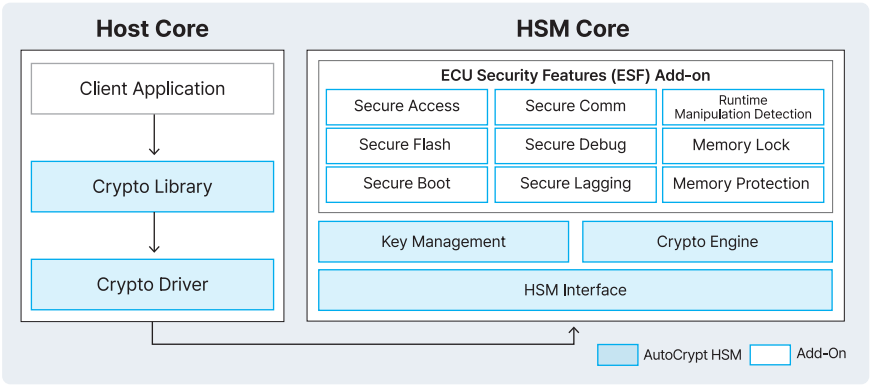
In-Vehicle Security Solution

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

AUTOCRYPT's in-vehicle 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.

AutoCrypt® HSM — Embedded Security Firmware for ECUs

AutoCrypt® HSM is an ASPICE CL2-certified 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 19 cryptographic algorithms
- Provides encryption, decryption, key and certificate storage and management
- Offers ESF add-on security features, seamlessly adapting to varying manufacturing requirements
- Supports both AUTOSAR and legacy platforms

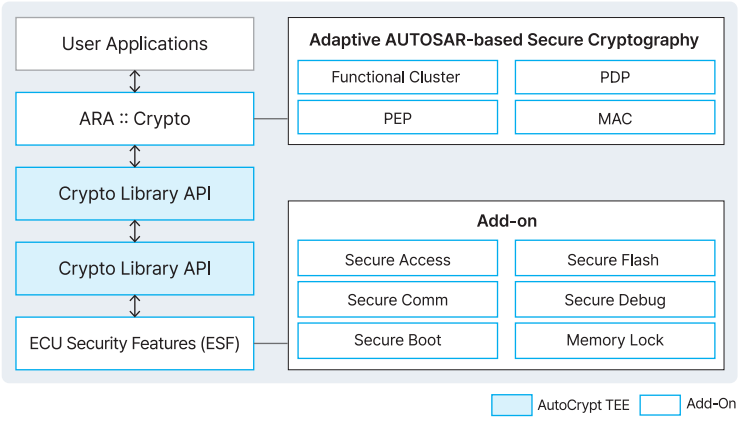
AutoCrypt® TEE — Enhanced Security Platform for SDVs

AutoCrypt® TEE is an ASPICE CL2-certified in-vehicle 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 CCU
- Contains all components for TEE implementation (APIs, drivers, OS components, monitor)
- Offers ESF add-on security features, seamlessly adapting to varying manufacturer requirements

Built to standards:

- Compatible with Adaptive AUTOSAR and deployable in legacy environments
- MISRA-C/C++ validated, ASPICE CL2 certified

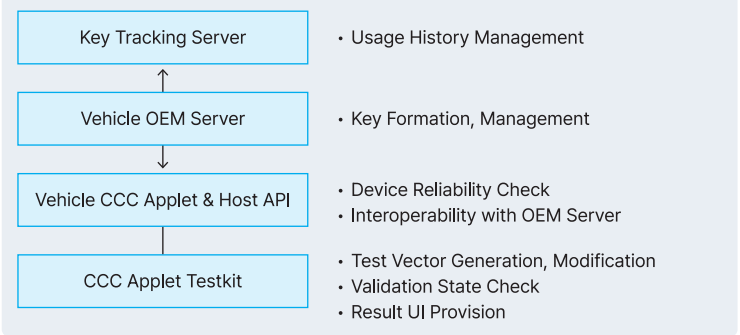


AutoCrypt® Digital Key — Safe, User-friendly Digital Key Solution

AutoCrypt® Digital Key provides a secure and convenient lock-and-key system for vehicles, ensuring seamless interoperability across mobile devices and vehicle platforms in compliance with CCC Digital Key Release 4 standards.

Establishes and provides full support for:

- Key Tracking server: management server for usage history and preferences
- Vehicle OEM server: used by automotive manufacturers to generate and manage digital keys
- Vehicle CCC applet and host API: deployed inside a vehicle's secure element (SE), responsible for verifying and connecting with the vehicle owner's smartphone

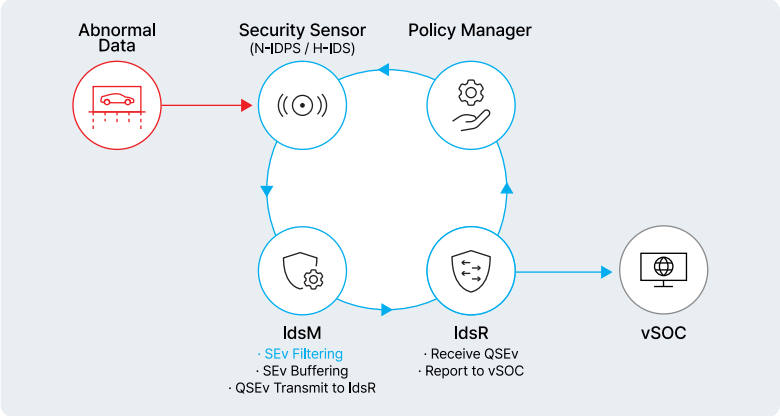


AutoCrypt® IDS — Intrusion Detection and Policy Management

AutoCrypt® IDS provides a vehicular intrusion detection solution that detects, filters and prevents cyberattacks against in-vehicle systems and can be linked to AutoCrypt® vSOC or third-party vSOCs.

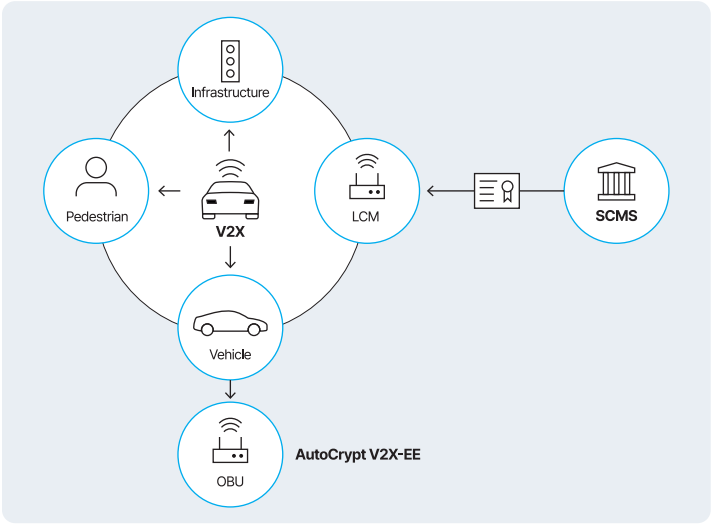
Proprietary Security Sensor

- 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



AutoCrypt® V2X-EE — Embedded Security Module for OBUs and RSUs

AutoCrypt® V2X-EE consists of a security module that is ready to be integrated into OBUs and RSUs to secure basic safety messages (BSM), enabling the end entity to sign and authenticate V2X communications from the Security Credential Management System (SCMS).



- Designed according to IEEE 1609.2 and 1609.2.1 standards, compatible with C-V2X
- Proprietary Local Certificate Manager stores SCMS certificates within each end entity
- Testing complete with all major V2X stacks

HW Platform: NXP.i.MX8DXL, NXP.i.MX8MP

PKI Spec.: ETSI, KR CAMP, KS, NA CAMP. CN YDT, CN GBT

V2X Message Spec.: ETSI, IEEE 1609.2, CN YDT

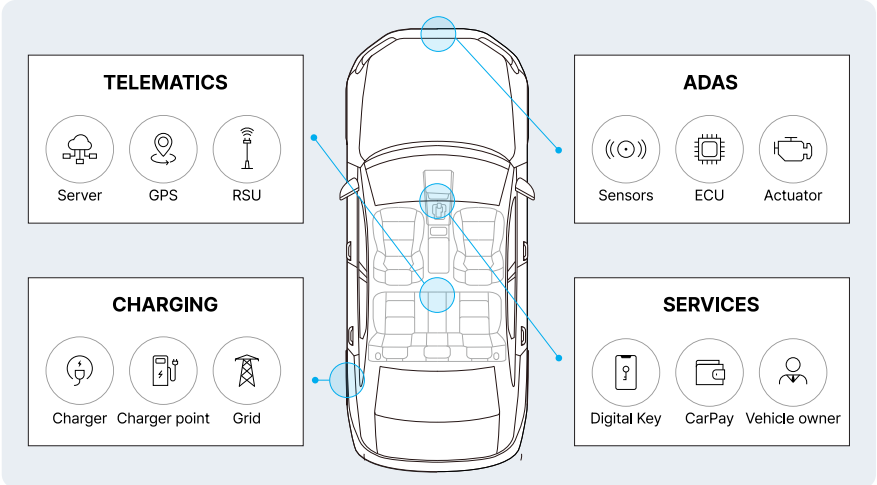
AutoCrypt® TLS — Secure Vehicle Communications

AutoCrypt® TLS supports TLS 1.3 with RFC8446, the latest communication security standard, and provides faster, more secure communication.

- Protects user, location, payment information from a variety of security threats while ensuring data security and integrity using critical encryption algorithms and authentication protocols

Compliant with industry standards and requirements

- PnC applications: OCPP Ver 1.6 and ISO 15118
- V2X applications: IEEE 802.11 and IEEE 1609.2
- OTA applications: WP.29 R155 regulations



APAC | Autocrypt Co., Ltd. | Seoul, South Korea | domestic@autocrypt.io
NORTH AMERICA | Autocrypt Inc. | San Jose, CA, USA | global@autocrypt.io
EUROPE | Autocrypt Technologies GmbH | Munich, Germany | europe@autocrypt.io

AUTOCRYPT