AUTOCRYPT

Secure First, Then Ride

AUTOCRYPT

Cars are evolving, and they're not alone. With the advent of electric, connected, and autonomous vehicles, the entire mobility ecosystem is now entering a new era. With hundreds of thousands, if not millions, of connections, there not only exists the potential of convenient transportation, but also the loss of valuable data and human lives. This is why security is crucial in mobility.

Based on decades-trusted technologies and security industry experience, AUTOCRYPT provides mobility security solutions for the evolving transportation systems of today and tomorrow. Solutions cover the entire mobility ecosystem from end to end, are compliant with global standards, and have been successfully implemented and tested in real-world testbeds and traffic systems.

Our goal is clear: to deliver on tomorrow's promises for better mobility and transportation, we need a vehicular environment that is secure for those inside and outside the vehicle. AUTOCRYPT makes that future a reality.

History

2020	- Development of PnC security system for OEM company H's rapid charge system - Certification for C-V2X compatibility supporting C-SCMS standards by CAICT under IMT-2020(5G) - Installation and operation of Ulsan and Gwangju C-ITS project security systems - Development of digital key and submission of PoC
2019	- **Autocrypt Co., Ltd. established,** spinning off from Penta Security Systems Inc. - Contract won for Korean Expressway Corporation's V2X-SCMS implementation project
2018	- Development of ISO-15118 standard EV Plug&Charge(PnC) security solution - Development of vehicle/smartphone connection authentication security system for conglomerate S - Installation of Jeju province C-ITS security system - Design of secure authentication system for Korean Expressway Corporation's C-ITS project
2017	- Development of security solution for EV charging system - Installation and operation of Hwaseong K-City autonomous driving testbed security system - Installation and operation of Yeoju autonomous driving security system
2016	- Installation and operation of Daejeon-Sejong C-ITS security system
2015	- **Official commercial launch of AutoCrypt®, Smart Car Security Solution**
2014	- Development of Vehicle Data Management System (VDMS) for automotive big-data processing - Security verification technology development for telematics smartphone application
2013	- Developed international standard (IEEE1609.2: 2013) technology for V2X environment based on WAVE communication
2011	- Authentication and encryption enhanced solution developed for vehicle-to-smart device sync connection
2007	- Development of automotive safety diagnostic device

Member Associations

Awards

2019 Best Auto Cybersecurity Product / Service

2020 Automotive Tech Company of the Year Finalist

2020 Automotive Cybersecurity Company of the Year

2020 Global Cyber Achievement Award

2020 Emerging AI+X Top 100 Company

Munich, Germany

Wuxi, China

Tokyo, Japan

Shanghai, China

Korea
Seoul (HQ)
Sejong
Busan

Singapore

Toronto, Canada

100%
Testing complete with all
V2X stack companies

54
partners and customers
worldwide

>20
patents filed globally

From beginning to end, AUTOCRYPT secures your mobility journey   OVERVIEW

VEHICLE SECURITY

◉ **AutoCrypt® V2X**

- Comprehensive V2X security solution with fully customizable integration including Public Key Infrastructure (PKI)
- Compliant with the latest standards (CAMP IEEE 1609.2, IEEE 1609.2.1, USDOT SCMS, C-SCMS, EU CCMS), with use cases in application for automotive ECU, embedded, mobile, and virtual environments
- Verification speeds exceeding 5G requirements

◉ **AutoCrypt® IVS**

- In-vehicle security solution ensures security reinforcement for ECUs, CAN Bus, and Ethernet
- Abnormal behavior / attack detection with automotive firewall and Intrusion Detection System (IDS)
- Testing and consultation available for compliance with global regulations (WP.29, R155, R156)

SECURE MOBILITY

◉ **AutoCrypt® PnC**

- Secures Plug&Charge charging, providing interoperability and mutual authentification
- Follows ISO 15118 and OCPP standards to ensure end-to-end protection from vehicle owner, OEM, Mobility Operator (MO) to Charge Point Operator (CPO)

◉ **AutoCrypt® FMS**

- Data received from vehicles are classified, processed, and analyzed to allow for service providers to improve existing services and pinpoint new business opportunities
- Cuztomized platforms and applications developed as fully managed service

◉ **AutoCrypt® V2D**

- Digital key with convenient mobile application allows for drivers to utilize phone in place of physical key
- Follows CCC Digital Key 2.0 Release standards with plans for 3.0 standards when updated
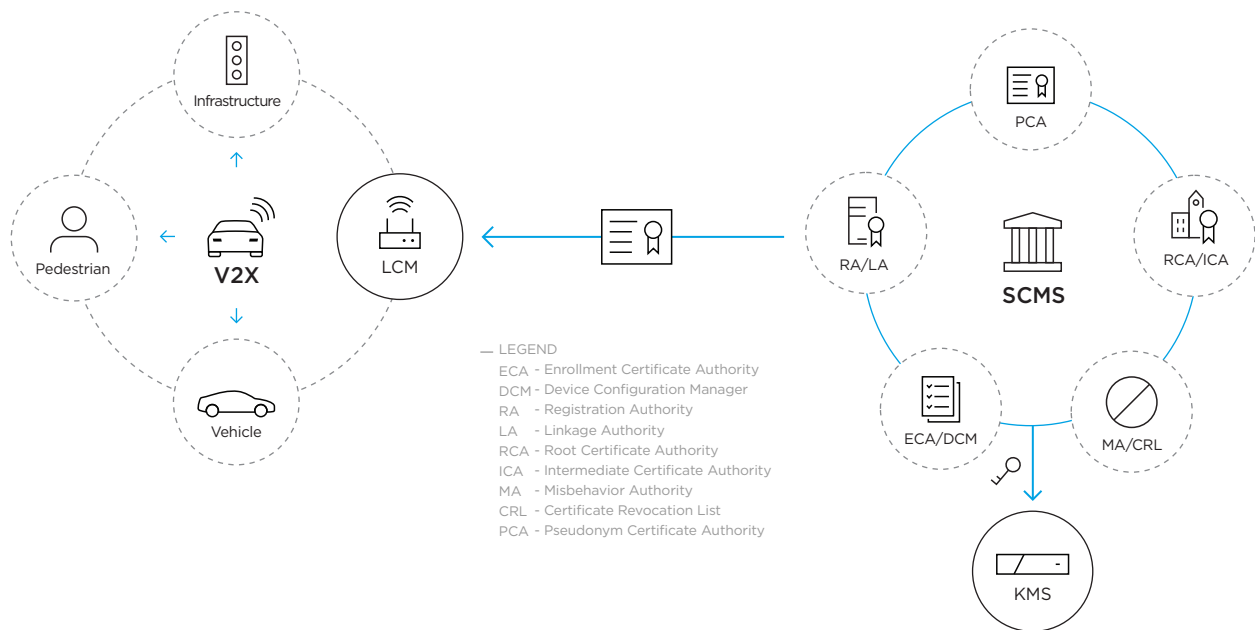
Vehicle Security

AUTOCRYPT provides a comprehensive and customized suite of offerings for securing vehicular communications in Intelligent Transport Systems (ITS), meeting established industry standards set by the Crash Avoidance Metrics Partnership (CAMP), the U.S. Department of Transportation (USDOT), and other leading organizations.

AutoCrypt® V2X — V2X Made Secure

AutoCrypt® V2X is an authentication and encryption system for vehicle-to-everything (V2X) communications, including vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-pedestrian (V2P) communications.

- Secures broadcast and receival of basic safety messages (BSM) and other data surrounding vehicle on-board units (OBUs) and roadside units (RSUs)
- Verification speeds exceed 5G performance requirements
- Designed according to IEEE 1609.2 communication standard for Wireless Access in Vehicular Environments (WAVE), IEEE 1609.2.1, USDOT SCMS, China-SCMS, and EU CCMS

LEGEND
ECA - Enrollment Certificate Authority
DCM - Device Configuration Manager
RA - Registration Authority
LA - Linkage Authority
RCA - Root Certificate Authority
ICA - Intermediate Certificate Authority
MA - Misbehavior Authority
CRL - Certificate Revocation List
PCA - Pseudonym Certificate Authority

Feature Components

AutoCrypt® V2X-PKI — Public Key Infrastructure

The V2X-PKI component provides certificate management used to authenticate end entities such as vehicles and traffic infrastructure in an Intelligent Transport System.

- Provides certificates for OBU, RSU including Enrollment Certificates, Identification Certificates, Pseudonym Certificates, and Application Certificates
- Revokes access to misbehaving/abnormal entities through certificate revocation list (CRL)
- Designed to comply with CAMP/USDOT Security Credential Management System (SCMS) standards
- Solutions also available for Europe's C-ITS Credential Management System (EU CCMS) and China Communication System Association (CCSA)

AutoCrypt® LCM — Local Certification Management

AutoCrypt® LCM allows for safe local storage and management of required certificates, encrypting and decrypting information for verification.

- Communicates with AutoCrypt V2X-PKI to safely store certificates
- Installed directly into on-board unit (OBU) for convenient signature validation
- Designed for ease-of-use, eliminating inconvenient aspects of certificate management

AutoCrypt® IVS   Complete In-Vehicle Security

AutoCrypt® IVS protects the vehicle's internal network from both internal and external threats, providing the security modules necessary for secure ECU communication. IVS DRA, an integrated management system, provides in-vehicle security updates and management by downloading logs and the latest policies and rules through a remote management server.
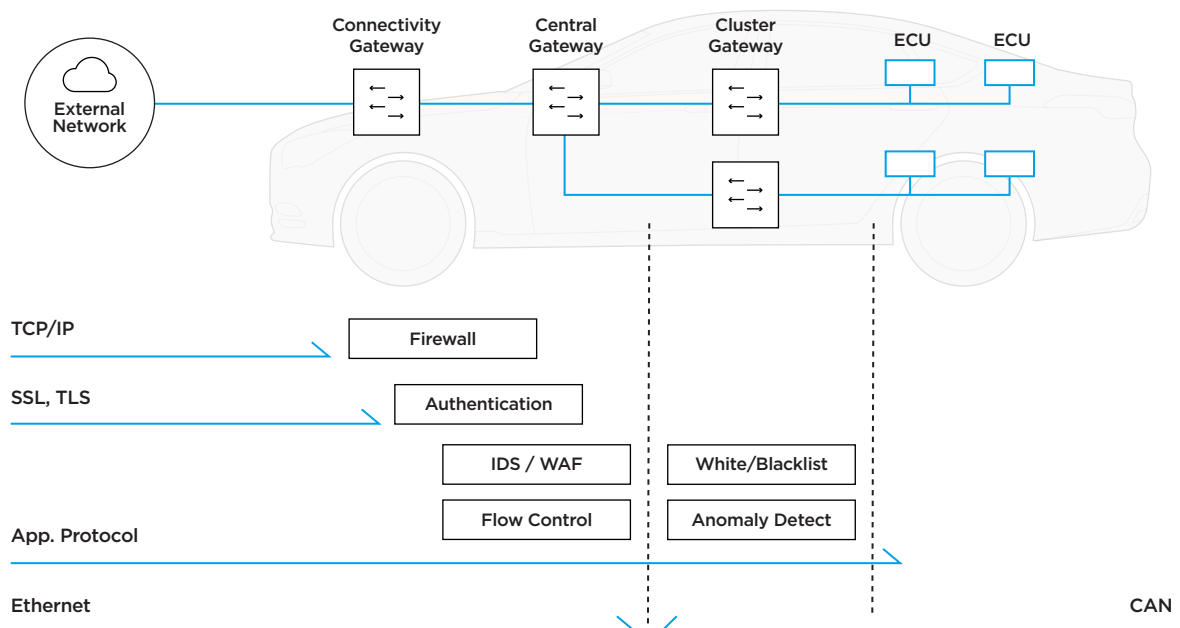
Feature Components
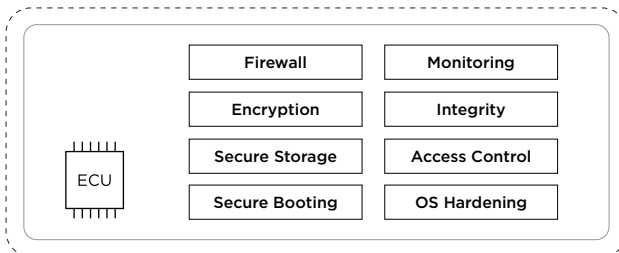
Security reinforcement and monitoring for ECUs
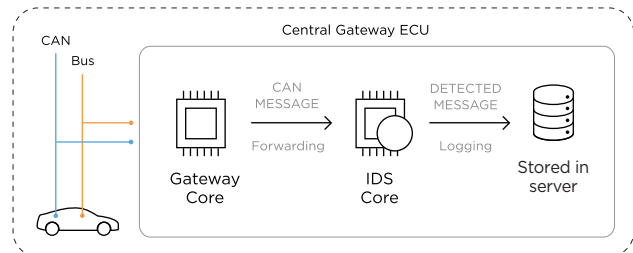
Abnormal behavior / attack detection for internal and external communication networks

WP.29 Compliant Offerings for Automotive Cybersecurity

AUTOCRYPT offers a comprehensive approach to comply with the UNECE WP.29 regulations for cyber security management systems for vehicles (UNR 155).

Consulting & Training

AUTOCRYPT security experts will work with you to conduct:

- Overview of existing CSMS
- TARA-based risk assessment
- Recommendations for security engineering

Security Product

AutoCrypt IVS (In-Vehicle Systems) provides security for ECUs and an Intrusion Detection System (IDS) for CAN bus network messages.

Testing

Regular CSMS testing with:

- Vulnerability Scanning
- Fuzz Testing
- Penetration Testing

Secure Mobility

AutoCrypt® enables security for the emerging electric mobility (e-mobility) market by protecting electric vehicles (EV) whenever they connect to electric vehicle supply equipment (EVSE). AutoCrypt® provides the necessary PKI components to enable certificate-based authentication between car manufacturers, mobility operators (MO), certificate provisioning system (CPS) providers, and charge point operators (CPO).

AutoCrypt® PnC   Secure Plug&Charge

With the growing numbers of electric vehicles and charging equipment, AutoCrypt® PnC ensures that electric vehicle supply equipment (EVSE) and their connections remain secure. AUTOCRYPT provides the necessary PKI components to enable certificate-based authentication between manufacturers (OEMs), mobility operators (MOs), certificate provisioning system (CPS) providers, and charge point operators (CPOs). With AutoCrypt® PnC, all entities of the electric vehicle experience can enjoy a seamless and secure Plug&Charge (PnC) experience.

- PnC security and PKI create robust and convenient authentication, authorization, and billing system
- In compliance with ISO 15118-2 standard for PnC charging and communications and VDE 2802-100-1
- Supports Open Charge Point Protocol (OCPP), verifying the contracts between charging station management systems (CSMS) and mobility operators
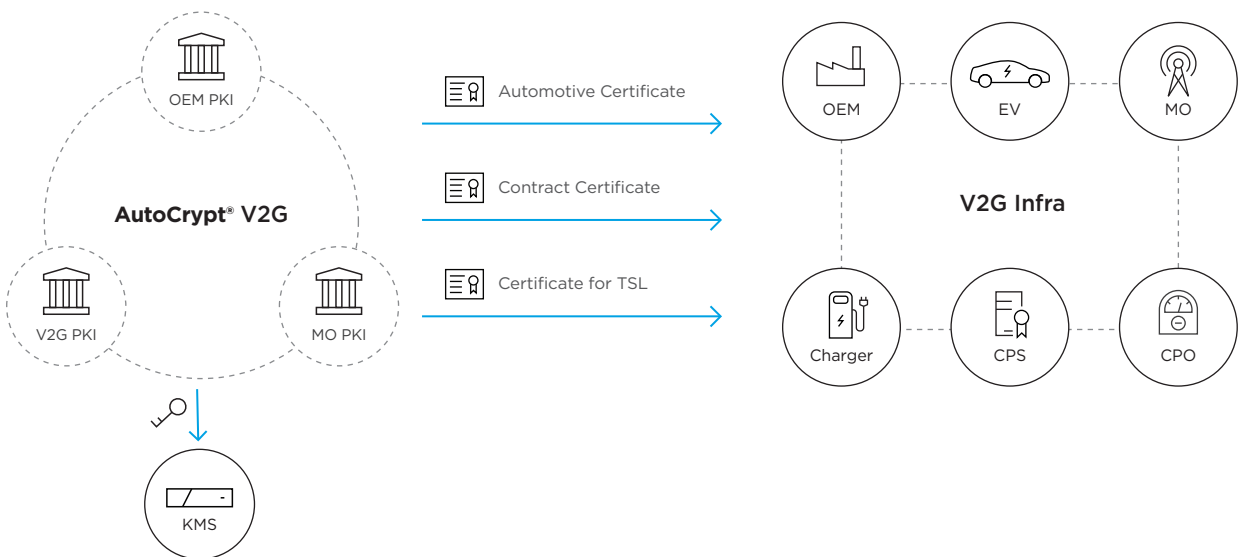
AutoCrypt® V2D   Total Digital Key

AutoCrypt® V2D allows for secure communication between connected vehicles and smart devices with a simple, secure digital key solution. With the growing Mobility-as-a-Service (MaaS) market, an interoperable and secure key solution will be central to service providers who operate car/ride sharing services or fleet services facilitated by connected and autonomous vehicles.

Highlights

- Generates and revokes digital vehicle keys, manages digital vehicle keys for multiple vehicles and users
- Supports communication via Bluetooth and NFC
- Provides PKI for certificate management in V2D infrastructure
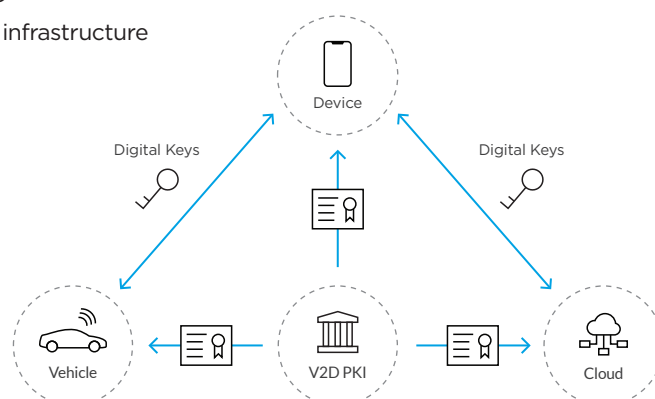
AutoCrypt® FMS

AUTOCRYPT's secure fleet management solution covers all aspects of smart mobility infrastructure, ensuring that everything from the fleet management platform to the secure operation of the fleet is covered. The modular solution can be customized and scaled to suit the service or enterprise's needs.

Fleet Management

- Safe, convenient collection of in-vehicle data in encrypted environment with proprietary OBD-II technology and/or software
- Big data analysis and data modeling using proprietary machine-learning technology, with insights shared through correlation analysis
- Identification of abnormal driving patterns and detection of in-vehicle error signals
- Optimal routes mapped from data including traffic and signal information

Securely manage and monitor data and resources through machine learning and artificial intelligence for the best fleet operational efficiency.

MDC1_O2B   MDC2_O2W   MDC2_O2L

Data collected:

- Vehicle data (battery condition, oil condition, TPMS)
- Driving data (position, speed, RPM, brake status, etc.)
- User data (age, preferences, etc.)
- V2X communication data (distance between vehicles, traffic light exchange)

Collected data allows for further development into customized solutions, allowing for a fully managed service, including development and design of applications, service operations, and comprehensive cybersecurity management.

Use cases:

- Fleet management platform
- Real-time taxi dispatch platform
- Integrated EV management platform
- Barrier-free transportation assistance system
- Social mapping application for barrier-free navigation

AUTOCRYPT's fleet management solution can be customized and combined with other products and solutions to provide enhanced security measures. With the expansion of mobility services, it is essential that security remains a priority.