hitex
EMBEDDED TOOLS & SOLUTIONS

Building a safe and secure embedded world

Security at ECU level

Automotive-qualified security stacks for HSMs

> CycurHSM

escrypt
SECURITY. TRUST. SUCCESS.

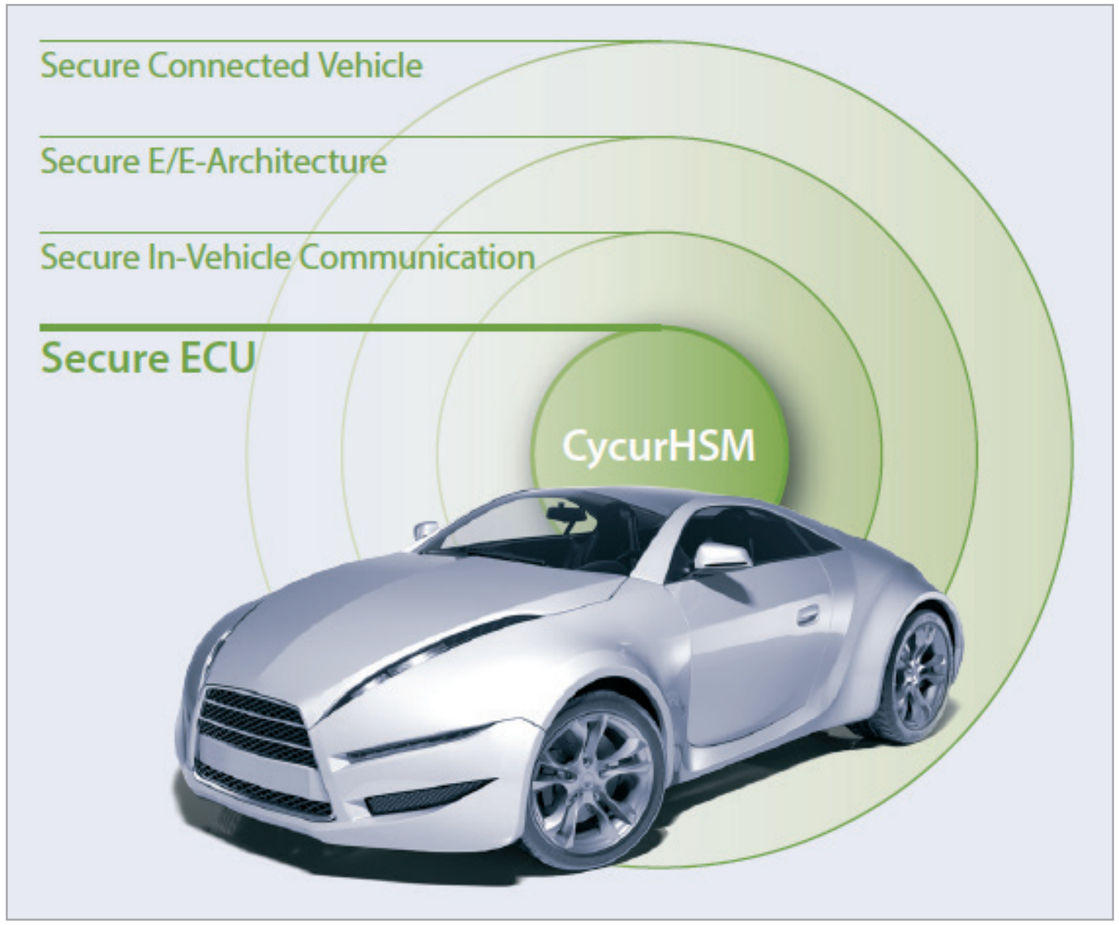
Overview

Modern vehicles are increasingly equipped with internet connectivity, which in turn is making vehicle IT systems more vulnerable to attacks. These systems must be protected against unauthorized access by intruders who may attempt to manipulate the ECU software (e.g. tuning) or manipulate the vehicle's anti-theft mechanism (immobilizer). There is also a risk that criminals could misuse the internet connection of the vehicle to access the in-vehicle communication system and carry out targeted manipulation of the vehicle's behavior.

ESCRYPT's new CycurHSM product is an innovative and flexible HSM security firmware that ensures secure boot of the ECU, secure in-vehicle communication, ECU component protection and secure flashing.

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



Completely adapted to Automotive

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 CryptoDriver) 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.

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
Field return analysis and HSM debugging		
HSM Update	x	x
Secure host flashing		x
HSM debug		x
Secure logging		x
HSM controlled secure access (challenge response protocols)		x
HSM core functionality and generic features		
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
Preemptive, parallel job processing	x	x
HSM lifecycle mode		x
Secure boot	x	x
Trusted boot		x
Runtime manipulation detection		x
Cryptographic and certificate features		
Basic cryptographic services (AES, CMAC, Hashing, key derivation, TRNG)	x	x
RSA (Digital Signature Algorithm)	x	x
ECDSA, ECBD, ECDH, ECDHE		x
Key exchange protocols (Diffie Hellman)		x
Certificate support (authenticity, parsing)		x

Maximum security for your ECUs

CycurHSM is a modular solution that provides security mechanisms for a multitude of security applications via a large number of open, standardized interfaces. That makes CycurHSM a great choice for seamless integration in automotive ECUs. CycurHSM supports ASIL-D for different safety use-cases.

hitex
EMBEDDED TOOLS & SOLUTIONS

Building a safe and secure embedded world

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 customerspecific applications with high-performance cryptographic demands
- ✓ Flexible: CycurHSM can be configured to meet your specific needs

Hitex Head Office, Germany

Hitex GmbH
Greschbachstraße 12
76229 Karlsruhe
Germany

Phone: +49-721-9628-0
Fax: +49-721-9628-149
Email: info@hitex.de

Hitex UK

Hitex (UK) Ltd
Millburn Hill Road
University of Warwick Science Park
Coventry CV4 7HS
United Kingdom

Phone: +44-24-7669-2066
Fax: +44-24-7669-2131
Email: info@hitex.co.uk

B-ESCRYPT-E001-2020