THE NEW MOBILITY PARADIGM

An Introduction to
Mobility Transformation and
Automotive Cybersecurity

AUTOCRYPT

Contents

DISCLAIMER: This document is for informational purposes only. Information is general in nature, and is not intended to and should not be relied upon or construed as a legal opinion or legal advice regarding any specific issue or factual circumstance. Information may not contain the most up-to-date information. Readers of the document should contact their automotive / cyber security solutions provider for the most up-to-date information to obtain advice with respect to solutions application.

All liability with respect to actions taken or not taken based on the contents of this site are hereby expressly disclaimed. The content on this document is provided "as is;" no representations are made that the content is error-free.

Introduction to Mobility Transformation

The unprecedented development in mobility has shifted the automotive industry with significant repositioning and retrenching.

By nature, hardly anything stays the same in the automotive industry. The paradigm shift has not only been opening up in many directions for pedestrians, drivers, but also for manufacturers and suppliers. These changes require major development in semiconductor content, as traditional vehicles are transforming into supercomputers on wheels.

Established companies are entering the market to maximize their resources to focus on developing new-age software and are determined not to be left behind in the participation of development of electric vehicles, low-power technology, and batteries via new business strategies.

Governments across the world are setting new goals to define travel time for urban areas as well as putting automated vehicles into public transportation systems. New regulations and government-initiated projects will help with the development of MaaS (mobility-as-a-service) deployments as well as towards using data and open platforms to build a technology-enabled mobility environment.

What does this mean for us?

Each year, electric vehicle sales reach an all-time high globally and it made it easier for the public to become more engaged with self-driving vehicles and emerging technologies, especially in Europe more than anywhere else in the world. The main reason behind this is that major cities in Europe have already announced plans to implement and invest further in amending regulations for both shared and private mobility, as improving connectivity is considered desirable as a public good.

For governments to measure growth and productivity effects of automation, they mostly focus on measuring the increase in interactions, productivity, competition, and market opportunities between cities – which not only offers economic growth, but also supply chain efficiency, and resilience through better connectivity.

And for most businesses, preparing for the future of mobility will lead to a big transformation that requires changes in management framework, systems, and operations.

Furthermore, according to McKinsey, investment activities have also accelerated, leaving the E-hailing and Semiconductor sectors to lead the investment trend followed by AV sensors, ADAS components, connectivity, infotainment, and EV and charging.

The Automotive Revolution

According to McKinsey, electrified vehicles have become more viable and competitive, and are expected to expand market share by 2030. Although China still accounts for the largest market (44 percent!) in the world, the EV market share expanded to 26 percent in Europe (growing by 44 percent, the highest rate since 2016) reaching 590,000 units.

With the exception of Hong Kong, 9 of the top 10 markets for EV penetration were all in Europe. This is expected to pose major changes for manufacturers and suppliers. Although China and the United States have been heavily affected by the pandemic, the sales are expected to rebound through various policy changes including tax exemptions and zero-emission vehicle programs.

One of the fastest-growing EV manufacturers, Tesla increased its global market share to 16 percent in 2019 to 18 percent in 2020 with Model 3 and Y leading the majority of sales. Additionally, Tesla is expanding its global manufacturing footprint starting off with the construction of its Shanghai plant in 2019 and is expected to build its next plant in Germany in 2021.

With this paradigm shift, the behavior of the consumers towards mobility and transportation is also changing, meaning that potentially at least one out of ten cars sold in 2030 may be a shared vehicle and subsequently, the market for fit-for-purpose mobility solutions will rise. Moreover, with the mobility industry becoming more complex and diversified, competition is expected to increase drastically amongst OEMs and new entrants such as mobility solution providers.

However, until fully autonomous vehicles are commercially available, ADAS (advanced driver assistance systems) is playing a huge role in preparing regulators, manufacturers, and consumers. The goal for mobility security providers here is to make sure that the shift is smooth as possible, allowing advanced safety to take place before the official deployment.

Autonomous Driving & V2X

An autonomous vehicle is capable of sensing its surroundings and adjusting its behaviors, reducing the amount of human intervention needed for driving.

In 2014, the SAE (society of automotive engineers) published a scale to define 5 different autonomy levels of autonomous driving. We're here to walk you through the detailed definitions of each level of autonomous driving.

Levels 0-2: Partial Automation
(Human monitoring required)

Level 0 No Automation
The driver performs all driving tasks.

Level 1 Single Automated System
Steering or accelerating assistance.
Cruise control.

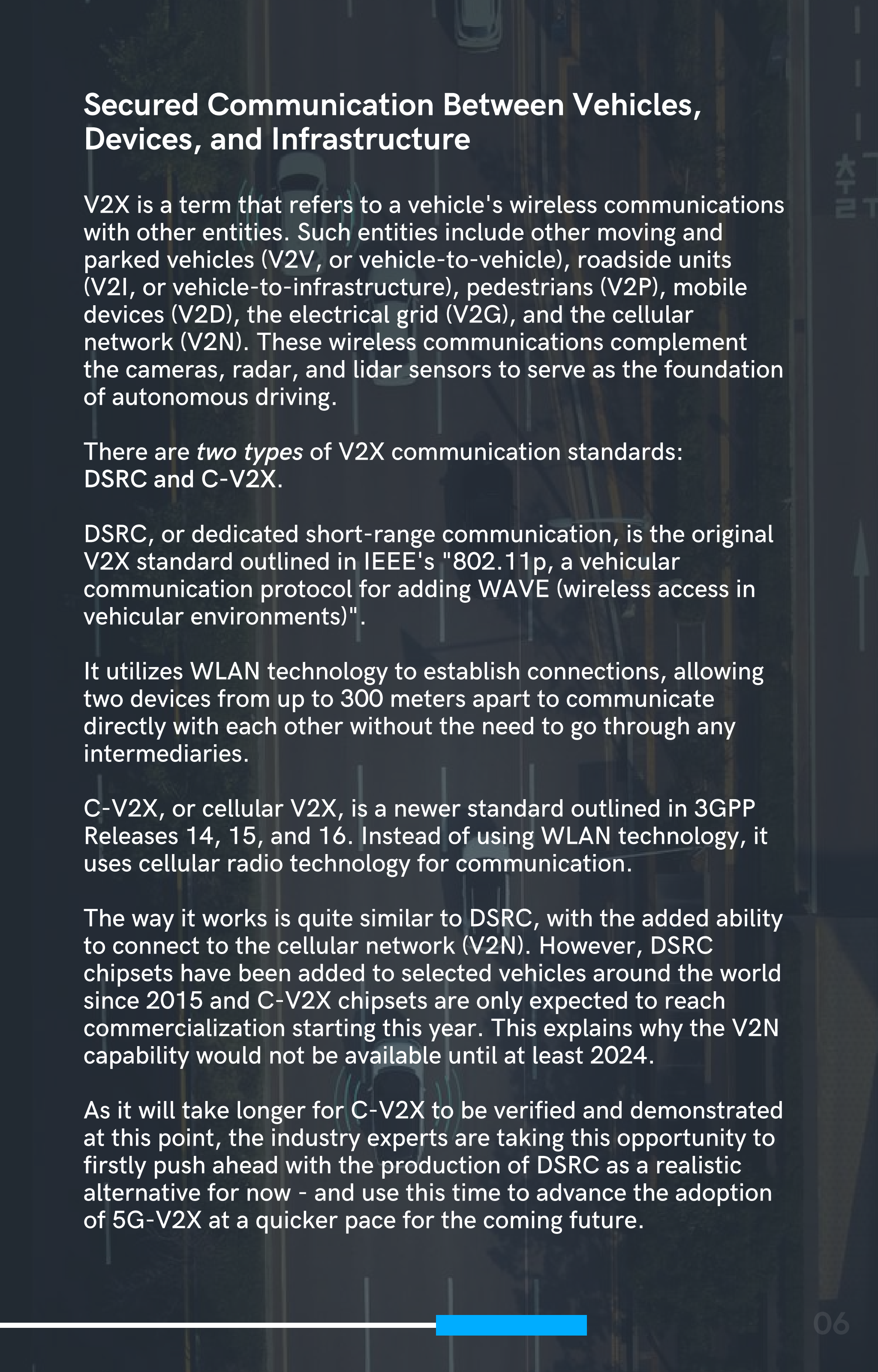
Level 2 Partially Automated System
Most driving tasks performed automatically.
Driver still needs to override when needed.

Levels 3-5: Automated System Driven

Level 3 Conditional Automation
All driving tasks performed with geofencing tech. Driver can override if needed.

Level 4 High Automation
Zero human interaction required.

Level 5 Full Automation
ADAS: Advanced Driver Assistance Systems.
Driver can take over anytime.



Secured Communication Between Vehicles, Devices, and Infrastructure

V2X is a term that refers to a vehicle's wireless communications with other entities. Such entities include other moving and parked vehicles (V2V, or vehicle-to-vehicle), roadside units (V2I, or vehicle-to-infrastructure), pedestrians (V2P), mobile devices (V2D), the electrical grid (V2G), and the cellular network (V2N). These wireless communications complement the cameras, radar, and lidar sensors to serve as the foundation of autonomous driving.

There are *two types* of V2X communication standards: DSRC and C-V2X.

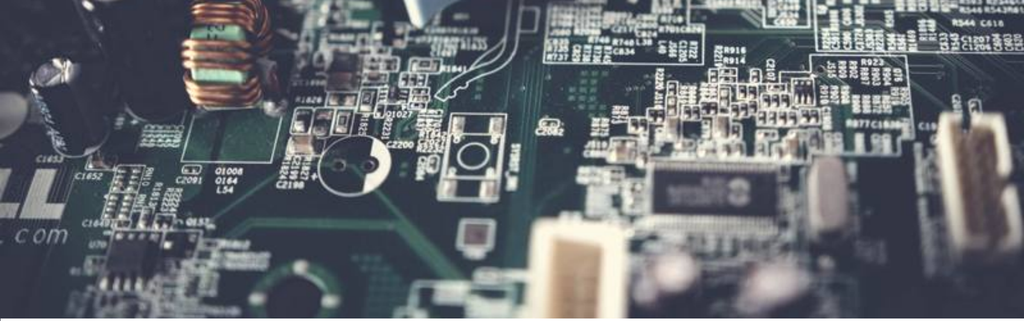
DSRC, or dedicated short-range communication, is the original V2X standard outlined in IEEE's "802.11p, a vehicular communication protocol for adding WAVE (wireless access in vehicular environments)".

It utilizes WLAN technology to establish connections, allowing two devices from up to 300 meters apart to communicate directly with each other without the need to go through any intermediaries.

C-V2X, or cellular V2X, is a newer standard outlined in 3GPP Releases 14, 15, and 16. Instead of using WLAN technology, it uses cellular radio technology for communication.

The way it works is quite similar to DSRC, with the added ability to connect to the cellular network (V2N). However, DSRC chipsets have been added to selected vehicles around the world since 2015 and C-V2X chipsets are only expected to reach commercialization starting this year. This explains why the V2N capability would not be available until at least 2024.

As it will take longer for C-V2X to be verified and demonstrated at this point, the industry experts are taking this opportunity to firstly push ahead with the production of DSRC as a realistic alternative for now - and use this time to advance the adoption of 5G-V2X at a quicker pace for the coming future.



Recent Developments

Autonomous driving relies on various sets of technologies: most definitely sensors (surprisingly, lidar sensors have been equipped on cars for over a decade, while cars with V2X communication technologies entered the market starting in 2017!) and cameras for real-time data collection as well as wireless communication technology for fusioning, to ultimately advance the overall development of the technology.

The sensors equipped around the vehicle shoot out laser lights to the surroundings and receive feedback so that the vehicle can adjust itself to adapt to the environment. V2X technology is then utilized for collaborative driving to make transportation systems and vehicles smarter at the same time, and aim to overcome the technical limitations of the existing sensors and communication method.

□However, we need to first get the facts straight for safety applications. After more than a decade of cross-country field tests, DSRC went into production in the US, Europe, Korea, and Japan. Similarly, C-V2X also gained momentum in China and is moving ahead with the deployment. As both technologies have different advantages, it is critical to understand the differences and deploy accordingly.

Though just like any other emerging technologies, there are a few things to consider before we integrate the technology into our lives. What really makes autonomous vehicles autonomous is the ability to detect and let the vehicle control, and most importantly, sensor the surrounding environment to drive the vehicle on its own – which brings us back to Level 5, the fully automized driving technology.

V2X Security

The world is expecting a few automotive manufacturers, including Tesla, to achieve Level 5 autonomous driving technology in the next few years. This brings us back to the most legitimate concern - safety. Can we fully trust self-driving vehicles, let alone rest while it takes us to our destinations?

This is where the most important security technology, V2X security comes in.

As vehicles are no longer a simple means of transport, but an integrated service that provides a wide range of functions, the need for total security for connected and autonomous vehicles is increasing dramatically. For a vehicle to operate safely, the most important thing is to secure it with V2X security technology.

Whether the manufacturer chooses WAVE or C-V2X, either communication method must meet the standard of employing reliable security in order to successfully implement the V2X communications system.

This means that the connections between vehicles, devices, and infrastructures need security for the BSMs (basic safety messages) between OBU (on-board units) and RSU (roadside units) via encryption and digital signature technologies, so that it protects and ensures secured communications.

Additionally, with emerging threats targeted at autonomous vehicles, charging platforms, and fleet management systems, safeguarding the vehicle itself isn't enough for us to enjoy the technologies with maximized benefits.

In-Vehicle Systems (IVS)

Inside autonomous vehicles, there are approximately 150 ECUs (electronic control unit) and they are embedded minicomputers in a vehicle that control its electrical systems, which then determine the vehicle's movement. A modern car today contains around 80 of these units. Some of the ECUs include the ECM (engine control module), PCM (powertrain control module, and TCM (transmission control module). These units serve as the car's computer.

Also, it is expected that autonomous vehicles will contain more than 300 million software codes by 2030. After all, these connected vehicles will not only serve as a means of transportation, but will be able to provide telematics, V2X, charging systems, and different types of smart devices for us in the near future.

In order for autonomous vehicles to employ these emerging technologies, the vehicles must deploy OTA (over-the-air) technology to get up-to-date vehicle systems such as infotainment, and navigation services that are secure and efficient.

Electric Vehicles and Plug&Charge (PnC)

Plug&Charge is a technological concept outlined in ISO 15118 – the international standard for V2G (vehicle-to-grid) communication interface – currently applied at many EV charging stations across the globe.

It is essentially a secure communication protocol that allows the vehicle to communicate seamlessly with the charging station and the electrical grid, enabling a completely automated charging and payment process without the need for human intervention, so that the driver can simply plug and charge the vehicle at any charging station without having to carry credit cards once enrolled in a membership.

As the number of EV charging stations ticks just above 1 million across the world, it is more important than ever to secure both vehicles and charging stations through OCPP (open charge point protocol) and verify between the contract, CSMS (charging station management systems), and mobility operators in order to safely deliver energy to the vehicle.

Fleet Management & MaaS

As a few major trends influence the automotive sector, it's leading to huge and rapid changes and challenges for both traditional manufacturers and service providers. Moreover, as the new era of transportation approaches, more and more businesses are striving to differentiate themselves in the market and trying to integrate themselves into offering more value-added, customer-centered mobility services.

An ideal fleet management system is connected to the vehicle and must be able to allow the owners to manage vehicle information in real-time, while also connecting accrued data to big data-based AI and make full use of it for accident prevention and maintenance.

Mobility-as-a-Service: MaaS

MaaS describes the shift towards mobility provided as a service that includes support in each step of transportation, from travel planning to payment support. The key is to offer various mobility solutions for travelers that best meet their travel needs and by providing one efficient platform that enables the best transport experience, MaaS can also accelerate and improve the autonomous driving industry and bring new opportunities and business models to serve unmet demands.

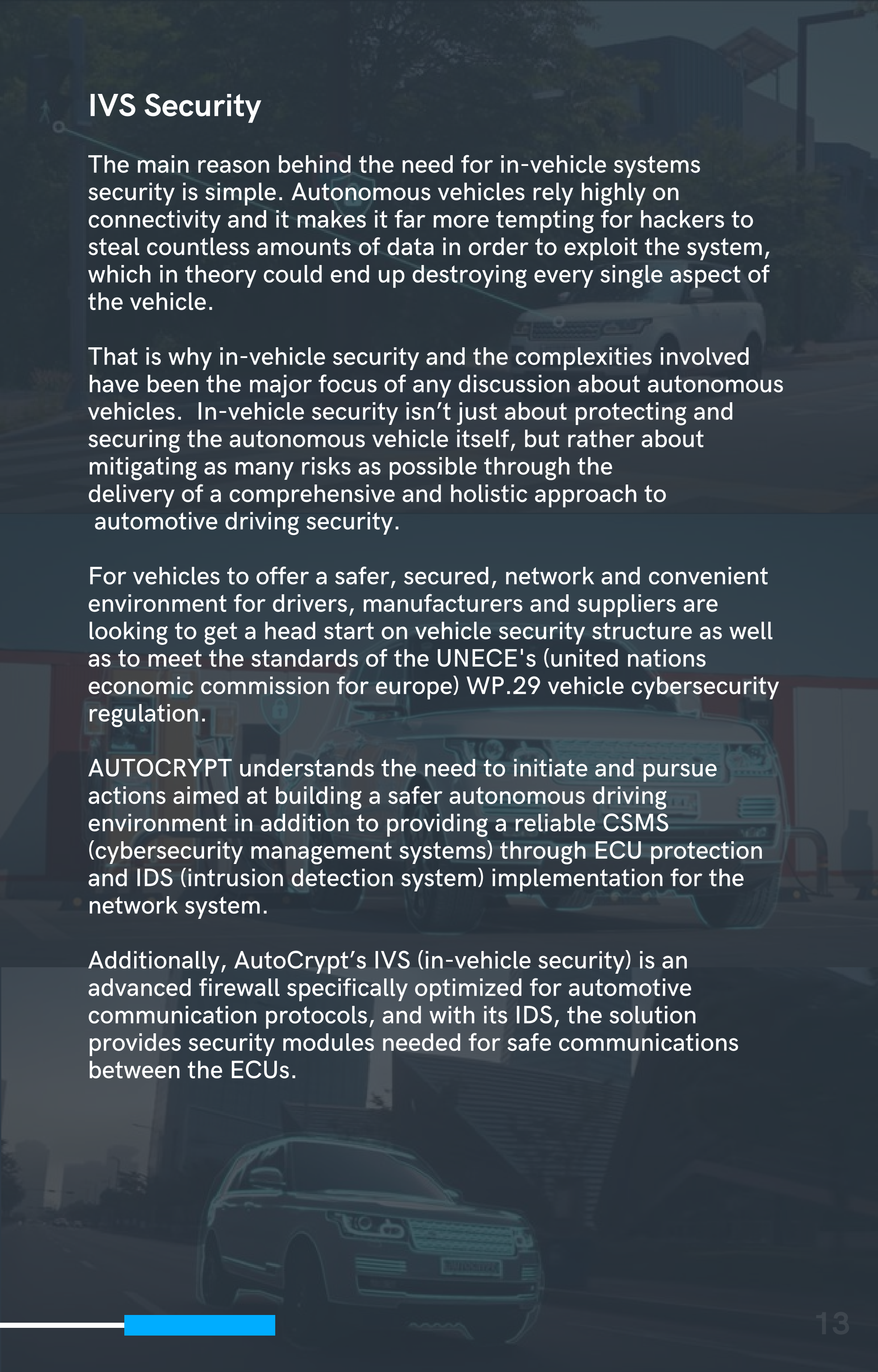
Mobility Security Solutions

The recent growth of on-demand transport services is changing mobility patterns and the way people move and interact. Such changes signal the emergence of a new transportation system.

The new transportation system integrates various transportation and mobility services into a combined package. It is no longer a simple means of transport, but an integrated service that provides a wide range of functions like subscriptions and payments.

In order for this transformational change to move forward, AUTOCRYPT is pursuing an integrated focus strategy to further strengthen and ease the distribution of the foremost important security solutions for the changing mobility industry.

AUTOCRYPT provides the most essential needs such as V2X, V2G (Plug&Charge), and FMS security for game players that are ready to evolve their value proposition from "automotive manufacturer" to "mobility service provider".



IVS Security

The main reason behind the need for in-vehicle systems security is simple. Autonomous vehicles rely highly on connectivity and it makes it far more tempting for hackers to steal countless amounts of data in order to exploit the system, which in theory could end up destroying every single aspect of the vehicle.

That is why in-vehicle security and the complexities involved have been the major focus of any discussion about autonomous vehicles. In-vehicle security isn’t just about protecting and securing the autonomous vehicle itself, but rather about mitigating as many risks as possible through the delivery of a comprehensive and holistic approach to automotive driving security.

For vehicles to offer a safer, secured, network and convenient environment for drivers, manufacturers and suppliers are looking to get a head start on vehicle security structure as well as to meet the standards of the UNECE's (united nations economic commission for europe) WP.29 vehicle cybersecurity regulation.

AUTOCRYPT understands the need to initiate and pursue actions aimed at building a safer autonomous driving environment in addition to providing a reliable CSMS (cybersecurity management systems) through ECU protection and IDS (intrusion detection system) implementation for the network system.

Additionally, AutoCrypt’s IVS (in-vehicle security) is an advanced firewall specifically optimized for automotive communication protocols, and with its IDS, the solution provides security modules needed for safe communications between the ECUs.

V2X Security

Utilizing user authentication and data encryption technologies, AutoCrypt V2X is a security solution that secures wireless communications by authenticating the sender and receiver, and by encrypting the messages in transmission. By doing so, it safeguards the sensitive information with regards to the driver and the vehicle, while ensuring that the data being transmitted is not altered in any way.

AUTOCRYPT also provides a PKI (public key infrastructure) solution, complementing AutoCrypt V2X via certificate-based authentication (IEEE 1609.2) for end entities. Through certificate generation, distribution, and revocation, it enhances the reliability of V2X communication.

PnC Security

As explained earlier, Plug&Charge (PnC) is a technical concept introduced by ISO 15118, the international standard for charging EVs. It basically allows drivers to charge the vehicles as it automatically identifies itself and starts recharging the battery, through a user-convenient and secured way of charging EVs at any charging stations across the world that supports this standard.

For this to work safely, AUTOCRYPT’s V2G security solution allows both ends to be authenticated for the realization of secure mobility connectivity. It protects both the vehicle and its supply equipment during the entire PnC process and provides secure communication modules and certificate management for all participants involved in this process using PKI technology.

Fleet Management System

Fleet management solutions like AutoCrypt FMS are here to improve the whole fleet management system so that it can collect, analyze, and deliver data safely and efficiently through data analysis and customized developments.

AUTOCRYPT's FMS provides the simplest mobility services with data collection from real-time ride-hailing platforms, through its proprietary hardware technology, MDC1-O2B. Ride-hailing or taxi platforms not only conveniently secure all data in an encrypted environment for the protection of personal identification information, but also gain insight through data modeling and correlation analysis from AUTOCRYPT's machine-learning technology and big data.

Use cases include:

- Mobility Management System
- Real-time Taxi Dispatch Platform
- EV Integrated Management System
- Barrier-Free Transportation Assistance

About AUTOCRYPT

Secure First, Then Ride

AUTOCRYPT is an automotive cybersecurity solutions provider based in Seoul, South Korea. Initially developed in-house at Penta Security in 2007, AUTOCRYPT spun off as a separate entity in 2019, carrying over more than a decade's worth of experience and expertise. Its core business areas are V2X, PnC, and FMS security, along with consulting services. AUTOCRYPT has been leading major C-ITS projects in South Korea for smart road and highway V2X capabilities through its core security solutions.

With offices in South Korea, China, Japan, and Canada, along with strong partnerships across Europe and North America, AUTOCRYPT's security solutions are widely accessible to testbeds, OEMs, Tier-1 suppliers, and automotive software or service providers located across the world.