Stand 11.05.2026

Hardware Security Module (HSM) der AURIX™-Plattform - Live-Online-Training

**Ziele -
Ihr Nutzen**

Sie kennen die Architektur, die On-chip-Peripherie und die Besonderheiten (insbesondere systemrelevante Beziehungen zur Host-Seite) des HSM-Moduls der AURIX™ Familie.

Sie können Low-Level-Treiber für diese Hardware schreiben und einsetzen und Interaktion mit der Host-Seite betreiben, Beispiele für Ihre Zwecke adaptieren und mit einem Debugger testen.

Demos und Übungen vertiefen die theoretischen Inhalte.

Ihre Vorteile:

Effektiver und zeitsparender Einstieg in die Gesamtthematik

Systemweiter Ansatz

Elektronische Unterlagen

Teilnehmer

Hardware- und Software-Architekten, Hardware- und Software-Entwickler, Testingenieure, Funktionsentwickler, Systemdesigner

Voraussetzungen

HSM-NDA mit Infineon; Erfahrung mit Programmierung und Aufbau eines Mikroprozessor-/Mikrocontrollersystems; Security-Basiswissen; AURIX System-Kenntnisse (idealerweise durch vorherigen Besuch unseres AURIX-2G Trainings)

Live Online Training

* Preis je Teilnehmer, in Euro zzgl. USt.

Anmeldecode: L-HSM

Präsenz-Training - Deutsch

Termin	Dauer
18.06. – 19.06.2026	2 Tage

Live-Online - Englisch

Dauer
2 Tage

Präsenz-Training - Englisch

Termin	Dauer
18.06. – 19.06.2026	2 Tage

Stand 11.05.2026

Hardware Security Module (HSM) der AURIX™-Plattform - Live-Online-Training

Inhalt

Introduction

Inside Hardware Security Module

CPU Subsystem Overview

System Aspects (Configuration, Boot, Reset, Debug)

Bridge

Timer Module and Watchdog

True Random Number Generator

Hash Module

Advanced Encryption Standard - 128 Bit (AES-128)

Public Key Cryptography (PKC) Module

HINWEIS:

Für die Teilnahme an diesem Training ist ein gültiges HSM-NDA (Non-disclosure Agreement) mit Infineon erforderlich.