Thales nShield Certified Systems Engineer (nCSE)
Technical Accreditation Course

Ziel und Zielgruppe:

Die Schulung gibt einen Überblick über die Thales-Produktserie “nShield”. Thematisiert werden u.a. die grundsätzliche Funktionsweise, die System-Architektur sowie Installation und Konfiguration von nShield-HSMs (Hardware Security Module). In praktischen Übungen werden die Themen Installation, Konfiguration und Desaster-Recovery vertieft.

Die Teilnahme an der Schulung vermittelt u.a. folgende Fähigkeiten:

- Vollständige Konfiguration eines nShield-HSMs für den Einsatz in einer Security World
- Erstellung und Wartung einer Security World
- Erstellung und Verwaltung von Administrator- und Operator-Card-Sets (OCS und ACS)
- Schlüsselerzeugung im HSM mittels Kommandozeile
- Kenntnisse über die wichtigsten Kommandozeilen-Befehle

Die Schulung richtet sich in erster Linie an Administratoren und Projektmitglieder und vermittelt alle grundlegenden Kenntnisse, die für den operativen Betrieb von nShield-HSMs notwendig sind.
Für die Teilnahme an der Schulung existieren keine formalen Voraussetzungen, Grundlagenwissen im Bereich Kryptographie ist aber hilfreich.

Die Schulung endet mit einer schriftlichen Prüfung und, sofern diese bestanden wird, mit der Zertifizierung zum nShield Certified Systems Engineers (nCSE).

Rahmen:

Schulungsumfang: 2 Tage
Teilnehmer: Max. 4 Personen
Uhrzeit: 09:30 - 18:00 Uhr
Ort: Düsseldorf
Sprache: Deutsch (Lehrmaterialien: Englisch)
Schulungsgebühr: 2.600 Euro / Person (inkl. Gebühren für Prüfung und Zertifizierung durch Thales)
1.950 Euro / Person (bei Verzicht auf Prüfung und Zertifizierung)

Schulungsinhalte:

1. Einführung & Thales-Firmenporträt

- nShield und Thales: Historie und Märkte
- Produkt-Architektur

2. Grundlagen der Kryptographie und PKI

- Symmetrische Kryptographie
- Asymmetrische Kryptographie
- Digitale Signaturen
- Digitale Zertifikate und PKI

3. Hardware Security Modules (HSMs)

- Grundlagen – Was sind Hardware Security Modules?
- nShield Connect (Appliance)
- nShield Solo (Einsteckkarte)
- nShield Edge (USB)

4. Hardware Security Modules - Anwendungsfälle

- PKI
- Transparente Verschlüsselung von Datenbanken
- SSL / TLS

5. Security World

- Security World – Einführung und Konfiguration
- Operator Cardsets (OCS) und Administrator Cardsets (ACS)
- Mehr-Augen-Prinzip
- Keyblobs
- Schlüssel-Erzeugung
- Schlüssel-Verteilung
- Schlüssel-Hierarchie und -Management

6. Installation und Konfiguration

- Front-Panel-Menü (nShield Connect)
- Betriebsmodi und Kommandozeilen-Tools

- Installation der Software

7. Erstellung und Konfiguration einer Security World

- Erstellen / Laden einer Security World auf einer Connect
- Erstellen / Laden einer Security World auf einer Solo / Edge

8. Wartung und Disaster-Recovery

- Update von Firmware und Client-Software
- Grundlagen SNMP-Monitoring
- Ersetzen eines ACS
- Ersetzen eines OCS

9. Optionale Features

- Remote Operator
- Secure Execution Environment (SEE) / Codesafe

Praktischer Teil (1)

- Anbindung eines Clients an eine nShield-Connect
- Aufbau und Konfiguration eines RFS (Remote File System)
- Hinzufügen von Clients
- Aktivieren von Features
- Exportieren von Log-Files

Praktischer Teil (2)

- Installation der Client-Software (Windows)
- Erstellung und Administration einer Security World auf einer Connect (mittels Front-Panel und CLI)
- Erstellung eines OCS
- Erstellung von Schlüsseln

Praktischer Teil (3)

- Disaster-Recovery
  - Zurücksetzen eines OCS-Passwortes
  - Ersetzen eines OCS
  - Wiederherstellung im Fehlerfall