

Course Title: Luna HSM Professional Certification Course

Duration: 5 Days (40 Hours)

Training Mode: Theory + Hands-on Live Labs

Day 1 – Introduction & Foundation of Luna HSM

Module 1 – Fundamentals of Hardware Security Modules (HSM)

- What is an HSM? Use cases and industry adoption
- Cryptographic Offloading vs Key Security
- PKCS#11, JCE, KMIP, REST – overview of APIs
- Role of HSM in Banking, PKI, IoT, Authentication and Blockchain

Module 2 – Luna HSM 7 Product Line Overview

- Luna Network HSM 7 architecture
- Models, capacities, performance specs
- Luna Password-Authenticated vs PED-Authenticated models
- HSM High Availability concepts

Module 3 – Luna HSM Concepts and Architecture

- Partitions, Crypto Officer, Crypto User
- Domains, cloning, replication

- HA Cluster Design Concepts
- FIPS 140-2/3 standards and compliance

Hands-on Lab:

Activate and explore Luna appliance management interface (CMU & WebUI). Initial HSM discovery.

Day 2 – Deployment & Initialization

Module 4 – Luna HSM Setup & Installation

- Physical and network configuration
- Luna Client installation (Windows & Linux)
- Firewall & routing requirements for HSM

Module 5 – HSM Initialization & Authentication Methods

- HSM initialization workflow
- PED Authentication: Blue, Black, Red PED keys
- Password-based authentication & PIN policies
- Secure Remote PED Configuration

Module 6 – Partition Creation and Assignment

- Creating, assigning and activating partitions
- Role creation: SO, CO, CU
- Exporting / importing client certificates

Hands-on Lab:

Initialize HSM, configure authentication, create partition and register clients.

Day 3 – Crypto Services & Application Integration

Module 7 – Key Management and Crypto Objects

- Key generation, storage, wrapping and destruction
- Persistent and session keys
- RSA, ECC, AES, SHA — supported algorithms
- Key backup & cloning between partitions

Module 8 – Application Integration with Luna HSM

- Using PKCS#11, JCE & OpenSSL with Luna
- Integrating Luna with:
 - Apache / Nginx TLS Offloading
 - MS CA / EJBCA / Keycloak
 - Database encryption modules (Oracle / MS SQL / MySQL)

Module 9 – Load Balancing and High Availability

- Creating an HA group
- Failover, resync and cluster monitoring
- Session and persistent key considerations

Hands-on Lab:

Generate RSA/ECC keys via Luna; integrate Luna with Apache HTTPS offloading; configure HA cluster with 2 partitions.

Day 4 – Backup, Security Controls & Maintenance

Module 10 – Backup and Recovery

- Luna Backup HSM & Secure Backup tokens
- Remote Backup options
- Recovery testing & business continuity checklist

Module 11 – Security Hardening & Audit

- Secure boot & firmware lifecycle
- Syslog & SNMP monitoring
- Network lockdown, SSH hardening, dual control & quorum settings
- Compliance requirements – PCI-DSS, GDPR, RBI, NIST

Module 12 – Troubleshooting & Diagnostics

- Luna logs and diagnostics commands
- Common errors & failure scenarios
- Client connectivity troubleshooting
- PED link & authentication failures

Hands-on Lab:

Backup HSM partition, restore keys to a new partition, log analysis and troubleshooting scenarios.

Day 5 – Advanced Operations & Certification Assessment

Module 13 – Multi-Site & Cloud Deployments

- Multi-site key replication
- Cloud HSM hybrid deployment
- Integration with DPoD (Luna Cloud HSM)

Module 14 – DevOps & Automation

- Scripting and automation with Luna CLI
- REST & KMIP integration
- Ansible / Terraform automation use cases

Module 15 – Real-World Use Cases & Final Evaluation

- PKI deployment case study
- Banking / Tokenization / UPI-style HSM scenarios
- Blockchain wallet key hardening
- Final certification practical + MCQ exam

Hands-on Lab:

Deploy automated key lifecycle management using scripts. Restore backup to cloud partition and validate access.