Empowering Tomorrow's Automotive Software
www.etas.com

Automotive-qualified Security Stack for HSMs **ESCRYPT CycurHSM**

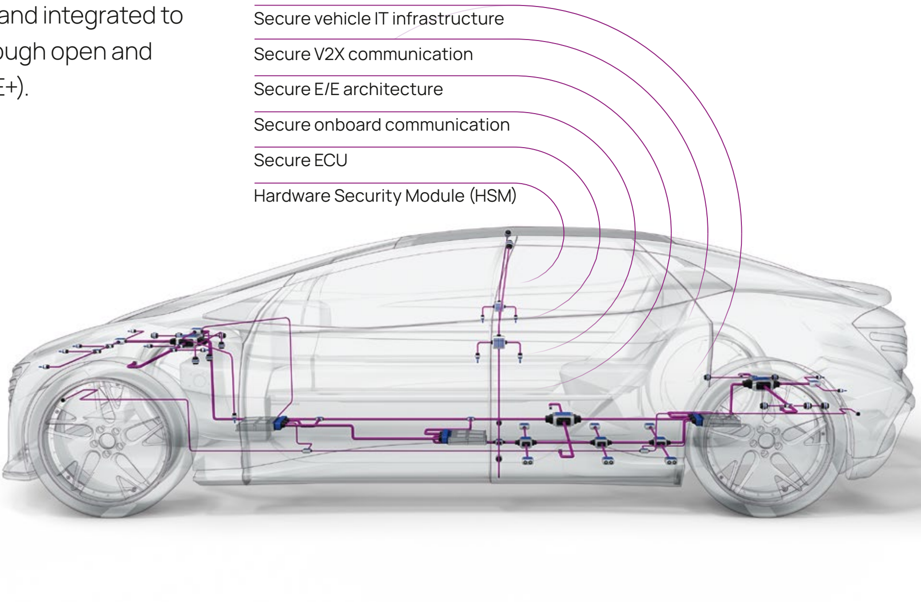
Overview

For security at ECU level, pure security solutions alone in software cannot sufficiently protect the integrity of a secure system. Hardware Security Modules (HSM) are a necessary prerequisite to harden embedded systems against attacks, to ensure confidentiality of data and provide protection to maintain the integrity and authenticity of the system.

ESCRYPT CycurHSM is a complete security software stack used in applications for HSM-embedded automotive microcontrollers. It is adapted to support a wide range of available automotive HSM implementations by different silicon manufacturers. ESCRYPT CycurHSM is a modular and flexible HSM firmware which can be easily customized and integrated to HSM-enhanced security applications through open and standardized interfaces (e.g. Autosar, SHE+).

ESCRYPT CycurHSM has been implemented in hundreds of successful projects with TIER-1s and OEMs worldwide, further underscored by a proven record in the field in millions of vehicles. ESCRYPT CycurHSM is a highly optimized HSM firmware implementation that ensures the highest level of ECU security.

ESCRYPT CycurHSM is accredited with the world's first ISO standard certificate for road vehicle cybersecurity "ISO/SAE 21434:2021 Road vehicles – Cybersecurity engineering" with the highest security level CAL4 (Cybersecurity Assurance Level 4).


Secure vehicle IT infrastructure
Secure V2X communication
Secure E/E architecture
Secure onboard communication
Secure ECU
Hardware Security Module (HSM)

Supported features

ETAS offers ESCRYPT CycurHSM with a comprehensive feature set:

Cryptographic and certificate features

- Asymmetric crypto algorithms:
  - RSA
  - ECDSA, ECBD, ECDH, ECDHE, EdDSA
- Basic cryptographic services
  - Symmetric ciphers (e.g AES)
  - MAC generation and verification (e.g. CMAC, HMAC)
  - Random number generation (e.g. TRNG, PRNG)
  - Hashing
  - Key derivation functions
- Certificate support (authenticity, parsing)
- Chinese algorithms
- Key exchange protocols (Diffie-Hellman)

Field return analysis and HSM debugging

- Fail-Safe HSM Update
- HSM-controlled Secure Access (Challenge Response Protocol)
- HSM Debug
- HSM Dump
- Secure Host Flashing
- Secure Logging

HSM core functionality and generic features

- Bank swap SOTA support
- Component protection (SHE+ support)
- EEPROM emulation to extend flash endurance
- HSM Lifecycle Mode
- HSM RAM mode
- Memory Unlock (flash password protection)
- Multi-core support
- Runtime manipulation detection
- Secure Boot / Trusted Boot / Authenticated Boot and other boot modes
- Secure storage of data and keys
- Support for systems with large number of keys (> 100)
- Trust Anchor based on signatures
- Preemptive, parallel job processing

OEM specific features

- Qualified OEM specific configurations including support for OEM specific protocols and functions

And many more!

Interested to know more or have a specific use-case? Please contact us.

ESCRYPT CycurHSM is a highly optimized and flexible security firmware that can be configured for your individual use case.

Your benefits with ESCRYPT CycurHSM

- **User friendly**
  Can be seamlessly integrated in non-AUTOSAR and AUTOSAR automotive applications
- **Fast**
  Based on a real-time operating system to ensure real-time HSM features
- **Trustworthy**
  Contains no open-source software in productive code
- **Comprehensive**
  Encapsulates all required security functions needed to satisfy OEM automotive security requirements
- **Future-oriented**
  Satisfies next-gen requirements and new cybersecurity regulations (ISO21434..)
- **Top quality**
  Has been developed to the highest quality standards (ASPICE, ISO 26262 ASIL D) and can be used in safety-criticial applications
- **Secure**
  Offers a powerful hardware/software co-design platform for customer-specific applications with high-performance cryptographic demands
- **Flexible**
  Can be configured to meet your specific needs and is free of hidden costs

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

Further product information:
www.etas.com/CycurHSM