

Security mit CANoe.Ethernet und Security Manager

Agenda VectorAcademy

Lernformat:	Dieser Kurs wird als Remotekurs angeboten
Dauer:	5h
Zielgruppe:	Erfahrene CANoe.Ethernet Anwender im Kfz/Nfz
Voraussetzungen:	Gute CANoe und CANoe.Ethernet Kenntnisse inklusive der Basisprotokolle (OSI Layer 1-4) und Anwendungsprotokolle (DoIP, SOME/IP, AUTOSAR PDU)
Ziel:	Überblick und Einordnung der gängigen Security Mechanismen und Protokolle für TLS/DTLS und IPsec. Kenntnisse zu den Phasen während einer sicheren Kommunikation und zu verwendeten Unterprotokollen. Vorgehensweise und praktische Umsetzung beim Messen, Simulieren und bei der Fehlersuche mit CANoe (Umsetzung von Security in AUTOSAR ist nicht Bestandteil dieses Workshops).

1. Einführung

- > Hauptziele der Security
- > Automotive Cyber Security im OSI Schichtenmodell
- > Aufgaben, verwendete Methoden, Algorithmen und Protokolle im Überblick

2. Security Grundlagen

- > Symmetrische und asymmetrische Kryptografie
- > Hashing, Message Authentication Code und Signaturen
- > Zertifikate, Key Exchange und Cipher Suite

3. Security durch CANoe.Ethernet und dem Security Manager

- > Vector Security Manager und sein CANoe Client
- > Public Key Infrastructure
- > Typische Anwendungsfälle beim Messen, Simulieren und Offline-Analyse

4. Transport Layer Security (TLS) und Datagram TLS (DTLS)

- > TLS/DTLS Phasen und verwendete Unterprotokolle
- > TLS/DTLS in der Praxis mit CANoe und dem Security Manager
- > Authentifizierung durch Zertifikate
- > Übungen zu verschiedenen Anwendungsfällen
- > Beispiele für unterschiedliche Realisierungsmöglichkeiten

5. IPsec im Transport Mode mit Authentication Header

- > Aufbau einer Security Association mit IKEv2 Protokoll
- > Sichere Datenübertragung mit Authentication Header im Transport Mode
- > Übung: Security Profil und Simulation mit CANoe