escrypt
SECURITY. TRUST. SUCCESS.

CycurHSM

Software Stack for Hardware Security Modules

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 Bosch HSM implementations by different silicon manufacturers. CycurHSM provides the technology for fulfilling requirements regarding a flexible HSM firmware that provides open and standardized interfaces (e.g. AUTOSAR CSM) to HSM-enhanced security applications.

ESCRYPT has extensive experience in implementing HSMs through a long history of industrial and research projects.

The new CycurHSM product from ESCRYPT is a security firmware specifically designed for the Bosch HSM and its derivatives. CycurHSM will support all available HSM implementations from different silicon manufacturers.

CycurHSM provides highly optimized HSM software that ensures the highest level of ECU security.

Typical Hardware Security Modules do not satisfy automotive requirements. Integrating an external, additional chip inside an ECU can lead to higher costs and increased sensitivity to attacks on the communication interface between the ECU application core and the HSM.

CycurHSM offers a new innovative technology for automotive-qualified HSMs, such as the Bosch HSM and its derivatives. It lowers costs for integrating HSM-enhanced security inside ECUs and raises efficiency and flexibility.

CycurHSM provides the flexibility to implement further custom-engineered applications.

ESCRYPT 2018/05

escrypt
SECURITY. TRUST. SUCCESS.

CycurHSM

Details

General

Supports all available implementations of the Bosch HSM:

- Provides a standardized API to access the HSM
- Usage of all available hardware accelerators (TRNG, AES-128 bit engine)
- Secure debug under HSM control
- Support of security applications (secure boot, secure flashing, secure debug, etc.)
- Layered software architecture based on an ISO 26262 certified real-time operating system
- Integration of ESCRYPT's CycurLIB to provide additional cryptographic primitives (Hashing, MAC, RSA, ECC)
- Modular structure to directly adapt the software to the customer's need
- Encapsulation of all security mechanisms to fully use the main functionality of the HSM
- Provision of a hardware-protected secure execution environment
- Full support of HSM technologies
- Fully programmable, additional customer applications can be easily integrated inside the HSM

RTA-OS Component

- RTA-OS is a real time operating system specifically designed to meet all requirements of automotive ECU's
- Todays RTA Solutions are powering more than 1 billion ECUs on the road

AUTOSAR compliant

- Seamless integration in AUTOSAR as cryptographic service manager (CSM), including host sided HSM device drivers (CRY layer) and a PKCS#11 interface for non-AUTOSAR applications

Features & Benefits

- Design is based on a real-time operating system to ensure real-time characteristics of the HSM
- Hardware-shielded protected storage for cryptographic keys or secure logging
- Encapsulates all required security functions needed to satisfy a broad set of automotive security requirements
- Implemented to account for highest quality standards
- Powerful hardware/software co-design platform for customer-specific applications with high-performance cryptographic demands
- Customer-specific configuration possible