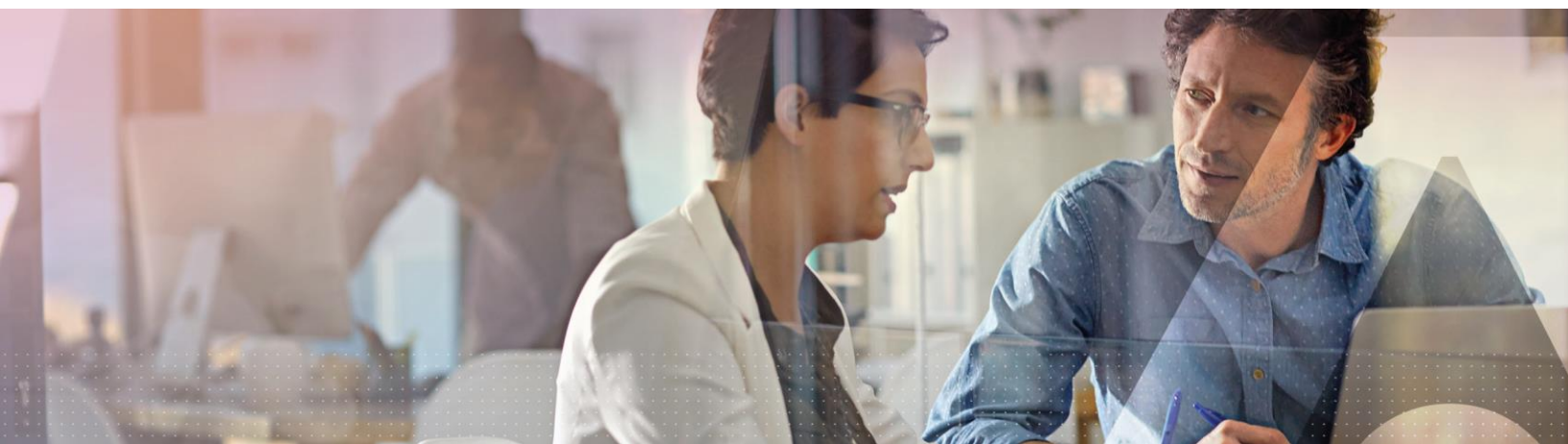


CipherTrust DSP - Professional Certification Course TRAINING AGENDA



CipherTrust DSP Professional Certification Course

Overview

CipherTrust Data Security Platform (DSP) is an integrated suite of data-centric security products and solutions that unify data discovery, protection and control in one solution.

Thales has pushed the innovation envelope to remove complexity from deploying data security, accelerate time to compliance and secure cloud migrations.

The platform provides powerful tools to:

- Discover and classify the data that your organization should be protecting
- Protect against external threats and insider abuse with robust encryption, granular access controls, and tokenization strategies
- Control your data, wherever it is stored, with strong centralized key management

This self-paced certification course focuses on the CipherTrust Data Security Platform and its integrated solutions. The training sessions will be in the form of narrated presentations, and the hands-on lab practices will be available over a remote virtual lab.

Student interaction and email based Q&A with the instructor is available throughout the entire course, during regional business hours.

An active internet connection is required to attend each online training session and view course material.

Training Objectives

- Overview of the CipherTrust Solution and its basic functions
- Understand the aspects and tools of the CipherTrust product suite
- Evaluate device architecture and usage schemes
- Deep dive into Application support (Oracle TSE, KMIP and more)
- Install and configure CipherTrust Transparent Encryption (lab exercise for CTE Ransomware Protection)
- Cover backup and restore operations
- CipherTrust REST-API support

Duration

Maximum of 5 days.

Thales Certification Exam

This course prepares you to take the CipherTrust DSP Professional Certification Exam. Included in the price is one exam voucher redeemable for up to 30 days post-training. Students who pass the certification exam are entitled to a certificate and a digital badge.



Modules and Sessions

Module 1 – CipherTrust DSP Overview and Basic Functions

- Review the CipherTrust Management Server, terminology and components, solution architecture and system requirements
- Cover new features introduced in CipherTrust
- CipherTrust first initialization and IP configuration

Lab Practice:

- Review functionality, usage of the CipherTrust Web UI using the *ksadmin* user
- REST-API samples
- CipherTrust DSP Clustering

Module 2 – CipherTrust Transparent Encryption (CTE)

- CipherTrust Transparent Encryption Solution overview
- Discuss Licensing schemes
- CTE Terminology
- CTE Integrations

Lab Practice:

- Install and configure CTE on Windows Server, protecting a folder and using LDT to encrypt and decrypt data, using the *dataxform* tool
- Install and configure CTE on Linux CentOS 7, protecting a directory, and debugging options
- Install and configure CTE RWP

Module 3 – CipherTrust Cloud Key Manager (CCKM)

- CCKM Solution overview
- Videos – demonstrating the CCKM configuration flow with Amazon AWS, and Microsoft Azure

Module 4 – CipherTrust Key Management Interoperability Protocol (KMIP)

- CipherTrust Key Manager Interoperability Protocol (KMIP) Solution overview

Lab Practice:

- Configure KMIP Integration with VMWare vSphere

Module 5 – CAKM Agent, encrypting Oracle Database with TDE

- CAKM Agent, encrypting Oracle Database with TDE Solution overview

Lab Practice:

- Install, and configure CAKM Agent, and integrate the CAKM agent with Oracle database

Module 6 – CipherTrust Tokenization

- CipherTrust DSP Tokenization Solution overview

Lab Practice:

- Tokenization CT-VL configuration

Module 7 – CipherTrust Data Security Platform As-a-Service

- CipherTrust Data Security Platform As-a-Service Solution overview

Certification Exam.

Additional questions about Thales Technical Training?

Contact the CPL Technical Training Team: cpltechnicaltraining@thalesgroup.com