In-Vehicle Systems Security

End-to-end cybersecurity for embedded vehicular systems and software

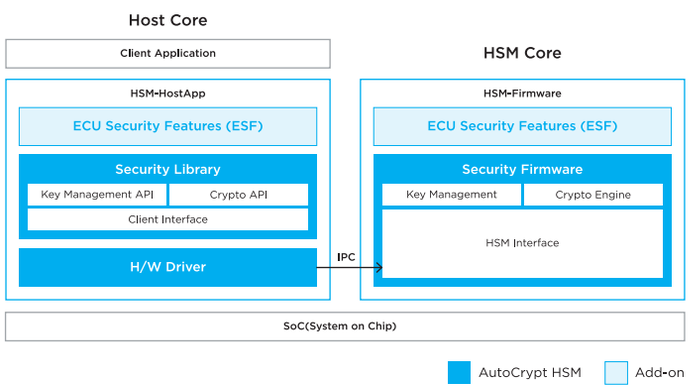
AUTOCRYPT's in-vehicle systems security solutions provide a wide range of embedded security software, components, and add-ons tailored for both AUTOSAR and legacy environments. Leveraging proprietary cryptographic technologies, AUTOCRYPT delivers customized cybersecurity solutions, ensuring full compliance with ISO 21434 and UN R155/156.

Embedded Security Firmware for ECUs

AutoCrypt® HSM

AutoCrypt® HSM is a software module that seamlessly integrates the hardware security module (HSM) into the AUTOSAR environment. This ensures the secure access of ECUs and acts as a trust anchor for in-vehicle communications.

- Establishes future-proof security ecosystem with 18 cryptographic algorithms
- Provides encryption, decryption, key and certificate storage and management
- Offers ESF add-on security features, seamlessly adapting to varying manufacturer requirements
- Supports both AUTOSAR and legacy platforms



Enhanced Security Platform for SDVs

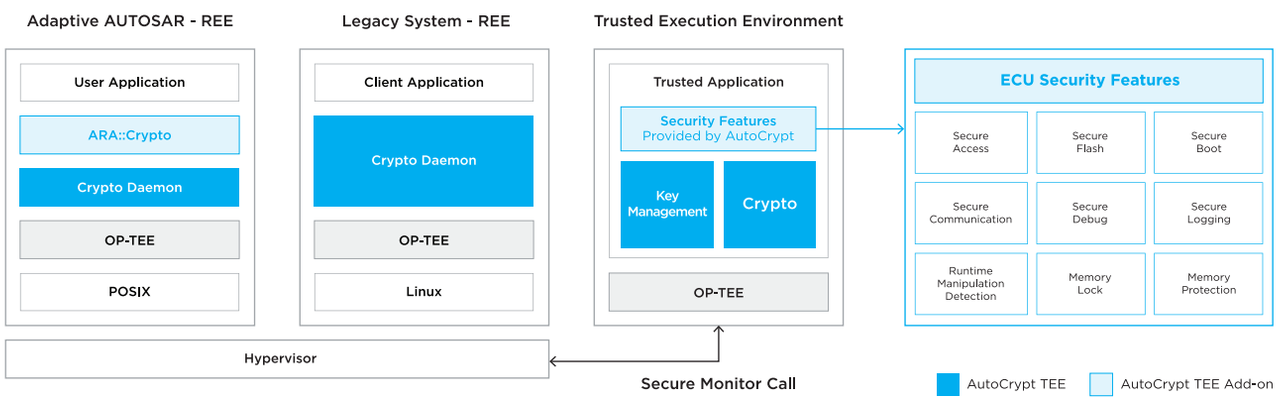
AutoCrypt® TEE

AutoCrypt® TEE is an ASPICE CL2-certified in-vehicle systems security solution dedicated to advanced software-on-a-chip (SoC) platforms. It implements a secure trusted execution environment (TEE) within each component of the application processor.

- Best suited for advanced applications including ADAS, IVI, and the central communications unit (CCU)
- Contains all components needed for TEE implementation, including APIs, drivers, OS components, and a secure monitor
- Offers ESF add-on security features, seamlessly adapting to varying manufacturer requirements

Built to the following standards

- Compatible with Adaptive AUTOSAR
- Deployable in legacy environments
- GlobalPlatform API compliance
- TrustZone for ARM-A technical specs supported
- MISRA-C/C++ validated
- ASPICE CL2 certified

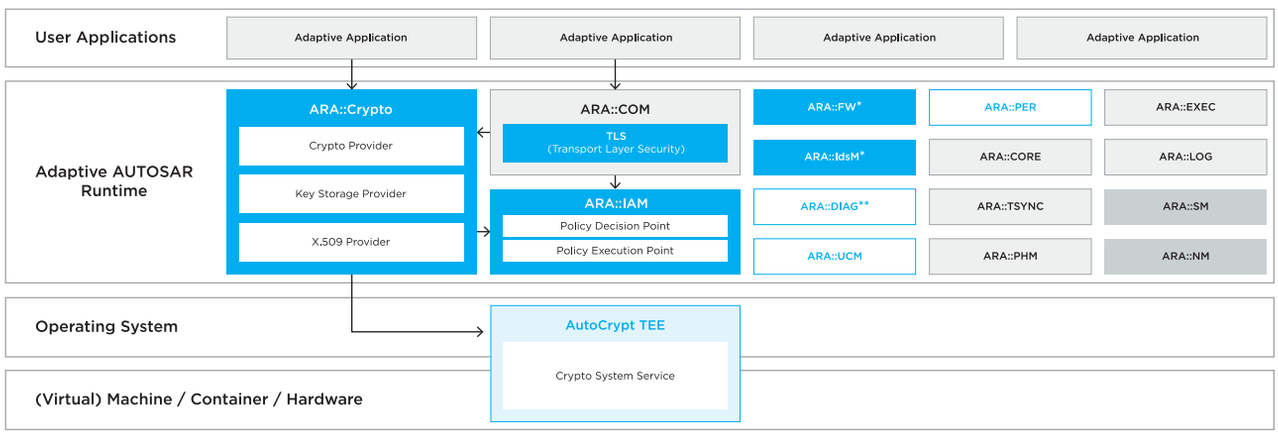


Adaptive Security Library for AUTOSAR

AutoCrypt® ASL

AutoCrypt® ASL is an adaptive security library that covers intrusion detection and mitigation, identity and access management, cryptographic functions, and an advanced firewall.

- Secure communications and access control (ARA::IAM)
- Cryptographic functions and certificate features (ARA::CRYPTO)
- Intrusion detection and threat mitigation (ARA::IDSM)
- Advanced firewall (ARA::FW)



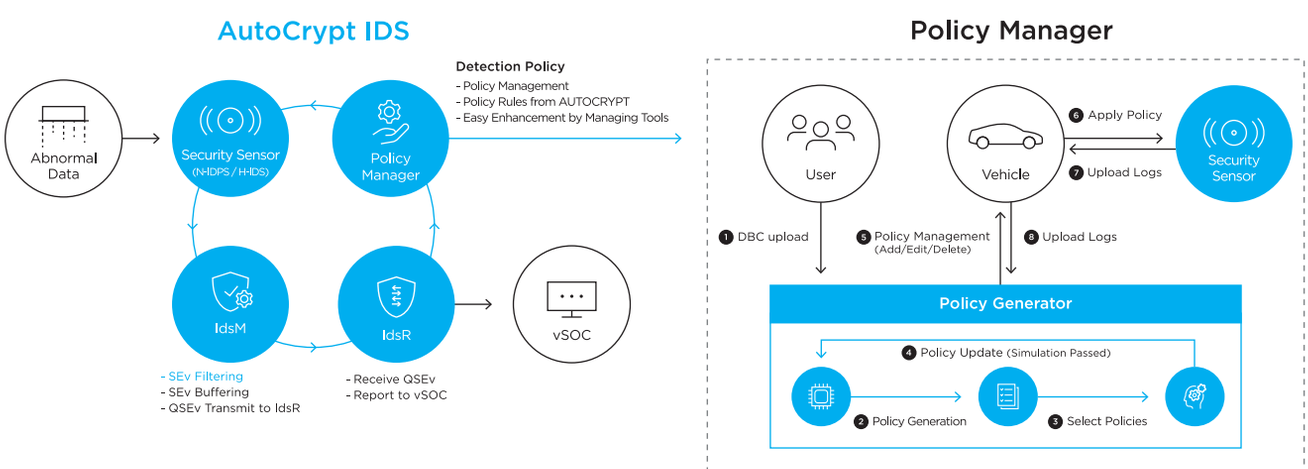
*ARA::FW, ARA::IdsM → Developed according to R22-11
**ARA::DIAG → Developed according to R21-11

AutoCrypt ASL | Partial Support | Add-on

Intrusion Detection and Policy Management

AutoCrypt® IDS

AutoCrypt® IDS provides a vehicular intrusion detection solution that detects, filters, and prevents cyberattacks against in-vehicle systems.



AutoCrypt IDS

- Proprietary **Security Sensor**
- **N-IDS** detects abnormal data in the network
- **H-IDS** identifies abnormal behaviour in the ECUs
- **IdsM** evaluates detected security events (SEv) and sends qualified cases (QSEv) to the IdsR
- **Policy Manager** automatically updates detection policies and applies them to the Security Sensor
- Can be linked to **AutoCrypt® vSOC** or third-party vSOCs

AUTOCRYPT

APAC Autocrypt Co., Ltd | Seoul, Korea
NORTH AMERICA Autocrypt Inc. | Irvine, CA, USA
EUROPE Autocrypt Technologies GmbH | Munich, Germany

CONTACT global@autocrypt.io