HSM TRAINING

Upgrade Your Hardware Security Module (HSM) Skills with Training from Encryption Consulting LLC

Class Audience ›› Beginners | Intermediate | Advanced

About The Course

Our HSM Training is tailored for individuals seeking expertise in setting up, deploying, and monitoring Hardware Security Modules (HSMs) from nShield, Thales Luna 7, Utimaco, and Cloud HSMs. Our course adopts a hands-on approach to provide a deep understanding of HSM cryptographic operations. Throughout the course, attendees cover foundational cryptography concepts, master the management of HSMs, and engage in real-world scenarios illustrating HSM use cases.

We take a vendor-agnostic approach to train you to set up, deploy, and monitor nShield and Thales Luna Hardware Security Modules (HSMs)

Why Attend Our HSM Training?

In-Depth Knowledge: Dive into the core concepts of HSMs and understand their role in securing sensitive data.

Hands-on Experience: Learn from seasoned professionals with 20+ years of consultation experience and leverage their hands-on expertise from various industries.

Tailored Learning: We offer customizable training dates for groups of 3 or more attendees to ensure a personalized learning journey.

Vendor-Agnostic Approach: Our training helps to navigate diverse HSM systems, enhancing adaptability and market relevance.

nShield
Course Breakdown

Hands-on expertise in setup, key management, and troubleshooting.

Module 01: Introduction to PKI

- Module Overview
- Module Agenda
- Basics of Cryptography
- What is Cryptography?
- Types of Cryptography
- Symmetric Key Cryptography
- Asymmetric Key Cryptography
- Symmetric vs Asymmetric Key Cryptography
- Hybrid Encryption
- Hash Function
- Digital Signatures
- Where to use Cryptography?
- Public Key Infrastructure (PKI)
- Digital Certificates

Module 02 - Introduction to the nShield HSM

- Module Overview
- Module Agenda
- Introduction to HSMs
- What is an HSM?
- Why do you need an HSM?
- HSM vs Software-based solution
- FIPS 140-2 Compliance
- FIPS 140-2 Level 3
- Integration of HSMs
- PKI with HSM
- IoT with HSM
- Code Signing with an HSM
- Cloud Services with an HSM
- TLS/SSL Environments with an HSM
- Introduction to the nShield Family
- The nShield Family
- Portable USB HSM
- PCIe Embedded HSM
- Network Attached HSM
- nShield as a Service (nSaaS)
- Security World and Card Sets
- Security World
- Card Sets

Module 03 - Configuration and Setup

- Module Overview
- Module Agenda
- nShield Client Software Installation
- nShield Software Architecture
- Installation Steps
- Important File Locations
- Client Considerations
- Basic HSM Configuration
- nShield Connect Front Panel
- HSM Network Configuration
- RFS Configuration
- Purpose of RFS
- Setup RFS
- Setup Autopush
- Export HSM Log to RFS
- HSM Clients
- Client Features
- Enrolling Clients using Front Panel
- Nethsmenroll command
- Lab Exercise 1

Module 04 - Security World and Keys

- Module Overview
- Module Agenda
- About FIPS Mode
- What is FIPS Mode?
- FIPS Mode Drawbacks
- Security Worlds and Creation
- Security World Settings
- ACS K:N Considerations
- Creating a Security World
- Loading a Security World
- Operational Modes and Utilities
- nShield Edge
- nShield Solo
- Command Line Module
- Enquiry Utility
- Nfkminfo Utility
- Application Keys and OCS Card Creation
- Application Key Tokens
- Key Protection
- Operator Card Sets (OCS)
- Key Generation - OCS cards
- Key Generation using Keysafe
- Lab Exercise 2

Module 05 - HSM Administration and Upgrades

- Module Overview
- Module Agenda
- About Remote Administration
- Remote Operator vs Remote Administrator
- Remote Administration
- Dynamic Slots
- Authorized Card List
- Firmware Update
- Firmware Update Considerations
- Firmware Update Warning
- Identifying & Updating Firmware
- Updating nShield Connect
- Remote Upgrade - Front Panel
- Remote Upgrade - Command Line
- Disaster Recovery
- Passphrase Recovery
- Administrator Cardset Recovery
- Replace OCS/Key Recovery
- Rocs Utility
- KeySafe
- KeySafe Software

Module 06 - Advanced HSM Features

- Module Overview
- Module Agenda
- Load Sharing
- What is Load Sharing?
- HSM Pool Model
- PKCS#11 Library
- Feature Activation
- Optional Features
- Available Features
- Enable Features - PCIe & USB HSM
- Enable Features - Network HSM
- Loading Features Remotely
- CodeSafe
- What is CodeSafe?
- CodeSafe Application

Luna
Course Breakdown

Master deployment, configuration, and security best practices.

Module 01: Introduction to PKI

- Module Overview
- Module Agenda
- Basic Cryptographic Principles
- What is Cryptography?
- Types of Cryptography – Symmetric Key Cryptography
- Types of Cryptography – Asymmetric Key Cryptography
- Types of Cryptography – Hash Function
- Public Key Infrastructure (PKI)
- Digital Certificates
- Hardware Security Module (HSM)
- Introduction to HSM
- Why do we need an HSM?
- Risks of Storing Keys in Software or Outside an HSM
- Certifications FIPS 140-2 Level 3
- FIPS 140-2 Level 3
- HSM Integrations
- Integrating PKI with HSM
- Integrating IoT with HSM
- Integrating Code Signing with HSM
- Integrating Cloud Services with HSM
- Integrating TLS/SSL Environments with HSM
- Luna HSM Product Line
- Introduction to Luna HSM Product Line
- Luna Network HSM
- Luna PCIe HSM
- Luna Network HSM & Luna PCIe HSM Models
- Luna USB HSM
- Data Protection on Demand Services
- Luna Backup HSM

Module 02 - Multifactor Quorum Authentication

- Module Overview
- Module Agenda
- Introduction to PED
- What is the PED?
- Password vs PED
- Luna PED & PED Keys
  Luna PED
- PED Keys
- Types of PED Keys
- PED Keys – “M of N Quorum”
- Remote PED
- Introduction to Remote PED
- PED Key Best Practices
- Introduction to PED Key Best Practices
- Package Verification & Secure Transport Mode
- Package Verification
- Secure Transport Mode
- Lab Exercise

Module 03 - HSM Management & Configuration

- Module Overview
- Module Agenda
- Licensing
- Licensing – Partitions
- Licensing – Clients
- Licensing – Package & Installation

  Luna Network HSM Management
- Introduction to Luna Network HSM Management
- Appliance Users
- Introduction to Appliance Users
- Recover Account
- HSM Roles
- Separation of Duties
- HSM Configuration
- HSM Initialization
- Policies & HSM Capabilities
- Partitions
- What are Partitions?
- Partitions Cloning Domains
- Partition Multitenancy
- Partition – Level Roles
- Partition Viewing, Creation Activation & Sizing
- Partition Utilization Metrics (PUM)
- FIPS Operational Mode
- Lab Exercise 3

Module 04 - Luna Client

- Module Overview
- Module Agenda
- Luna Client
- What is Luna Client?
- Luna Client Compatibility
- Luna Client Utilities

  Luna Client LunaCM
- Luna Client VTL
- Luna Client CKDemo , CMU & Multitoken
- Chrystoki – Client Configuration File
- Luna Minimal Client – Docker
- Client Network Authentication
- NTLS – Network Trust Link Service
- Introduction to NTLS
- NTLS Certificates
- NTLS IPCheck
- NTLS High Level Steps
- STC – Secure Trusted Channel
- Introduction to STC
- STC Identities
- STC Security
- STC Security Parameters
- NTLS vs STC

Module 05 - Product Administration

- Module Overview
- Module Agenda
- HSM Backup
- Introduction to HSM Backup
- HSM Backup Flexibility
- HSM Backup Best Practices
- Luna Backup HSM (B7XX Series)
- Local, Remote & Cloud Backup
- Local Backup
- Remote Backup
- Remote Backup Services (RBS)
- Luna Cloud HSM - Backup Services
- Appliance Configuration Backup
- High Availability & Load Balancing
- Introduction to High Availability & Load Balancing
- High Availability
- Load Balancing
- High Availability – Replication
- High Availability – Failover
- High Availability – Recovery
- High Availability – Synchronization
- High Availability – Standby
- High Availability – Only Mode
- Key Migration
- Migrating to Luna 7
- Clustering
- Introduction to Clustering

Module 06 - HSM Auditing & Security

- Module Overview
- Module Agenda
- HSM Audit Logging
- Introduction to HSM Audit Logging
- HSM Audit Logging - Audit Officer
- HSM Audit Logging – Integrity
- HSM Audit Logging – Performance
- HSM Audit Logging – Time Sync
- HSM Audit Logging – Categories
- HSM Audit Logging – Log Secret
- HSM Audit Logging – Rotation
- HSM Audit Logging – Disk Full
- HSM Audit Logging – Sample
- Monitoring & Logging
- Introduction to Monitoring
- Log Categories & Severity
- Remote Logging
- Simple Network Management Protocol (SNMP)
- Appliance Status Codes
- Status Codes – ISO
- Status Codes – IST
- Status Codes – OOS
- Tamper Events
- Introduction to Tamper Events
- Tamper Events – Policies
- Upgrades
- Software & Firmware Upgrades
- Reimaging the Appliance
- Lab Exercise

Module 07 - Advanced Configurations

- Module Overview
- Module Agenda
- Luna SDKs & APIs
- SDK & API
- Slots and Sessions
- JSP (Java Service Providers)
- Label vs Slot
- JSP Setup
- Crypto Officer vs Crypto User
- Application Object Handler
- Microsoft Interfaces
- FM - Functionality Module
- Introduction to FM
- FM – Hardware
- FM – Policies
- FM – Secure Memory File Systems
- Impact of FM
- FM SDK and Utilities
- SKS & PKA
- SKS – Scalable Key Storage
- SKS and SMK
- PKA – Per Key Authorization
- REST API & CCC
- REST API
- CCC – Crypto Command Center
- Lab Exercise 7

Certificate of Completion

Every student that attends and completes the full training scoring 70% in the HSM exam will receive a certificate of completion. The certificate will allow student to qualify for ISC2 continuing education credit for annual CPE commitments.

What Our Students Say

The EC training for nShield HSMs (xc-Mid) was a good and thorough experience. I was able to clearly see and practice through the use and configuration of Security Worlds, HSM configurations using both command line and panel controls, deployment, the use and management of keys and cryptography, use and connectivity of an RFS server, creation and management of the ACS and OCS card sets, adding, enrolling and configuring clients.

Bill Sites
Pfizer (Senior PKI Manager)

I am delighted to recommend Encryption Consulting HSM Training Course. I completed this course while serving as a Principal Security Consultant at BlueCross BlueShield of Tennessee. This course provided me with critical insights and advanced skills in implementing | designing and configuring Hardware Security Modules. The training was comprehensive and practical, covering critical aspects of HSM deployment, configuration, and management. The hands-on experience and real-world applications were particularly valuable, enabling me to implement robust security measures effectively in my organization. As a result of this training, I was able to strengthen our enterprise data protection strategies and ensure compliance with industry standards.

Michael Audu
BlueCross BlueShield (Principal Cybersecurity Engineer)

Contact Us

- info@encryptionconsulting.com
- +1- 469-815-4136

ENCRYPTION
CONSULTING

Global Headquarters 130 N Preston Rd,
Prosper, TX 75078, USA