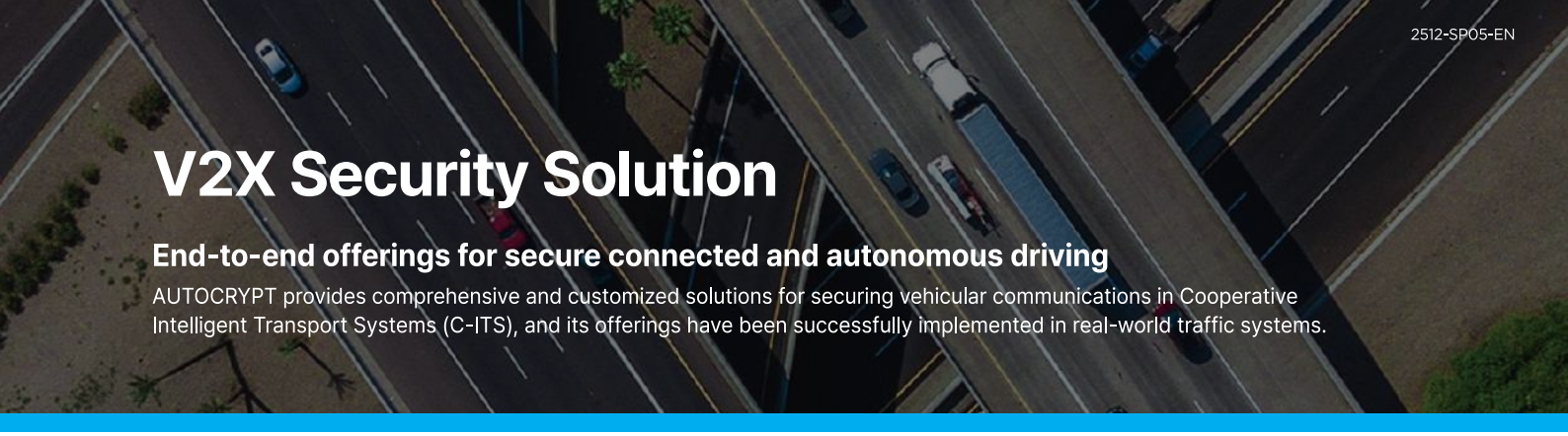


V2X Security Solution

End-to-end offerings for secure connected and autonomous driving

AUTOCRYPT provides comprehensive and customized solutions for securing vehicular communications in Cooperative Intelligent Transport Systems (C-ITS), and its offerings have been successfully implemented in real-world traffic systems.

End-to-end offerings for V2X security

AutoCrypt® V2X-EE
Security module for end entities(OBU, RSU)

AutoCrypt® V2X-PKI
SCMS backend for certificate management

AutoCrypt® MBD
Misbehavior detection and reporting

AutoCrypt® IMS for SCMS
SCMS dashboard

AutoCrypt® CLS
Edge server for V2X communications

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

Supported Boards

- i.MX 6
- i.MX 8
- Custom boards with board-specific package

Supported HSMs

- Autotalks SECTON/CRATON2
- NXP SXF 1800
- Infineon SLS37 prototype
- ThinkTech M2000
- HED

AutoCrypt® V2X-PKI — Facilitating management of certificates for V2X communications

With both PKI-as-a-Service (PaaS) and on-premises deployment options available, **AutoCrypt® V2X-PKI** provides comprehensive certificate management to authenticate entities (enrollment, issuance, revocation, etc.) in Cooperative-Intelligent Transport Systems.

Lifecycle Management

- Manages the entire certificate lifecycle, from issuance to revocation
- 24/7 monitoring system and customer support

Worldwide Compliance

- World's first and only V2X PKI platform that supports all three major SCMS standards (US SCMS, EU CCMS, and Chinese C-SCMS)

Scalability

- Easily scalable as V2X deployment grows
- Supports deployment of millions of certificates

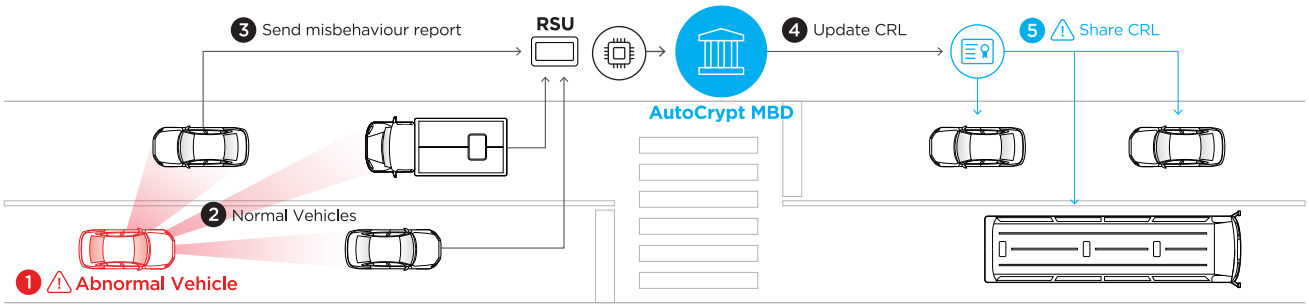
Cost Reduction

- No need for local servers
- No need for software installation and maintenance

AutoCrypt® MBD

Safeguarding V2X communications with misbehavior detection

AutoCrypt® MBD consists of a local MBD embedded into OBUs, and a global MBD deployed in the V2X PKI server, enabling misbehavior reporting and certificate revocation for V2X communications, compatible with all major V2X PKI standards.



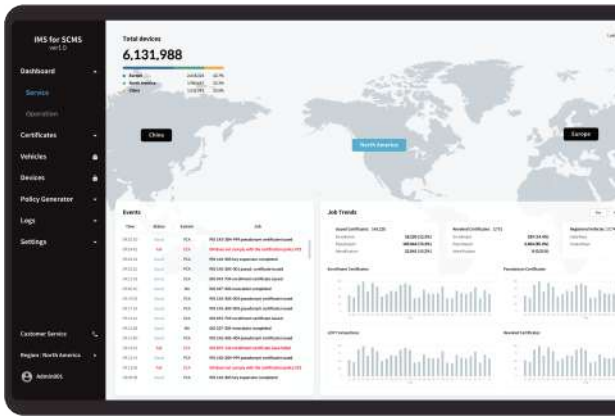
The local and global MBD work to indicate and report abnormal behavior, which is then compiled into a certificate revocation list (CRL), stored by AutoCrypt® V2X-EE in the RSUs and OBUs, blocking the certificate from participating in V2X communications.

AutoCrypt® IMS for SCMS

Dedicated user interface for V2X certificate management

AutoCrypt® IMS for SCMS is an Integrated Management System tool that allows for the convenient and simple management of all V2X certificates in an easy-to-use dashboard interface.

- Centralized management for certificates across different regions
- Dashboard for both static and dynamic operation management with real-time data updates
- Manage certificate issuance, expiry, and system health checks
- Customized architecture integration for OEM backend
- 24/7 customer service channels and helpdesk operation
- Use case with all C-ITS projects currently in operation in South Korea, covering over 3,000 miles of smart roads



Supported certificates

- Enrolment certificates
- Identification certificates (for OBUs)
- Pseudonym certificates (for OBUs)
- Application certificates (for RSUs)

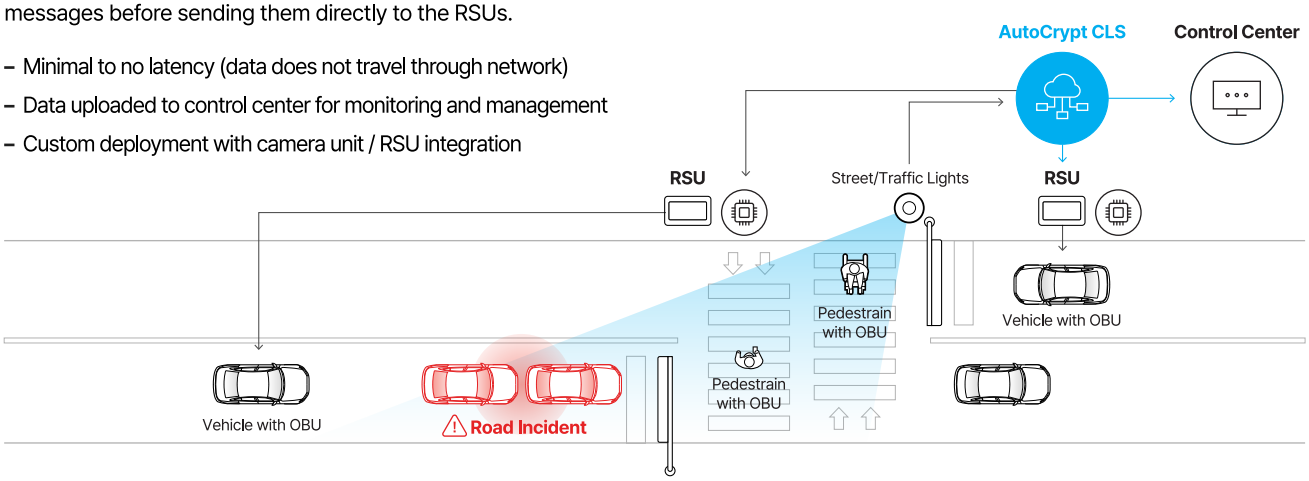
AutoCrypt® CLS

Edge server for real-time V2X communications

AutoCrypt® CLS (C-ITS Local Station) is a C-ITS infrastructure unit that acts as an edge server for V2X communications in a local area. It can be deployed at traffic intersections with a CLS unit, one RSU, and up to ten traffic cameras.

The unit receives sensor data sharing messages (SDSM) from the traffic lights and cameras, converting them to V2X messages before sending them directly to the RSUs.

- Minimal to no latency (data does not travel through network)
- Data uploaded to control center for monitoring and management
- Custom deployment with camera unit / RSU integration



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