Optimum Protection of AUTOSAR ECUs with a Hardware Security Module

Case Study Firmware for Hardware Security Modules (vHSM)

The Challenge
Improving cybersecurity with efficient and secure firmware for hardware security modules.

With the increasing degree of networked ECUs and vehicles, the demands on data security are also increasing. The development of a secure E/E architecture in the vehicle requires, among other things, complex cryptographic calculations in the ECUs. For this purpose, semiconductor manufacturers integrate Hardware Security Modules (HSM) into their microcontrollers, which accelerate these calculations and represent a Hardware Trust Anchor (HTA). This serves as a trustworthy source of cryptographic calculations. To use these HSMs, a firmware is required that could be seamlessly used in an AUTOSAR ECU project and securely operated using standard interfaces.

The Solution
The firmware vHSM from Vector.

Vector has developed the firmware vHSM on the basis of its extensive experience in cybersecurity and AUTOSAR basic software. vHSM controls the HSM and is interfaced by the AUTOSAR 4.3 stack on the application side via a standardized crypto driver interface. vHSM is part of the Vector AUTOSAR solution and available for various microcontrollers.

Features and functions:
> Isolated execution of cryptographic functions, e.g. basic cryptographic functions as well as symmetrical and asymmetrical procedures, using hardware accelerators such as AES or TRNG.
> Functions for the isolated storage of secrets and key material.
> Secure Boot support: A chain of trust is established by interacting with a Flash Bootloader (FBL).
> Providing a Security Event Memory.
> Debugging capabilities during development by delivering source code.

The Advantages
vHSM offers more security and efficiency than a pure software implementation on the application side.

> Increased security with better performance and isolation of cryptographic calculations by using dedicated hardware.
> Great flexibility through modular and extensible software. The software can easily be adapted to special requirements and functions.
> Increased security by using a library of state-of-the-art algorithms for cryptographic procedures and for key derivation.
> Secure storage of secrets such as key material, certificates, mileage, without exchange of secrets between application and hardware security modules.
> Seamless interaction with AUTOSAR basic software and Flash Bootloader for applications such as Secure Boot, Secure OnBoard Communication (SecOC) and code signing.

Integration of the vHSM firmware in an AUTOSAR and FBL environment.