Stand 03.07.2024

Hardware Security Module (HSM) of the AURIX™ Platform - Live Online Training

**Ziele -
Ihr Nutzen**

You know the architecture, on-chip peripherals and features (especially related to the host aspects) of the HSM module of the AURIX™ device family.

You get to write and apply low-level drivers for this hardware, interact with the host, adapt examples as required and test them with a debugger.

Numerous demos and exercises intensify the theoretic content.

YOUR BENEFIT:

Efficient and compact jump-start into the overall topic

System-wide approach

Training documentation in electronic format

Teilnehmer

Hardware and software architects, hardware and software developers, test engineers, design engineers, system designers

Voraussetzungen

HSM NDA (non-disclosure agreement) with Infineon; experience in microcontroller/microprocessor system programming and architecture; basic security knowledge; AURIX system knowledge (ideally, based on our AURIX-2G training)

Live Online Training

30.01. – 31.01.2025	1.500,00 €	2 Tage

* Preis je Teilnehmer, in Euro zzgl. USt.

Anmeldecode: LE-HSM

Präsenz-Training - Englisch

Termin	Dauer
05.09. – 06.09.2024	2 Tage

Live-Online - Deutsch

Termin	Dauer
30.01. – 31.01.2025	2 Tage

Präsenz-Training - Deutsch

Termin	Dauer

Stand 03.07.2024

05.09. – 06.09.2024 2 Tage

Hardware Security Module (HSM) of the AURIX™ Platform - 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

IMPORTANT NOTE:

A valid HSM NDA (non-disclosure agreement) with Infineon is a pre-requirement to attend the course.