THALES

gemalto
a Thales company

Technical Training

CPL CERTIFICATION COURSE OFFERING

Contents

Thales's Certification Courses

Thales's Cloud Protection and Licensing solutions allow organizations to enhance network access security, strengthen VPN security for remote access, protect data and keys on local and remote computers, and simplify password management and protection — all with the industry's broadest range of authenticators, management platforms, appliances and security applications.

For each product or solution, an introductory session is provided, followed by a guided lab session in which the student installs and configures the product(s). Certification is granted after completing the course and passing the relevant certification exam.

Authentication Certification Courses

The Authentication Certification courses provide students with all the tools needed to install and support the eToken product suite, SafeNet Trusted Access (STA) and SafeNet Authentication Service (SAS) authentication services. As part of the curriculum, participants will learn how to integrate Thales's authentication products into existing environments and set up secure identity access solutions using these products.

These courses are designed to cover the most relevant topics related to the implementation and deployment of Thales's authentication solutions. The obtained knowledge is practiced and deepened through practical exercises in hands-on sessions.

Gemalto-SafeNet PKI Certification

The Gemalto-SafeNet PKI Certification Course is aligned with all of our PKI product releases and supported solutions.

This course focuses on the Thales tokens, IDPrime MD smart cards, middleware and management systems. The course sessions cover SafeNet Authentication Client (SAC), vSEC:CMS and different authentication schemes.

Through the lab sessions, students will practice various security solutions and certificate-based authentication, enrolling software and hardware authenticators and more.

Course Agenda

- Authenticators (Smart cards and tokens complete offering including eToken 5300).
- SafeNet Authentication Client (SAC) implementation with USB tokens and new Thales cards.
- vSEC:CMS Extend training (Using the new Activation tool, SQL and HSM support, Enrolling certificates to smart card, installing and configuring the VSEC self-service, configuring and installing the VSEC virtual smart card)
- Authentication Log investigation
- Microsoft ADCS HSM implementation
- Pre-boot and disk encryption solutions (Hands-on for Microsoft Bit Locker)

Cloud Authentication - SafeNet Trusted Access (STA)

This three-day certification training is a comprehensive course focusing on our authentication server and our access management solutions provided as SafeNet Trusted Access (STA) services.

In the three-day training, students participate in theoretical discussion and lab sessions, while acquiring a practical understanding of how to deploy STA cloud services and manage the solution.

Course Agenda

- Solution Technical Overview
- On-boarding and Provisioning
- Push OTP
- User Synchronization and Management
- Provisioning
- STA Console
- Authentication Agents
- Account Manager and Operator Roles
- Managing Token Policies
- Alerts and Reporting
- Pre-authentication Rules
- Applications Integration with STA
- Access Management Policies

SAS SPE/PCE Advanced Certification Course

The SAS SPE/PCE Certification Course is targeted at engineers who have completed the STA Cloud Authentication Certification course.

In this advanced, three-day training, students will focus on setting up the SAS PCE/SPE (on premise) server, organization and user management, solution integrations, server replication, and troubleshooting skills. The majority of this course consists of hands-on and lab practice.

Course Agenda

- SAS SPE/PCE Server Installation
- Token Provisioning (focusing on the MobilePASS token)
- NPS Agent for RADIUS Authentication

- FreeRADIUS Server and Agent Setup
- LDAP Integration and Auto Provisioning Services
- PCE server Integration with ProtectServer HSM
- Management API Review
- Server Management (Licensing, Allocation Handling, and more)
- Full High Availability Configuration (SAS HA Controller Service; Server Replication)

Hardware Security Module (HSM) Certification Courses

Thales's Hardware Security Modules (HSMs) provide reliable protection for applications, transactions and information assets by securing cryptographic keys. HSMs are the fastest, most secure and easiest application security solution to integrate for enterprise and government organizations to achieve regulatory compliance, reduce the risk of legal liability and improve profitability.

Payment HSM - payShield Certification Course

The Thales payShield Certification Course is a classroom training that provides an overview of how the payShield 10000 hardware security module (HSM) is used in a banking environment.

A detailed understanding of how to operate the HSM and carry out key management duties.

In this training, students will develop the knowledge and practical skill needed to set up, deploy and maintain payShield Hardware Security Modules (HSMs) and maximize the value of these devices for your organization. In hands-on sessions, you will master common installation and administration tasks that prepare you to set up, use and manage payShield HSM devices in your own environment - from taking the device out of the box to configuring a fully functional system. Topics include configuration, installation, key management, smart card management, disaster recovery and maintenance. payShield Manager & payShield Monitor are also part of this course.

Designed for system administrators and application developers with a basic understanding of cryptography and key management, this class covers the role played by the payShield family of payment HSMs in securing transactions for financial applications along with best practices for rolling out these devices in your organization.

Course Agenda

- Payment World Introduction
- payShield HSM introduction
- Product Basics
- Product Configuration.
- payShield Manager
- Console Commands
- Client Configuration
- Host Functions
- Product Management
- Product Monitoring
- Magnetic Stripe and EMV Technology
- HSM Use Cases

DPoD (Data Protection on Demand) Certification Course

The Data Protection on Demand (DPoD) certification course provides a full overview of the platform, whether you are a service provider or a local administrator for your organization. In this training you will learn about the DPoD marketplace, the different use cases, success stories and integrations supported by the platform.

The course also provides a deeper dive into the technology behind DPoD, showcasing the different mechanism for enabling advanced features such as high availability, backup, logging and user management. If you are interested in migrating existing cryptographic data to or from DPoD you will find the necessary information in this training as well.

This certification course also includes various labs for different user roles to help you better understand the operation and maintenance revolving around the DPoD platform.

Course Agenda

- Introduction to the DPoD platform
- Detailed use cases
- Client configuration
- Roles in DPoD
- Product operation & configuration

General Purpose HSM Certification Course

The General Purpose HSM Certification course focuses on the main HSM types in use, and in particular, the SafeNet Luna Network HSM 7. The theoretical part of this course focuses on product description, solution architecture, deployment, and maintenance, while the practical sessions include product administration, integration, and troubleshooting. These are all hands-on sessions in which a Luna 7 HSM is installed and configured to demonstrate a working solution. Certification is granted after completing the course and passing the relevant certification exam.

Course Agenda

- Hardware Security Modules Overview
- Luna Product Family Overview
- Device Offering
- Order Information and Licensing
- Common Use Cases
- Device Architecture

- Usage Schemes
- Troubleshooting
- System Configuration
- Client Configuration
- High Availability
- Migration Methods
- Backup Methods
- Audit and Logging
- HSM Tools
- Functionality Modules
- APIs

Luna EFT HSM Certification Course

The Luna EFT HSM provides FIPS 140-2 Level 3-certified physical and logical protection to the cryptographic keys used to secure financial transactions. As a PCI-certified HSM, Luna EFT adheres to the highest level of security in the industry.

This course provides the student with the basics needed to install and integrate a Luna EFT HSM, as well as practical exercises in hands-on sessions. The course focuses on the setup of the Luna EFT appliance, EMV regulations support, and advanced options.

Course Agenda

- Introduction to the World of Electronic Payments
- Transaction Processing and Card Issuance
- Magnetic Stripe and EMV Technology
- Point-to-Point Encryption (P2PE) Overview (Derived Unique Key Per Transaction (DUKPT))
- Global Platforms
- Hands-on Labs (including writing and executing scripts to simulate a real-world environment)

ProtectServer 2 Certification Course

The ProtectServer 2 certification course is targeted towards an audience eager to learn how to work with Thales's ProtectServer platform. Starting from basic configuration and administration and building your way up to understand how to perform more complex operations and integrations, along with learning about and experimenting with functionality modules (Please note: this training does not cover coding tutorials on how to build FMs). You will learn more about the eco-system the ProtectServer lives in, how to operate the different toolkits for various environments (C, Microsoft, etc) and experience the simulation platform of ProtectServer.

Course Agenda

- ProtectServer Overview
- Device Offering
- Order Information and Licensing
- Common Use Cases
- Device Architecture
- Usage Schemes
- Troubleshooting
- System Installation and Configuration
- Basic Configuration
- High Availability
- Backup Methods
- Audit and Logging
- HSM Tools
- Functionality Modules

Data Encryption and Control Certification Courses

Thales's Data Encryption and Control solutions focus on data - providing persistent protection of sensitive data throughout its lifecycle, wherever it resides.

Information is protected at every moment - when it is created by an employee on a company laptop, shared with a business partner via email, stored in an enterprise database, processed by an application, or accessed by a field employee on a mobile device. Security extends from the data center and cloud computing environment to desktops, laptops, mobile devices, and removable media. Even if a device is lost, stolen, or misappropriated, its data remains protected from all unauthorized users.

Thales KeySecure appliances are at the heart of all Thales data encryption and control solutions, using hardware-based encryption or a virtual-based solution for cloud environments. KeySecure appliances deliver the highest level of data security available in a commercial solution, covering the broadest variety of data types. KeySecure offers a unified platform with data encryption and granular access control capabilities that can be applied to databases, applications, mainframe environments, and individual files. By providing centralized management of keys, policies, logging, auditing, and reporting functions, KeySecure simplifies management, helps ensure regulatory compliance, and maximizes security.

Vormetric Certification Course

The Vormetric Data Security Manager (DSM) and Vormetric Transparent Encryption (VTE) Certification course incorporates theoretical domain knowledge, as well as labs application guidelines, centering around the heart of Vormetric Data Security Platform products.

In this course, students will learn how the DSM creates, stores and manages the encryption keys that protect data, allows administrators to specify data access policies, administer DSM users and logical domains, generate usage reports, register new hosts, access security logs, manage third-party keys, digital certificates, and more.

Course Agenda

- Vormetric Solution Overview
- DSM and VTE Product Overview
- Users and Security Domains
- Policies and Keys for Transparent Encryption
- Securing Big Data
- Bring Your Own Key to the Cloud

The Vormetric Encryption solution consists of two major components:

- Vormetric Data Security Manager

- Vormetric Encryption Expert Agents

The flexibility and scalability of the Vormetric Encryption design stems from its separation of the Data Security Manager from the Encryption Expert Agents. The Data Security Manager provides centralized administration of encryption keys and data security policies, while the Encryption Expert Agents provide protection of structured and unstructured data stores that can include database and file server files, folders, documents, image scans, voice recordings, logs, and more.

KeySecure Certification Course

The KeySecure Certification course concentrates on Thales's KeySecure product suite, in particular, the available appliances, key and policy management and an overview of the solutions for databases, applications, and file servers.

In this three-day advanced course, students will focus on data center protection, including data center encryption, available appliances and integration with databases, applications and file system types.

Throughout the course the student will achieve a deep understanding of key and policy management and the process of database record encryption, encryption at the application layer and file encryption using the KeySecure solution.

The instructor will provide a feature overview and in depth technical analysis for each product and solution. This session is followed by a guided lab session in which the student will install and configure the products.

Course Agenda

- KeySecure Product Family Overview
- KeySecure Solution and Key and Policy Management
- Overview of Data Center and Endpoint Solution Suites
- Solution Integration
- Physical and Virtual Appliances
- KeySecure Licensing
- KeySecure Database Encryption
- ProtectDB and KeySecure for Database Security
- Database Encryption Process
- Use Cases for Database Encryption
- KeySecure Application Encryption
- ProtectApp and KeySecure for Application Security
- Application Encryption Processes

- Use Cases for Application Encryption
- KeySecure File Encryption
- ProtectFile and KeySecure for File Server Encryption
- Understanding Access Policies
- Use Cases for File Servers
- Tokenization Solution
- The need for Tokenization
- Tokenization Vs Encryption
- Secure Vaultless Tokenization

KeySecure k170v Certification

Thales's next generation SafeNet Virtual KeySecure product is the k170v model built on prevailing cloud-based technologies. The 170v provides a cloud friendly, key management solution with a REST interface and microservices based architecture. The k170v has been built to easily deploy and scale in a variety of enterprise environments.

This course focuses on the Thales k170v and the use and integration of all Thales connectors. The course sessions cover SafeNet k170v, ProtectApp, ProtectDB, Protect File, Tokenization manager.

Throughout the lab sessions, students will practice various security solutions and encryption based solutions in order to protect any sensitive data in a physical environment or cloud based environment.

Course Agenda

- Keysecure Overview, Product history, new features and design
- Dockers containers, Micro services.
- REST API's, ksctl
- k170s Installation and configuration
- Advanced Administration, Advanced Features Bluetooth solutions
- ProtectApp, ProtectDB, Protect File, Tokenization manager installation and configuration

Network Encryption Security Certification Course

Thales's high-speed WAN encryptors provide the fastest, simplest, and easiest way to integrate network security solutions for enterprise and government organizations that need to protect mission-critical data.

With organizations expanding and becoming more geographically dispersed, the global collaboration between partners, suppliers, and customers is forcing a requirement for secure and transparent high-speed communications across the network. Enterprise network and security engineering groups must reach an appropriate balance between enabling communication while securing corporate information.

With proven reliability, scalability, highest throughput and lowest latency, Thales's network security devices are the ideal solution for protecting massive amounts of data in motion (including time-sensitive voice and video streams) and are designed to integrate seamlessly into a network topology and provides full crypto agility.

In this two-day course, students will participate in classroom sessions in which the instructor will provide information on the available network encryption products, the solution's architecture, considerations for installation and configuration and management options. The classroom session is followed by guided lab sessions in which the student will install and configure the network encryption products.

Course Agenda

- Network Essentials for Understanding WAN Encryption
- Thales Encryption Products Review
- Product Features and Architecture
- Deployment Considerations
- Encryptor Configuration and Management
- Certification and Key Management
- Management options and best practice

ProtectV Certification Course

Thales's ProtectV solution is the industry's first comprehensive high-availability solution for protecting data in the cloud. ProtectV enables you to unify encryption and control across virtualized and cloud environments, improving your business agility and lowering your costs by securely migrating even your most private, highly regulated data to the cloud. Organizations can be safe in the knowledge that they retain access to and control of encryption keys at all times.

In addition, ProtectV enables organizations to address the specific security and compliance requirements in cloud environments.

In this two-day course, the instructor will focus on a high-level overview of virtualization and cloud environments, ProtectV operation in VMware environments and Amazon Web Services (AWS), an in-depth architecture overview of the ProtectV solution and more.

Course Agenda

- Virtualization and Cloud Environments
- ProtectV Solution Components and High-Level Architecture Deployment Considerations
- Different platforms:
    - AWS
    - Microsoft Azure
    - VMWare
- Virtualization platform overview for PV
- ProtectV solution components and high level architecture
- KeySecure Appliance Overview
- KeySecure Integrations
- Preparing KeySecure for ProtectV
- ProtectV and VMWare
- ProtectV and Microsoft Azure
- Securing AWS with ProtectV
- ProtectV Manager Administration
- ProtectV Manager HA
- ProtectV Manager RESTAPI
- KeySecure Monitoring and Logging
- ProtectV Client Architecture
- ProtectV Client Images on Windows and Linux Platforms
- ProtectV Manager Architecture
- Key Hierarchy for ProtectV and KeySecure

Contact Us

For all office locations and contact information, please visit thalesgroup.com.

January, 2020