecycle Manager 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 DigiCert University via the DigiCert Partner Portal. Click on the "Enable" menu option to automatically access your DigiCert University account. 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 Trust Lifecycle Manager Technical Professional

Earners of the DigiCert Trust Lifecycle Technical Professional certification have hands-on experience planning the deployment and installation of an on-premise public key infrastructure (PKI). They can install and configure the required infrastructure services and install and configure DigiCert ONE core services. They are familiar with the component architecture of the system, can setup a private certificate authority hierarchy and can manage certificate profiles.