



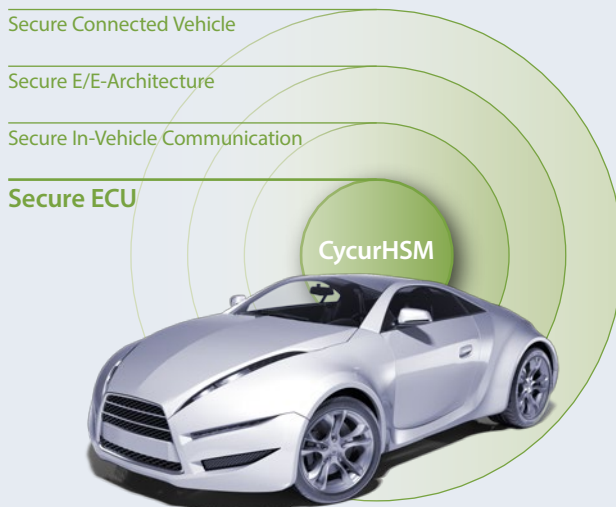
## Automotive-qualified Security Stack for HSMs

### Overview

For security at ECU level, pure security solutions 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 of the software.

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. AUTOSAR CSM) to HSM-enhanced security applications.

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



CycurHSM secures the nucleus – ECU in ESCRYPT's holistic security approach.

ESCRYPT now offers CycurHSM 2.x version with additional features. CycurHSM 1.x can still be used in production projects where only 1.x features are required. Maintenance of CycurHSM 1.x will still be provided by at least 2023.

Features	CycurHSM 1.x	CycurHSM 2.x
<b>Field return analysis and HSM debugging</b>		
HSM Update	x	x
HSM-secured host flashing		x
HSM Debug		x
HSM-controlled Secure Access (Challenge Response protocols)		x
<b>HSM Core Functionality and Generic Features</b>		
Preemptive, parallel job processing	x	x
HSM Lifecycle Mode		x
Secure Storage of data and keys	x	x
Support for systems with high number of keys (> 100)		x
Component Protection (SHE+ Support)	x	x
EEPROM emulation to extend flash endurance	x	x
HSM RAM mode	x	x
Multi-Core Support	x	x
Secure Boot	x	x
Trusted Boot		x
Runtime manipulation detection		x
<b>Cryptographic and certificate features</b>		
Basic cryptographic services (AES, CMAC, Hashing, key derivation, TRNG)	x	x
RSA (Digital Signature Algorithm)	x	x
ECDSA		x
Key exchange protocols (Diffie Hellman)		x
Certificate support (Authenticity, Basic Parsing)		x

## 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

