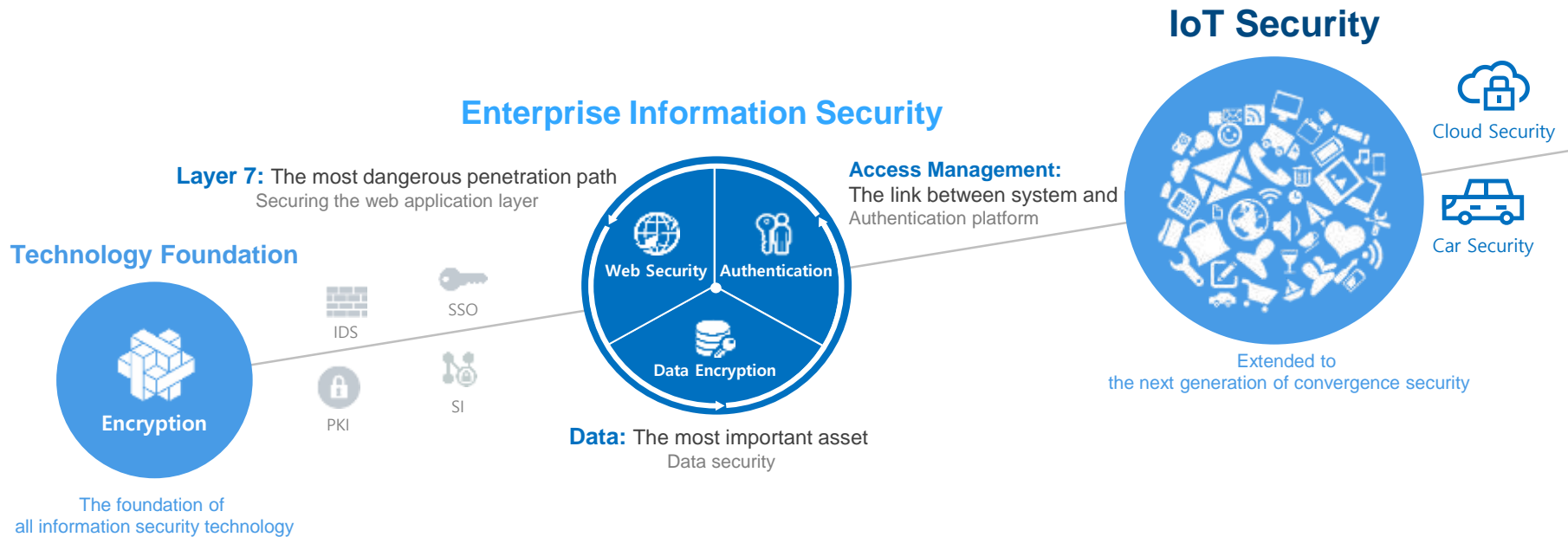# Smart Security for Smart Cars

Introduction to AutoCrypt®

SangGyoo SIM, Ph.D.
sgsim@pentasecurity.com
Head of PICL (Penta IoT Convergence Lab.)

Penta SECURITY a leader in web, IoT, and data security solutions and services

Driving innovations across encryption, authentication, and signature-free firewall detection technology, Penta Security enables resilience in an era of hyper web integration and connectivity.

IoT Security

Enterprise Information Security

Layer 7: The most dangerous penetration path
Securing the web application layer

Access Management:
The link between system and
Authentication platform

Technology Foundation

IDS

SSO

Web Security Authentication

Data Encryption

PKI

SI

Encryption

Cloud Security

Car Security

Extended to
the next generation of convergence security

Data: The most important asset
Data security

The foundation of
all information security technology

Company Overview

Founded	July 1997	**Business Area**	Data Encryption, Web Security, Authentication Platform
CEO/Founder	Seok-woo Lee	**Client**	3,300 clients from government, public, corporate, education, finance sectors
Staff	250 employees (150 in R&D and tech support)		Data Encryption Platform **D'Amo**
Located	Seoul, Republic of Korea	**Products**	Web Security Solution **WAPPLES**
Overseas Branch	Tokyo, Japan, and Houston, TX, USA		Web Access Management & SSO **ISign+**
Overseas Network	Singapore, Thailand, Australia, New Zealand, Malaysia, Indonesia		Car Security, IoT Security, Next-Generation Security Products

New Market: IoT Security

"Secure First, then Connect"
The core principle of IoT security

Key Management Infrastructure

Authentication

Encryption Authentication — Things

Encryption Authentication — Cloud

Network Security

Data

Data Mining

Humans ↔ Business System
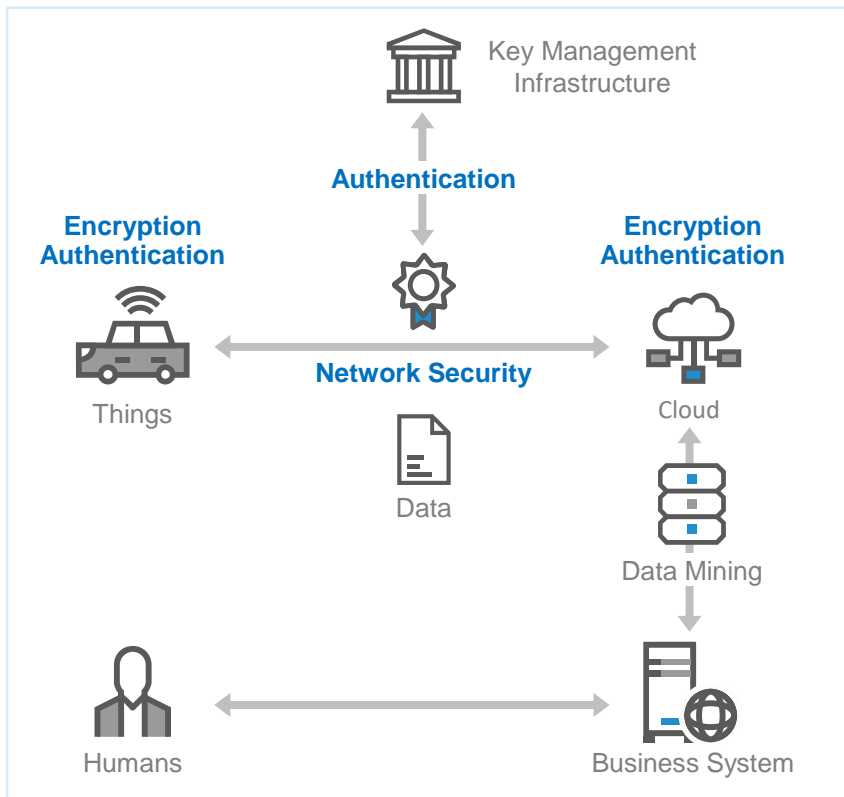
Encryption — Hardware encryption, lightweight encryption module, database encryption, key management

Network Security — SSL-VPN, application firewall, data integrity, end-to-end encryption

Authentication — Hardware device authentication, PKI device/user authentication, mobile authentication

Security Services — Monitoring, remote control, anomaly analysis, machine learning

1. Smart Car : AutoCrypt®

Security solution for smart vehicles and Cooperative Intelligent Transport Systems (C-ITS)

AutoCrypt PKI	AutoCrypt LCM	AutoCrypt V2X	AutoCrypt KMS
AutoCrypt IDS	AutoCrypt WAF	AutoCrypt V2G	AutoCrypt VDM

AUTOCRYPT

2. Smart Factory : PENTA Smart Factory Security™

Security solution for secure data collection, monitoring, and process control

Hardware Encryption Module   White Box Encryption Module
Database Encryption   Internal Encryption Key Storage
SSL-VPN   Application Firewall   /   Device and Firmware Authentication
Certificate-based Authentication   Data Encryption / Integrity Monitoring
PC and Mobile Authentication   /   Security Monitoring

3. Smart Energy : PENTA Smart Energy Security™

Authentication and encryption solution, securing everything from metering devices to relevant infrastructure

Hardware Encryption Module   Lightweight Encryption Module
Message Encryption / Authentication   Internal Encryption Key Storage   /
SSL-VPN   /   Message Authentication / Virtual Signature
Mutual Authentication   Key Generation / Distribution and Management

4. Smart Home : PENTA Smart Home Security™

Security solution for secure communication of household smart devices

Internal Encryption Key Storage   /   Device and Firmware Authentication
Certificate-based Authentication   Data Encryption and Integrity Monitoring
PC and Mobile Authentication   /   Security Monitoring

# Experiences about Connected Car
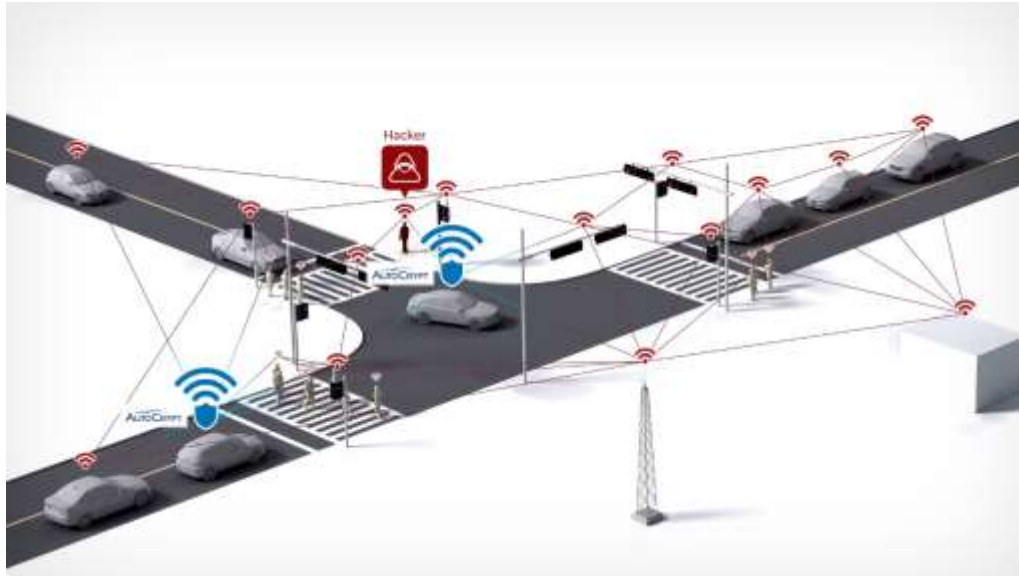
Secure First, then Connect™ … Cars

Security for Electricity Vehicle Charging System (M)
Security for Rail Transportation System (G)
2017. Security for C-ARS (G)
    (Cooperative Automated Driving Roadway System)

2016. Security for C-ITS Testbed (G)
    (Cooperative Intelligent Transportation System)

Firewall for Smart Cars (G)
2015. AutoCrypt® Launched **AUTOCRYPT**

Vehicle Data Management System (M)
2014. Telematics Security (consulting) (M)

2013. V2X Security over WAVE (M)

2012. Security for Patrol Car

2011. Security between Vehicle
    and Nomadic(mobile) Device (M)

2007. Security between Vehicle and Diagnostic Device (M)
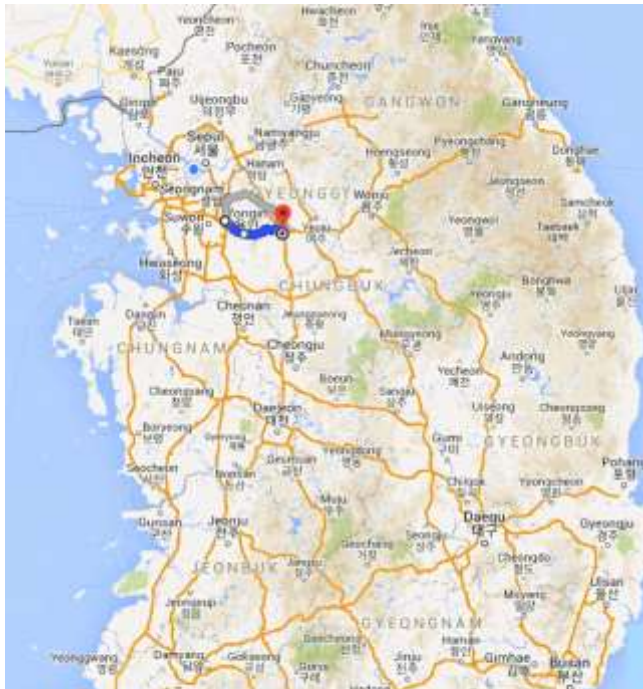
(G) for Government   (M) for Manufacturer

Achievements – Pilot Projects with Security Deployed

❑ C-ITS Testbed : July 2014 ~ July 2017
   ❖ 3,000 OBUs and 80 RSUs over 87.8Km
     of smart highway between Saejong and Daejeon, South Korea
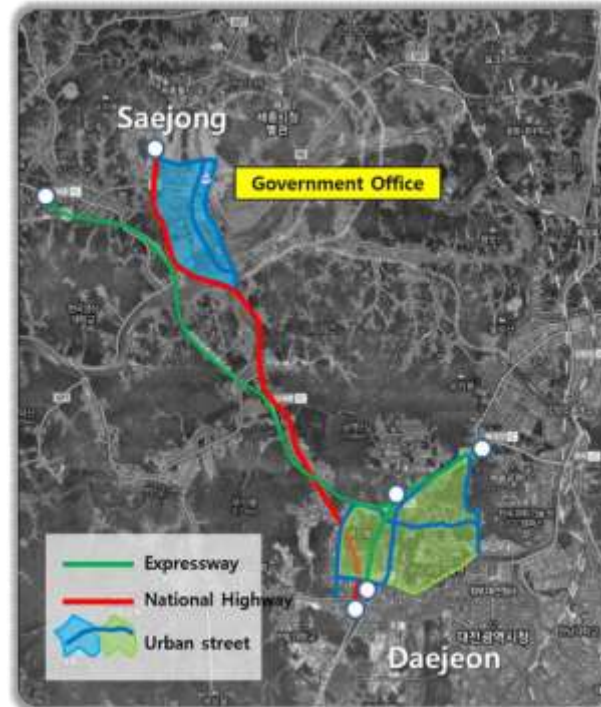
Achievements – Pilot Projects with Security Deployed

❑ C-ARS (Cooperative Automated Driving Roadway System): July 2015 ~ July 2020

Trend Keywords for Smart Cars

Security   Platform   Autonomous   Connectivity   Electrification

S P A C E

https://www.csis.org/analysis/implications-ultra-low-cost-access-space

Public

Trend Keywords : Electrification

Electric vehicles would account for **35%** of all new vehicle sales.

The Rise of Electric Cars

By 2022 electric vehicles will cost the same as their internal-combustion counterparts. That's the point of liftoff for sales.

Projected annual sales   Cumulative sales

500 million vehicles

Electric vehicles would account for 35% of all new vehicle sales.

400

300

200

100

0

2015 '16 '17 '18 '19 '20 '21 '22 '23 '24 '25 '26 '27 '28 '29 '30 '31 '32 '33 '34 '35 '36 '37 '38 '39 '40
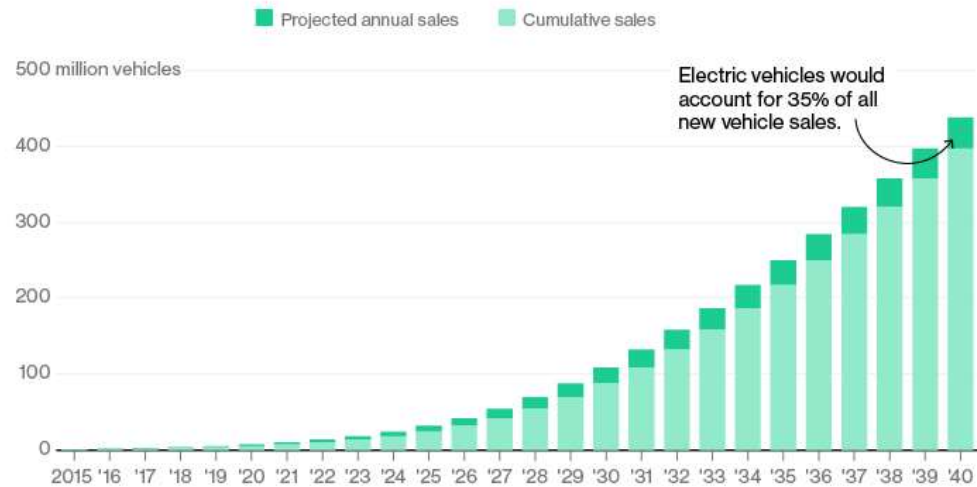
Sources: Data compiled by Bloomberg New Energy Finance, Marklines

Bloomberg

AutoCrypt : Smart Security for Smart Cars

Penta SECURITY

8

Public

Trend Keywords : Connectivity

V2H(Home)

V2V (Vehicle-to-Vehicle)

Manufacturer

Government

Telematics
V2N (Vehicle-to-Network)
V2S (Vehicle-to-Service)

V2I (Vehicle-to-Infra)
I2V (Infra-to-Vehicle)

TelCo

V2D (Vehicle-to-Nomadic Device)   **V2P (Vehicle-to-Pedestrian)**

TelCo (Mobile Manufacturer)
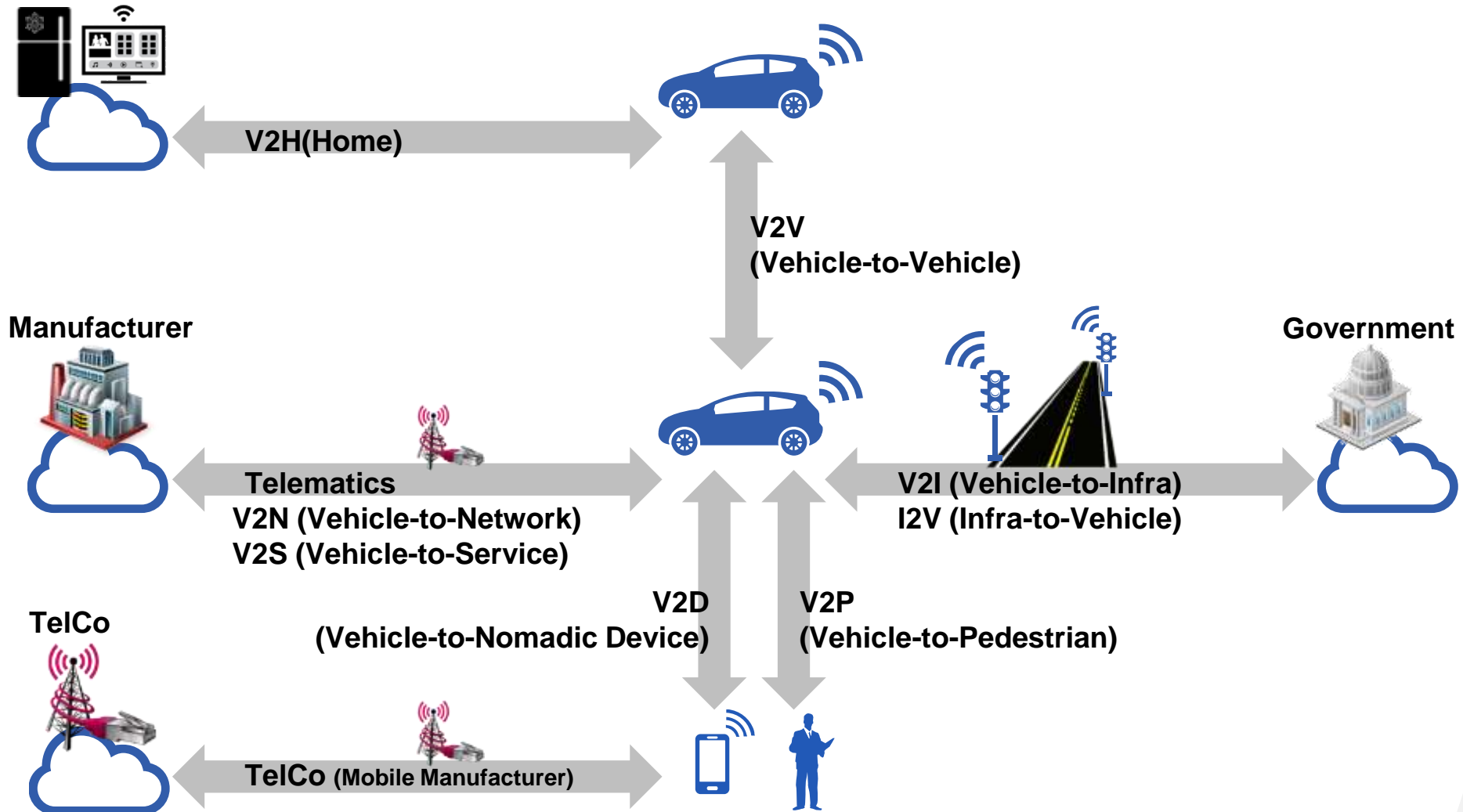
Trend Keywords : Autonomous

How many new cars may be fully autonomous by 2030?
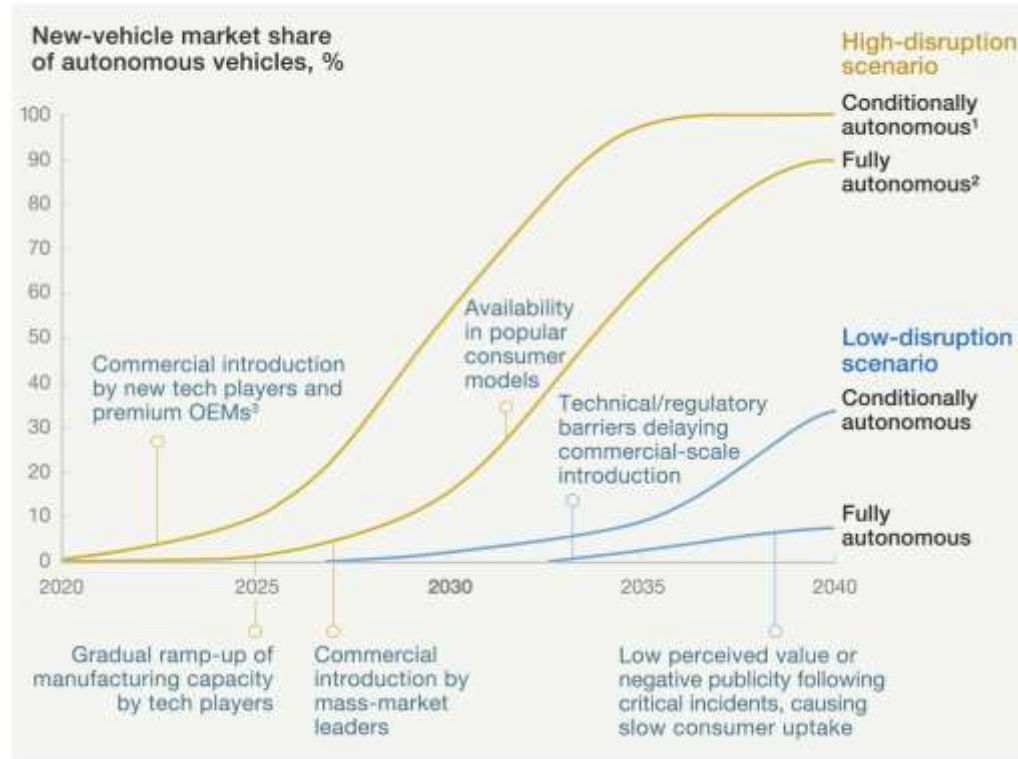
https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/disruptive-trends-that-will-transform-the-auto-industry

Trend Keywords : Platform

ISO 20077, ISO 20078 – Road Vehicles – Extended vehicle (ExVe)

Trend Keywords : Security

Smart Appliances Gone Rogue
Later morning
Remote kill switch

Bitdefender

Cybersecurity Concept for Connected Car

S4. Secure Platform
- Crypto library
- Secure boot & Remote Attestation
- Secure Update
- HW trust anchor(HTA)

S3. Secure Internal Communication
- Authentication, Confidentiality & Integrity of Messages
- Key Management

S2. Secure Gateway
- Controls traffic flow
- Detects malicious traffic
- Privacy & Data Security

S1. Secure External Communication
- Secure communication to anything

Device, Infrastructure, Vehicle, Cloud, Diagnostics, Person(Owner, Driver, Pedestrian), etc.

External Network

Gateway

Internal Network

ECU

Public

S1. Secure External Communication

Manufacturer

Government

Cellular V2X

V2I/I2V

| Security : IEEE1609.2 |
| Transport : IEEE1609.3 |
| Network : 3GPP(4G/5G) |

| Security : IEEE1609.2 |
| Transport : IEEE1609.3 |
| Network : IEEE802.11p |

Certificate

Certificate

Cross Certification

**Certificate Authority
(of Manufacturer)**

**Certificate Authority
(of Government)**

S1. Secure External Communication : C-ITS

Cooperative Intelligent Transportation System

Secure Communication (V2I)

Secure Comm. (V2V)

Sender

Receiver

Retrieving the sender's certificate

Generating the signature

OBU

OBU

AutoCrypt® LCM

Traffic Info. + Signature + Certificate

Verifying the signature

Validating the certificate

SCMS	IEEE 1609.3
IEEE1609.2	
IEEE802.11p	
OS	
HW	

SCMS	IEEE 1609.3
IEEE1609.2	
IEEE802.11p	
OS	
HW	

AutoCrypt® V2X

SCMS : Security Credential Management System
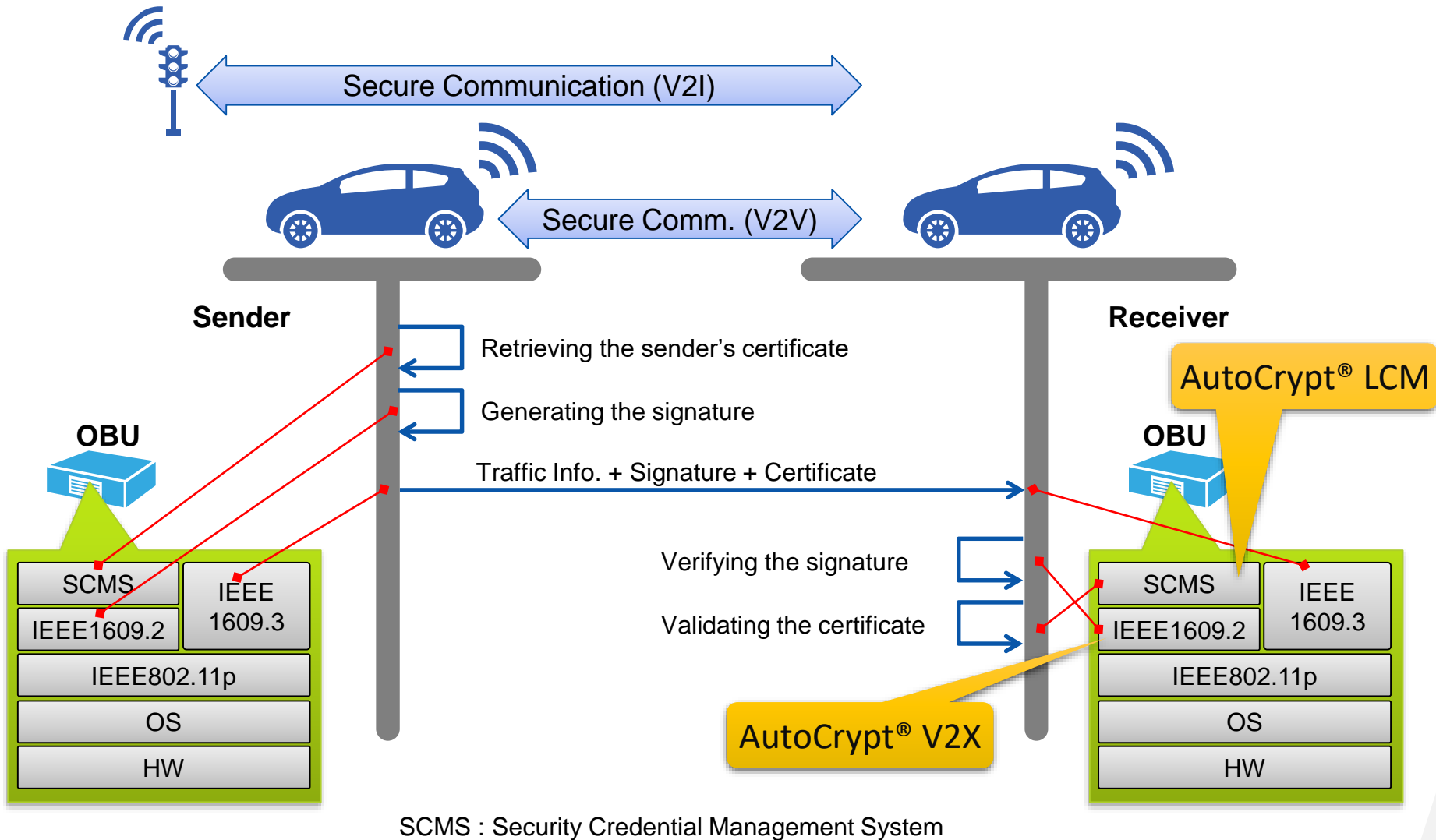
S1. Secure External Communication : PKI

AutoCrypt® PKI

Root CA

Intermediate CA

Enrollment CA

Pseudonym CA

Misbehavior Authority

Enrollment RA

RA

Linkage Authority

Linkage Authority

Dev. Conf. Manager

— Infra Certificate Issuing
— Enrollment Certificate Issuing
— Pseudonym Certificate Issuing
— Misbehavior Reporting & CRL Distribution
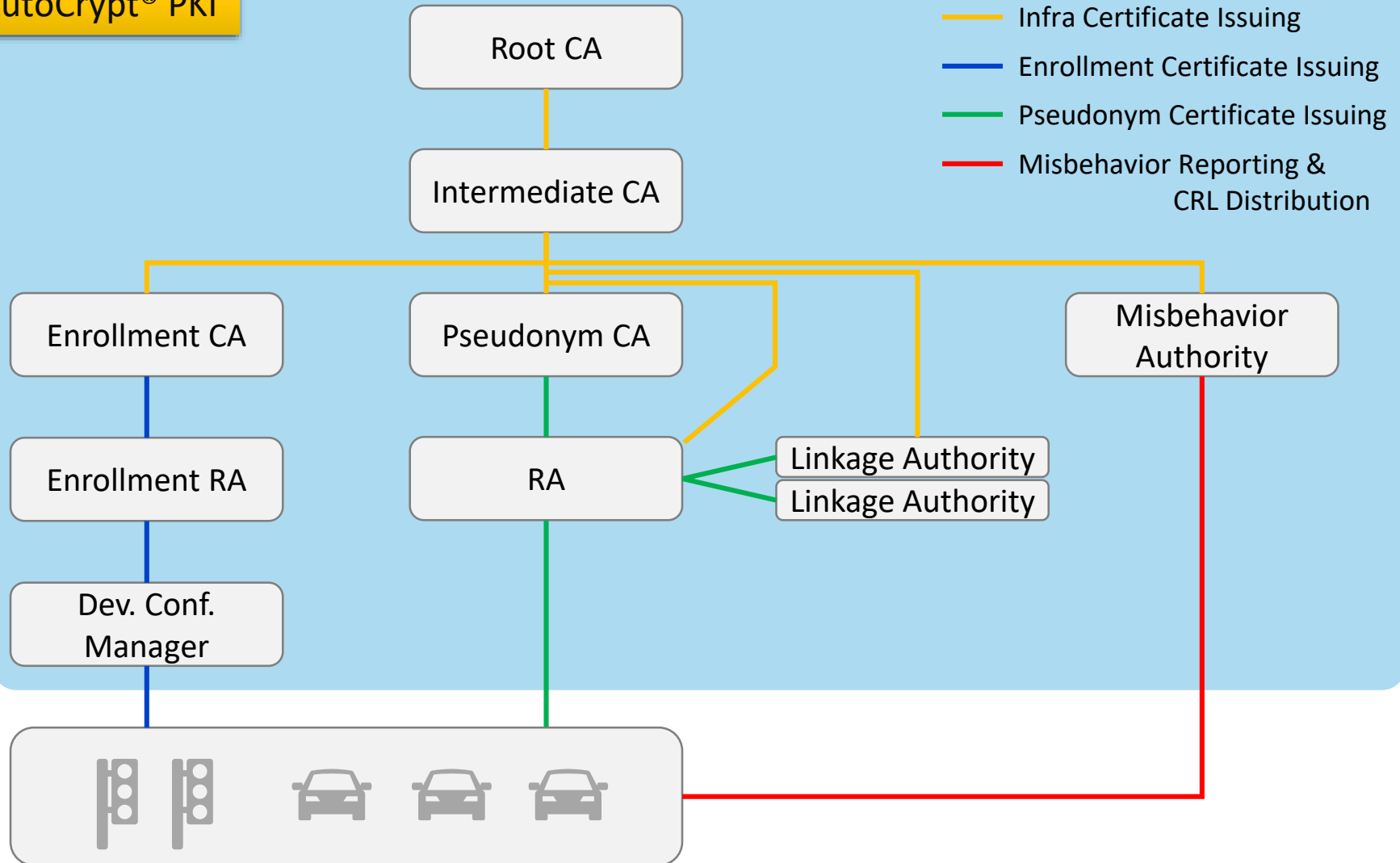
S1. Secure External Communication – eVehicle Protocols

- OCA : Open Charge Alliance
- OCPP : Open Charge Point Protocol
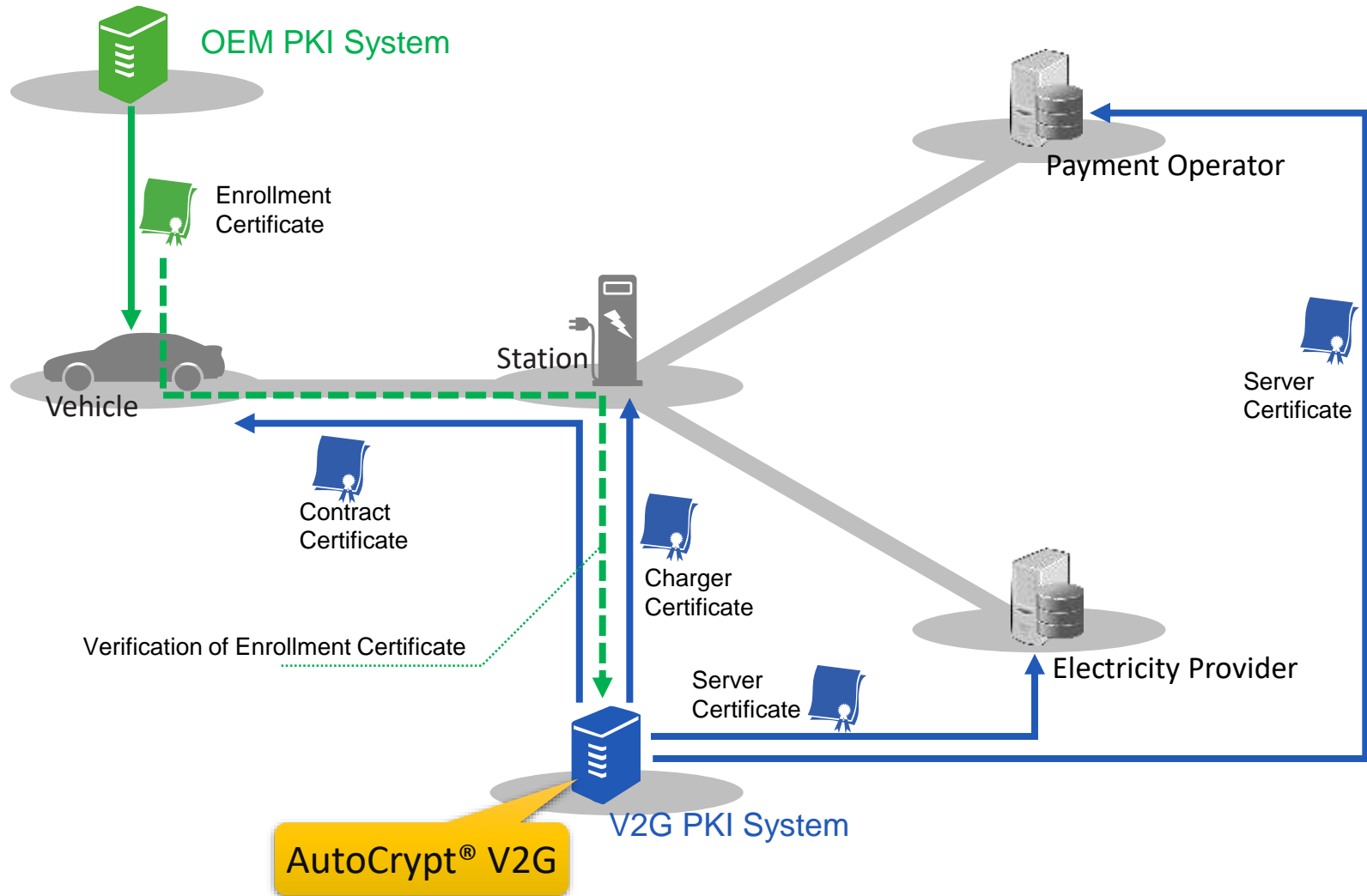- OSCP : Open Smart Charging Protocol

Payment Operator

OCPP

- Authentication
- TLS Secure Communication

Station

Vehicle

ISO 15118

- Encryption using TLS
- Authentication
- Signing billing receipt

OSCP / ISO 61850

- TLS Secure Communication
- Message Authentication

Electricity Provider
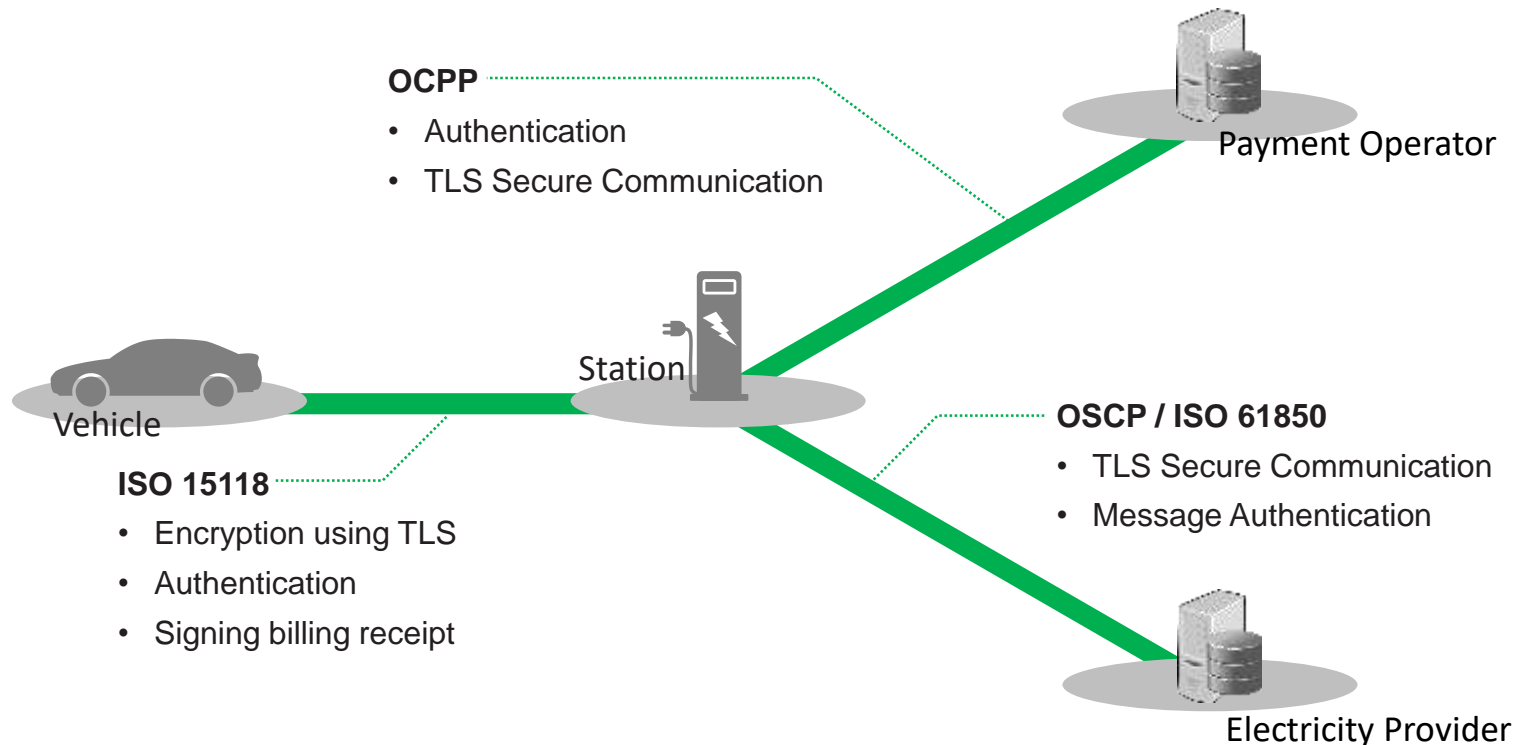
OCA

- OCPP standardizes the communication between the charge spot and the party that operates the charge, thereby allowing CSO back-ends and charge spots of different vendors to communicate.

- OSCP(Open Smart Charging Protocol) allows a DSO to vary the capacity available to charge stations in time, given the varying predicted capacity needed for other consumers in an area.
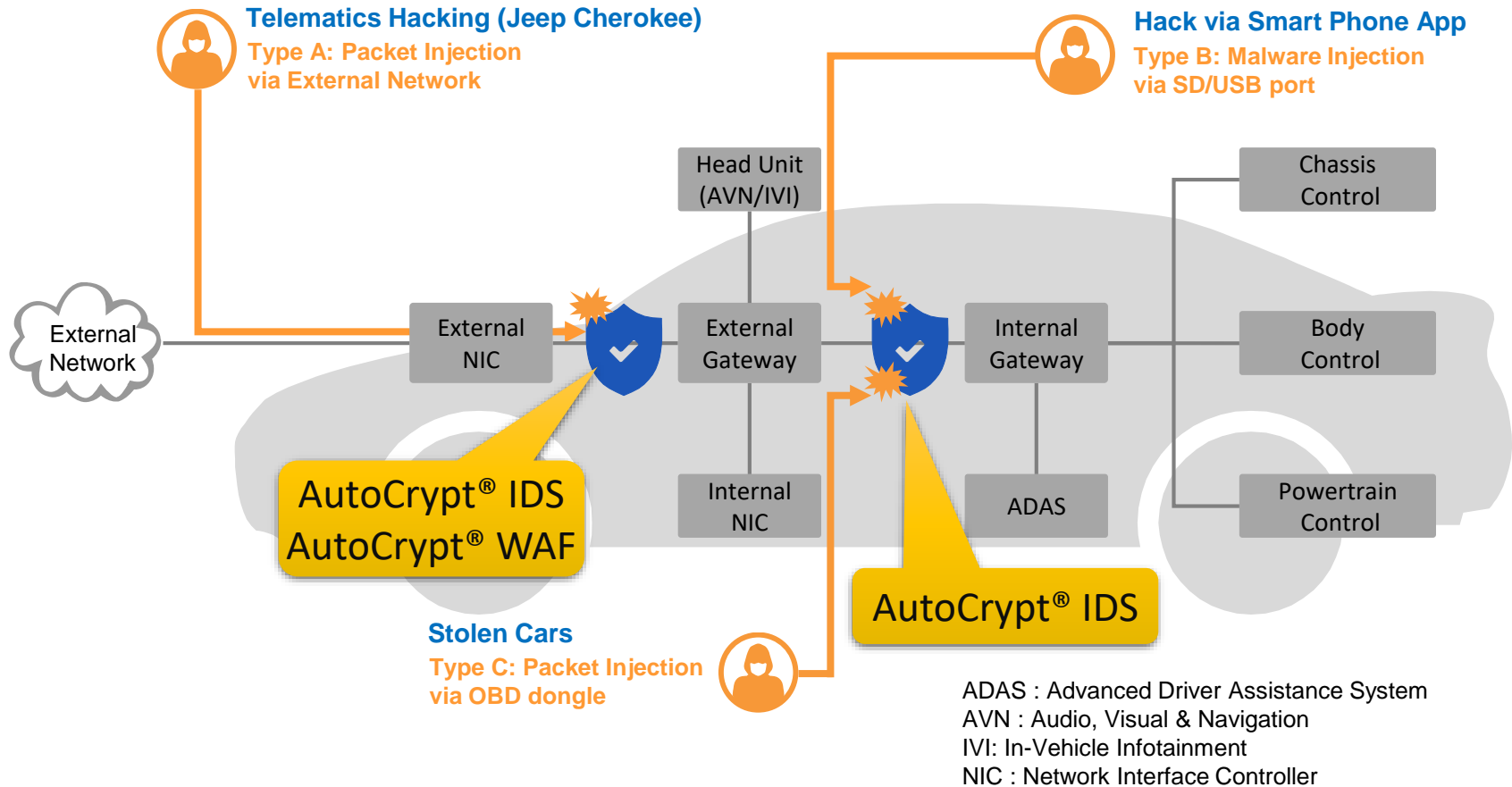
S1. Secure External Communication - Security Model for EV & EVSE

Electric Vehicle Supply Equipment

S2. Secure Gateway – Detects malicious traffic

Intrusion Detection System & Web Application Firewall

Telematics Hacking (Jeep Cherokee)
Type A: Packet Injection
via External Network

Hack via Smart Phone App
Type B: Malware Injection
via SD/USB port

External Network

External NIC

Head Unit (AVN/IVI)

External Gateway

Internal Gateway

Internal NIC

ADAS

Chassis Control

Body Control

Powertrain Control

AutoCrypt® IDS
AutoCrypt® WAF

AutoCrypt® IDS

Stolen Cars
Type C: Packet Injection
via OBD dongle

ADAS : Advanced Driver Assistance System
AVN : Audio, Visual & Navigation
IVI: In-Vehicle Infotainment
NIC : Network Interface Controller

S2. Secure Gateway – Controls traffic flow

Intrusion Detection System

Legend:
- → Designated Traffic
- → Undesignated Traffic
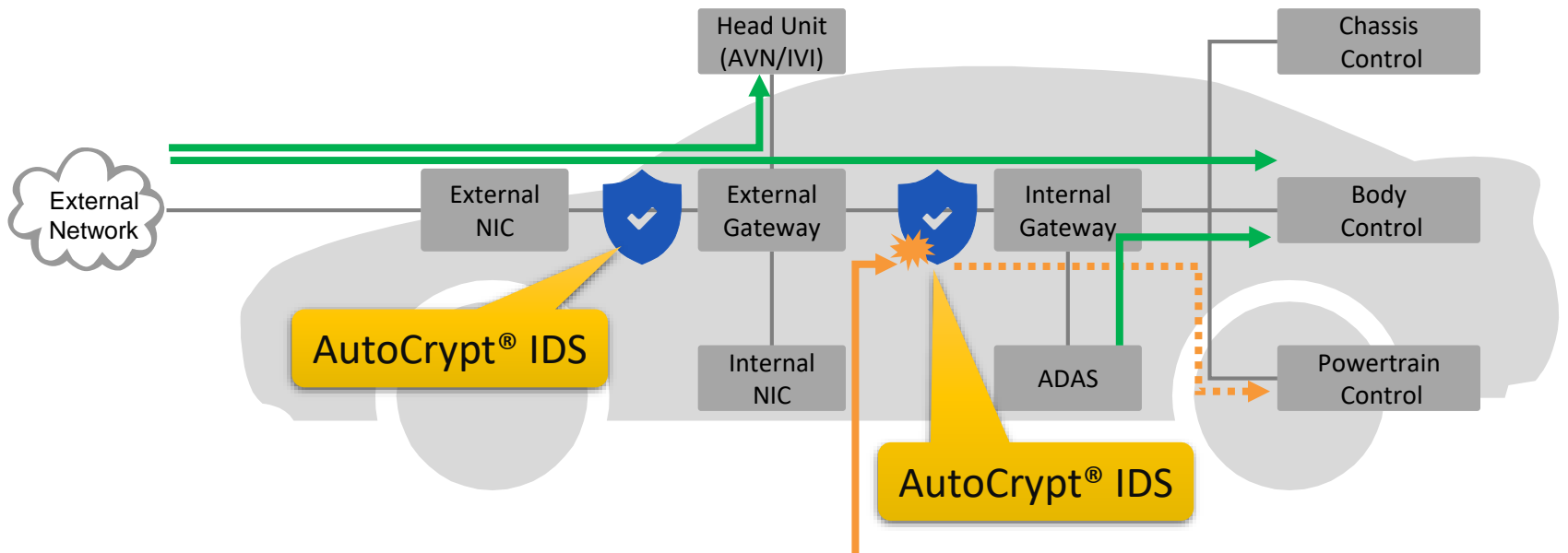
Head Unit (AVN/IVI) · External Network · External NIC · External Gateway · Internal NIC · Internal Gateway · ADAS · Chassis Control · Body Control · Powertrain Control

AutoCrypt® IDS

AutoCrypt® IDS

ADAS : Advanced Driver Assistance System
AVN : Audio, Visual & Navigation
IVI: In-Vehicle Infotainment
NIC : Network Interface Controller

S2. Secure Gateway – Data Security & Privacy Preserving

Vehicle Data Management

Cloud
(OEM, Government, 3rd Party)

External Network

External NIC

External Firewall

Head Unit (AVN/IVI)

External Gateway

Internal Firewall

Internal Gateway

Chassis Control

Body Control

Data Recording
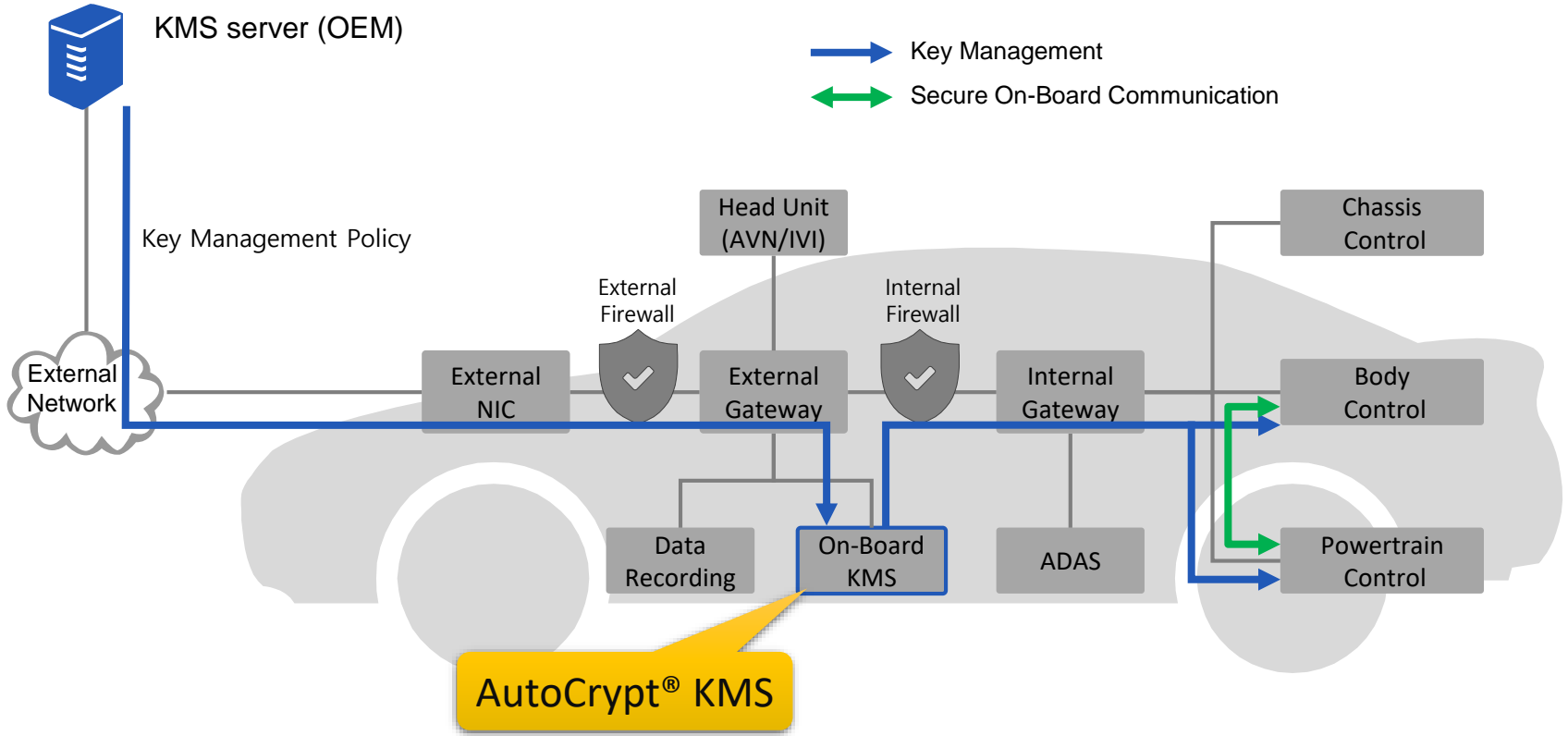
ADAS

Powertrain Control
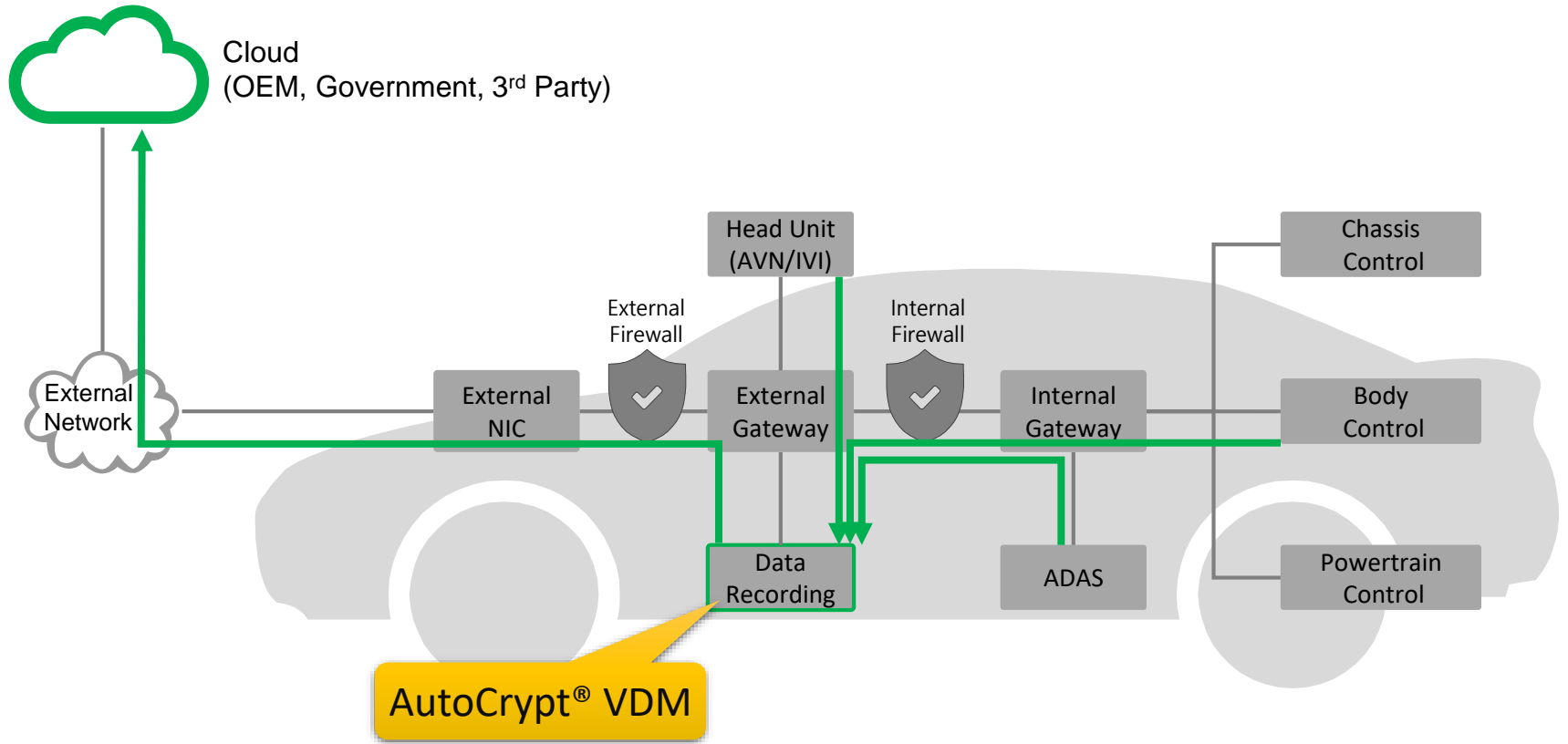
AutoCrypt® VDM

Data Security
& Privacy Preserving

ADAS : Advanced Driver Assistance System
AVN : Audio, Visual & Navigation
IVI: In-Vehicle Infotainment
NIC : Network Interface Controller

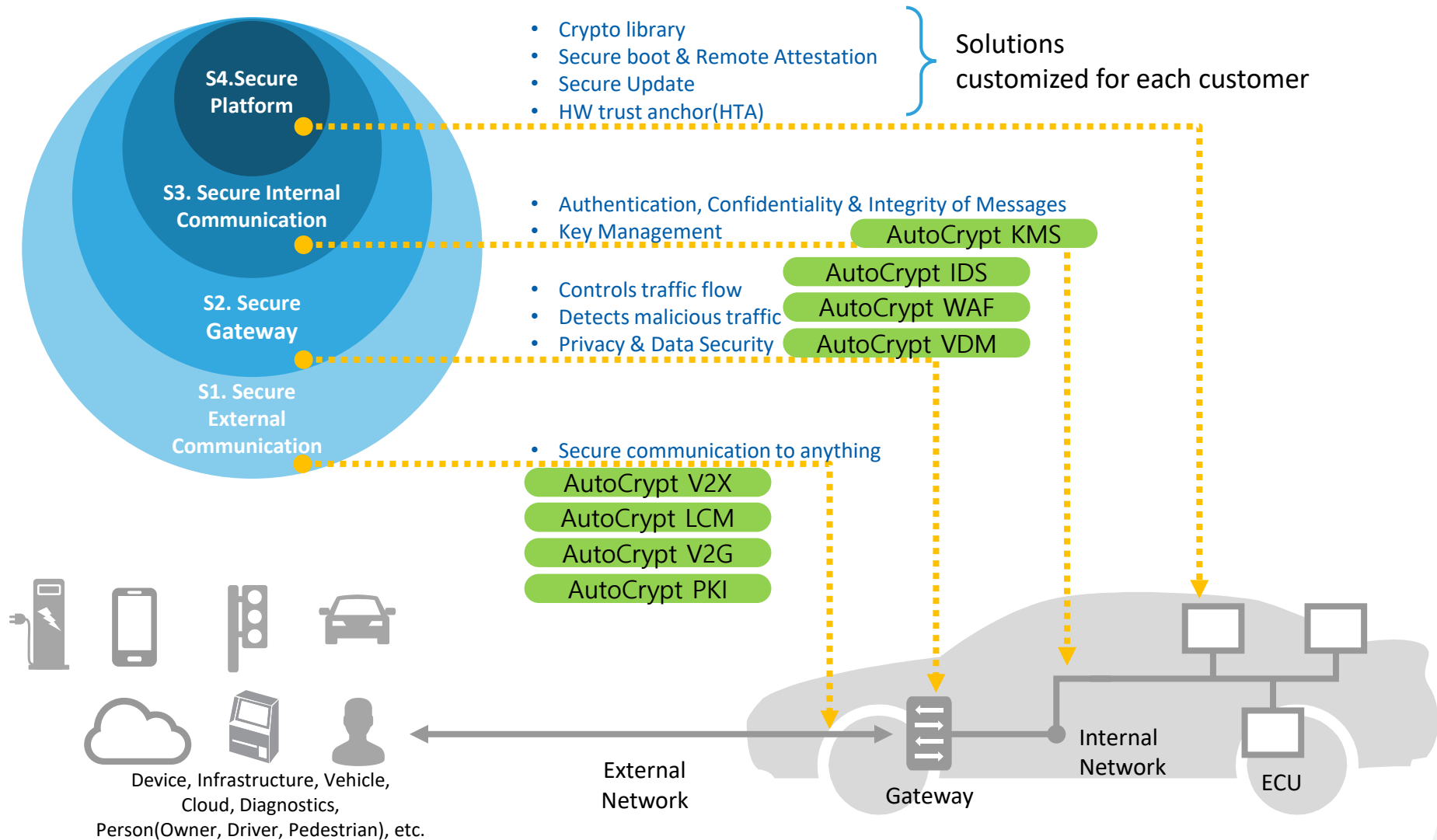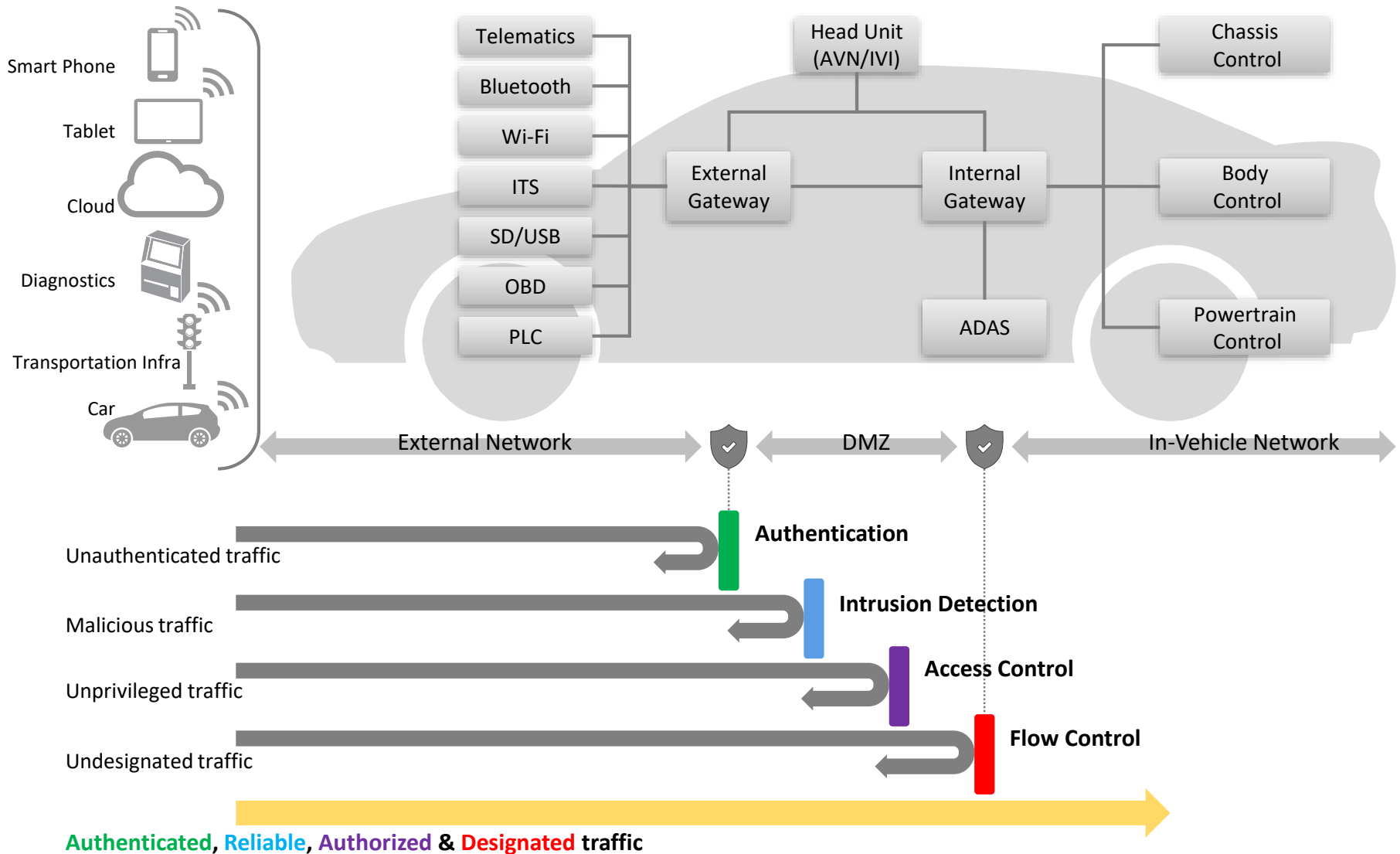# S3. Secure Internal Communication

Key Management System

ADAS : Advanced Driver Assistance System
AVN : Audio, Visual & Navigation
IVI: In-Vehicle Infotainment
NIC : Network Interface Controller
KMS : Key Management System

Cybersecurity Concept for Connected Car

- Crypto library
- Secure boot & Remote Attestation
- Secure Update
- HW trust anchor(HTA)

Solutions customized for each customer

S4. Secure Platform

S3. Secure Internal Communication

- Authentication, Confidentiality & Integrity of Messages
- Key Management

AutoCrypt KMS

S2. Secure Gateway

- Controls traffic flow
- Detects malicious traffic
- Privacy & Data Security

AutoCrypt IDS

AutoCrypt WAF

AutoCrypt VDM

S1. Secure External Communication

- Secure communication to anything

AutoCrypt V2X

AutoCrypt LCM

AutoCrypt V2G

AutoCrypt PKI

Device, Infrastructure, Vehicle, Cloud, Diagnostics, Person(Owner, Driver, Pedestrian), etc.

External Network

Gateway

Internal Network

ECU

Top 4 Security Primitives

Authenticated, **Reliable**, **Authorized** & **Designated** traffic

Demo : AutoCrypt® PKI/V2X/LCM

AutoCrypt® PKI

- Root CA
- Intermediate CA
- Enrollment CA
- Pseudonym CA
- Misbehavior Authority
- Enrollment RA
- RA
- Linkage Authority
- Linkage Authority
- Dev. Conf. Manager

Infra Certificate Issuing
Enrollment Certificate Issuing
Pseudonym Certificate Issuing
Misbehavior Reporting & CRL Distribution

Demo : AutoCrypt® IDS

Server (Data Analysis)

Data Gathering

Policy Setting

External Device

AutoCrypt IDS

Gateway

ECU

→ Traffic defined in Whitelist
→ Traffic defined in Blacklist
→ Traffic not defined in Whitelist/Blacklist

one more... authentiCA.cloud
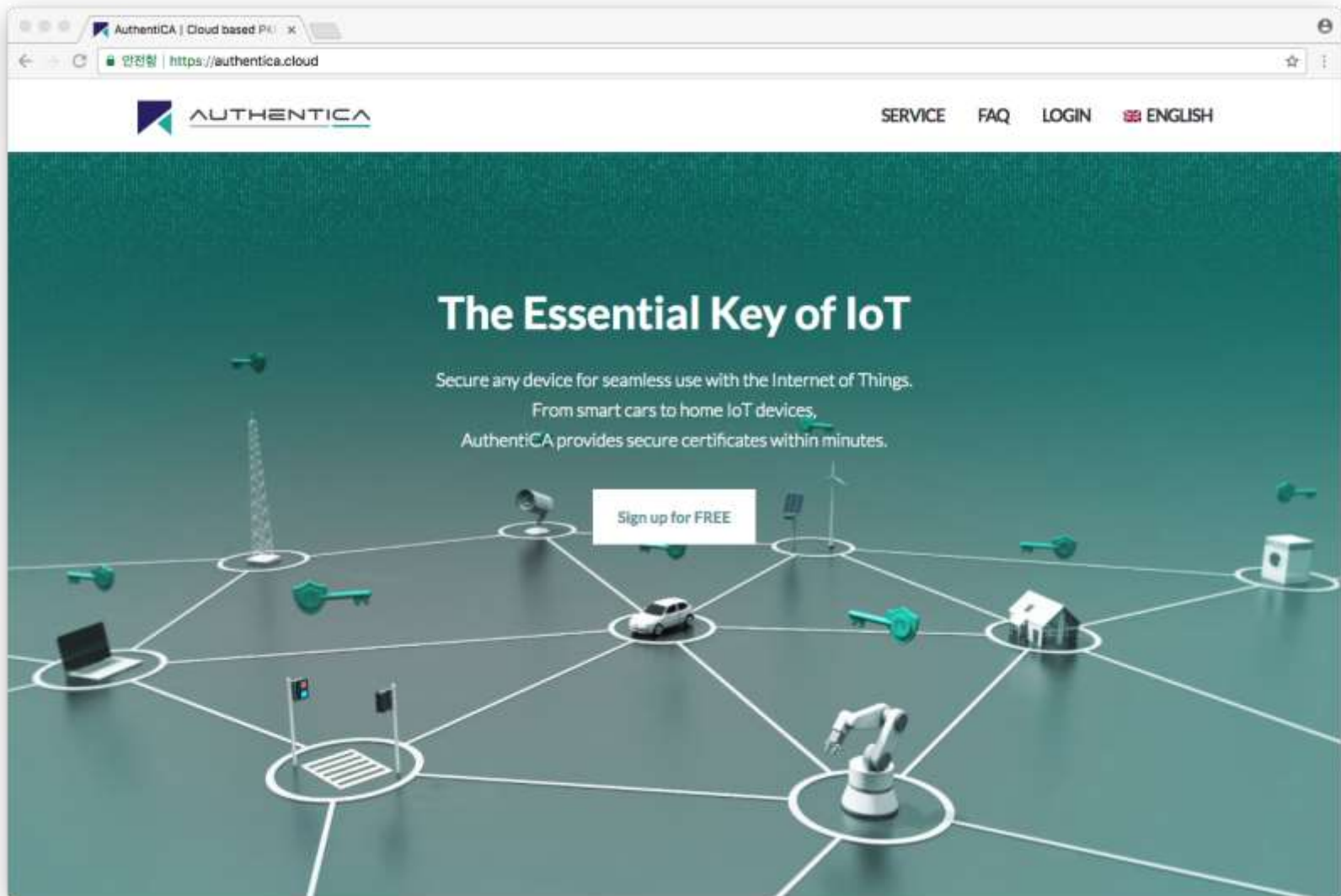
Meet AutoCrypt® @ E54-9 / Automotive World

Public

20 year **Anniversary**

Asian Cyber Security
Vendor of the Year

t h a n k   y o u

KOREA Yeouido, Seoul   www.pentasecurity.co.kr (HQ)
U.S.A. Houston, Texas   www.pentasecurity.com
JAPAN Shinjuku-Ku, Tokyo   www.pentasecurity.co.jp