escrypt
SECURITY. TRUST. SUCCESS.

CycurHSM

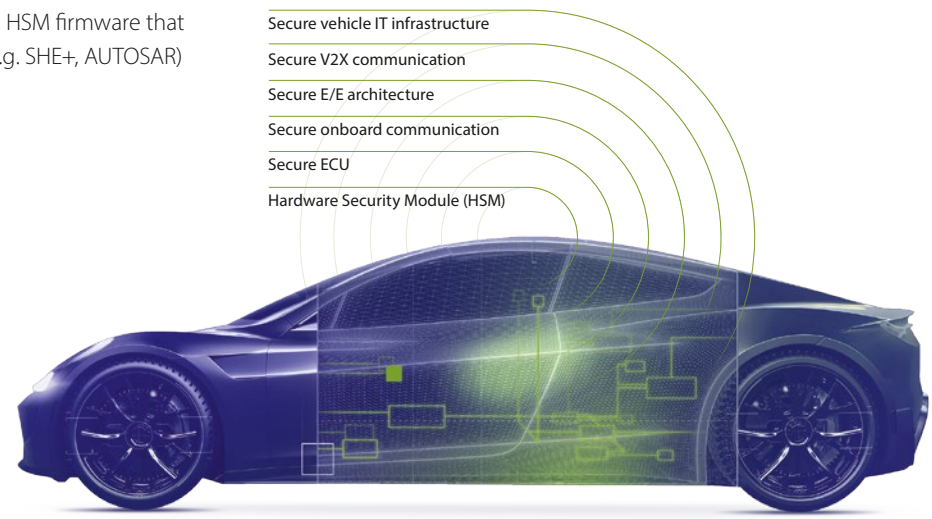
Automotive-qualified Security Stack for HSMs

Overview

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

CycurHSM is a complete software stack adapted to the available automotive HSM implementations by different silicon manufacturers. It fulfills requirements regarding a flexible HSM firmware that provides open and standardized interfaces (e.g. SHE+, AUTOSAR) to HSM-enhanced security applications.

ESCRYPT has more than 100 successful CycurHSM projects with TIER1s worldwide, with a millions of cars proven field record. CycurHSM is a highly optimized HSM firmware implementation that ensures the highest level of ECU security.



ESCRYPT 2021/01

Features

ESCRYPT offers CycurHSM 2.x with the feature set shown in the list below.

Cryptographic and certificate features

- Basic cryptographic services (AES, CMAC, Hashing, Key Derivation, TRNG, PRNG)
- Chinese algorithms
- RSA (Digital Signature Algorithm)
- ECDSA, ECBD, ECDH, ECDHE, EdDSA
- Key exchange protocols (Diffie-Hellmann)
- Certificate support (authenticity, parsing)

Field return analysis and HSM debugging

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

HSM core functionality and generic features

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

OEM specific features

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

Your benefits

- ✔ **User friendly**
  CycurHSM can be seamlessly integrated in automotive ECUs
- ✔ **Fast**
  CycurHSM is based on a real-time operating system to ensure real-time HSM features
- ✔ **Comprehensive**
  Encapsulates all required security functions needed to satisfy all OEM automotive security requirements
- ✔ **Top quality**
  CycurHSM has been developed to the highest quality standards (ASPICE, ISO 26262 ASIL D)
- ✔ **Secure**
  CycurHSM offers a powerful hardware/software co-design platform for customer-specific applications with high-performance cryptographic demands
- ✔ **Flexible**
  CycurHSM can be configured to meet your specific needs

Any questions?

Please contact us any time.

info@escrypt.com
Phone: +49 234 43870-200
www.escrypt.com

escrypt
SECURITY. TRUST. SUCCESS.