AUTOCRYPT

Secure New Mobility and Transportation

The car is evolving into a living space.

While the integration of cars with IT platforms offer convenience, safety concerns are also growing. Connecting cars to thousands of IT infrastructure means that there exists a potential of not only losing valuable assets, but also priceless human lives. This is why security is so critical in the cars of tomorrow.

Based on the core technologies and industry experience of Penta Security Systems, an enterprise IT security company for 22years, Autocrypt Co., Ltd. provides mobility security solutions for traffic systems of the future. Autocrypt solutions are compliant with global standards and have been implemented and successfully tested in various traffic system environments. The company continues to develop transportation solutions and services, with its steadfast commitment to safety and security.

In order to deliver on tomorrow's technological promises and convenience, we need to secure an ever-evolving vehicular environment so that vehicles can connect with the outside world with safety and trust. Autocrypt is working to make this future a reality.

History

2019
- Signed MOU with Hubject / ElaadNL to develop electric vehicle charging interoperability technology
- Joined the International Transport Forum (ITF) affiliated OECD
- Completed car manufacturer S company V2X security solution consulting
- Korea Expressway Corporation V2X security certification system demonstration system construction project
- Development of security solution for In- vehicle infotainment(IVI) of electronics manufacturer M company
- Development of certification authority demonstration system for V2X security certification system of Korea Intelligent Transportation System Association
- AutoCrypt® selected as TU-Automotive AWARDS 2019 best auto cybersecurity product / service
- Established security infrastructure for charging electric vehicles of KEPCO
- Seoul C-ITS demonstration project security system construction

2018
- Establishment of certification system for electric vehicle charging companies (MO) of KEPCO
- Establishment of C-ITS demonstration project security system in Jeju
- Commercialization of Gridwiz and EV plug and charge solution
- Development of smartphone - based C-ITS service for mobile manufacturer S company V2P (vehicle and smart device)
- V2X security informatization strategic plan for Korea Expressway Corporation
- Prototype of train autonomous driving control system (T2T) security module

2017
- Development of TLS / HSM security technology for completed car manufacturer H company V2G
- K-City autonomous driving experiment city (Hwaseong, Gyeonggi-do)
- Establish security certification system for autonomous cooperative driving at Yeoju Expressway
- Analyze security vulnerability of train control system (T2T) protocol and design security module for railway vehicles for Koera Railroad Research Institute
- Established certification center for development of smart autonomous driving cooperation road driving system
- Development of security technology for next generation IVI terminal

2016
- Development of core technology for detecting abnormal symptoms for autonomous smart car
- Construction of security certification system for Korea Expressway Corporation C-ITS pilot project (Daejeon-Sejong)
- Development of abnormal behavior detection function based on K-BrainPower machine learning

2015
- Launched korea's first auto security solution AutoCrypt®
- Smart car firewall prototype development

2014
- Development of security technology of completed car manufacturer H company's Vehicle Data Management System (VDMS)
- Developed smartphone app security verification technology for completed car manufacturer H company
- Secured korea's first vehicle communication security technology (IEEE 1609.2 standardization and test bed application)

2013
- Developed international standard (IEEE1609.2: 2013) technology for V2X environment based on WAVE communication

2012
- Development of police car navigation / telematics system certification / encryption

2011
- Enhance security by applying authentication and encryption for vehicle and external smart device interworking

2007
- Development of completed car manufacturer H company 's security device (security communication technology between vehicle and diagnostic device) for vehicle safety diagnosis device

Association and Standard Activities

International Transport Forum

OMNIAIR CONSORTIUM

CHARIN

ITS KOREA

CARCONNECTIVITY consortium®

KSGA Korea Smart Grid Association

Awards

TU-Automotive AWARDS

FROST & SULLIVAN

TU-Automotive Awards
Best Auto Cybersecurity
Product/Service 2019

Cybersecurity
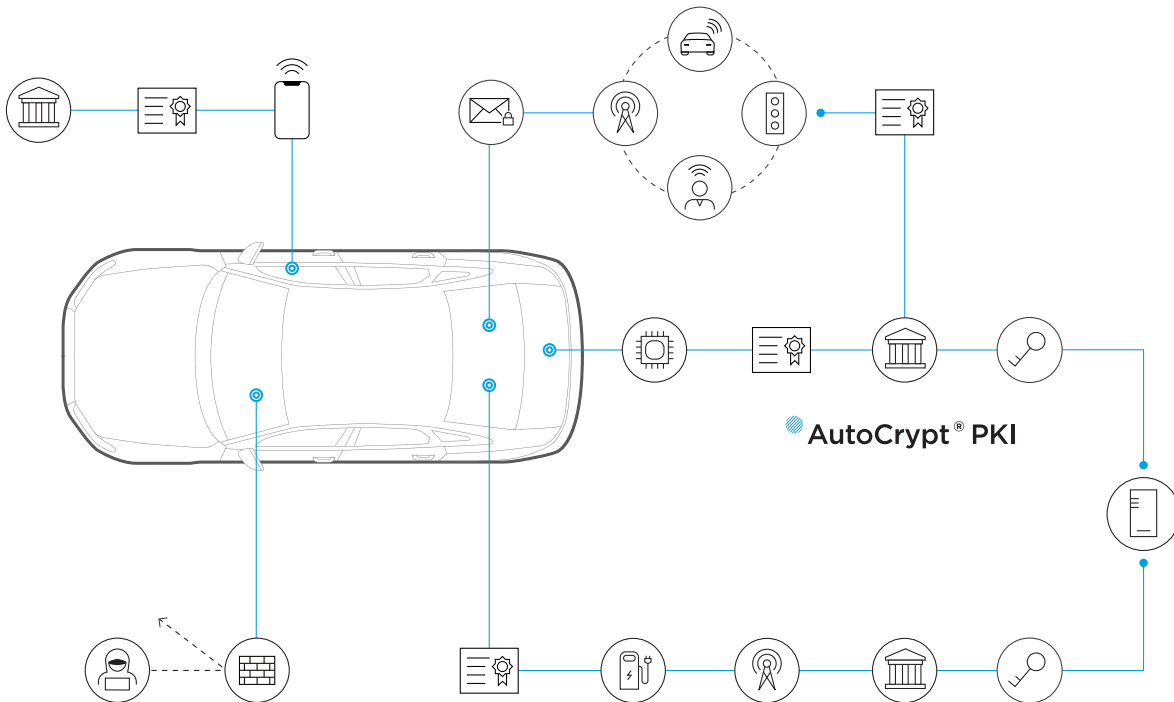Excellence Awards
Winner 2018

The beginning and end of the car, complete security is AutoCrypt®

AutoCrypt® is a total vehicle security solution for next-generation intelligent transportation systems (C-ITS) and smart cars
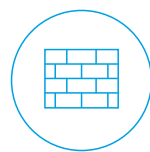
AutoCrypt® V2D   AutoCrypt® V2X

AutoCrypt® PKI

AutoCrypt® AFW   AutoCrypt® V2G

Security total solution customized for smart car

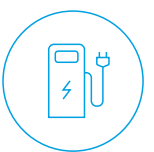### Intelligent Transport Systems

AutoCrypt® provides the core security components required to protect communication in Intelligent Transport System.
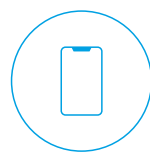
In-Vehicle Security

AutoCrypt® protects the internal systems of vehicles by detecting malicious or abnormal traffic and securely managing encryption keys used within internal networks.

Electric Car and Charging System

AutoCrypt® secures the Plug & Charge process by protecting electric vehicles and charging stations and preventing data from being hacked when plugged-in at supply stations.

Mobility Security Solution

AutoCrypt® enables secure interaction between vehicles and user devices for the provision of mobility services such as those that leverage mobile apps as digital keys to manage vehicle access.
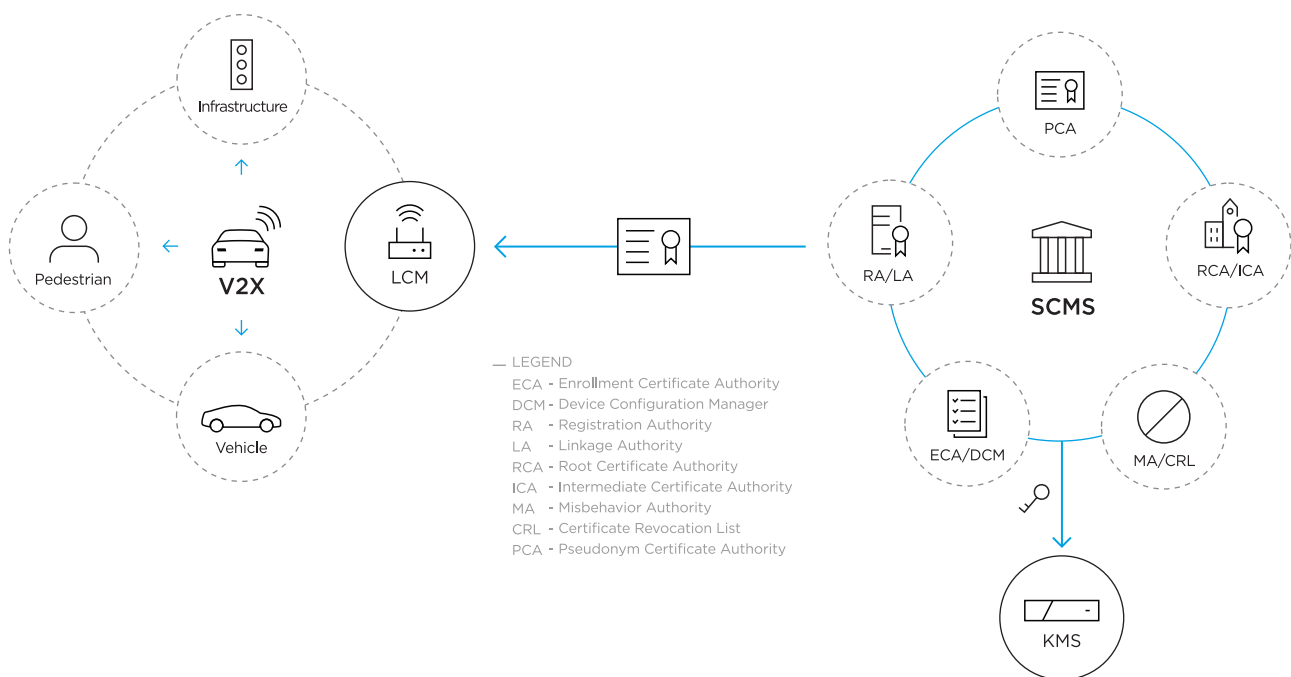
AutoCrypt® provides a comprehensive suite of solutions for securing communications in Intelligent Transport Systems (ITS) while meeting industry standards published by established organizations such as Crash Avoidance Metrics Partnership (CAMP), the U.S. Department of Transportation (USDOT), and other leading authorities.

AutoCrypt® V2X

Secure Communication System for Vehicles and Infrastructure

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

- Secures broadcast and receipt of basic safety messages (BSM) and other data between surrounding vehicle on-board units (OBU) and roadside units (RSU)
- Designed according to the IEEE 1609.2 communication standard for Wireless Access in Vehicular Environments (WAVE)
- AutoCrypt® LCM is a local certificate manager (LCM) that is installed in the OBU to manage certificates from AutoCrypt® PKI

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

AutoCrypt® PKI

PKI Authentication System for Vehicles and Infrastructure

AutoCrypt® PKI is a public key infrastructure (PKI) system that complements by providing certificate management used to authenticate end entities such as cars and traffic lights in an ITS.

- Enrolls new end entities into the system, provisions identification certificates and pseudonym certificates, and revokes access from misbehaving end entities
- Designed to comply with the CAMP/USDOT Security Credential Management System (SCMS), with solutions also available for the European Cooperative ITS (C-ITS) Credential Management System (CCMS)
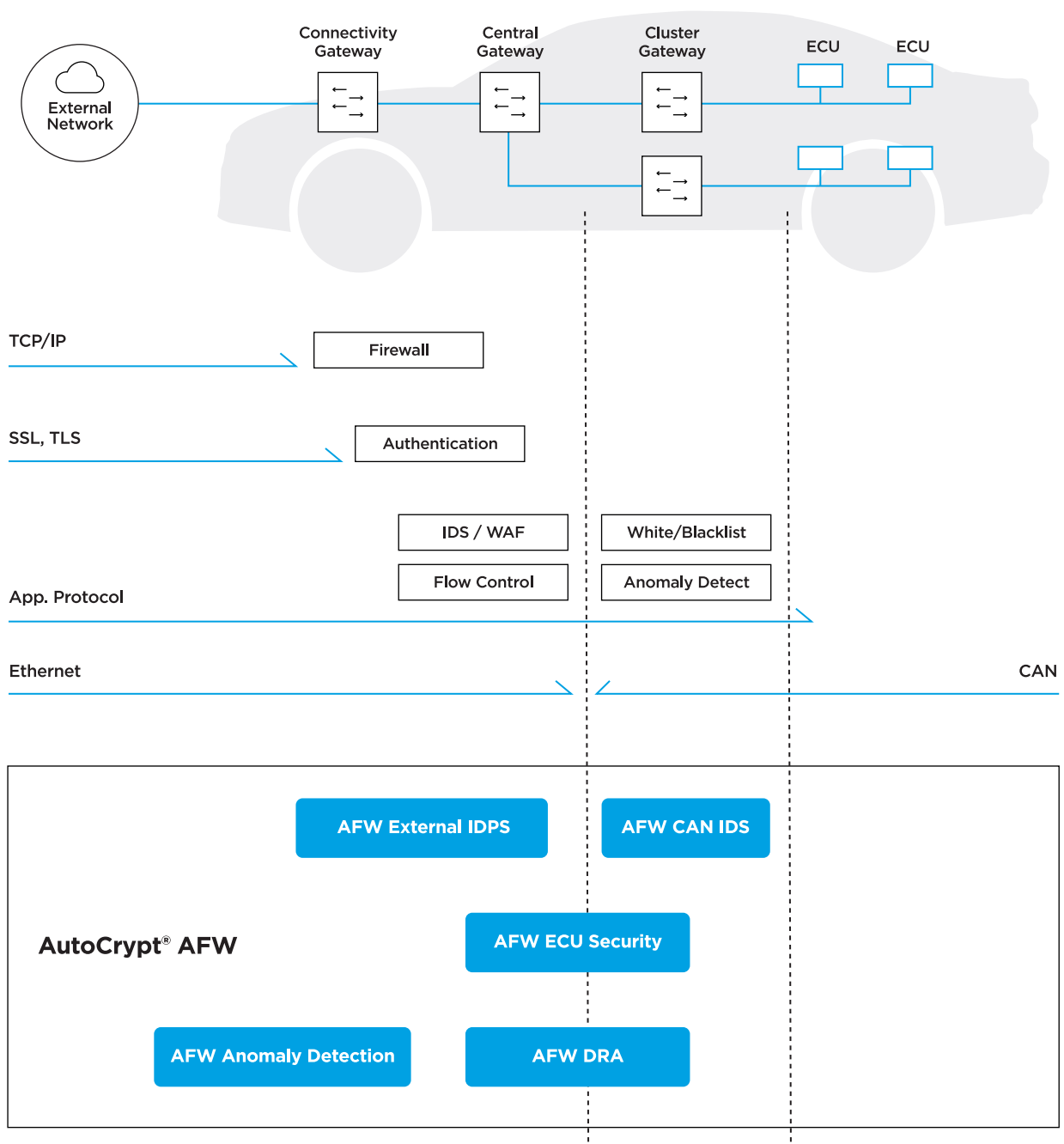
AutoCrypt® AFW

Security for In-Vehicle Systems

AutoCrypt® AFW series protects the vehicle's internal network from internal/external threats and provides the security modules necessary for secure ECU communication. AFW 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

- **AFW External IDPS** – Detects abnormal traffic from outside the vehicle and provides access control features
- **AFW CAN IDS** – Detect intrusion of In-vehicle's CAN network
- **AFW Anomaly Detection** - CAN signal anomaly detection based on machine learning technology
- **AFW ECU Security** - Secure Boot, Secure Storage, Encryption of Vehicle Communication Data based on HSM/TEE
- **AFW DRA**- Log Transfer, Transfer Download and Patching

Electric Car and Charging Systems

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® V2G

System Security for Electric Vehicle Charging Systems

AutoCrypt® V2G enables confidentiality, integrity, and availability in vehicle-to-grid (V2G) systems. Upon plugging the EVSE or charging station to the EV, AutoCrypt ® V2G allows for an effortless yet secure Plug & Charge (PnC) experience.

In addition to securing PnC communication, AutoCrypt ® V2G provides PKI for certificate management in the e-mobility service infrastructure.

- PnC security and PKI help create a robust and convenient authentication, authorization, and billing V2G system
- Support for ISO 15118-2 standard between electric car and charger for PnC charging
- Support for the Open Charge Point Protocol (OCPP) for secure communication with CPOs
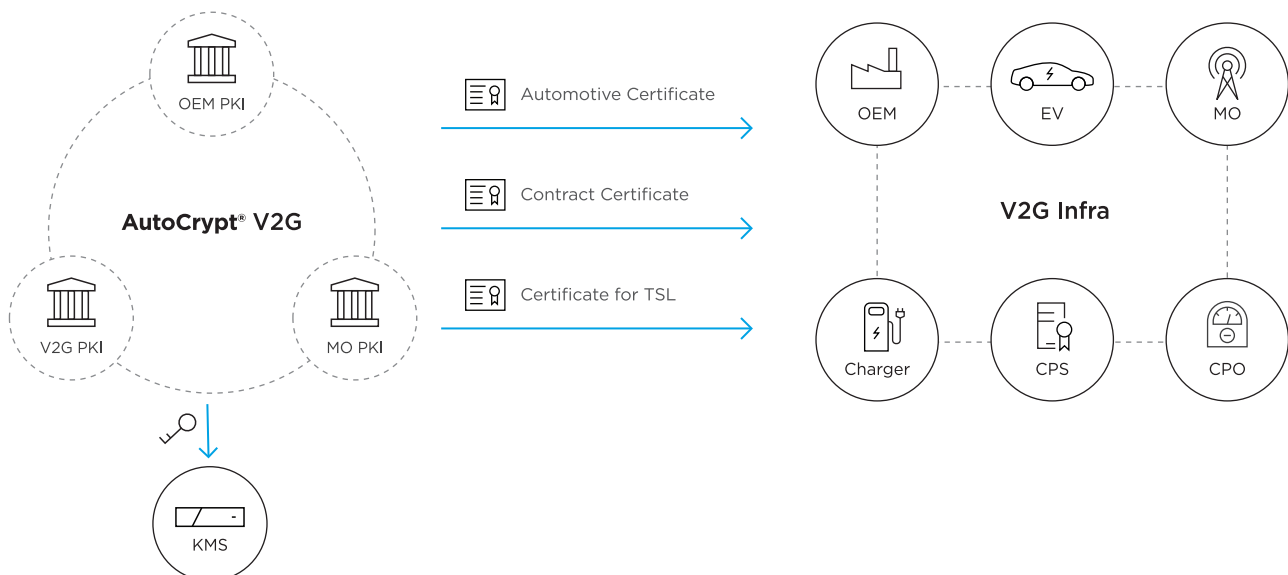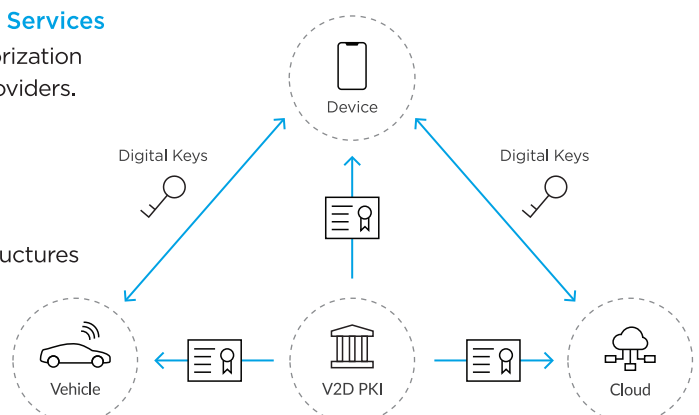

Mobility Security Solution

AutoCrypt® enables the secure communication between smart cars and smart devices which will be central to the emerging mobility-as-a-service (MaaS) market. MaaS providers that benefit include those operating car sharing services or logistics services facilitated by autonomous vehicles.

AutoCrypt® V2D

Secure Communication for Vehicles, Devices & Cloud Services

AutoCrypt® V2D provides secure authentication and authorization between vehicles, mobile devices, and backend service providers.

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

# Mobility Control and Data Solutions

AutoCrypt® FMS

Advanced Fleet Management System for Smart Car Environment

With security and convenience in mind, AutoCrypt® FMS collects, analyzes and re-processes large amounts of data from various mobility services. Our solution is directly applicable to taxi, transportation and car sharing services to improve service quality and create new revenue sources.

- Safe and convenient collection of in-vehicle data in an encrypted environment with plug-in data collectors and software
- Privacy protection through data encryption and anonymization
- Big data analysis and data modeling, using AutoCrypt's proprietary machine learning techniques, as well as insights through correlation analysis
- Identification of abnormal driving and detection of in-vehicle error signals
- Optimal routes using various information, such as traffic and signal information

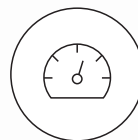**Mobility Operators**　　　　　　　　　　　　　　　　　　　　　　**AutoCrypt® FMS**

DATA

Real time control and analysis service based on user data
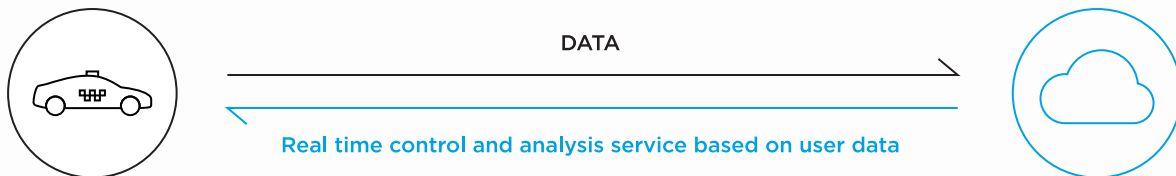
Collected Data Range
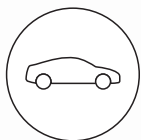
Vehicle data
Battery condition, oil condition, tire pressure, etc

Driving data
Position, speed, RPM, brake pedal status, etc.

User data
User age, gender, music preferences, etc.

V2X communication data
Distance warning message between vehicles, communication between vehicles and traffic lights

Extra service

Mobility Data Consulting

- Diagnosis of status data and business requirements
- Propose a clear solution using data causality.
- Forecast and verify data-based expected effects (eg accident rate, sales estimates, etc.)

Mobility Intelligence Solution

- Taxi call, route recommendation, driver compensation, electric car charging station guide, etc
- Provide shared mobility data source
- Strong security data management system

AUTOCRYPT