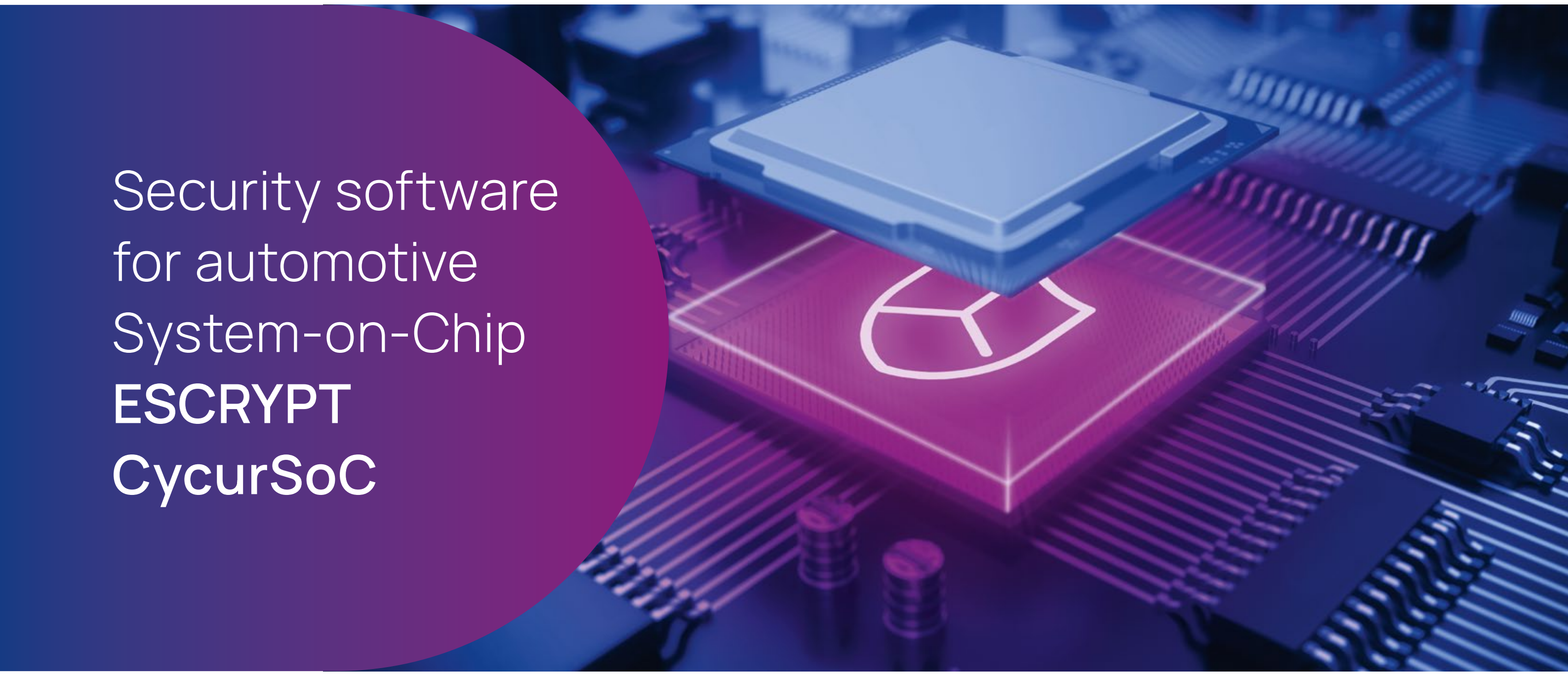
Empowering Tomorrow’s Automotive Software
www.etas.com

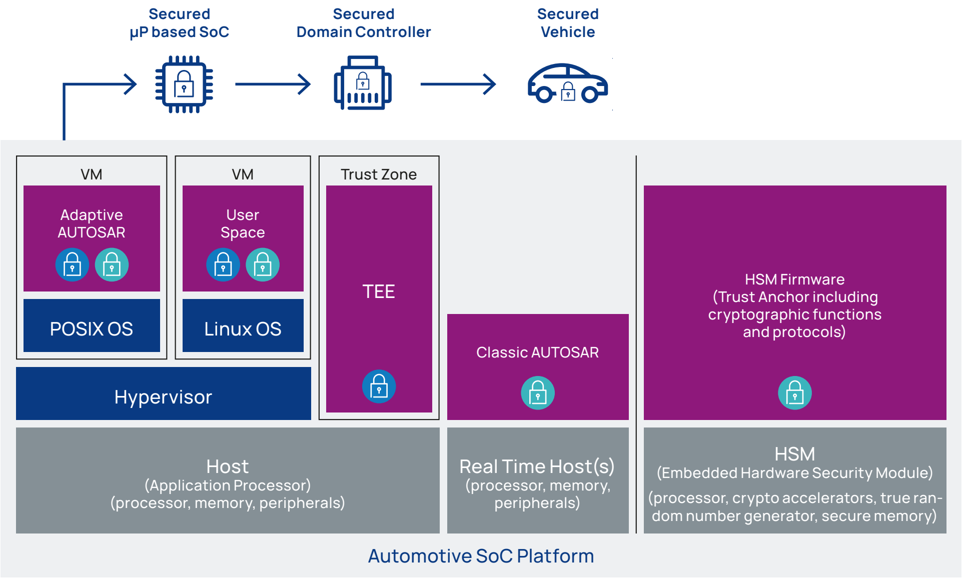


Security software for automotive System-on-Chip **ESCRYPT CycurSoC**

Enabling safety and trust for software-defined vehicles

Electrification, autonomous driving, Advanced Driver-Assistance Systems (ADAS) and infotainment systems are driving the emergence of powerful on-vehicle computing platforms. The key central component of each of these platforms is a microprocessor-based system-on-chip (SoC). These SoC platforms are enabling the vehicle E/E architecture evolution from traditional distributed ECUs to a more centralized domain architecture. Advanced E/E architectures host powerful software functionality that enhances customers’ experience and increases automation. These benefits are, however, accompanied by newly-introduced cybersecurity vulnerabilities and threats.

ESCRYPT CycurSoC is an embedded cybersecurity software solution for contemporary and future SoC-based automotive ECUs. Designed for automotive security use cases, it provides a complete set of security building blocks for heterogenous SoC architectures utilizing an HSM core and any other SoC CPU cores. The security solution is optimized for efficiency with minimal impact on available system resources. While supporting open and standardized interfaces (e.g., SHE+, AUTOSAR Classic and Adaptive), it is flexible and integrable with different embedded technology solutions, including virtual machines and various host environments.


Secured
µP based SoC
Secured
Domain Controller
Secured
Vehicle
VM
Adaptive AUTOSAR
POSIX OS
VM
User Space
Linux OS
Hypervisor
Trust Zone
TEE
Classic AUTOSAR
HSM Firmware
(Trust Anchor including cryptographic functions and protocols)
Host
(Application Processor)
(processor, memory, peripherals)
Real Time Host(s)
(processor, memory, peripherals)
HSM
(Embedded Hardware Security Module)
(processor, crypto accelerators, true random number generator, secure memory)
Automotive SoC Platform

HSM & TEE variants

- **ESCRYPT CycurSoC-HSM** is an HSM core firmware variant of the microprocessor (µP) based SoC platform.
- **ESCRYPT CycurSoC-TEE** is a Trusted Execution Environment (TEE) software variant of the µP based SoC platform that may not have an HSM core.
- Both variants can be offered separately, or they can complement each other, depending on the platform and security use cases.
- Both variants are designed to act as root of trust, and utilize SoC resources efficiently to maintain security integrity, robustness and zero trust concept.

🔒 **ESCRYPT CycurSoC-HSM Security Components**

🔒 **ESCRYPT CycurSoC-TEE Security Components**

ESCRYPT CycurSoC – The de-facto standard for µP-based SoC

- Implements security functionality that is critical to the creation of a security enclave on the HSM core or TEE host
- Offers cryptographic protocols and algorithms to the application
- Helps to effectively fulfill complex automotive OEM security requirements, while ensuring a smooth integration into the overall system architecture
- Retains integrity of data and functionality to achieve reliability , safety and data protection
- Is abstracted from the requirements of an OEM and the underlying silicon, thus enabling sourcing one security solution that fits all and saves on cost

Cryptographic features

- CMAC and HMAC
- Hashing
- Key derivation
- TRNG and PRNG
- Digital signature algorithms; ECDSA, EdDSA, RSA
- Symmetric and asymmetric encryption
- Authenticated encryption and decryption
- SHE+ support
- Key exchange algorithms; ECDH, ECDHE, ECBD
- Key wrapping and transport
- Key encapsulation mechanism (KEM)
- Key storage management and trust management
- Certificate handling
  - Parsing
  - Signing request
  - Revocation and CRL handling
  - Chain verification

HSM & host core

- Secure storage of data and keys in external flash
- Secure access
- Establish trusted channel amongst different cores on the SoC
- Support for E/E architectures with large number of keys
- Support for multi-CPU tenancy
- Support for virtualized environment
- Responsive operations in multi-CPU use cases
- HSM lifecycle mode
- Support for secure boot, trusted boot, authenticated boot and other boot modes
- Trust anchor based on signatures
- Runtime manipulation detection

Trust zone

- Integration with TEE operating systems
- Establish trusted channel between trust zone and other cores on the SoC
- Automotive grade security functionality, supporting trusted applications (TA) and the non-secure world

Your benefits with ESCRYPT CycurSoC

- **User friendly**
  Can be seamlessly integrated in automotive ECUs
- **Fast**
  Allows to be easily integrated with POSIX and real time operating systems
- **Comprehensive**
  Encapsulates all required security functions needed to satisfy all OEM automotive security requirements
- **Quality and reliability**
  Is being developed to high quality standards (ASPICE, ISO-21434 CSMS, ISO-26262 ASIL B)
- **Secure**
  Offers a powerful hardware/software co-design platform for customer-specific applications with high-performance cryptographic demands
- **Flexible**
  Can be configured to meet automotive customers' specific needs

Are you interested in ETAS products and solutions?
Please write to us at: **info@etas.com**

Further product information:
www.etas.com/CycurSoC