20 year Anniversary

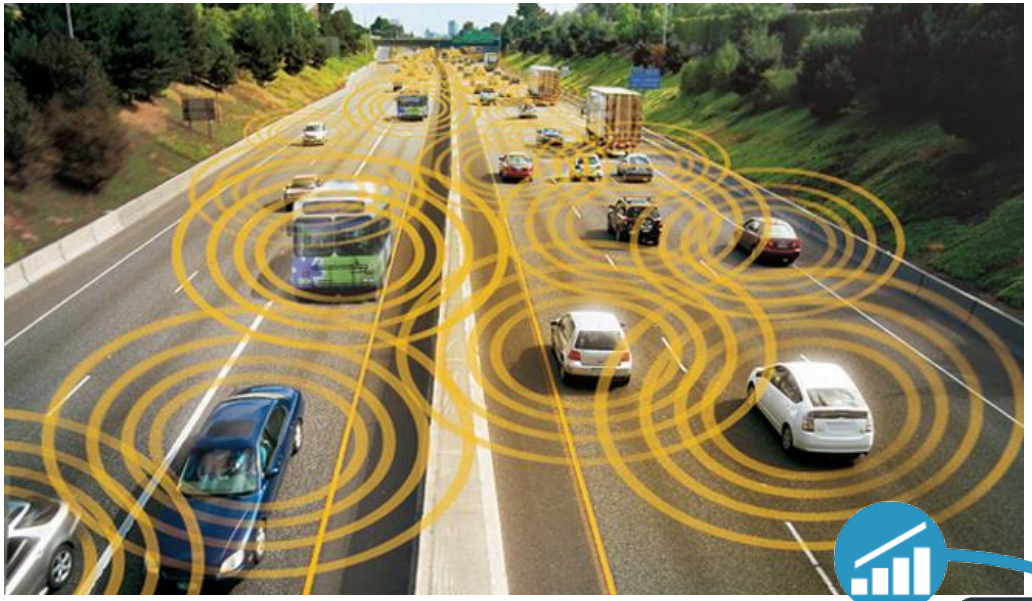
Asian Cyber Security Vendor of the Year

Penta SECURITY
cloud · iot · enterprise

Security for Connected/Autonomous Car

September 2017

Jaeson YOO
(jyoo@pentasecurity.com)
Chief Security Evangelist

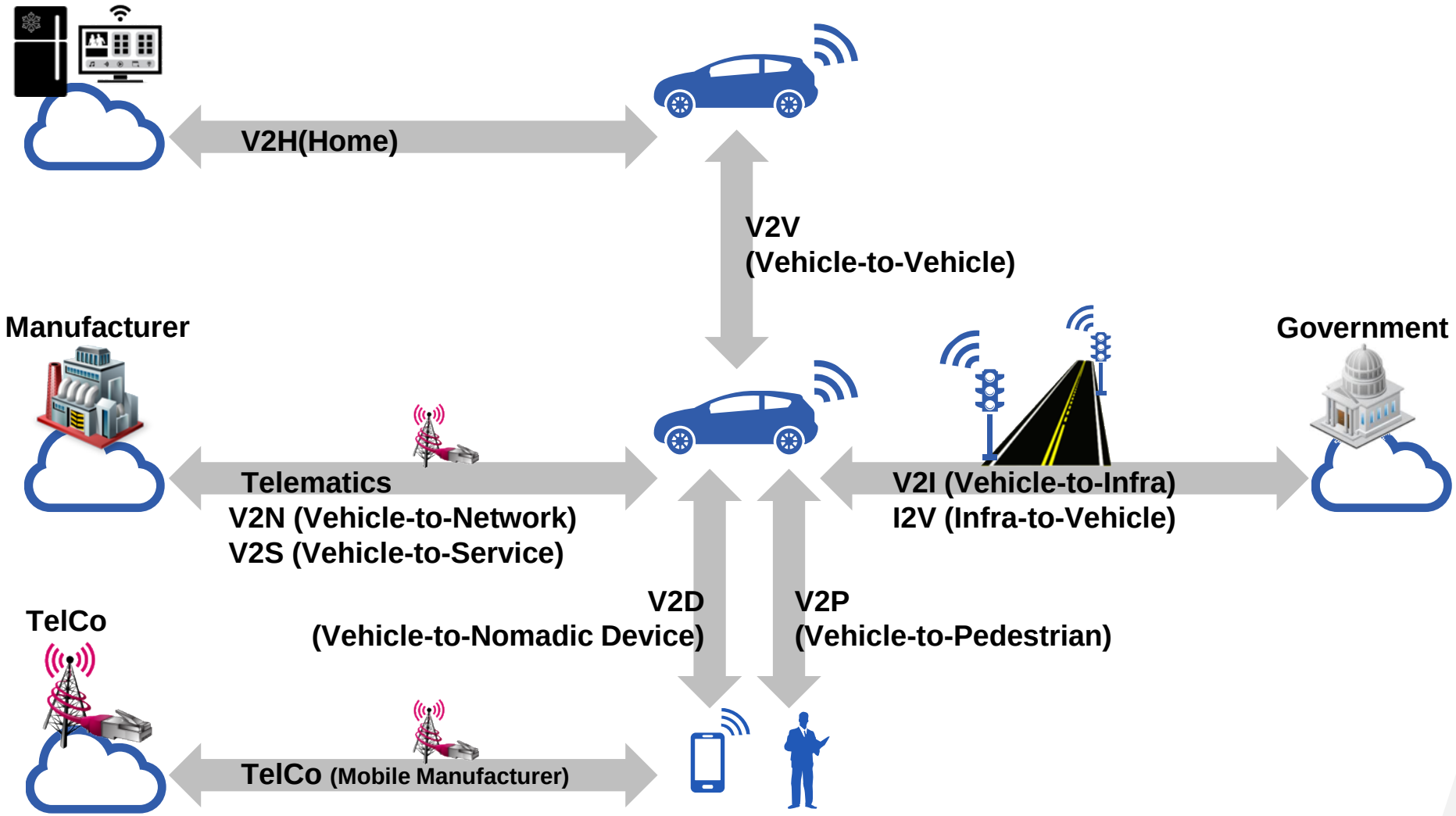


http://www.cleantech.com/isolated-car-to-connected-car-transportation-from-the-20th-to-the-21st-century/

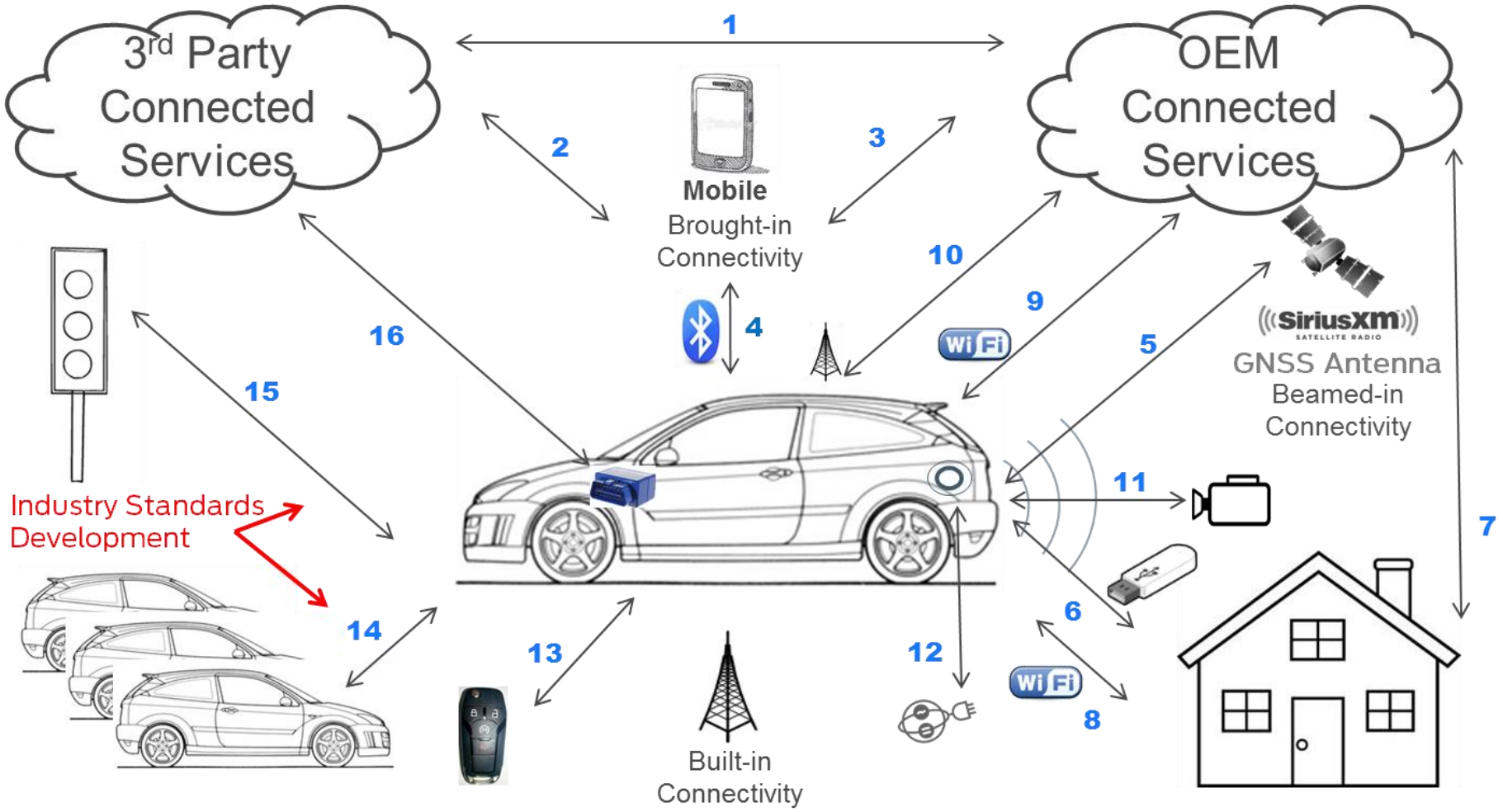
http://www.nanalyze.com/2017/04/10-connected-car-technology-startups/

http://www.rcrwireless.com/connected-cars-2/harman-connected-car-services-trends-tag6-tag99

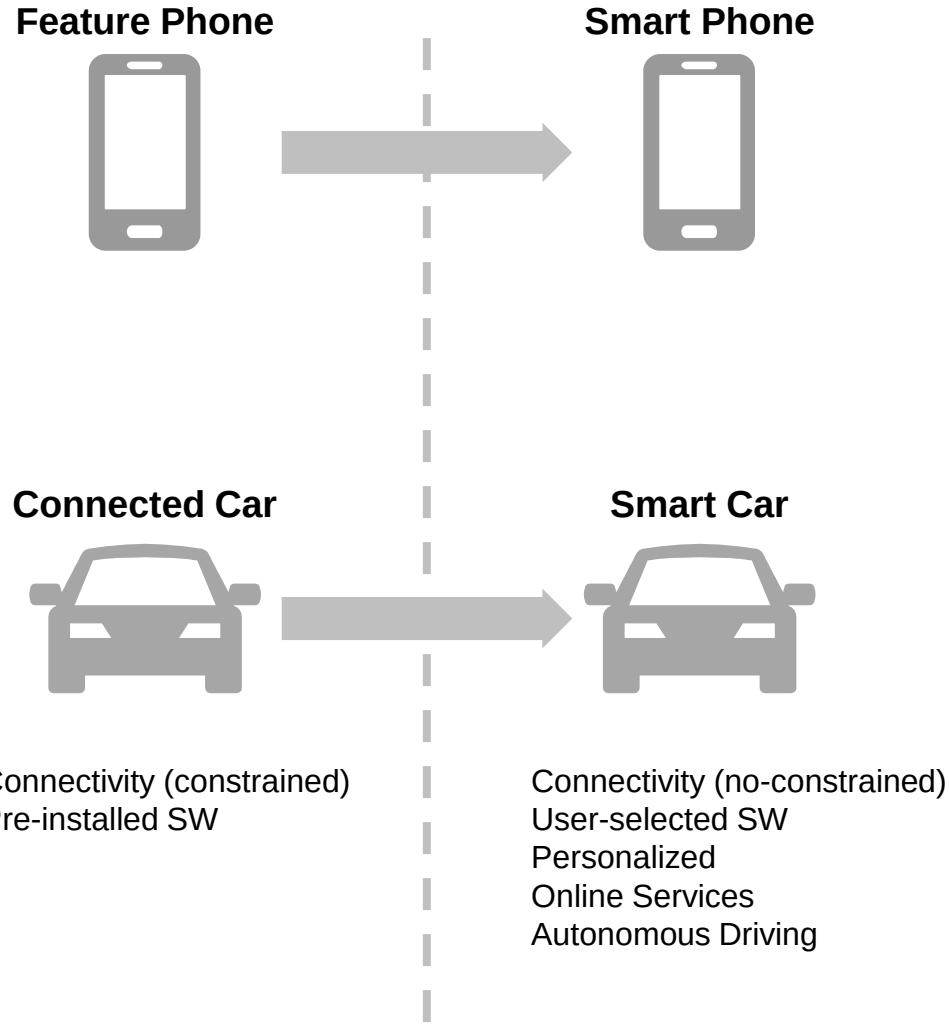
'All That Connections' of Connected Car



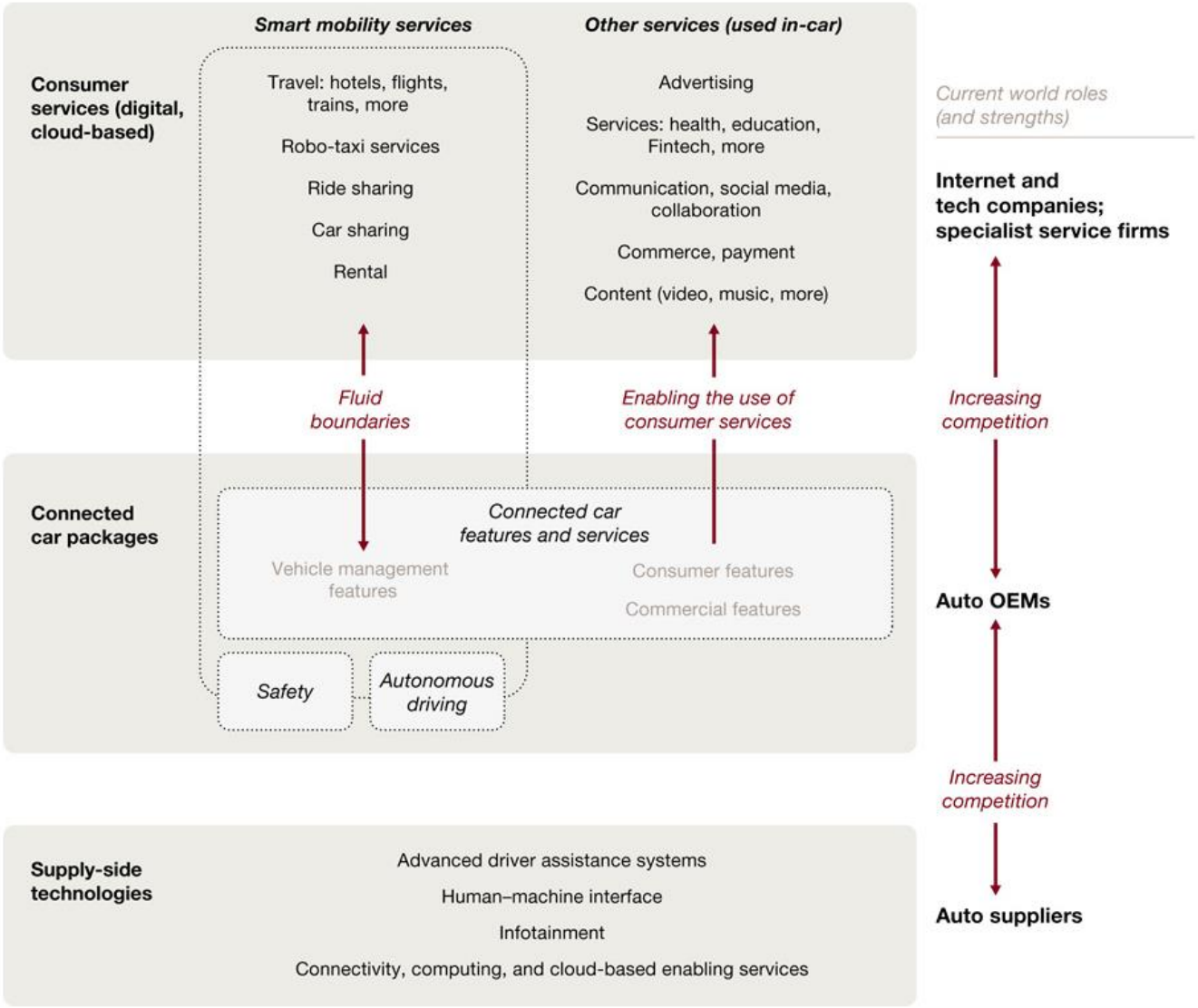
Extended Vehicle (ISO 20077 & 20078)



“Cars are mobile devices.”

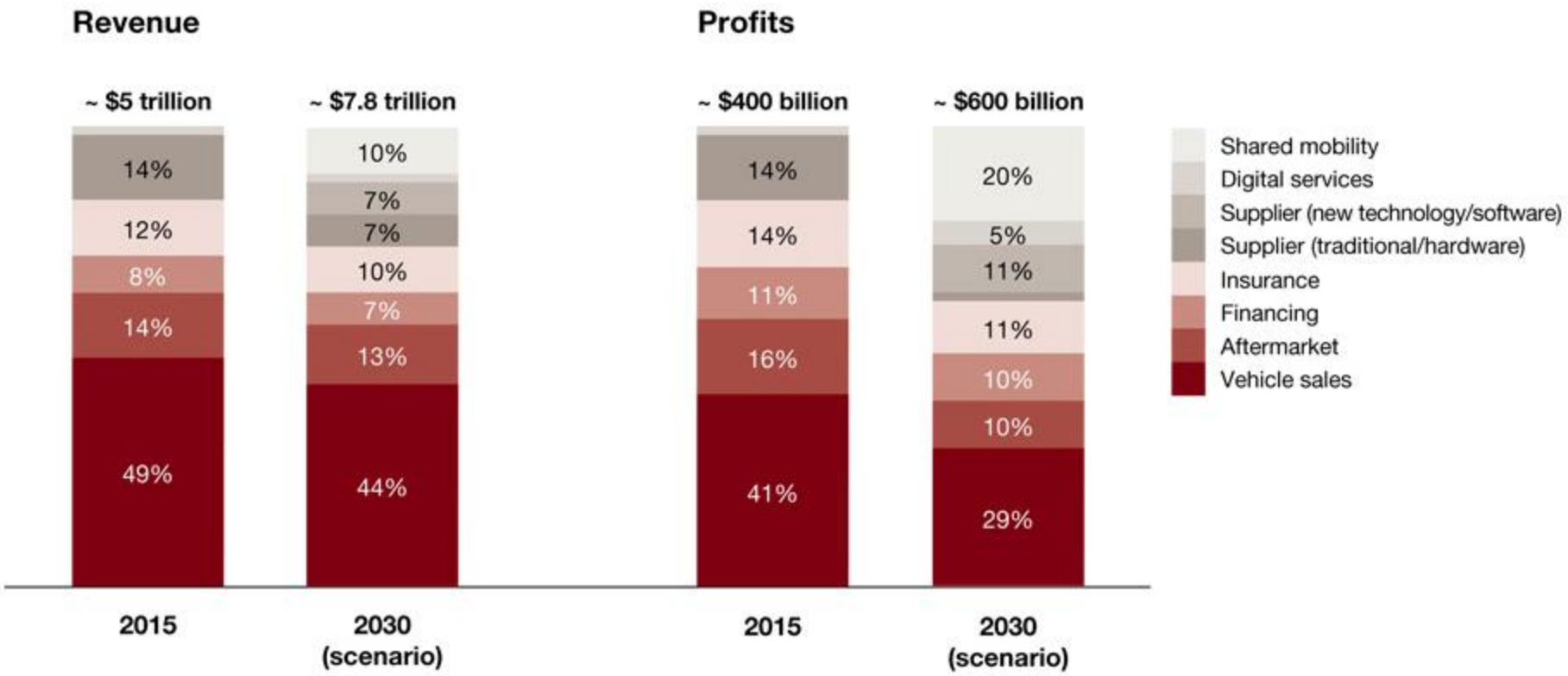


Connected Car Technologies & Services



https://www.strategyand.pwc.com/reports/connected-car-2016-study (2016.09)

Value Shifts in the Auto Industry, 2015-2030



Share addressable by today's OEM model declining to less than 70%

Share addressable by new entrants (digital services, mobility, new technology supply, Fintech, startup EV players) growing to more than 45% or $3.5 trillion

Share addressable by OEM declining from ~70% to less than 50%

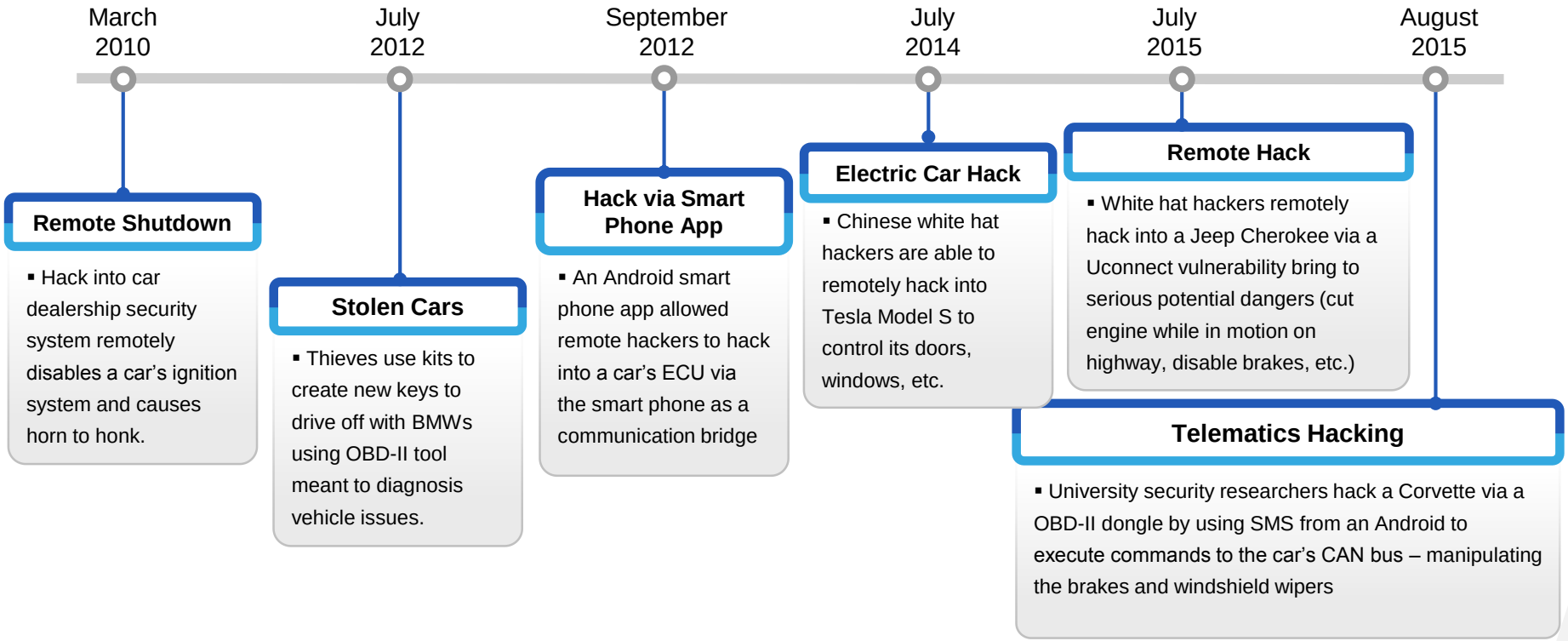
Share that can be captured by new entrants growing to 60% or $360 billion

https://www.strategyand.pwc.com/reports/connected-car-2016-study (2016.09)

Hacking Incidents

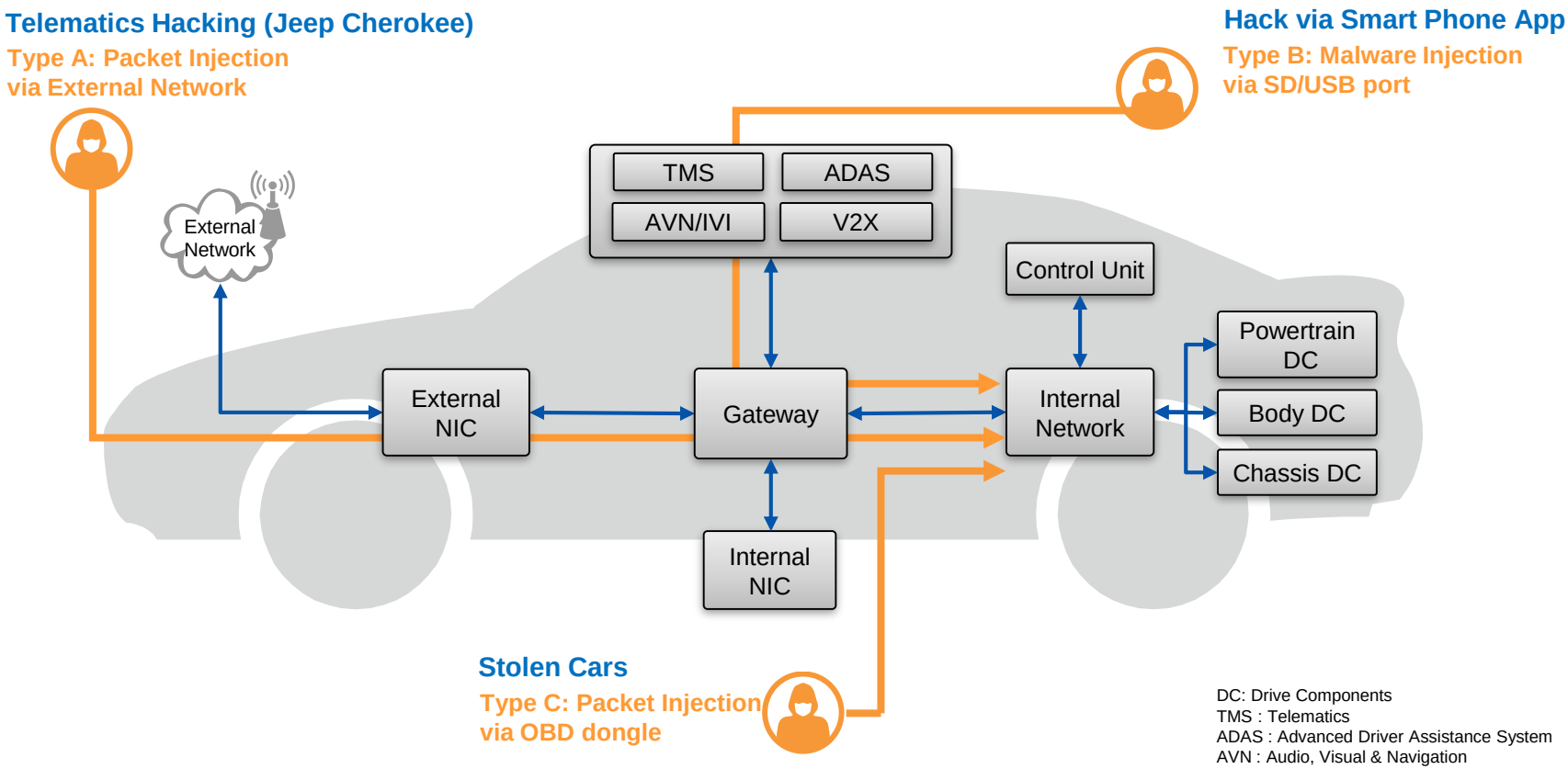
"Safety begins with Security"

The existing cyber threats that risked
monetary or physical loss are now being applied to
Vehicles which can place severe liability to a person's life.



Security Threats

The number of vehicular related hacking incidents become more present to the public as time goes by.
Vehicular vulnerabilities will continue to grow as the variety of car models increase.
Security will play an ever more important role in this evolving society of connected vehicles.



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

“SPY CAR” (Security and Privacy in Your Car) Act (2015.07)

❑ I. Cybersecurity Standards

- ❖ **Hacking protection**: all access points in the car should be equipped with reasonable measures to protect against hacking attacks, including isolation of critical software systems and evaluated using best security practices, such as penetration testing;
- ❖ **Data security**: all collected information should be secured to prevent unwanted access—while stored on-board, in transit, and stored off-board; and
- ❖ **Hacking mitigation**: the vehicle should be equipped with technology that can detect, report and stop hacking attempts in real-time.

❑ II: Privacy standards

- ❖ **Transparency**: owners are made explicitly aware of collection, transmission, retention, and use of driving data;
- ❖ **Consumer choice**: owners are able to opt out of data collection and retention without losing access to key navigation or other features (when technically feasible), except for in the case of electronic data recorders or other safety or regulatory systems; and
- ❖ **Marketing prohibition**: personal driving information may not be used for advertising or marketing purposes without the owner clearly opting in.

❑ III: Cyber dashboard

NHTSA, in consultation with FTC, should establish a **“cyber dashboard”** that displays an evaluation of how well each automobile protects both the security and privacy of vehicle owners beyond those minimum standards. This information should be presented in a transparent, consumer-friendly form on the window sticker of all new vehicles.

http://www.markey.senate.gov/news/press-releases/sens-markey-blumenthal-introduce-legislation-to-protect-drivers-from-auto-security-privacy-risks-with-standards-and-cyber-dashboard-rating-system

"SPY CAR" (Security and Privacy in Your Car) Act (2017.03)

❑ I. Cybersecurity Standards

- ❖ Protection against Hacking : equipped with reasonable measures to protect against hacking attacks.
  - Isolation Measures : to separate critical software systems from noncritical software systems.
  - Evaluation : evaluated for security vulnerabilities following best security practices, including appropriate applications of techniques such as penetration testing.
  - Adjustment : adjusted and updated based on the results of the evaluation
- ❖ Security of Collected Information
  - All driving data collected by the electronic systems that are built into motor vehicles shall be reasonably secured to prevent unauthorized access – (a) stored onboard, (b) transit to another location, and (c) offboard storage or use.
- ❖ Detection, Reporting, and Responding to Hacking
  - Any motor vehicle that presents an entry point shall be equipped with capabilities to immediately detect, report, and stop attempts to intercept driving data or control the vehicle.

❑ II. Cyber Dashboard

- ❖ inform consumers, through an easy-to-understand, standardized graphic, about the extent to which the motor vehicle protects the cybersecurity and privacy of motor vehicle owners, lessees, drivers, and passengers beyond the minimum requirements.

❑ III. Privacy Standards for Motor Vehicles

- ❖ Cont'd

https://www.congress.gov/bill/115th-congress/senate-bill/680

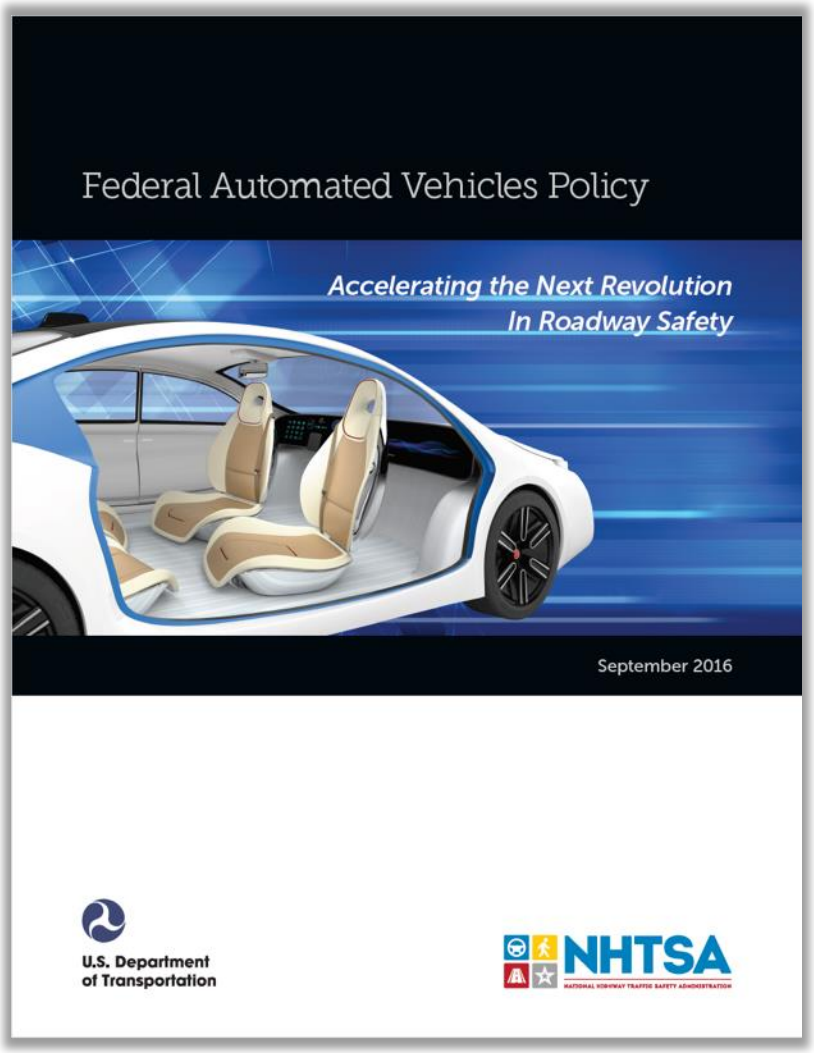
"SPY CAR" (Security and Privacy in Your Car) Act (2017.03)

❑ III. Privacy Standards for Motor Vehicles

- ❖ Transparency : Each motor vehicle shall provide clear and conspicuous notice, in clear and plain language, to the owners or lessees of such vehicle of the collection, transmission, retention, and use of driving data collected from such motor vehicle.
- ❖ Consumer Control : the option of terminating the collection and retention of driving data.
- ❖ Access to Navigation Tools : If a motor vehicle owner or lessee decides to terminate the collection and retention of driving data, the owner or lessee shall not lose access to navigation tools or other features or capabilities, to the extent technically possible.
- ❖ Exception : not apply to driving data stored as part of the electronic data recorder system or other safety systems on board the motor vehicle that are required for post incident investigations, emissions history checks, crash avoidance or mitigation, or other regulatory compliance programs.
- ❖ Limitation on Use of Personal Driving Information
  - A manufacturer (including an original equipment manufacturer) may not use any information collected by a motor vehicle for advertising or marketing purposes without affirmative express consent by the owner or lessee.
    - ✓ Consent requests shall be clear and conspicuous.
    - ✓ Consent requests shall be made in clear and plain language.
    - ✓ Consent requests may not be be a condition for the use of any nonmarketing feature, capability, or functionality of the motor vehicle.

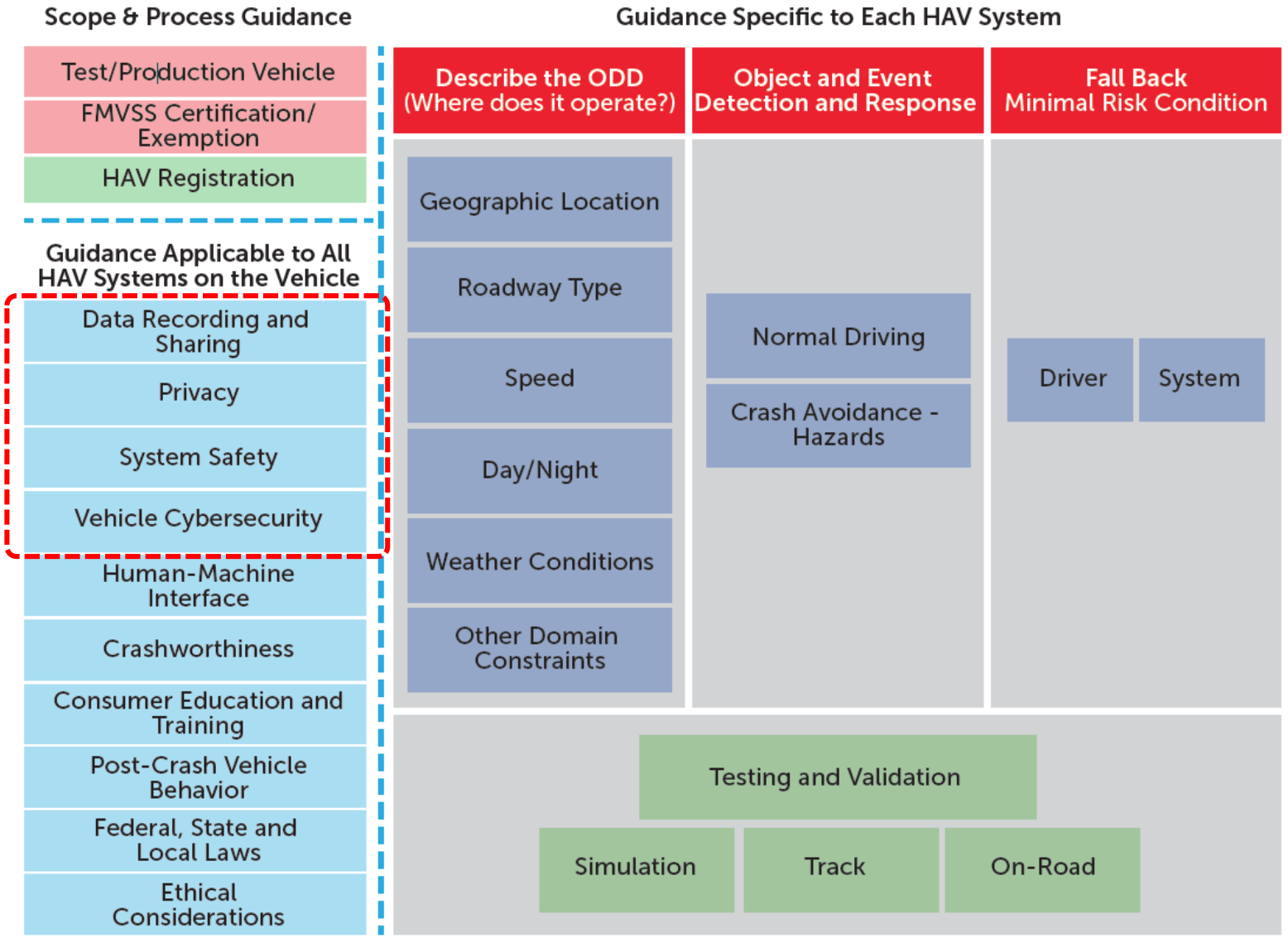
https://www.congress.gov/bill/115th-congress/senate-bill/680

“Federal Automated Vehicles Policy” (2016.09)

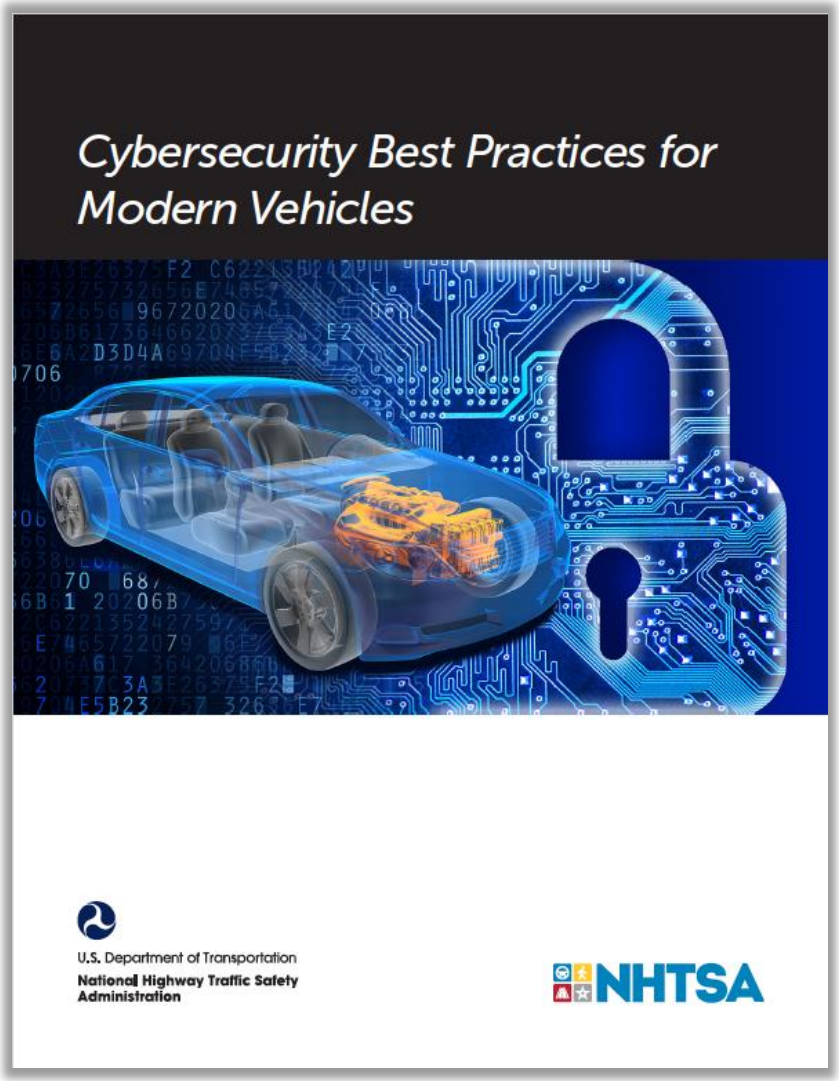


https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016/

"Federal Automated Vehicles Policy (2016.09)



Cybersecurity Best Practices (2016.10)



https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

Cybersecurity Best Practices (2016.10)

- Self-Auditing
  - Risk Assessment
  - Penetration Testing and Documentation
  - Self-Review
- Fundamental Vehicle Cybersecurity Protections
  - Limit Developer/Debugging Access in Production Devices
  - Control Keys
  - Control Vehicle Maintenance Diagnostic Access
  - Control Access to Firmware
  - Limit Ability to Modify Firmware
  - Control Proliferation of Network Ports, Protocols and Services
  - Use Segmentation and Isolation Techniques in Vehicle Architecture Design
  - Control Internal Vehicle Communications
  - Log Events
  - Control Communication to Back-End Servers
  - Control Wireless Interfaces

Declaration of Amsterdam

https://english.eu2016.nl/documents/publications/2016/04/14/declaration-of-amsterdam

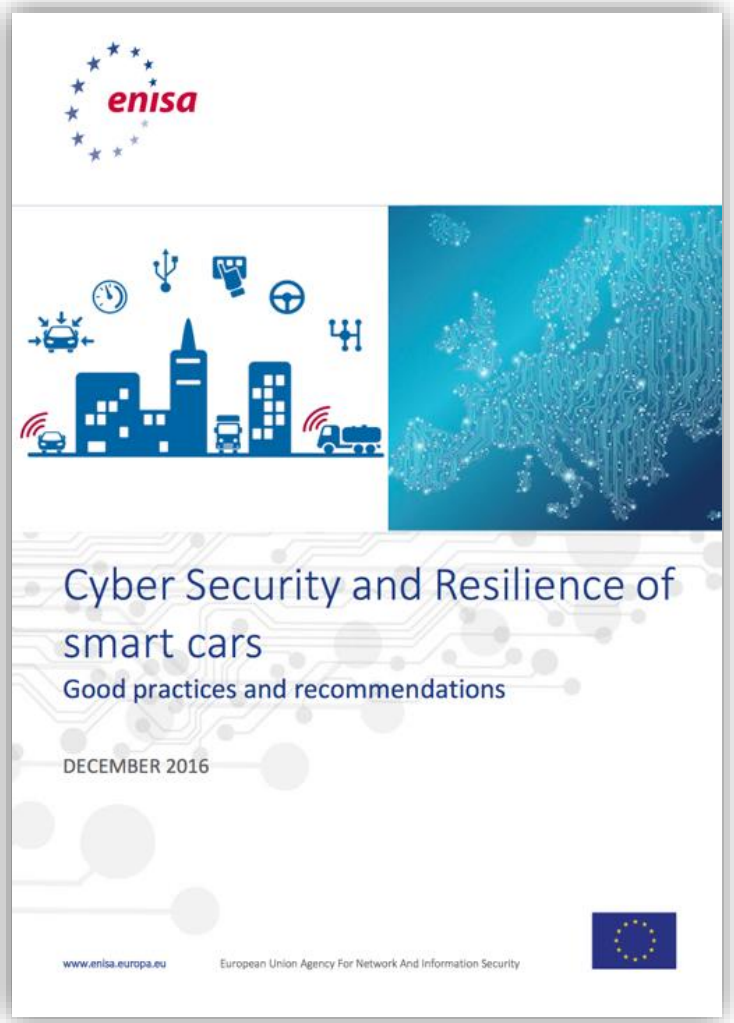
Joint Agenda

- a. Coherent international, European and national rules
  - The aim is to work towards the removal of barriers and to promote legal consistency. The legal framework should offer sufficient flexibility to accommodate innovation, facilitate the introduction of connected and automated vehicles on the market and enable their cross-border use.
- b. Use of data
  - Data generated through the use of connected and automated vehicles **can serve public and private value-added services**. Clarification is needed on the availability for public and private use and responsibilities of the parties involved.
- c. Ensure privacy and data protection
  - Respecting existing legislation on **privacy and data protection**, the conditions for the (re-) use and sharing of data generated by connected and automated vehicles need to be clarified.
- d. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication
  - In order to maximize benefits in road safety and environmental performance, it is essential to ensure that new services and systems are **compatible and interoperable at European level** and to coordinate investments towards reliable communication coverage, exploit the full potential of hybrid communications, where relevant, and improve the performance of location accuracy, benefiting in particular from the use of GALILEO and EGNOS.

Joint Agenda

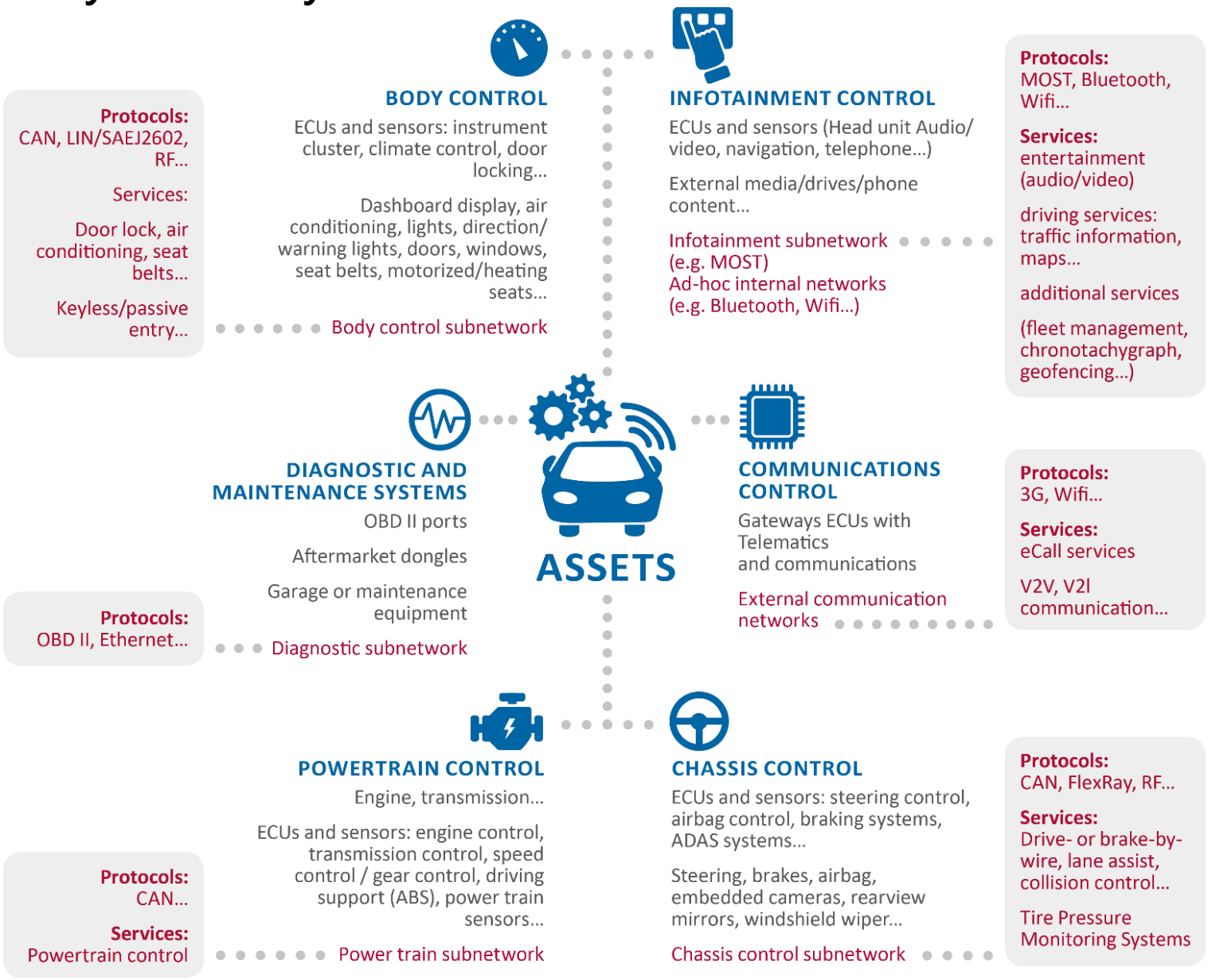
- e. Security
  - In the light of the increase in cyber-threats and serious vulnerabilities, it is essential to ensure security and reliability of connected and automated vehicle communications and systems. **Common trust models and certification policies** should be developed to prevent risks and support cybersecurity, whilst ensuring safe and interoperable deployment.
- f. Public awareness and acceptance
  - It is important to manage societal expectations, to raise awareness and increase acceptance and appreciation of connected and automated vehicle technologies.
- g. Common definitions of connected and automated driving
  - Common definitions of connected and automated driving should be developed and updated, based on the Society of Automotive Engineering levels (SAE levels) as a starting point.
- h. International cooperation
  - It is important to develop and maintain close cooperation with other regions, particularly the US and Japan, to work towards a global framework and international standards for connected and automated vehicles.

ENISA – Cyber Security and Resilience of Smart Cars



https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars/

ENISA – Cyber Security and Resilience of Smart Cars



ENISA – Cyber Security and Resilience of Smart Cars

DAMAGE / LOSS (IT ASSETS)

Loss of information in the cloud
Loss of (integrity of) sensitive information
Damage caused by a third party
Loss from DRM conflicts
Information leakage

FAILURES / MALFUNCTIONS

Failures / malfunctions of devices or systems
Failures or disruptions of the power supply
Software bugs
Failures / malfunctions of parts of devices
Failures or disruptions of communication links
Failures or disruptions of main supply

UNINTENTIONAL DAMAGES (ACCIDENTAL)

Information leakage or sharing
Erroneous use or administration of devices and systems
Using information from an unreliable source
Unintentional change of data in an information system
Inadequate design and planning or lack of adaption

PHYSICAL THREATS

Fault injection / glitching
Side channel
Access to HW debug ports

THREATS

ADVANCED PERSISTENT THREATS

LEGEND:
Threats perceived as significant by ≥80% answers
Threats perceived as significant by ≤60% answers

NEFARIOUS ACTIVITY / ABUSE

Denial of service
Malicious code / software activity
Manipulation of hardware & software
Manipulation of information
Unauthorised access to information system / network
Compromising confidential information
Identity fraud
Abuse of information leakage
Unauthorized use of administration of devices & systems
Unauthorized use of software
Unauthorized installation of software
Abuse of authorizations
Malicious software
Remote activity (execution)

NETWORK OUTAGE

EAVESDROPPING /INTERCEPTION / HIJACKING

Interception of information
Replay of messages
Interfering radiations
Man in the middle / session hijacking
Network reconnaissance and information gathering
Repudiation of actions

Transport - Vehicle Regulations / ... / Intelligent Transport Systems and Automated Driving (ITS/AD)

UN Task Force on Cyber security and OTA issues (CS/OTA)

Martin Dagan님이 작성, 11월 30, 2016에 최종 변경

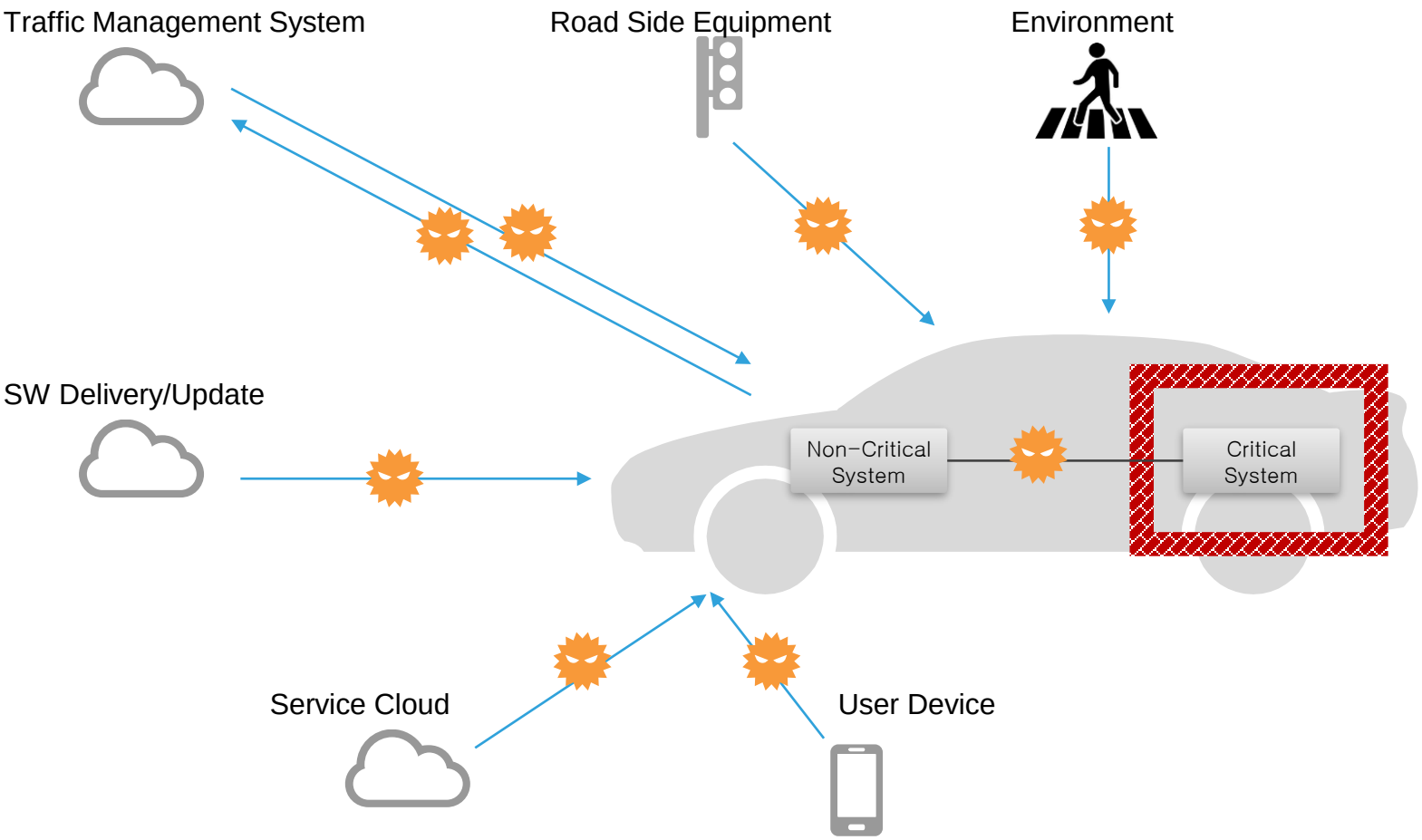
Browse the child pages below for more information on "UN Task Force on Cyber security and OTA issues" meetings documents.

10 하위 페이지

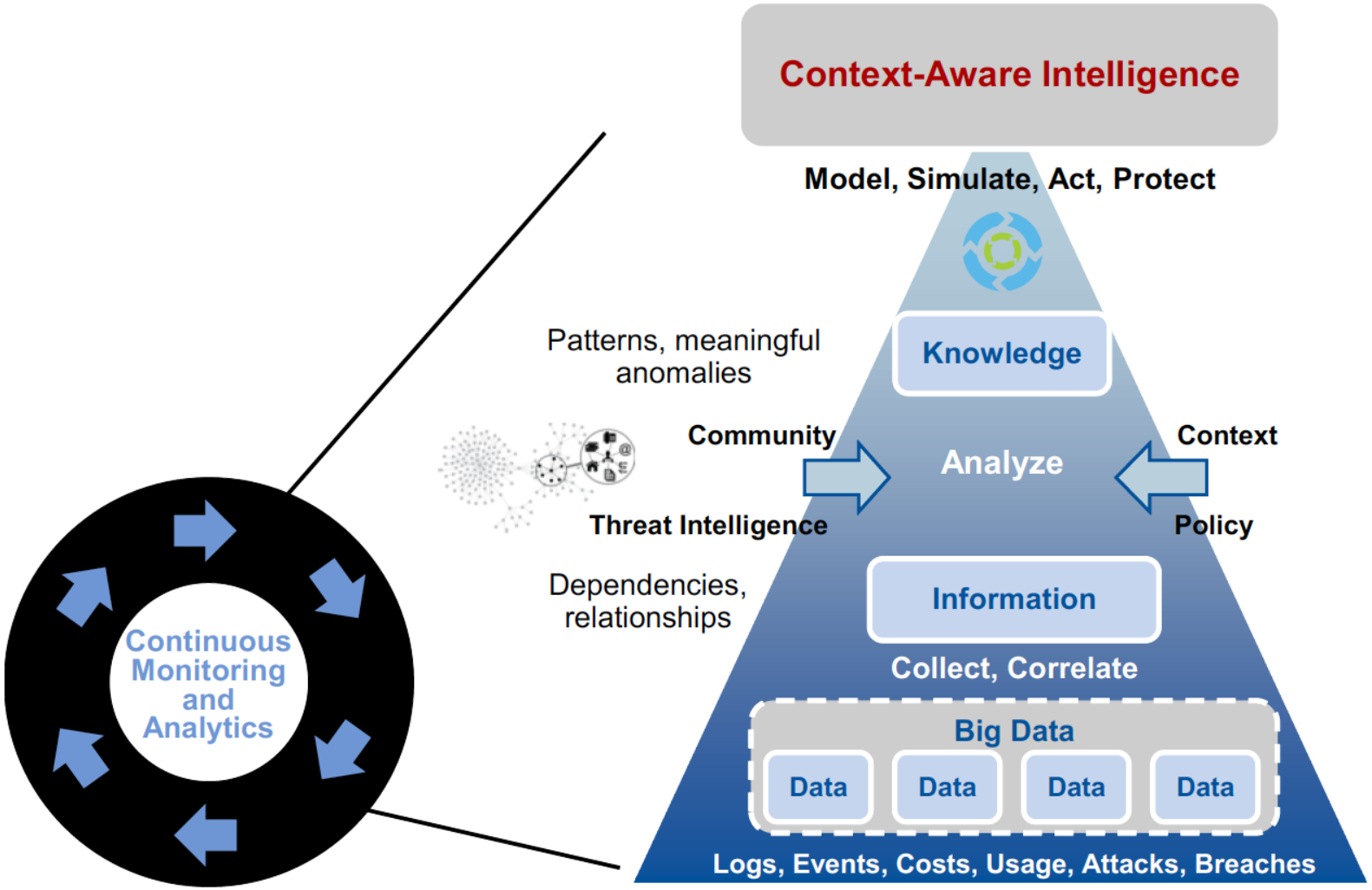
- CS/OTA 1st session
- CS/OTA 2nd session - review ToR
- CS/OTA 3rd session
- CS/OTA ad hoc "Threats"
- CS/OTA 4th session
- CS/OTA ad hoc "Threats 2"
- CS/OTA 5th session
- CS/OTA 6th session
- CS/OTA 7th session
- CS/OTA 8th session

https://wiki.unece.org/pages/viewpage.action?pageId=40829521

Threats for Autonomous Driving

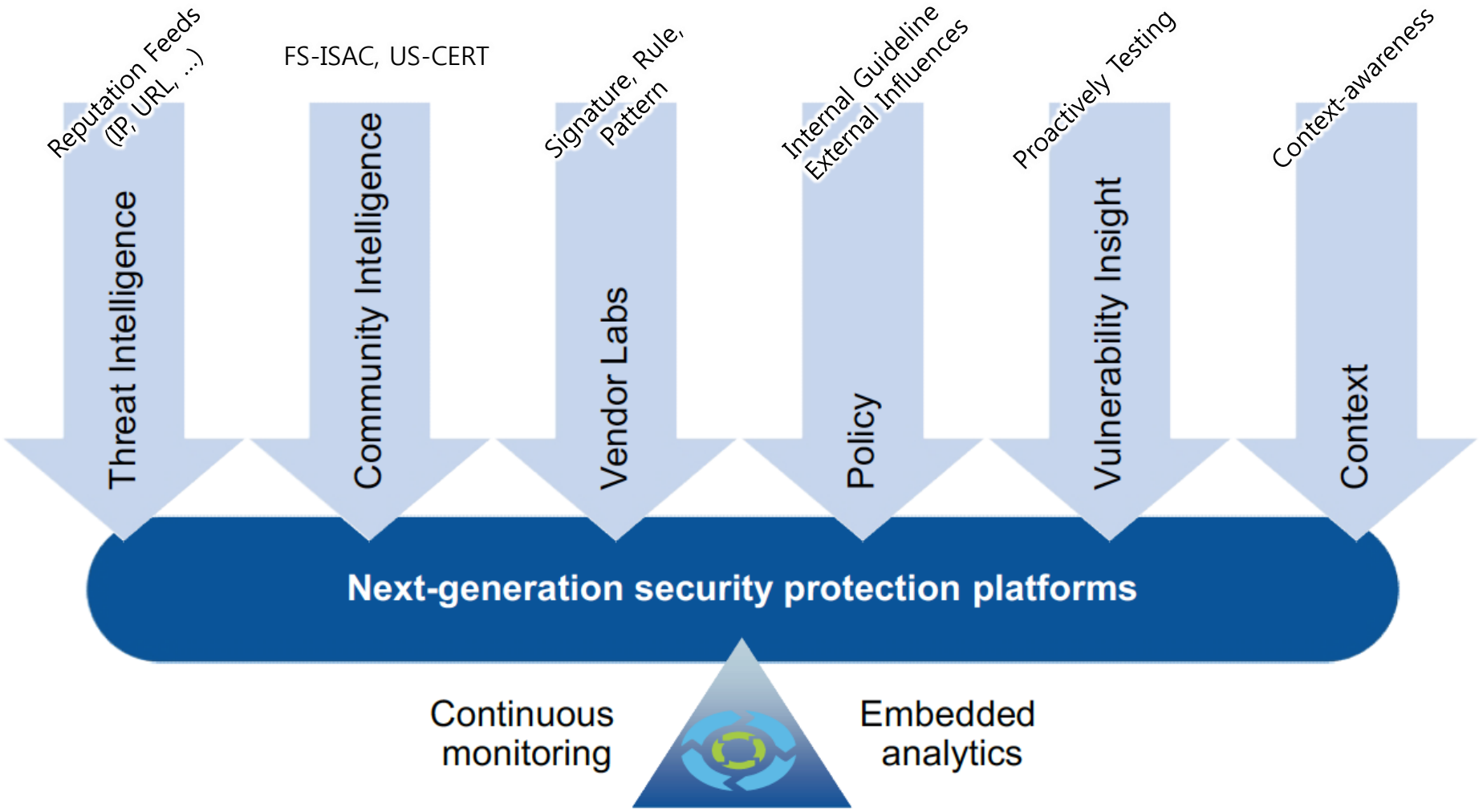


Adaptive Security Architecture (Gartner)



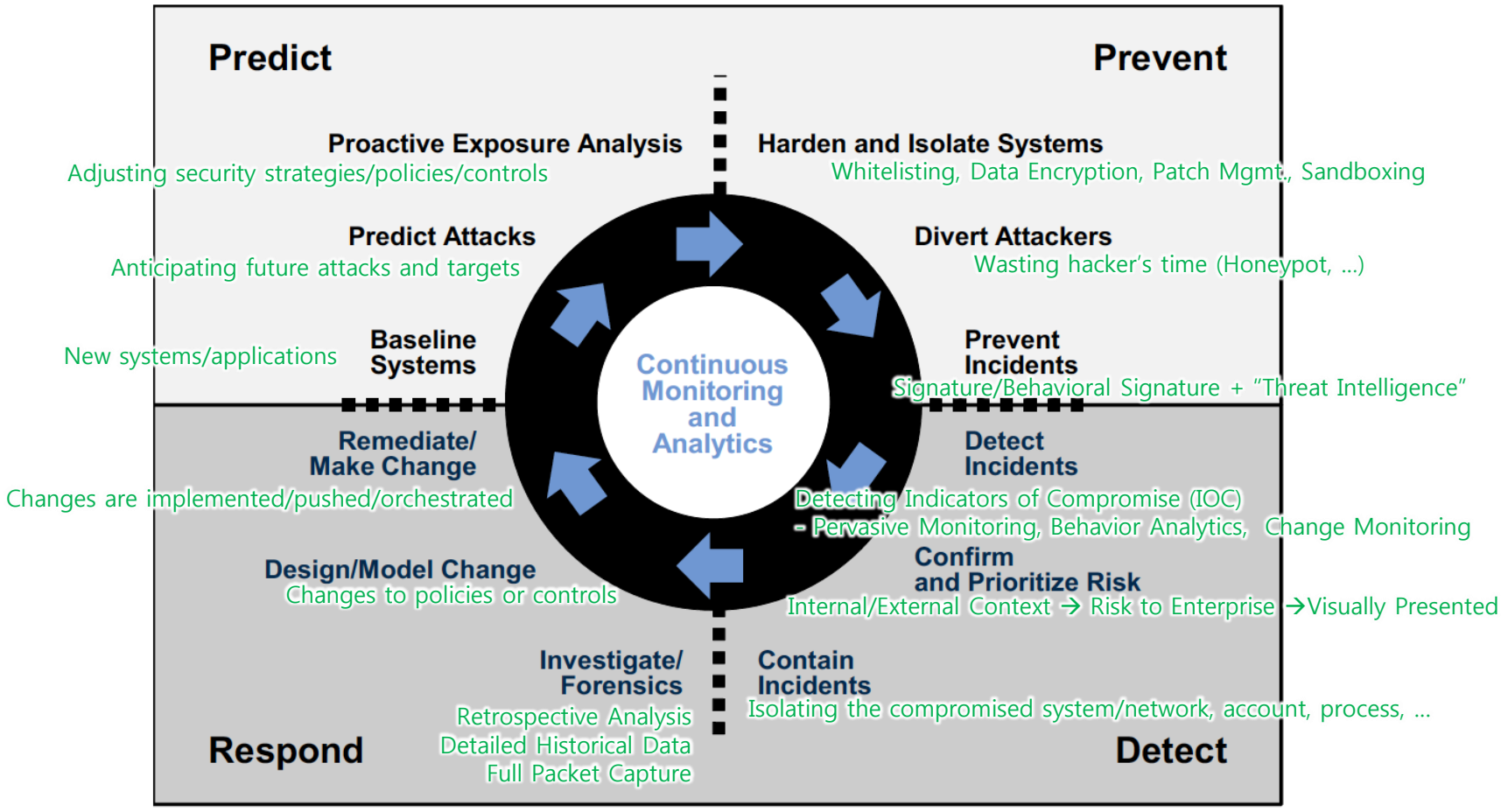
Source: Gartner (February 2014)

Inputs into the Adaptive Protection Architecture



Adaptive Security Architecture - Lifecycle

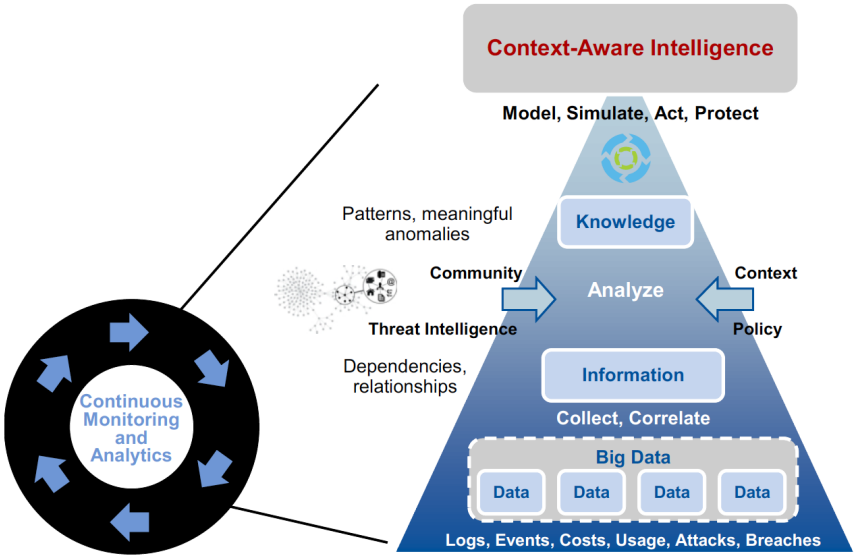
In-line, real time
(sub-second)



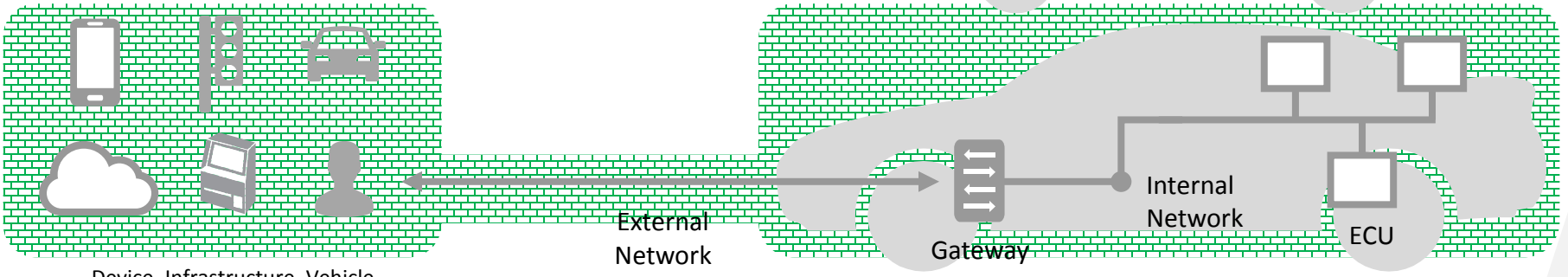
Post-incident
(minutes ~ months)

Near real time
(seconds ~ minutes)

Adaptive Security & Autonomous Car

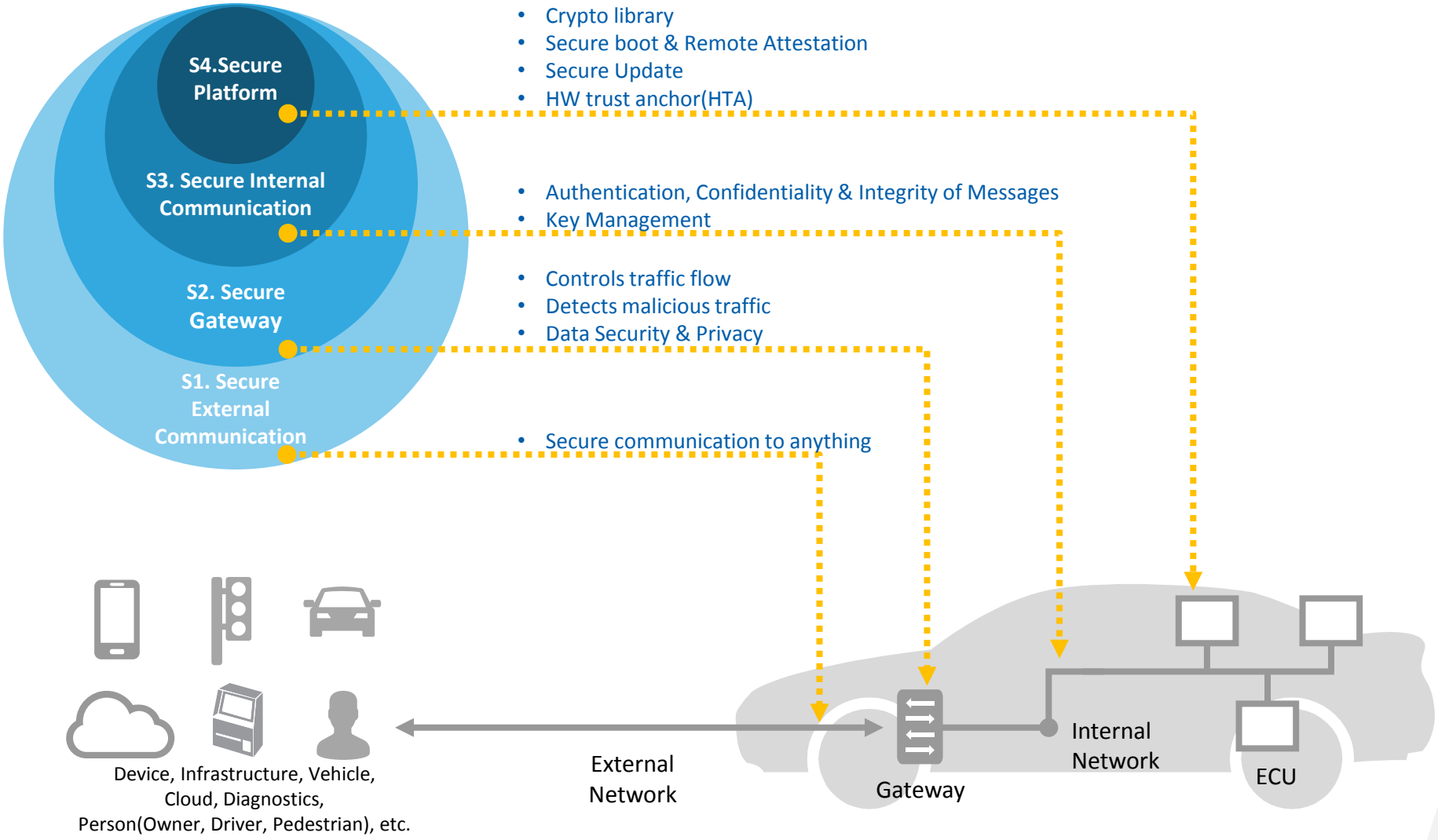


Source: Gartner (February 2014)

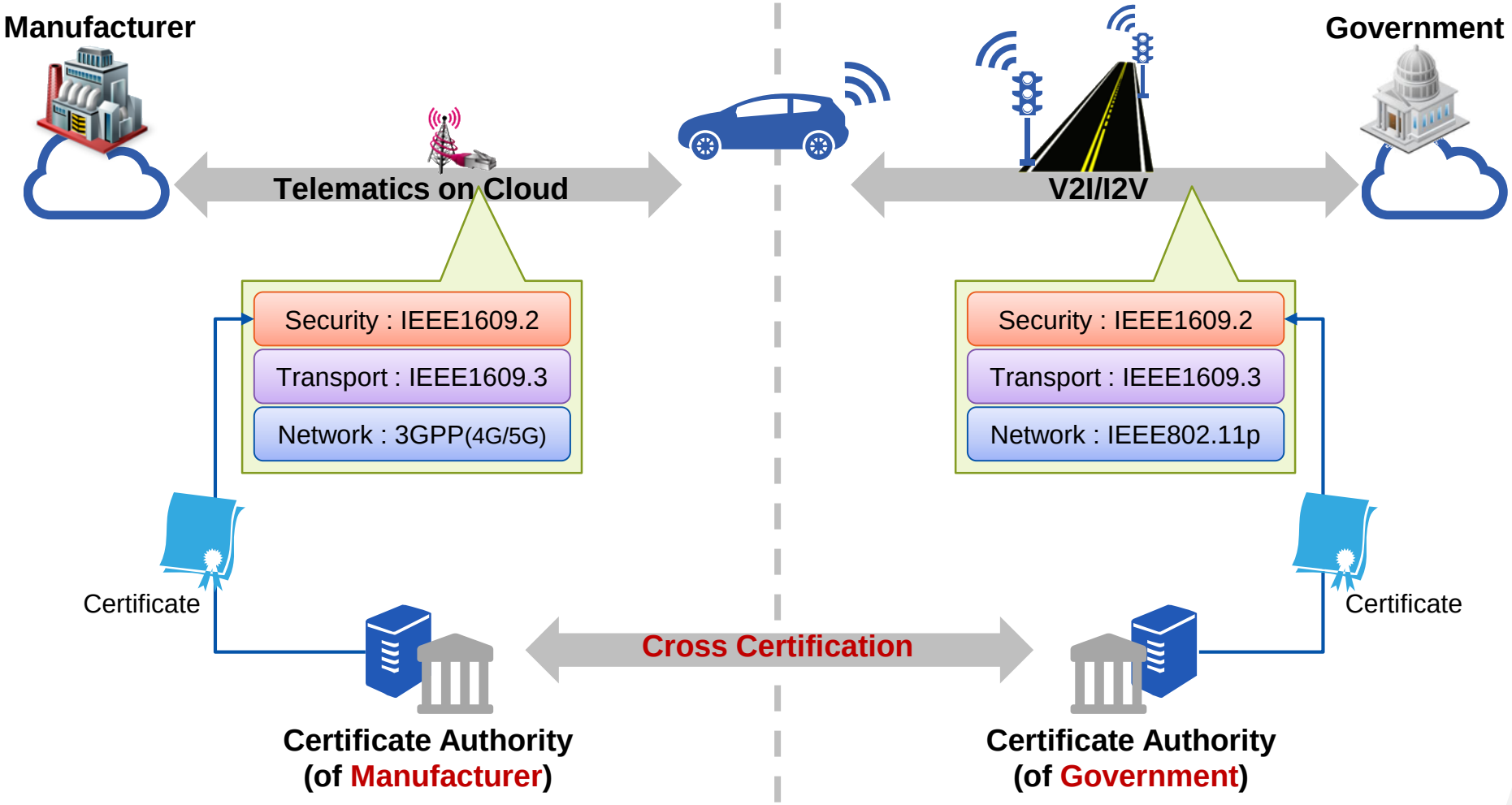


Device, Infrastructure, Vehicle,
Cloud, Diagnostics,
Person(Owner, Driver, Pedestrian), etc.

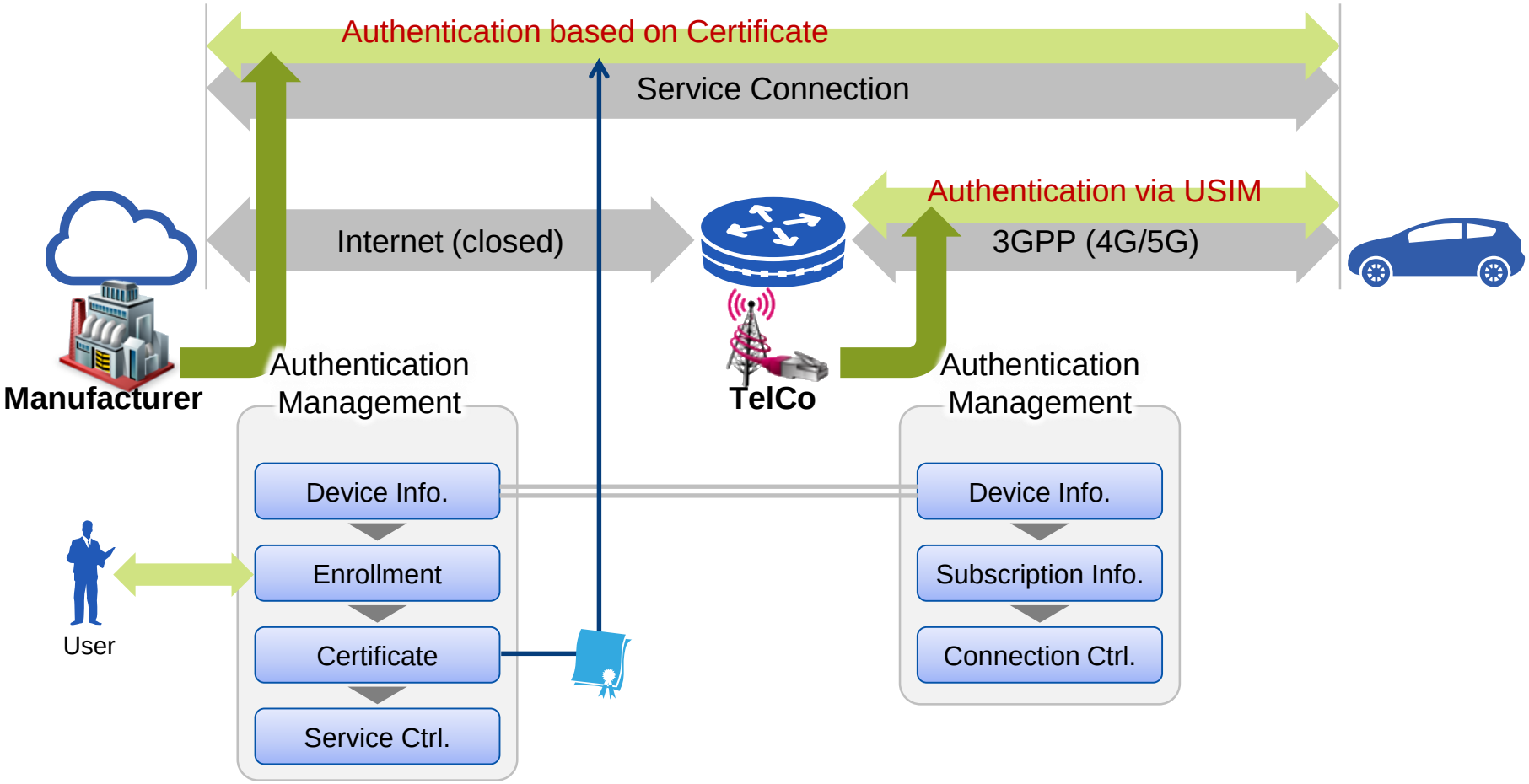
Cybersecurity Concept for Connected Car



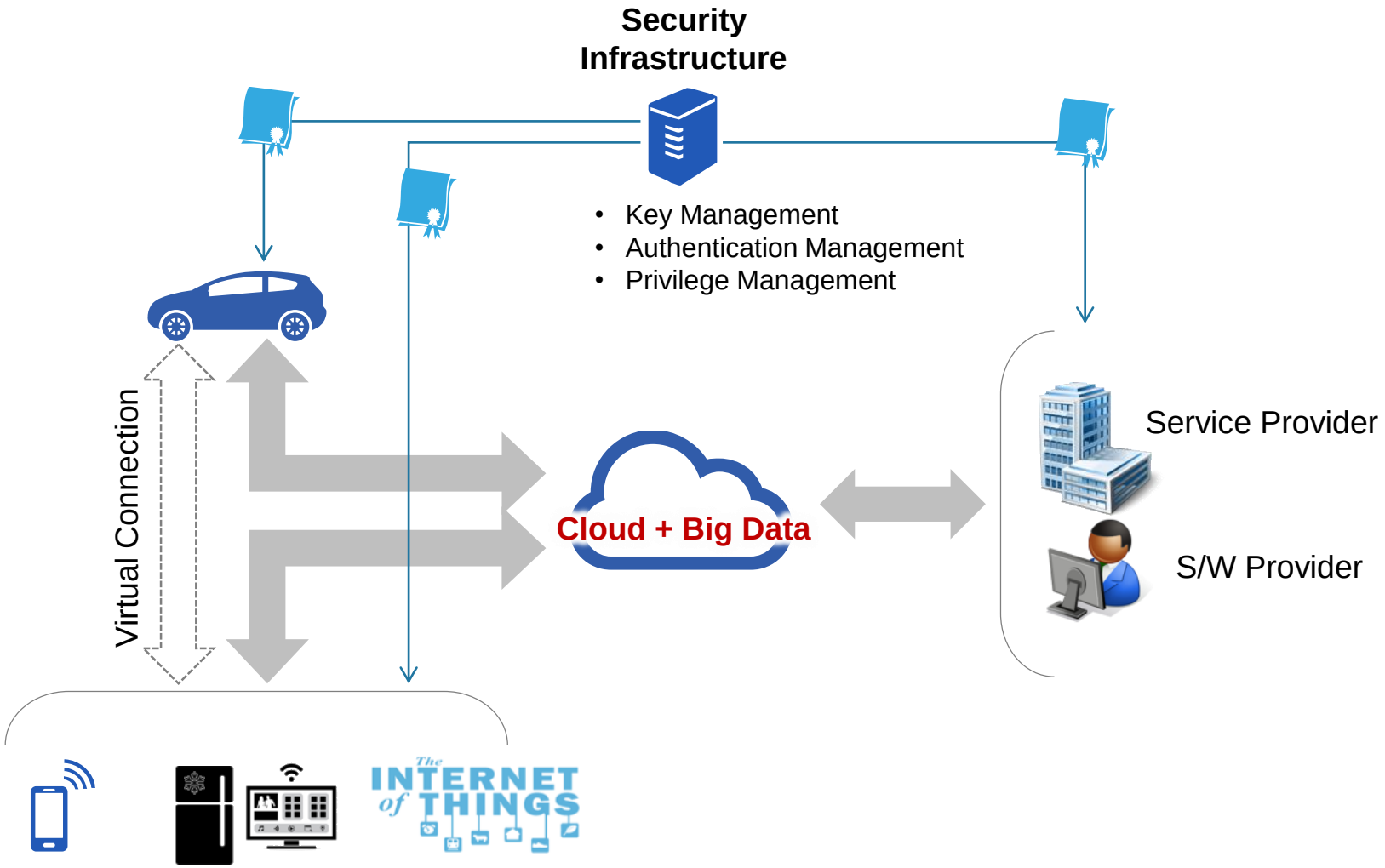
S1. Secure External Communication



S1. Secure External Communication – TelCo & Manufacturer



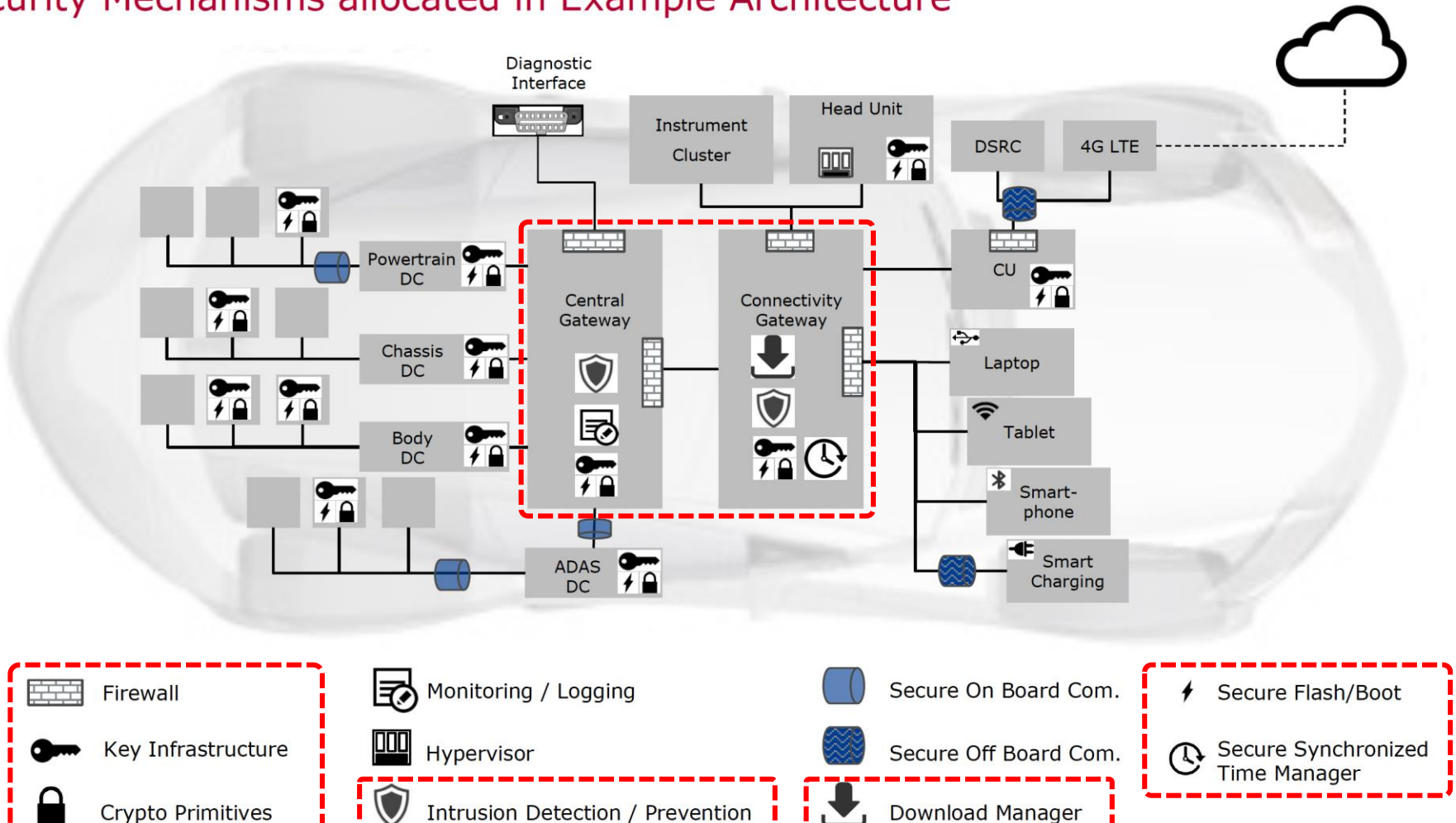
S1. Secure External Communication - Ecosystem and Security Infrastructure



S2. Secure Gateway

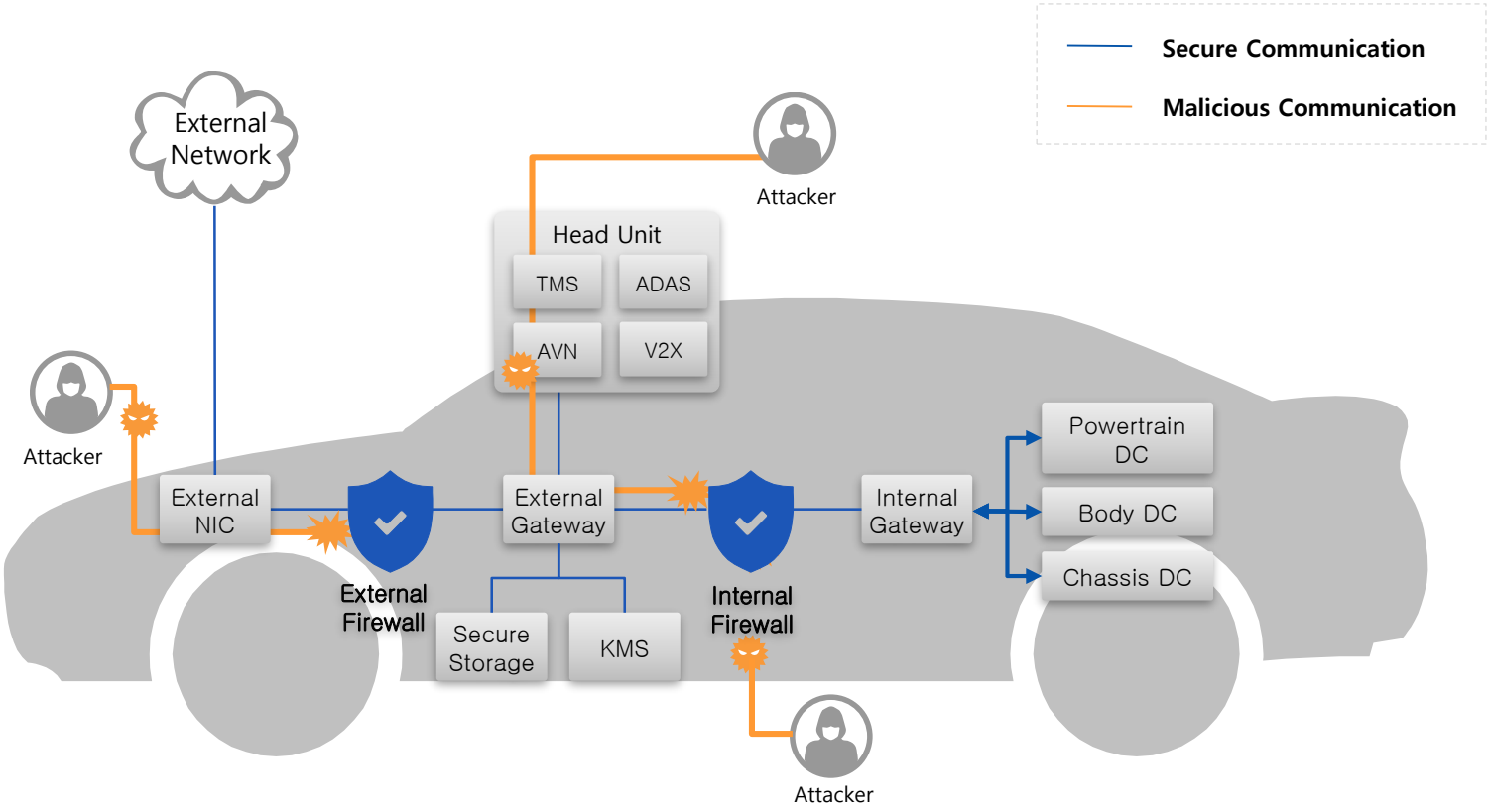
VECTOR

Security Mechanisms allocated in Example Architecture

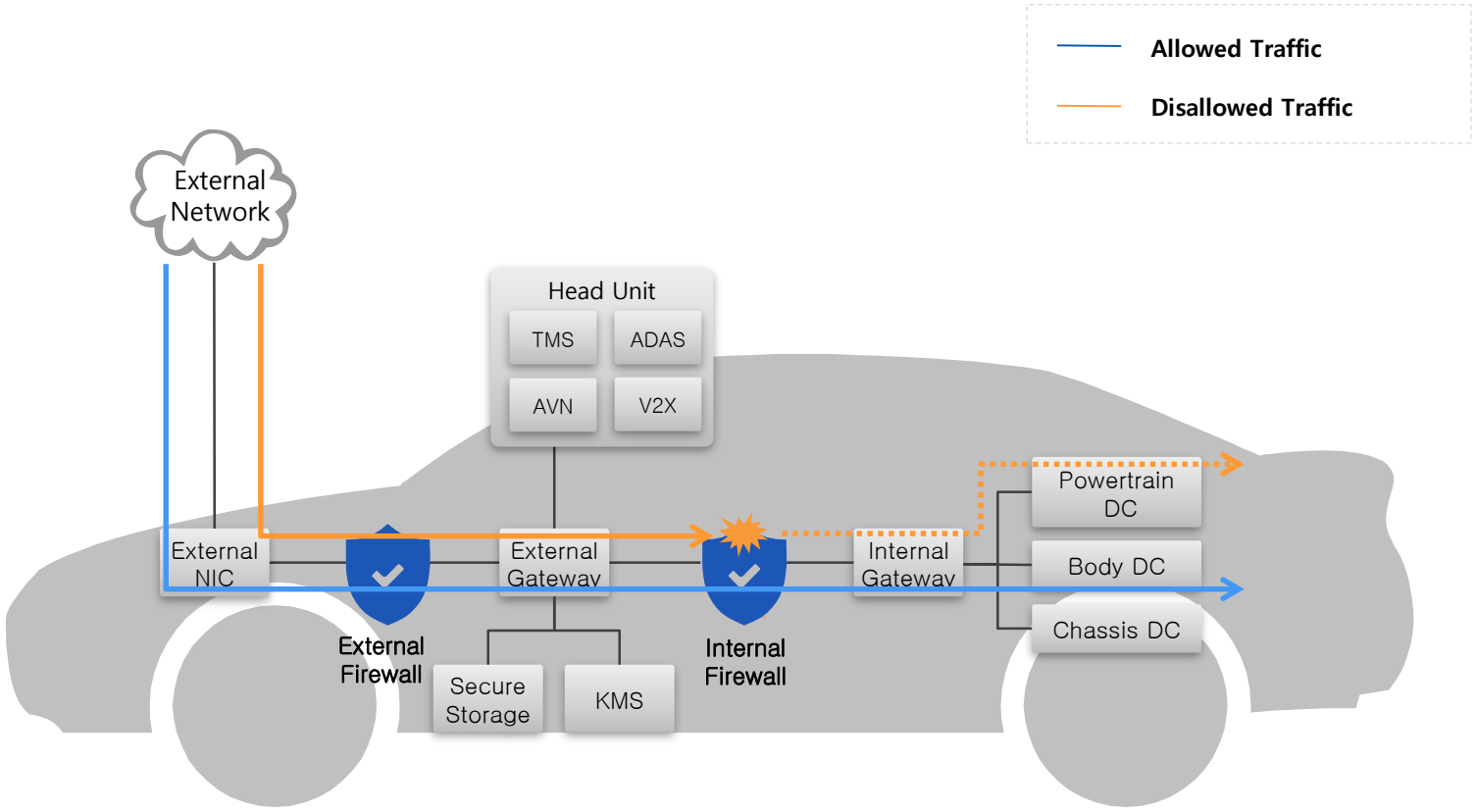


"Vector Cyber Security Solutions", AUTOSAR Users Group Meeting – 2016.08.01

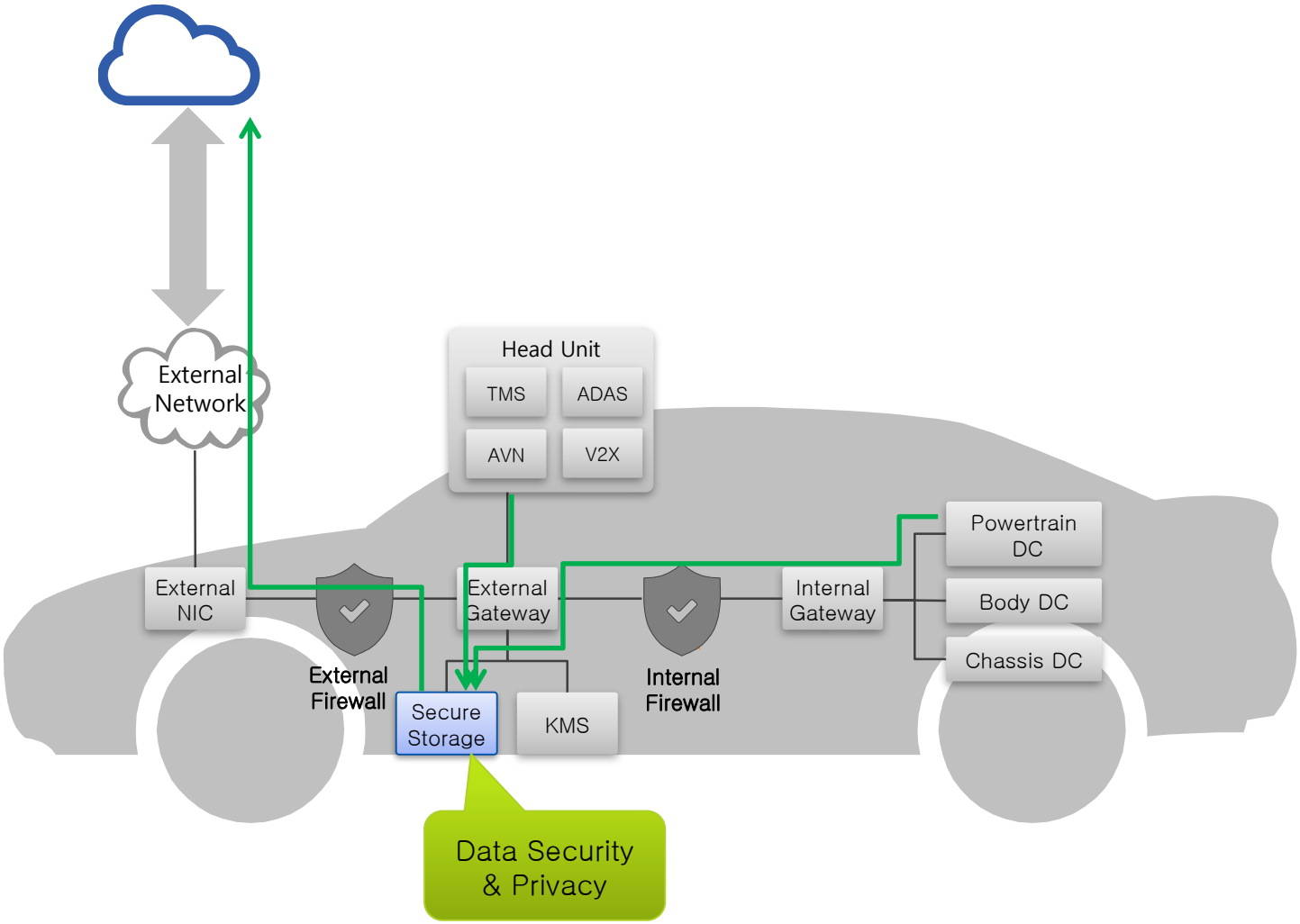
S2. Secure Gateway – Detects malicious traffic



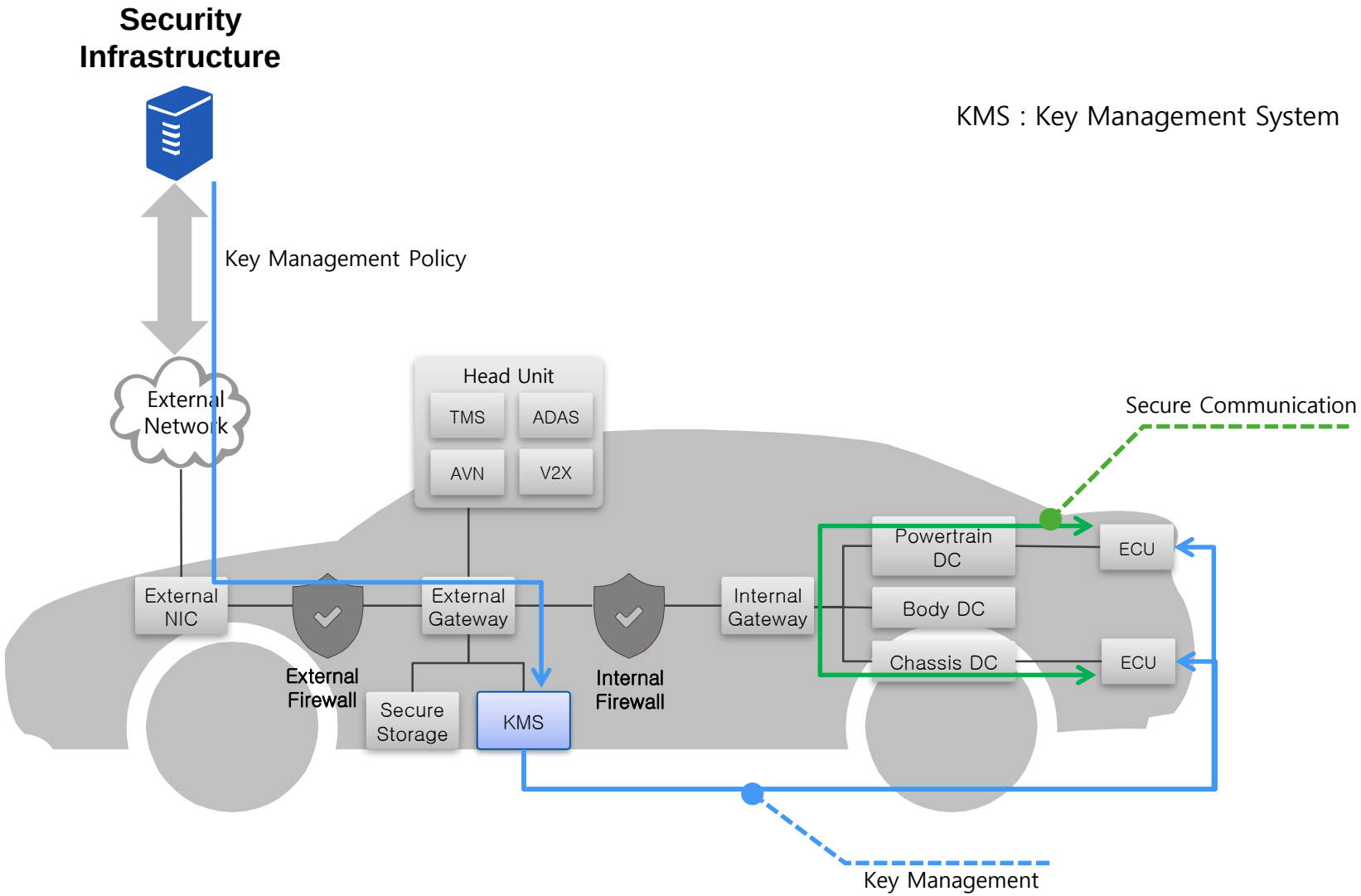
S2. Secure Gateway – Controls traffic flow



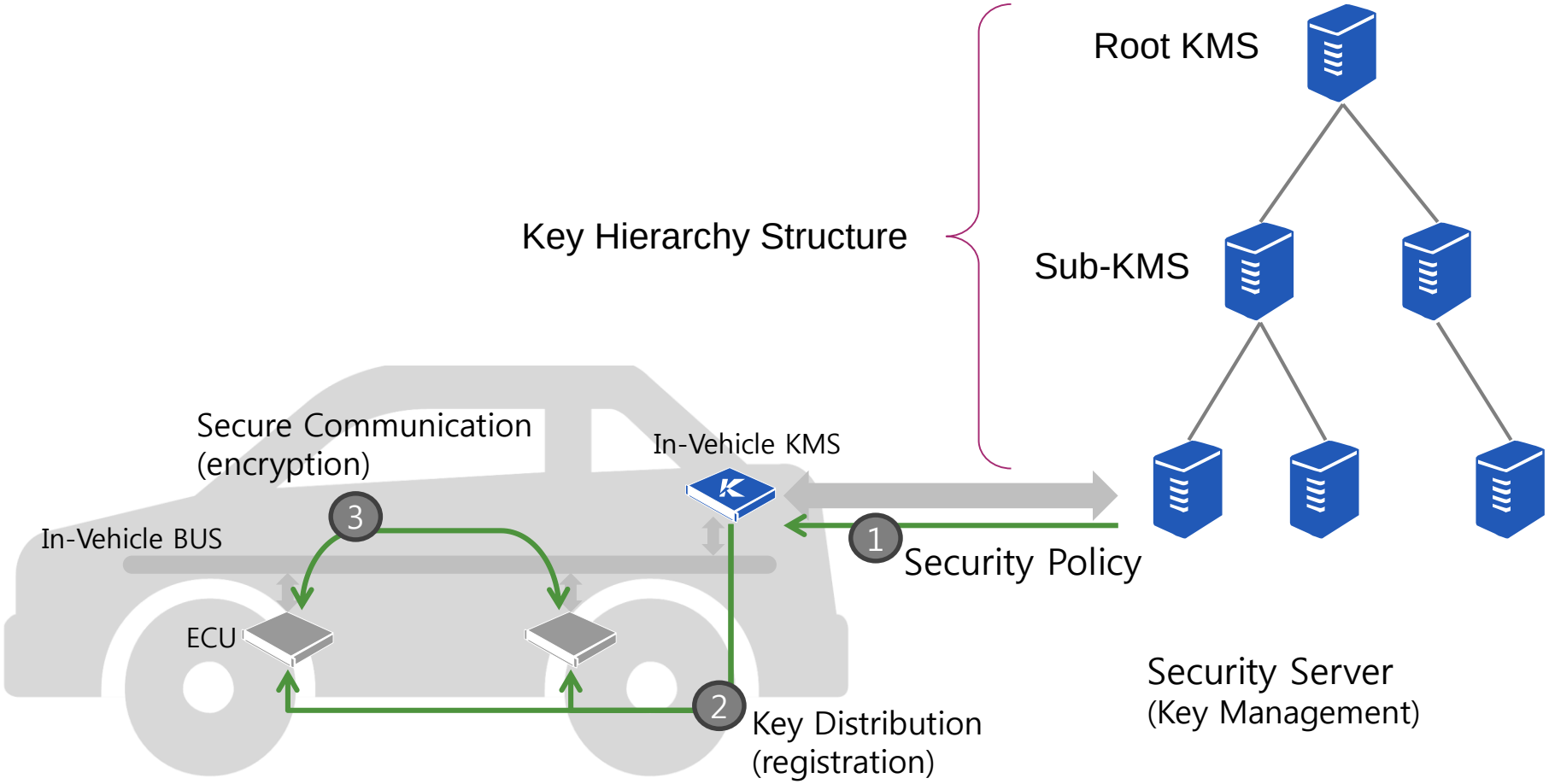
S2. Secure Gateway – Data Security & Privacy



S3. Secure Internal Communication

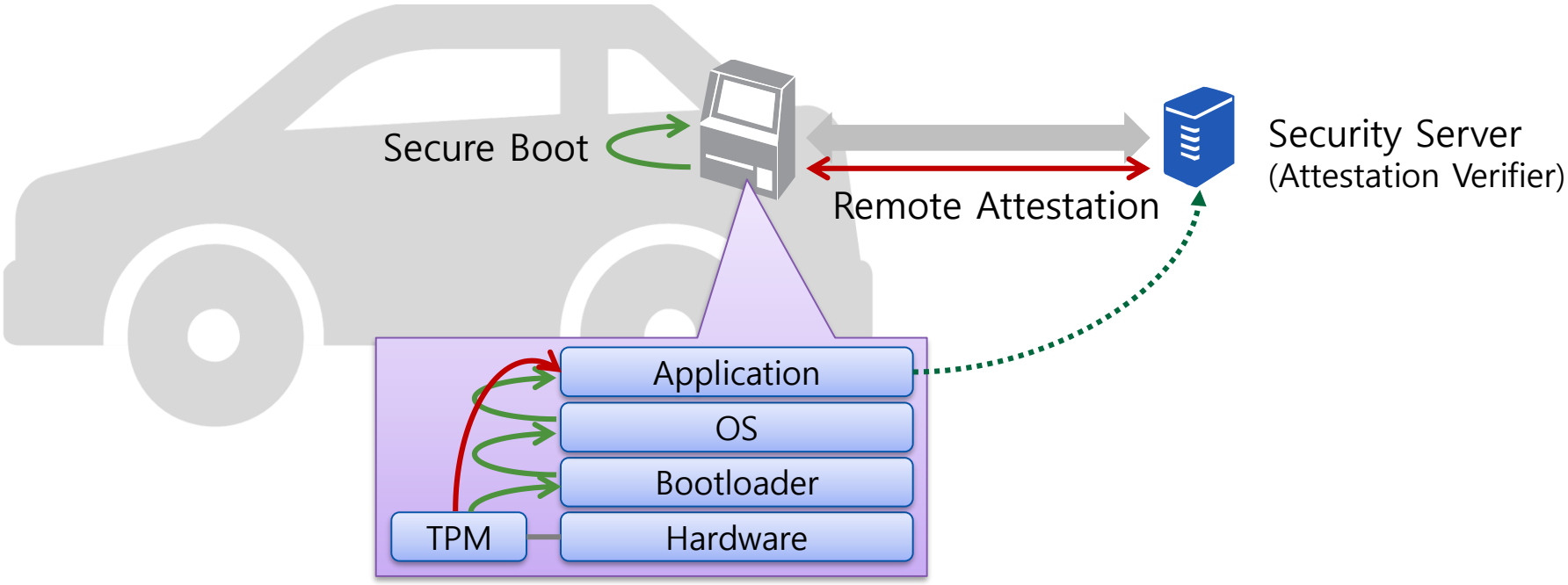


S3. Secure Internal Communication - Key Management



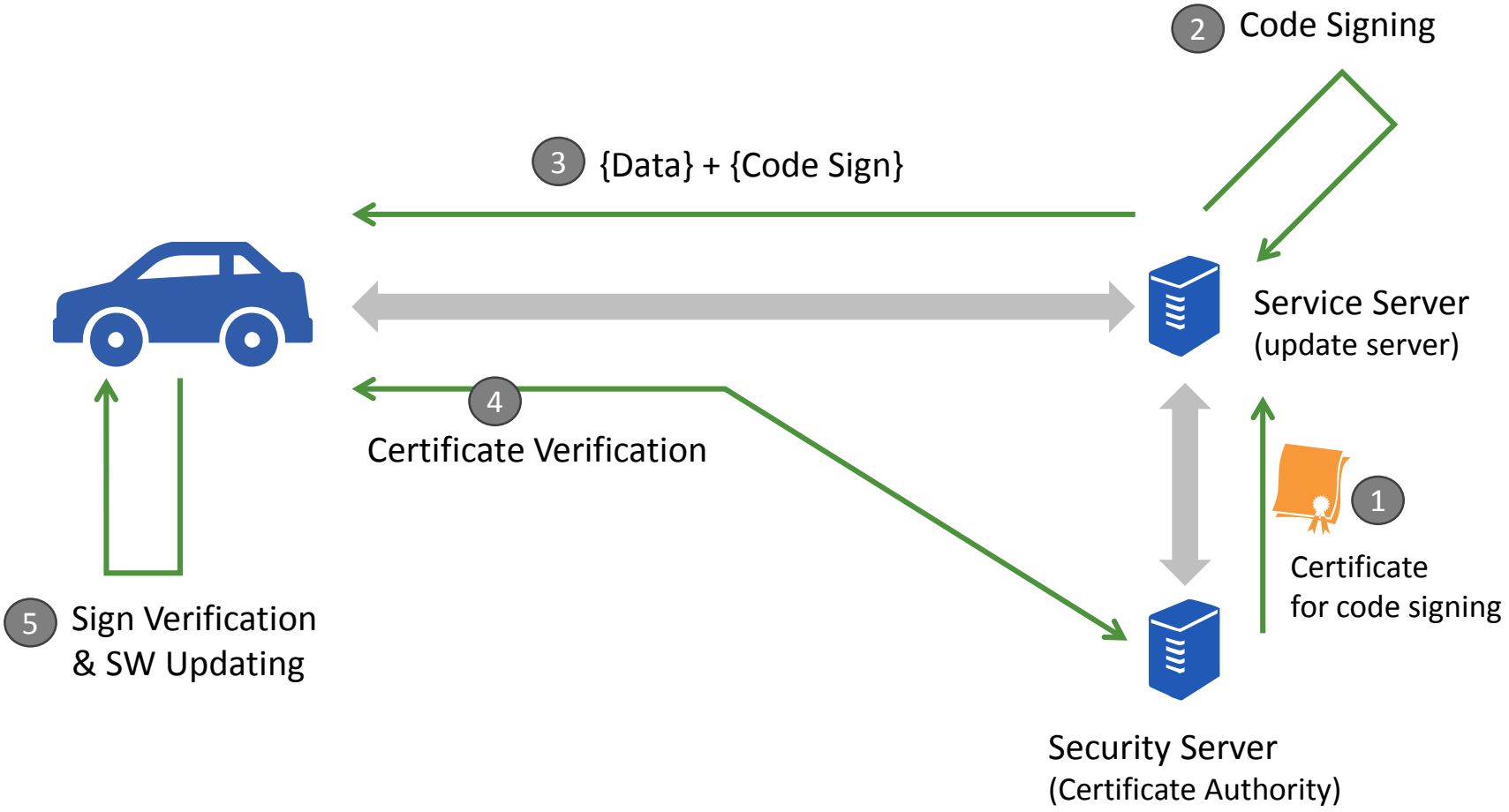
KMS : Key Management System

S4. Secure Platform - Secure Boot & Remote Attestation



TPM : Trusted Platform Module

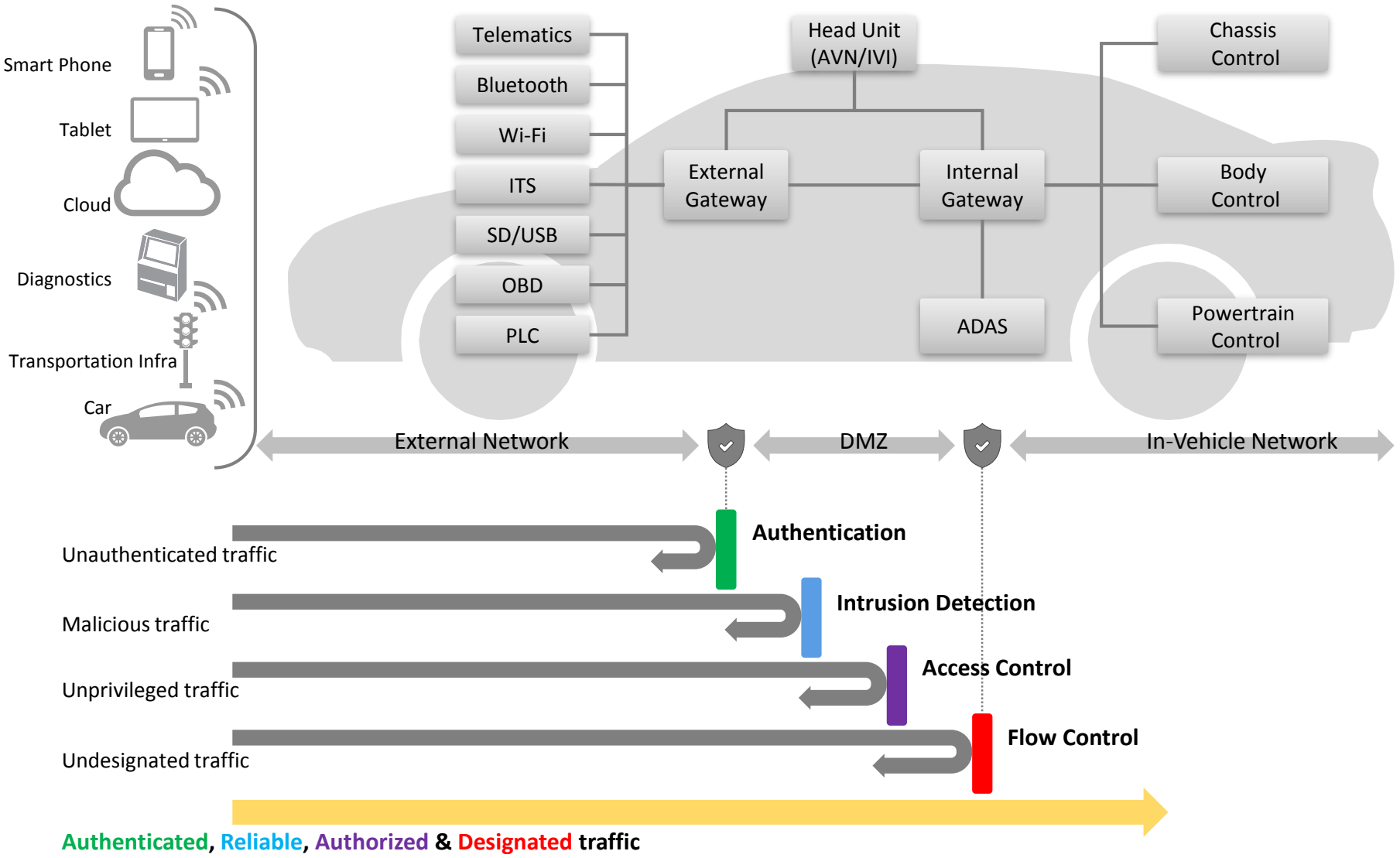
S4. Secure Platform - Secure Flash/Update



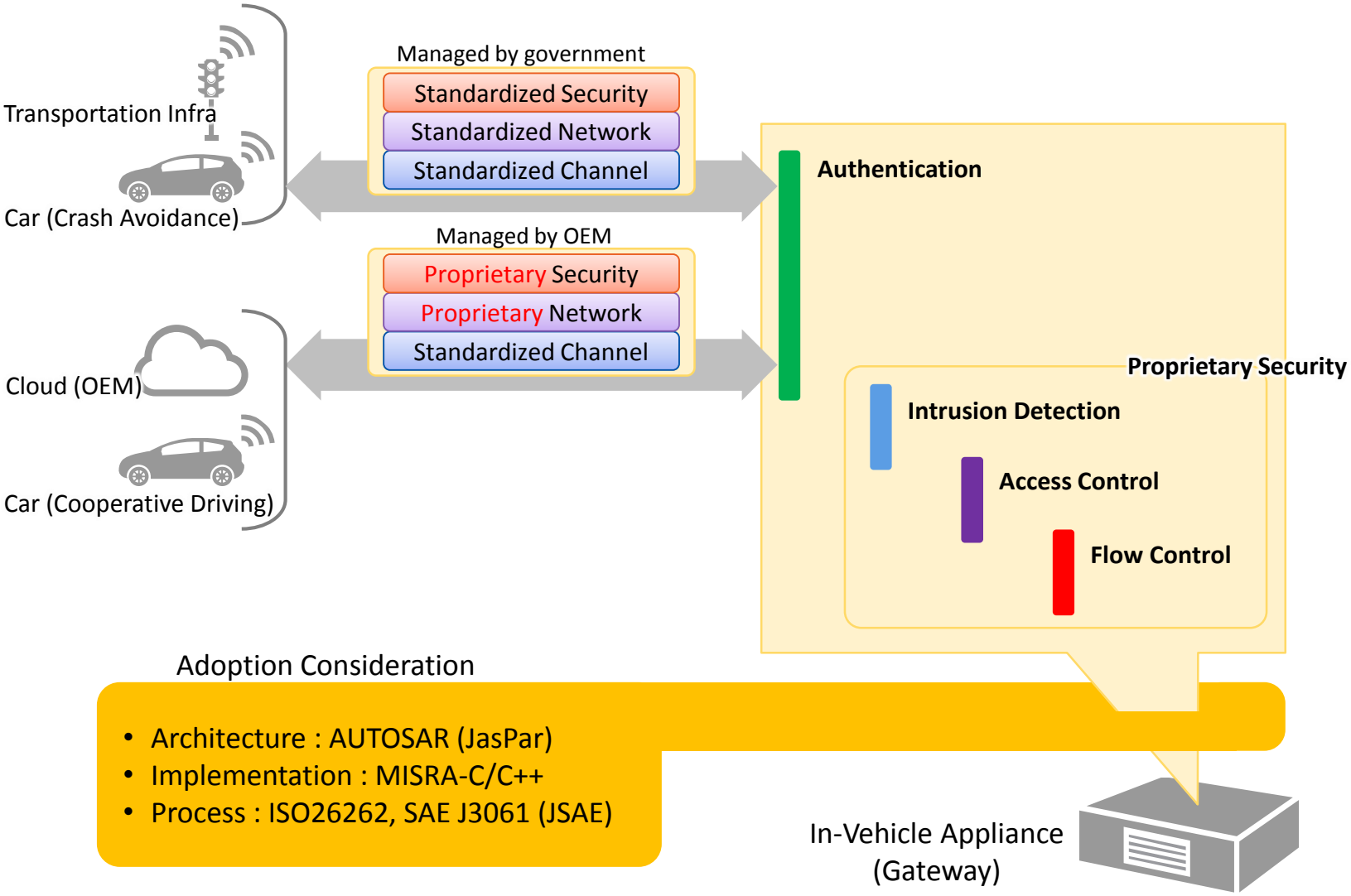
Security Primitives for Usecases

Usecase	S1	S2	S3	S4
A1. Secure Diagnostics	Authentication (GW)	Access Control (GW) Intrusion Detection (GW)		
A2. Integrity of Head Unit	Authentication (GW) Secure Comm. (GW)			Secure Update (HU) Secure Boot (HU)
B1. Secure Telematics	Authentication (GW) E2E Encryption (GW)	Access Control (GW) Flow Control (GW) Intrusion Detection (GW)		
B2. Secure Tethering				
B3. Secure Playback				
C1. Secure ITS	Authentication (GW)	Access Control (GW) Flow Control (GW) Intrusion Detection (GW)		
C2. Secure Service Delivery	Authentication (GW)	Download Manager (GW) Access Control (GW) Flow Control (GW) Intrusion Detection (GW)		Contents Integrity (ECU)
C3. Secure SW Delivery	Authentication (GW)	Download Manager (GW) Access Control (GW) Flow Control (GW) Intrusion Detection (GW)		Secure Update (ECU) Secure Boot (ECU)
C4. Data Security & Privacy	Authentication (GW)	Secure Storage (GW) Pseudonymization (GW) Access Control (GW)		
C5. Secure On-Board Comm.	Authentication (GW)		Key Management (GW) Security Policy (GW) Secure Comm. (ECU)	

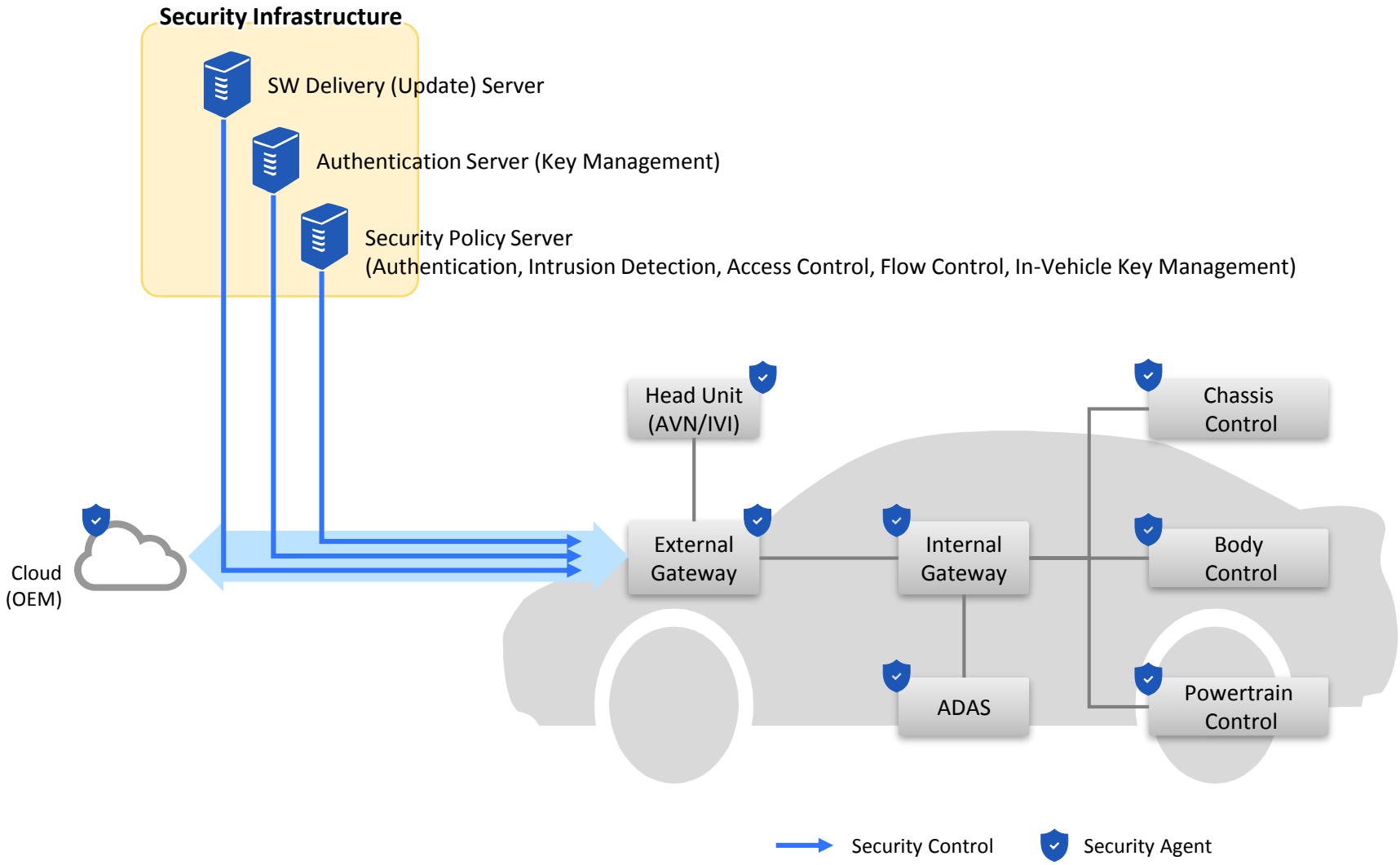
Top 4 Security Primitives



Adoption of the Top 4 Primitives

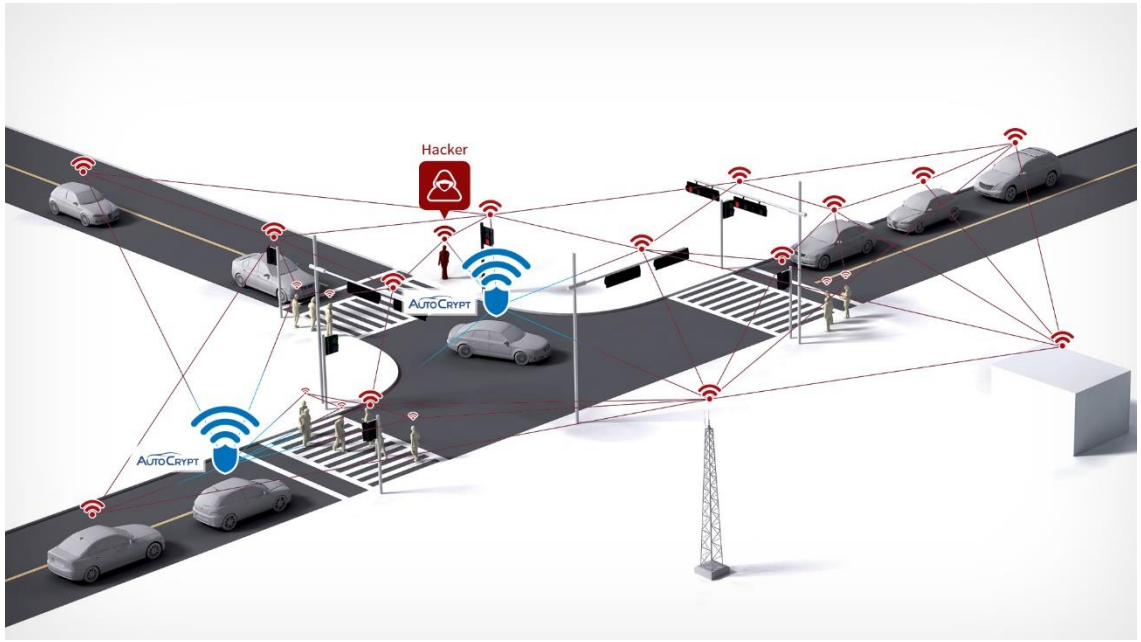


Management of Cybersecurity



AutoCrypt

Experiences about Connected Car



2017. vPKI for C-ITS, Autonomous Driving

2016. C-ITS Testbed

2015. Firewall for Vehicle
AutoCrypt® Launch

2014. Vehicle Data Monitoring System
Telematics Security

2013. V2X over WAVE

2012. Security for Patrol Car

2011. Security for Vehicle – Nomadic(mobile) Device

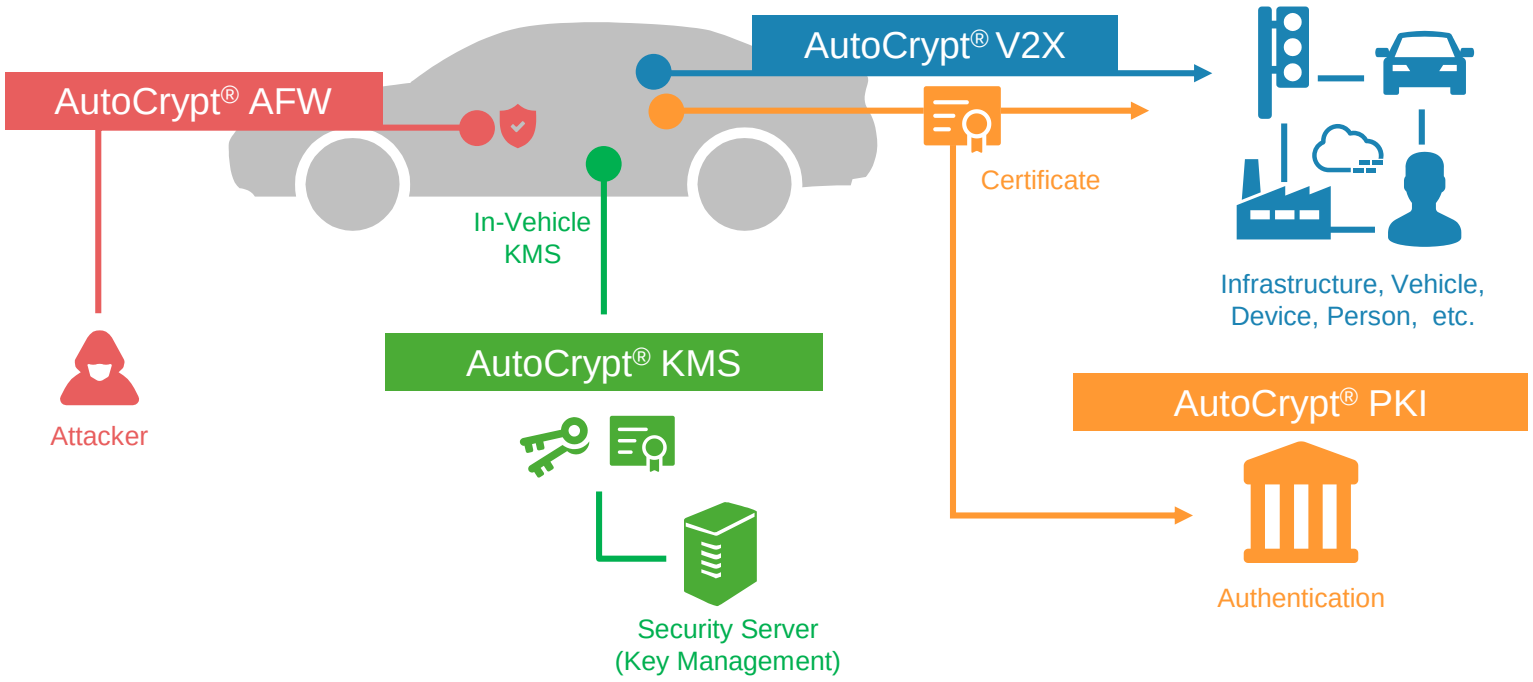
2007. Security for Vehicle – Diagnostic Device

AutoCrypt® Overview

Enforcing a new age of security within the connected car to ensure safety of the occupant.

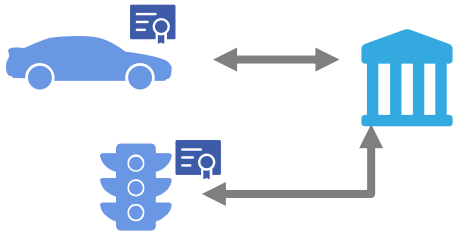
AutoCrypt offers the following products to cover different vulnerabilities existing for the connected car.

- **AutoCrypt V2X: Vehicle-to-Anything**
- **AutoCrypt PKI: Public Key Infrastructure**
- **AutoCrypt KMS: Key Management System**
- **AutoCrypt AFW: Advanced Firewall**

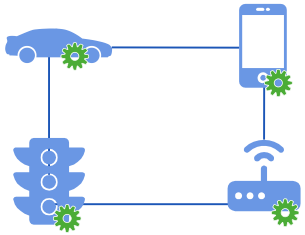


AutoCrypt® Major Features

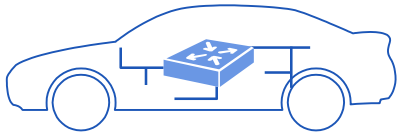
1 **Vehicle Public Key Infrastructure**



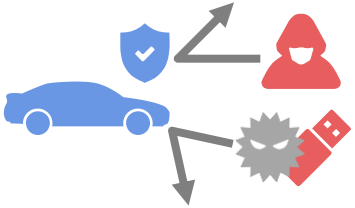
2 **Secure Communication**



3 **Control Traffic Flows**

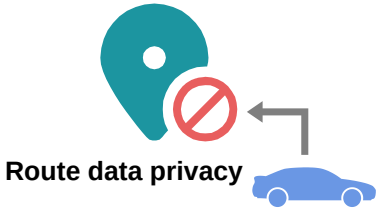


4 **Prevent Malicious Access**



5 **Key Management**

6 **Privacy Preserving**



AutoCrypt® V2X

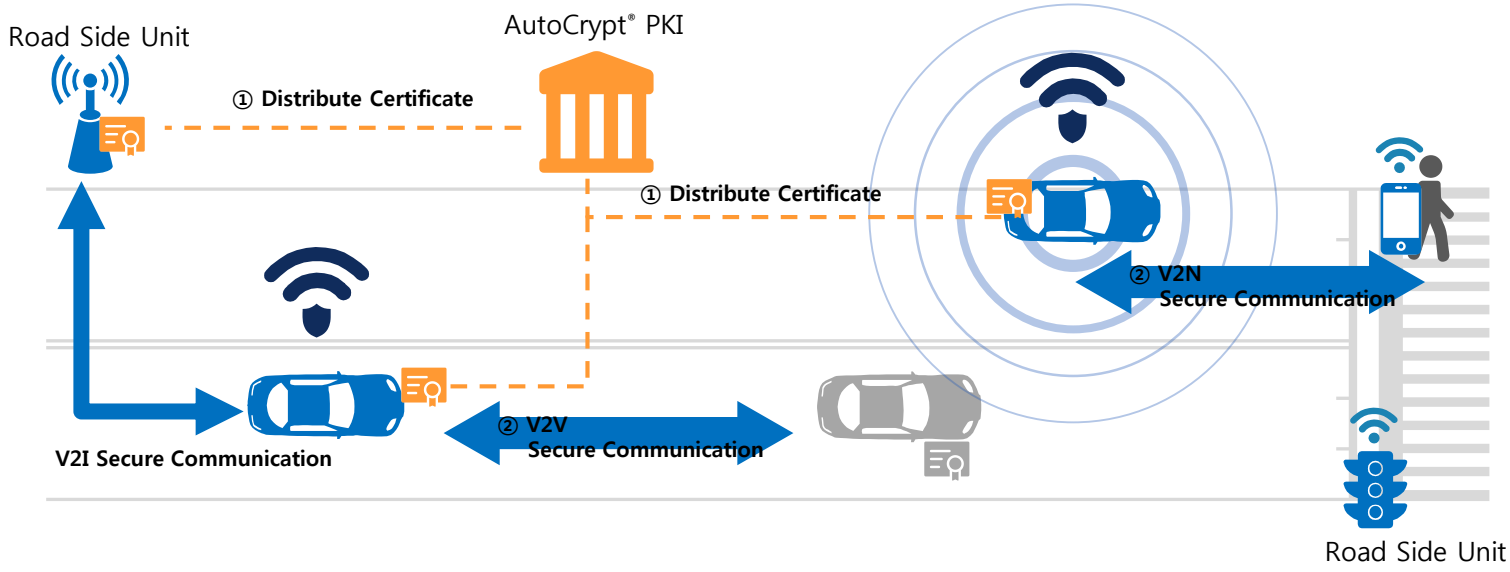
Vehicles use a AutoCrypt V2X module and AutoCrypt PKI to securely communicate based on a secure distributed certificate system. The “anything” can include infrastructure, devices, other vehicles.

- Allows for secure encrypted communication between the vehicle and RSUs (Road Side Unit), as well between the road and signal systems.
- AutoCrypt V2X is based off of IEEE1609.2* which makes it in compliance with CAMP VSC** & SCMS***.

* IEEE1609.2: Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages

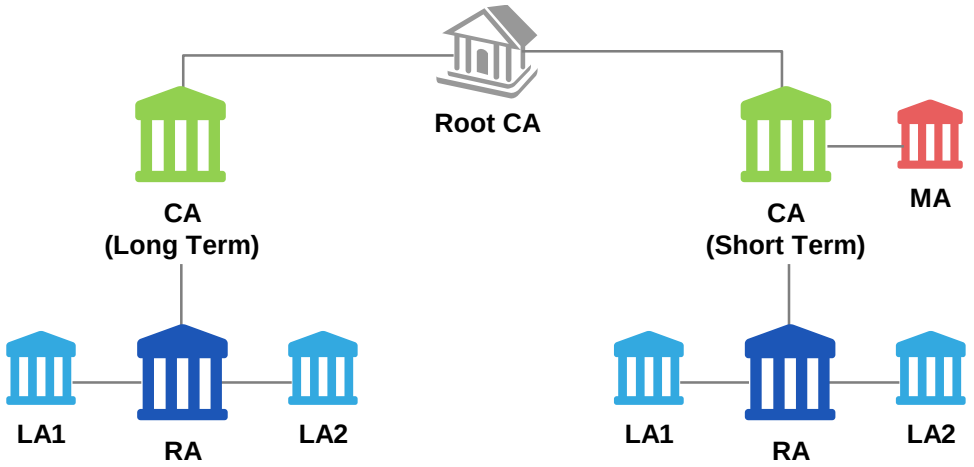
** CAMP VSC: Crash Avoidance Metrics Partnership - Vehicle Safety Communications

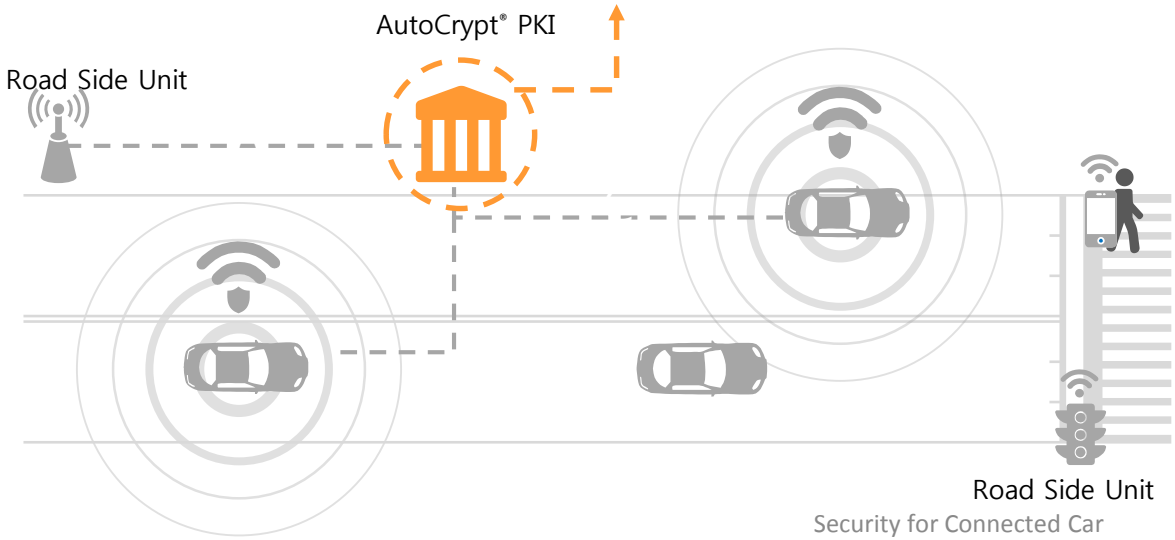
- *** Security Credential Management System



AutoCrypt® PKI

- **CA : Certificate Authority**
  - ✓ Generates PKI certificates necessary for V2X authentication
- **MA : Misbehavior Authority**
  - ✓ Monitors for certificate abuse or stolen certificates
- **RA(Registration Authority)**
  - ✓ Issues PKI certificates necessary
- **LA(Linkage Authority)**
  - ✓ Provides a anonymous ID for Pseudonym Certificates
  - ✓ Prevents exposure of driver privacy, e.g. location, etc.

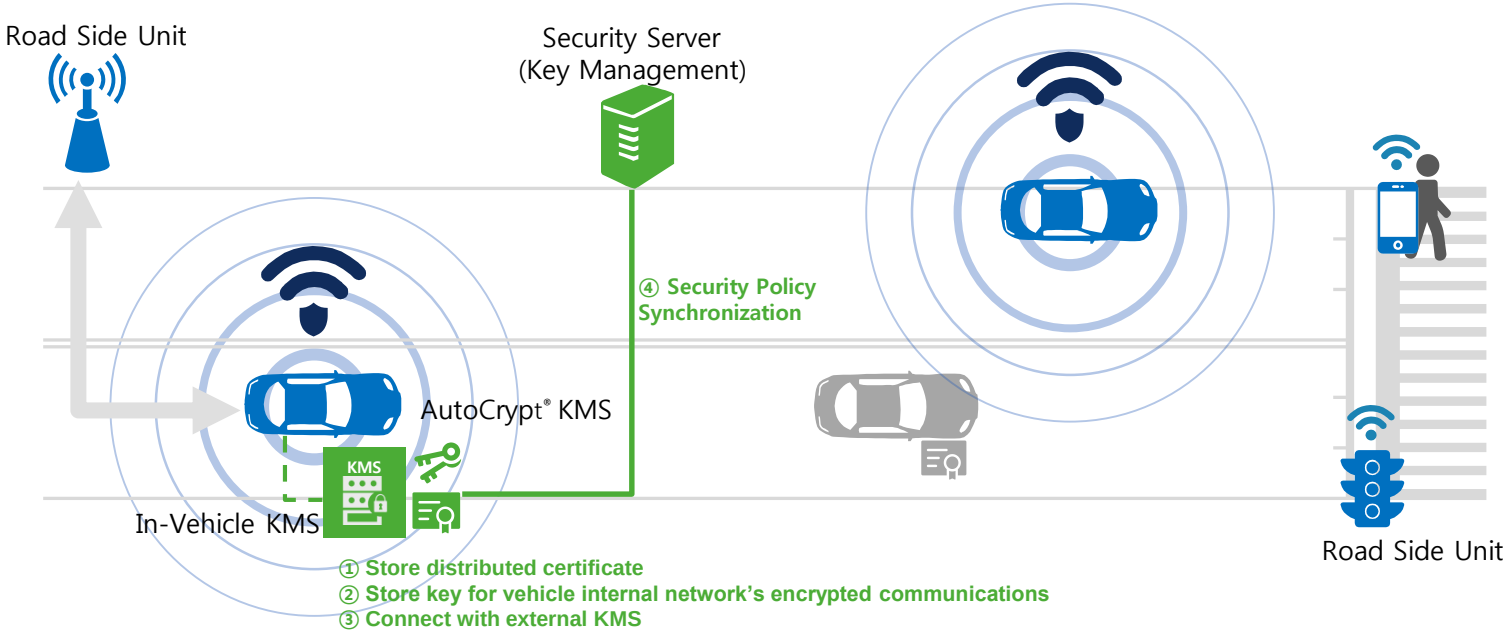




AutoCrypt® KMS

Encryption key and certificate cycle management

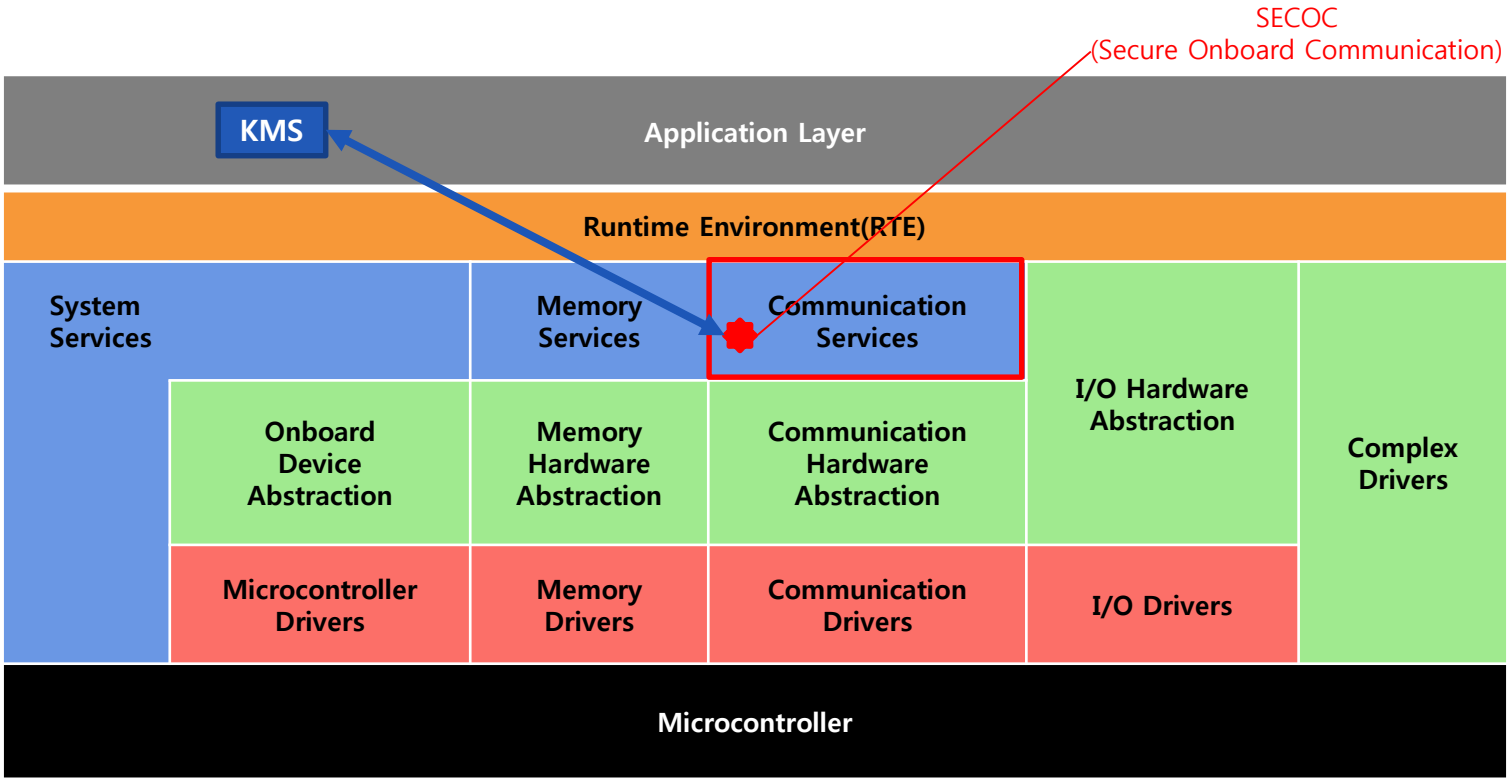
- Manages the entire in-vehicle encryption key life cycle process including generation and revocation
- Stores and manages keys from the moment issued from the security server
- The external KMS (Security Server) and the in-vehicle KMS continuously sync for constant security.



AutoCrypt® KMS

AUTOSAR Support (Tentative Launch: March 2017)

- Key Management Interface for the Communication Services aspect of AUTOSAR BSW (Basic Software)
  - Key management regarding specifically the SECOC (Secure Onboard Communication) section of Communication Services

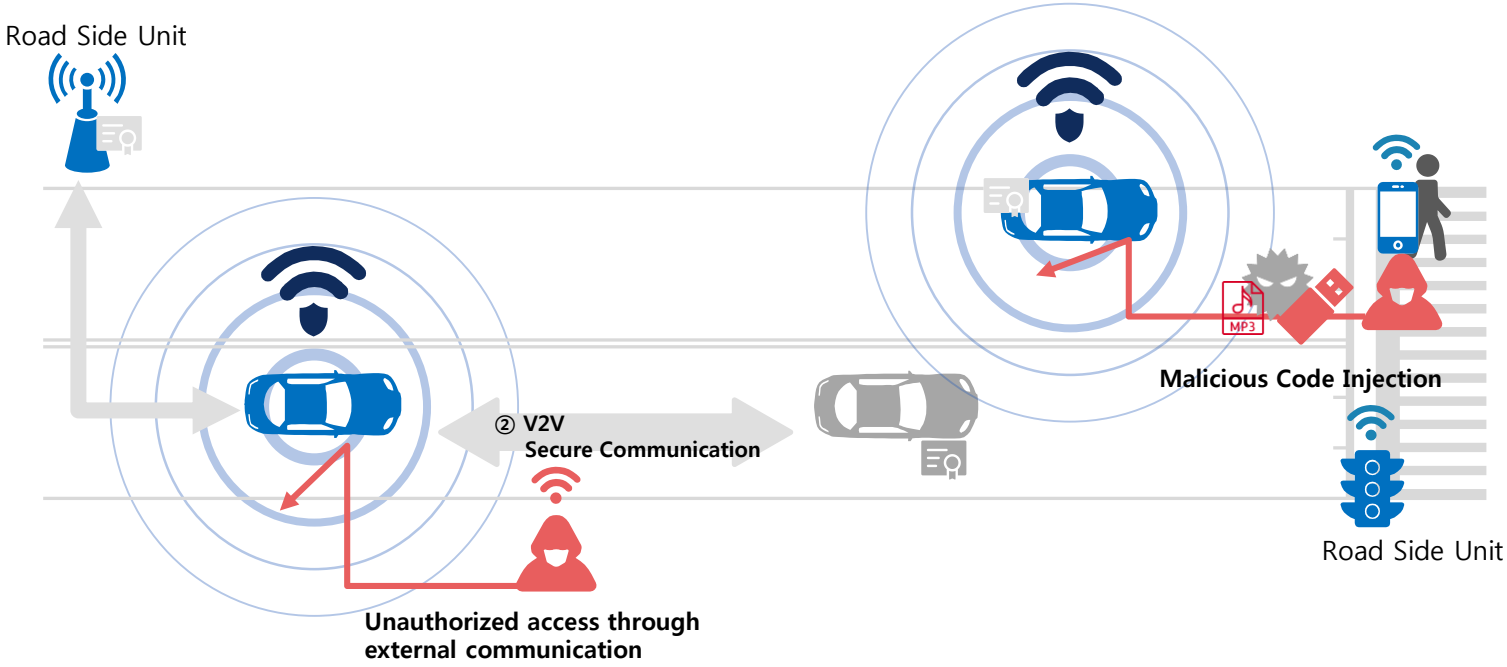


AUTOSAR Layered Software Architecture (www.autosar.org)

AutoCrypt® AFW (1/3)

AFW (Advanced Firewall) is an intelligent firewall that also features IDS/IPS capabilities. (1/2)

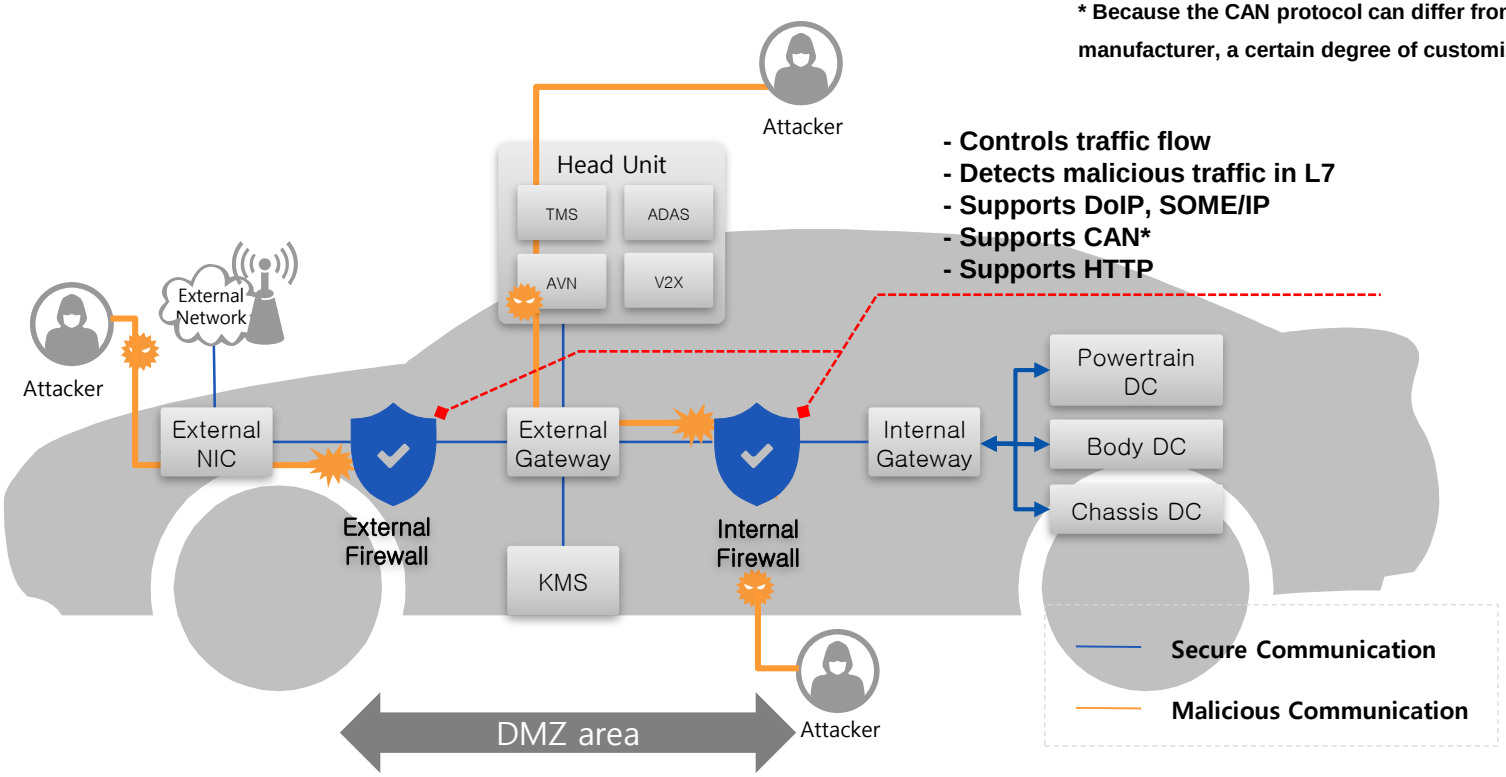
- Design Concept is based upon a Positive Security Model in which the user defines what is allowed and blocks all other traffic and access.
- The detection engine is based upon patented technology which does not rely on regular signature updates and utilizes a unique logic-based analysis to detect attacks.
- Detection support for protocols running at the Application Layer (L7) such as HTTP.



AFW (Advanced Firewall) is an intelligent firewall that also features IDS/IPS capabilities. (2/2)

- **Network Firewall & IDS/IPS**
  - Controls flow of traffic for both external and internal networks
  - Blacklisting to detect and block unauthorized access
  - Detects unusual behavior in traffic within internal network

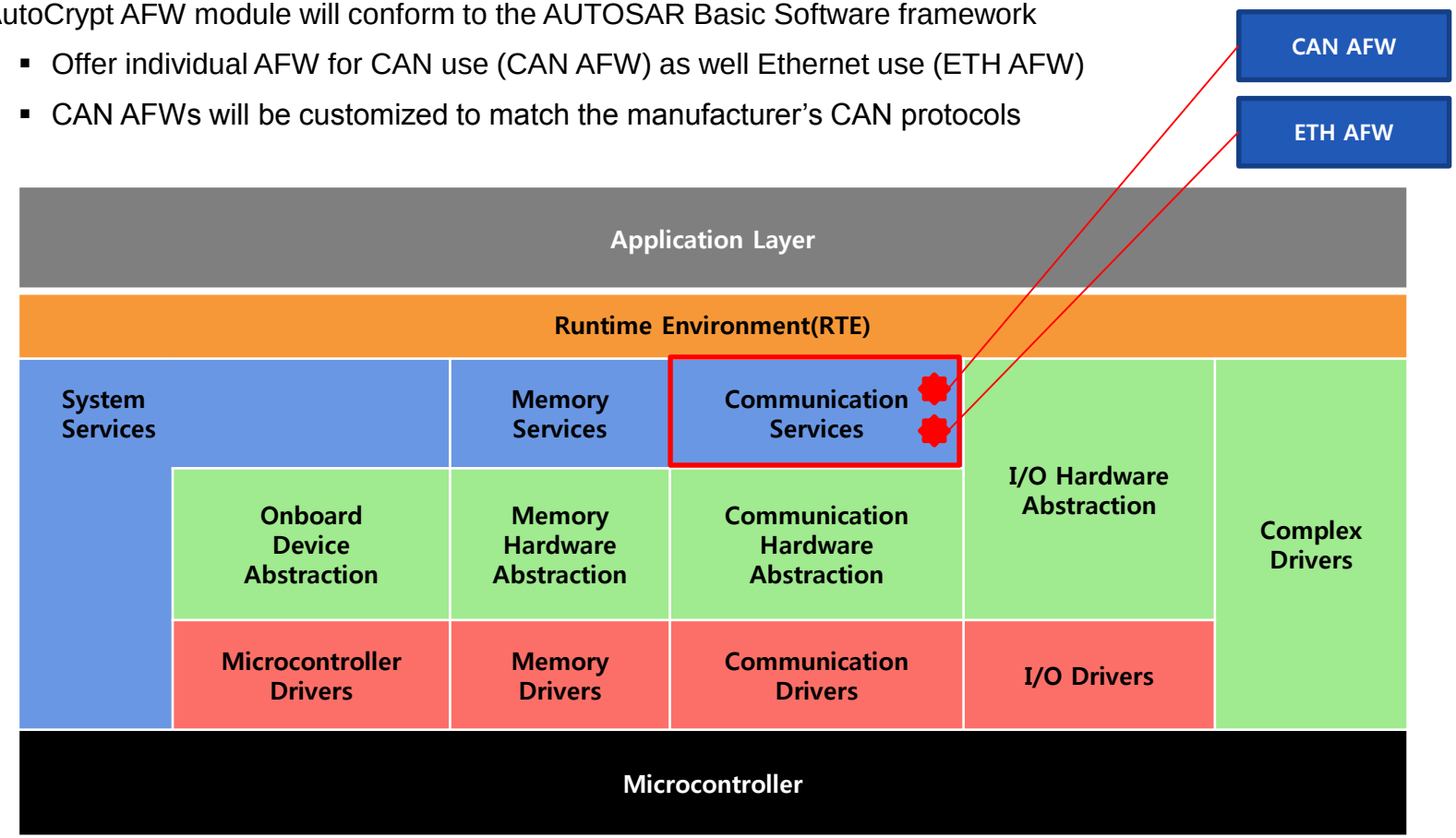
*** Because the CAN protocol can differ from manufacturer to manufacturer, a certain degree of customization is required.**



AutoCrypt® AFW (3/3)

AUTOSAR Support (Tentative Launch: March 2017)

- AutoCrypt AFW module will conform to the AUTOSAR Basic Software framework
  - Offer individual AFW for CAN use (CAN AFW) as well Ethernet use (ETH AFW)
  - CAN AFWs will be customized to match the manufacturer's CAN protocols



AUTOCRYPT

20 year Anniversary

Asian Cyber Security Vendor of the Year

thank you

Penta SECURITY

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