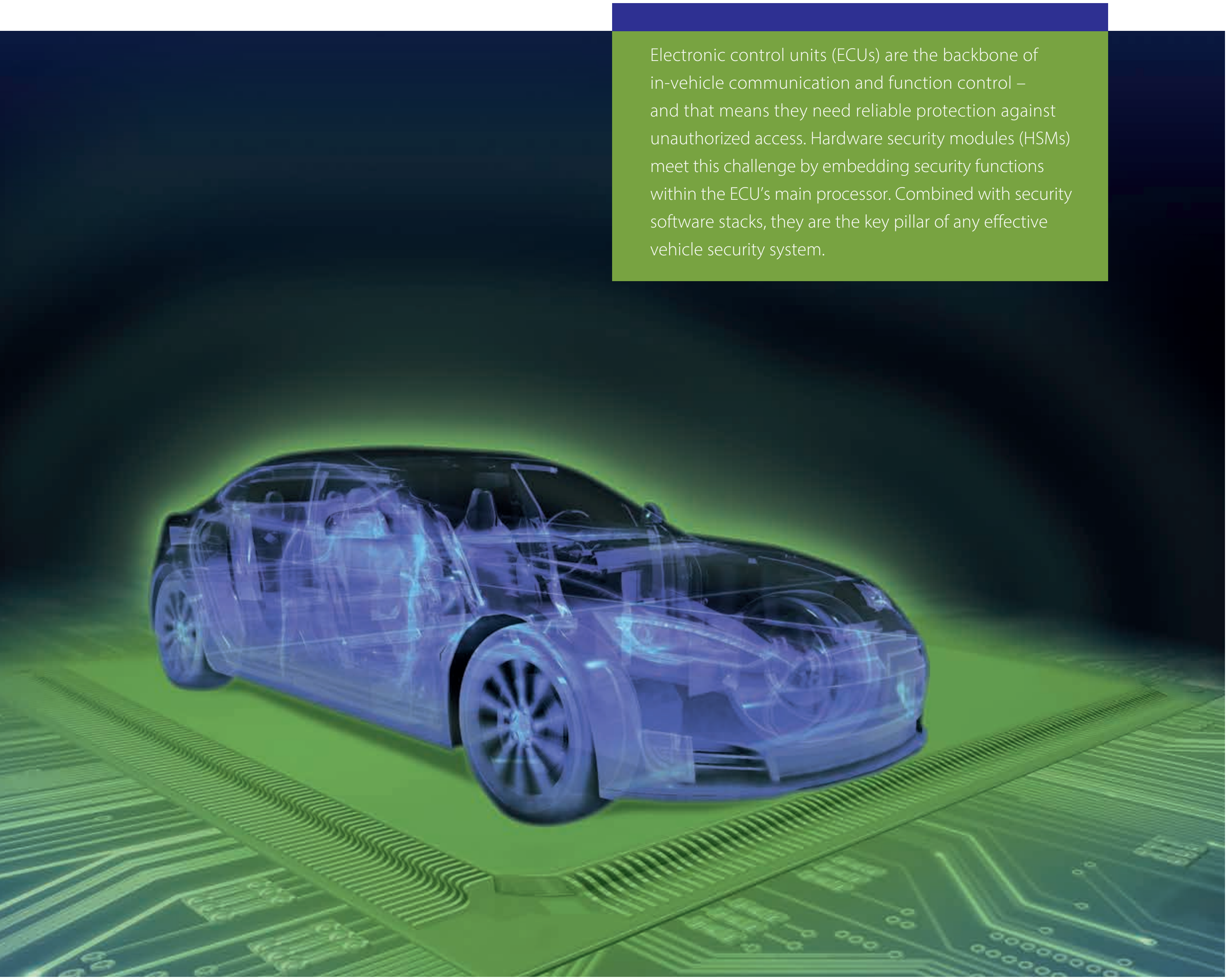
Automotive security from the inside out

Hardware security module (HSM) offers protection inside ECU's main processor

Electronic control units (ECUs) are the backbone of in-vehicle communication and function control – and that means they need reliable protection against unauthorized access. Hardware security modules (HSMs) meet this challenge by embedding security functions within the ECU's main processor. Combined with security software stacks, they are the key pillar of any effective vehicle security system.



When chip tuners access powertrain ECUs to modify system parameters, noise and emissions restrictions are the last thing on their mind. Yet perhaps even more unsettling is the very idea that they can access electronically controlled vehicle systems in the first place.

The problems that a malicious hacker could cause in a powertrain or chassis ECU simply do not bear thinking about. Every ECU in a vehicle's electrical system is a potential target, especially when it comes to connected vehicles. To prevent unauthorized software manipulation and access to critical key material, modern vehicles need robust IT security mechanisms to shield them from the outside world. That's exactly what hardware security modules (HSMs) do by implanting security functions right at the heart of ECUs.

Automotive-specific HSMs

HSMs are a form of hardware that physically encapsulates security functions. Specifically designed for IT security applications, these integrated chips typically have their own processor core, various types of memory (e. g., RAM, ROM, flash), and hardware crypto accelerators. HSMs must also meet specific standards for use in vehicles, and highly efficient integration is essential to keep costs down. Key requirements include secure interfaces between the ECU application and the HSM as well as debugging and testing interfaces for analyzing malfunctions. HSMs must be able to process cryptographic information with minimal latency and exhibit adequate resistance to the typical temperatures found in automotive environments.

Several leading chip manufacturers already offer hardware security modules with automotive-grade architecture, including Infineon, ST Microelectronics, Renesas, and NXP. Essentially, the HSM uses its own processor core to provide all the IT security functions required for automotive use cases. These include a 128-bit AES hardware accelerator, a true random number generator (TRNG) to generate key material, hardware-protected storage of cryptographic keys, flash and debugging functions, and the HSM's own RAM that is separate from system memory (see Figure 1).

Tailored security software and real-time communication

An automotive HSM only really comes into its own in combination with a secure software stack. If the HSM is the nucleus of vehicle IT security, then HSM security software is its genetic code. ESCRYPT provides this in the form of its CycurHSM security firmware, which is specifically tailored to automotive HSMs from a range of manufacturers. CycurHSM links the existing hardware security peripherals to the relevant HSM and host controller applications. The firmware also implements a comprehensive cryptographic library on the HSM including symmetric and asymmetric encryption mechanisms and additional HSM-based security functions. CycurHSM also includes the AUTOSAR-compliant and non-AUTOSAR-compliant interfaces required to integrate HSMs in standard vehicle ECUs.

The core element of the software architecture is a real-time operating system. This ISO 26262-certified system is specifically

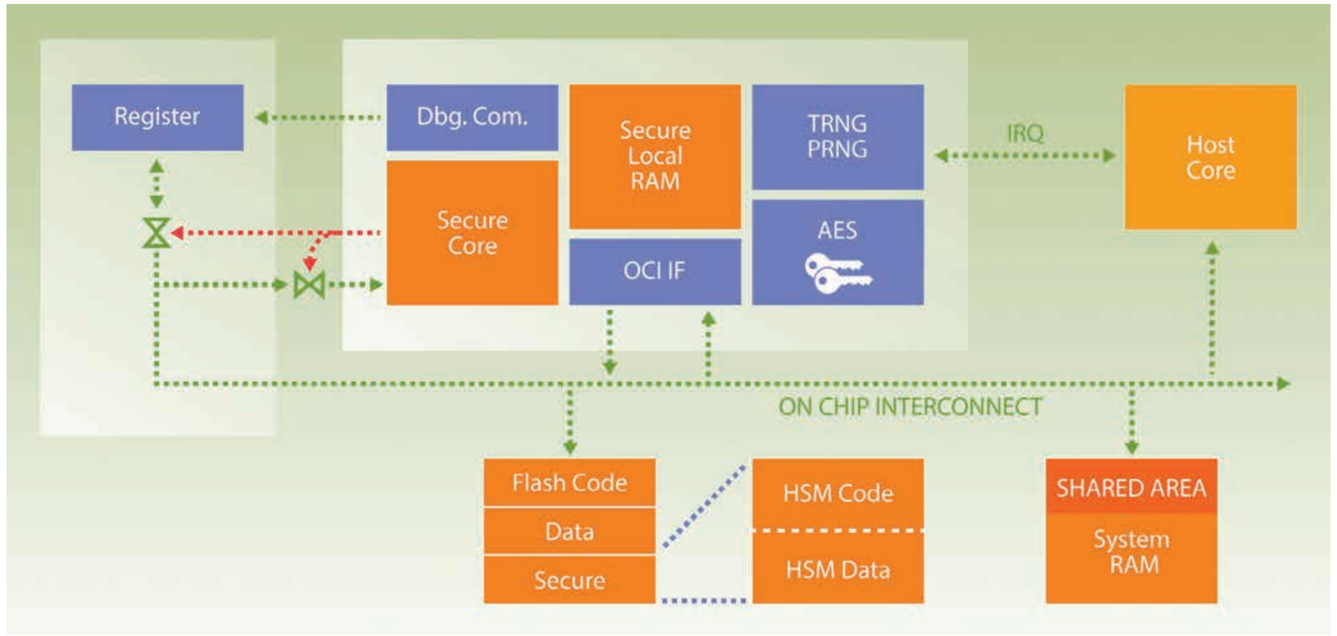


Figure 1: Hardware architecture of the hardware security module (HSM)

tailored to automotive ECUs and supports real-time HSM functions such as secure in-vehicle real-time communication. The operating system works with minimal runtime overhead and is MISRA-C-compliant. CycurHSM includes a session manager that implements priority-based task scheduling. For example, the validation of new messages on the vehicle bus takes priority over non-time-critical operations. It also incorporates a keystore manager that governs both access to and generation, storage, and deletion of key material in the HSM and supports symmetric and asymmetric keys of different lengths. The cryptographic library (CycurLIB) provides the cryptographic primitives (ECC, RSA) using the HSM's crypto accelerator. Where required, a SHE emulation can also be run on the HSM while accessing the cryptographic library in order to meet enhanced automotive-specific requirements (SHE+). In addition, dedicated HSM drivers secure communication between the HSM and host processor: an AUTOSAR-compliant crypto service manager (CSM) at the interface to the HSM ensures that AUTOSAR applications can access the module at any time (see Figure 2).

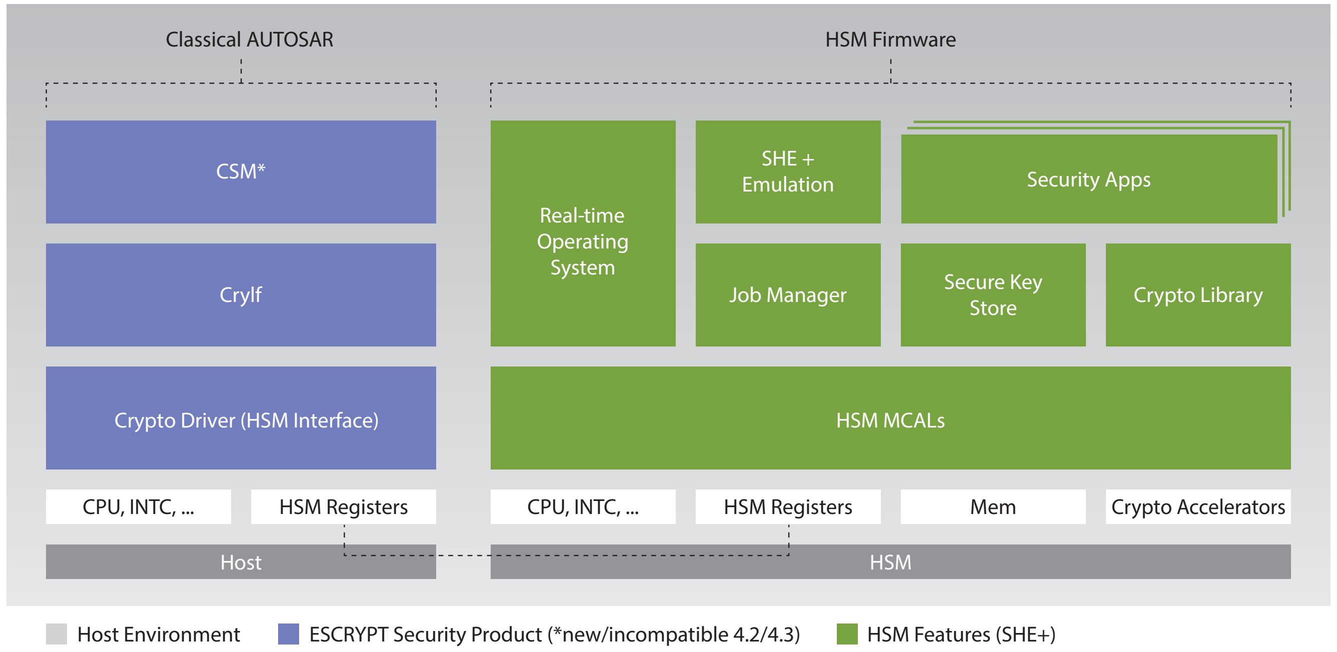


Figure 2: Software architecture of the hardware security module (HSM).

Multifunctional and easy to implement

Hardware security modules offer far more powerful features than purely software-based solutions. Since the HSM security functions are physically encapsulated, the ECU host controller can focus entirely on its own tasks. Combined with the HSM security software, this approach yields a turnkey solution with numerous advantages:

- Offers a powerful hardware/software co-design platform for customer-specific applications with high-performance encryption requirements
- Enables simple customer integration through standardized interfaces to HSM
- Fully programmable – can be configured to meet specific needs thanks to its modular structure
- Multicore support

This feature set enables the HSM software stack to support a broad array of security use cases. It provides a standardized interface that can be used to implement a variety of IT security functions either on the HSM itself or in concert with the host processor, in all cases based on strong cryptography. These functions start with secure boot – in other words checking the code stored in the flash memory each time the ECU is activated – and also include runtime manipulation detection and secure flashing as well as authentication of software download providers and a secure log function for reliably documenting security-critical events. The core principle in all these cases is mutual authentication of the requesting instance and the HSM. This also applies to secure debugging, which protects the ECU against unauthorized access to the debug port while simultaneously allowing authorized access for software debugging purposes. In this case, too, the HSM exercises control over communication and authentication.

New HSM firmware generation

The development of HSM hardware and software is progressing rapidly, and an increasing number of microcontrollers for ECUs now come with an automotive-specific hardware security module as standard. ESCRYPT is keeping pace with these developments by steadily improving its HSM software stack, CycurHSM. The latest generation of CycurHSM offers even more user-friendly and differentiated options for implementing customized IT security functions in ECUs. The new HSM firmware enables easy configuration via the applet manager plus activation of individual security features using the variant management system. The ASPICE-compliant software also comes with a flexible keystore architecture.

End-to-end protection is the name of the game when it comes to securing connected vehicles and their increasingly automated driving technologies in the future. Developers need to secure all the critical points in the connected environment by integrating technology such as intrusion detection systems, automotive firewalls, secure over-the-air software updates and secure V2X. End-to-end protection means embedding IT security functions right down at the most fundamental component levels of digital vehicle functions – in other words within the microprocessors of individual ECUs. That's exactly what hardware security modules can offer. They lie at the heart of today's developments in automotive security – and their future looks equally bright (see Figure 3). ■

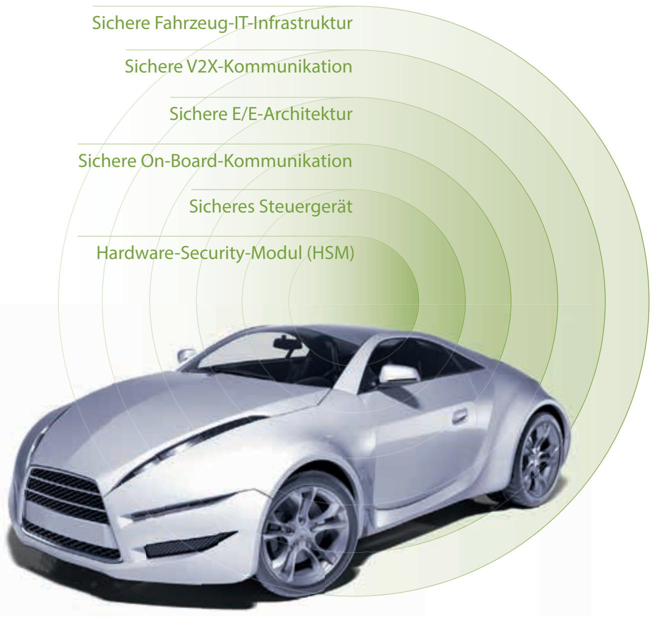

Sichere Fahrzeug-IT-Infrastruktur
Sichere V2X-Kommunikation
Sichere E/E-Architektur
Sichere On-Board-Kommunikation
Sicheres Steuergerät
Hardware-Security-Modul (HSM)

Figure 3: Hardware security modules (HSMs) lie at the heart of automotive security

Author

Dr. Frederic Stumpf is Head of Product Management at **ESCRYPT**.

ESCRYPT honored as "Innovator 2018"

Renowned German business publishing house **brand eins** recently released its annual ranking of the most innovative German companies – and ESCRYPT was one of the top performers. The company took a leading position among SMEs in the Technology and Telecommunication category, earning the accolade **"Innovator of the year 2018".**

Guided by specific selection criteria, more than 25,000 experts were asked to name innovation leaders from a pool of over 3,400 companies. ESCRYPT received an above-average number of recommendations in all three predefined innovation areas: products and services, process innovations, and corporate culture. **"We are delighted to have received this award,"** says Division Head Uwe Müller. **"More than ever, it's an incentive to ensure innovation continues to be the driving force at our company."** ■

brand eins Thema
2018
INNOVATOR DES JAHRES