Automotive Security implementation for Secure Driving

STMicroelectronics

September 2017

life.augmented

Smart Driving

Smart Driving is about putting the driving experience of the car occupants as the focus point

ST is making driving safer, greener and more connected through a fusion of technology

safer

more connected

greener

ST is making Driving More Connected and More Secure

More Connected

What More Connected Driving Means

- Bringing our personalized entertainment and connected experience into the car environment in a secure and easy to use manner
- Allowing vehicles to communicate with each other (V2V) and to the Infrastructure (V2I)

More Connected Driving Technologies

processors (audio, telematics, V2X, security), tuners, sensors, amplifiers, wireless connectivity, secure elements

life.augmented

ST is making Driving More Connected and More Secure

More Secure

What More Secure Driving Means

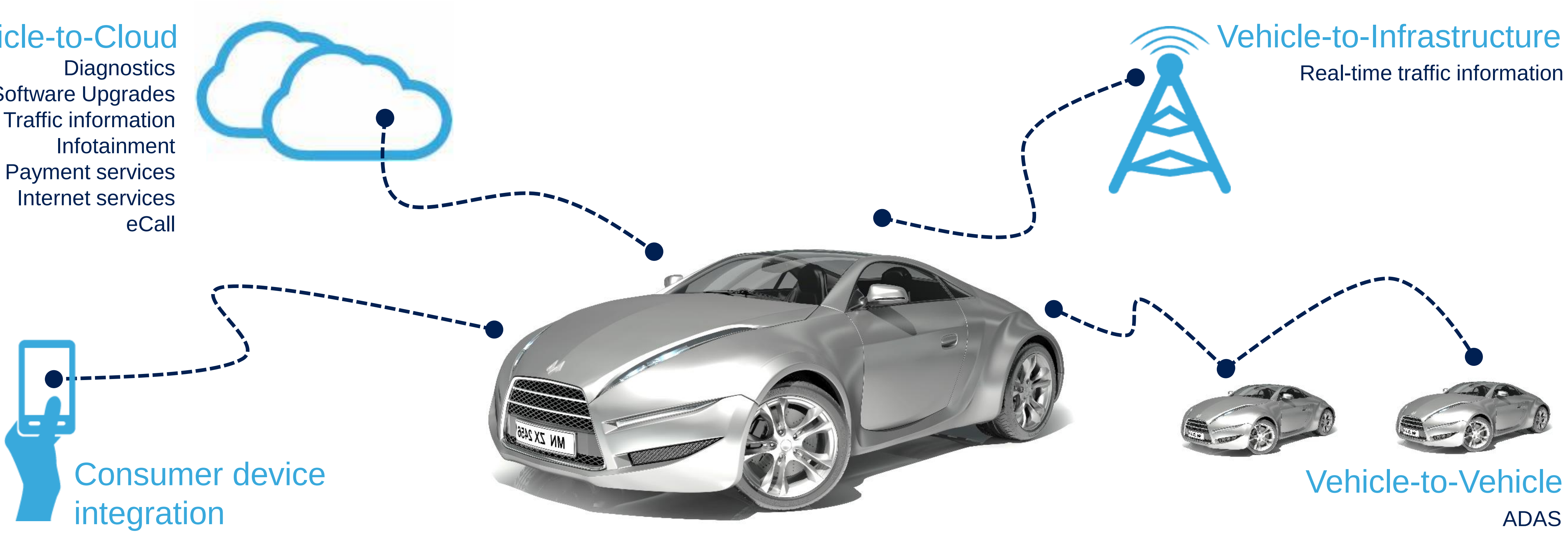
- Securing the Vehicle to Infrastructure communications
- Securing internal car networks
- Securing remote user interactions with the vehicle

More Secure Driving Technologies
Processors with eHSM (Gateway, Body), Secure Elements

life.augmented

Smart Driving Connected Services

Connected vehicles enable additional services



Vehicle-to-Cloud

Diagnostics
Software Upgrades
Traffic information
Infotainment
Payment services
Internet services
eCall

Vehicle-to-Infrastructure

Real-time traffic information

Consumer device integration

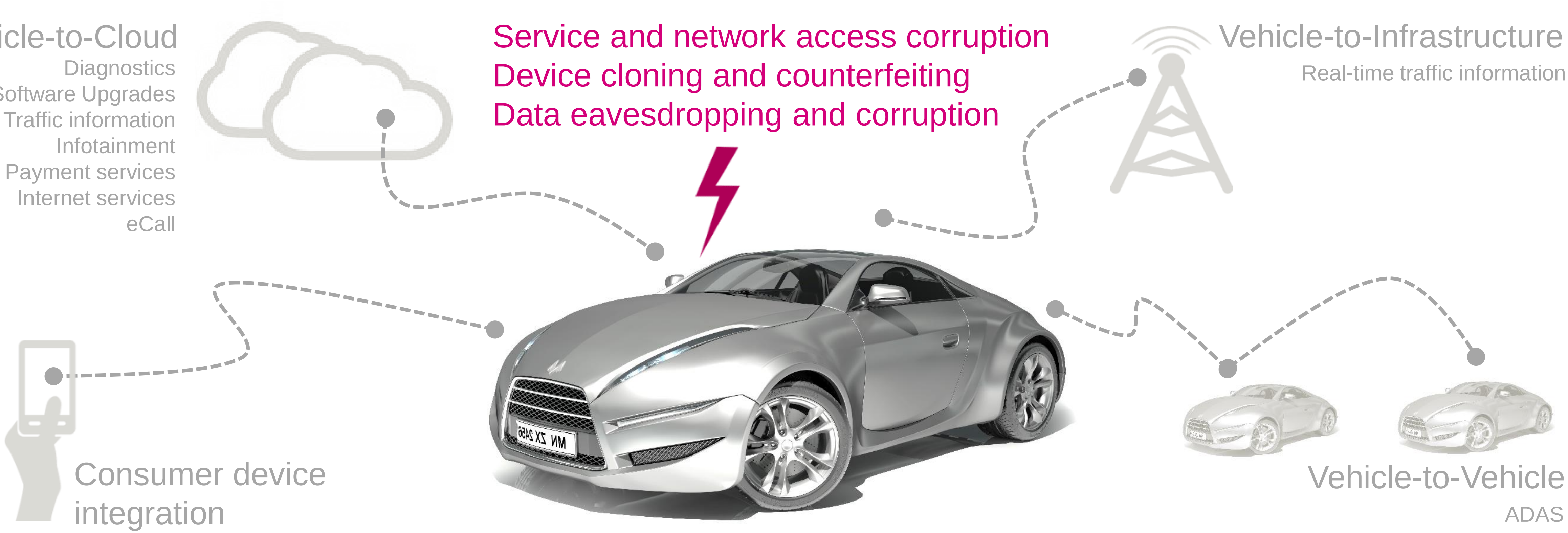
Smartphones
Tablets

Vehicle-to-Vehicle

ADAS

Smart Driving threats

Connected vehicles become more vulnerable to attacks



Vehicle-to-Cloud

Diagnostics
Software Upgrades
Traffic information
Infotainment
Payment services
Internet services
eCall

Service and network access corruption
Device cloning and counterfeiting
Data eavesdropping and corruption

Vehicle-to-Infrastructure

Real-time traffic information

Consumer device integration

Smartphones
Tablets

Vehicle-to-Vehicle

ADAS

Connectivity : Benefits and Risks

The benefits of the connected car are clear and so are the risks

- Increasing number of ECUs in vehicles combined with increased network capability (internal vehicle networks wired/wireless) creates more targets for compromising vehicle security

- Upgrading software to patch vulnerabilities

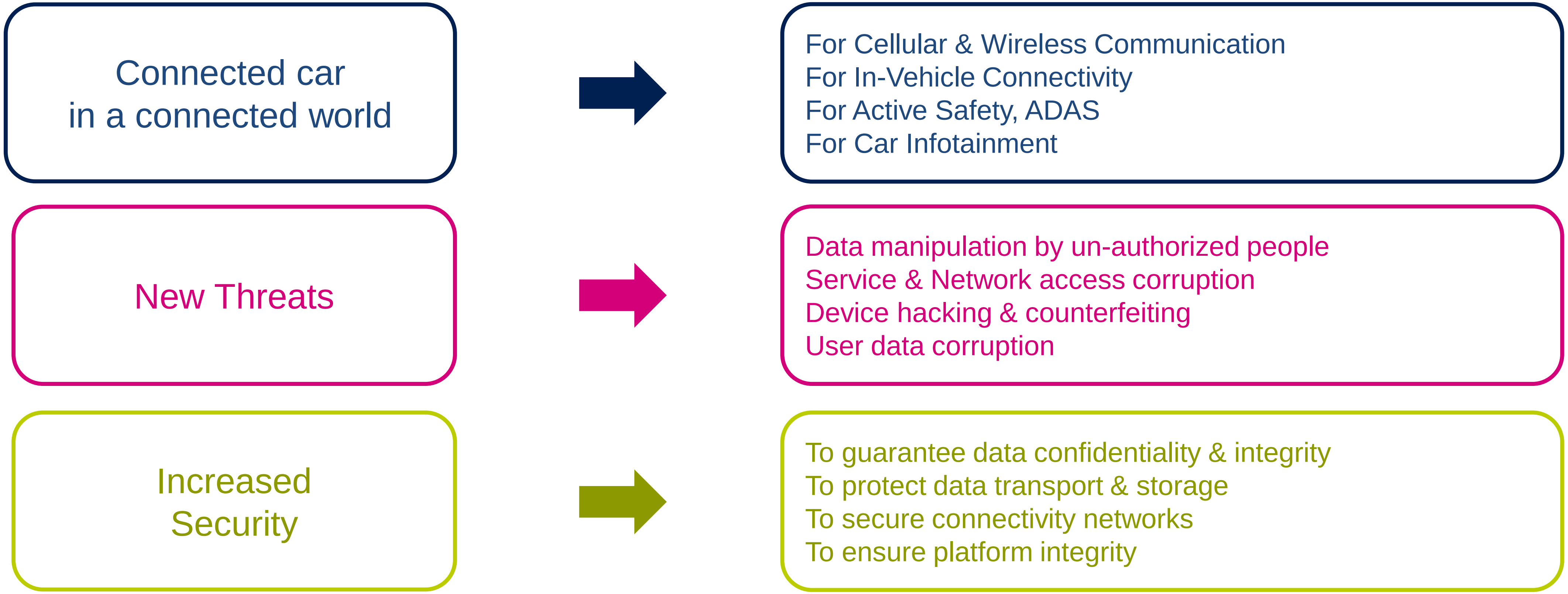
- High bandwidth in-vehicle networks and lower bandwidth V2X networks need to be secured from physical and remote attacks

100%

of Cars will be connected by 2025

Security is Not an Option

Connected cars need security



Connected car
in a connected world

For Cellular & Wireless Communication
For In-Vehicle Connectivity
For Active Safety, ADAS
For Car Infotainment

New Threats

Data manipulation by un-authorized people
Service & Network access corruption
Device hacking & counterfeiting
User data corruption

Increased
Security

To guarantee data confidentiality & integrity
To protect data transport & storage
To secure connectivity networks
To ensure platform integrity

life.augmented

Security objectives

Implementing security in connected vehicles ensures safety and privacy

Objectives

Passenger safety

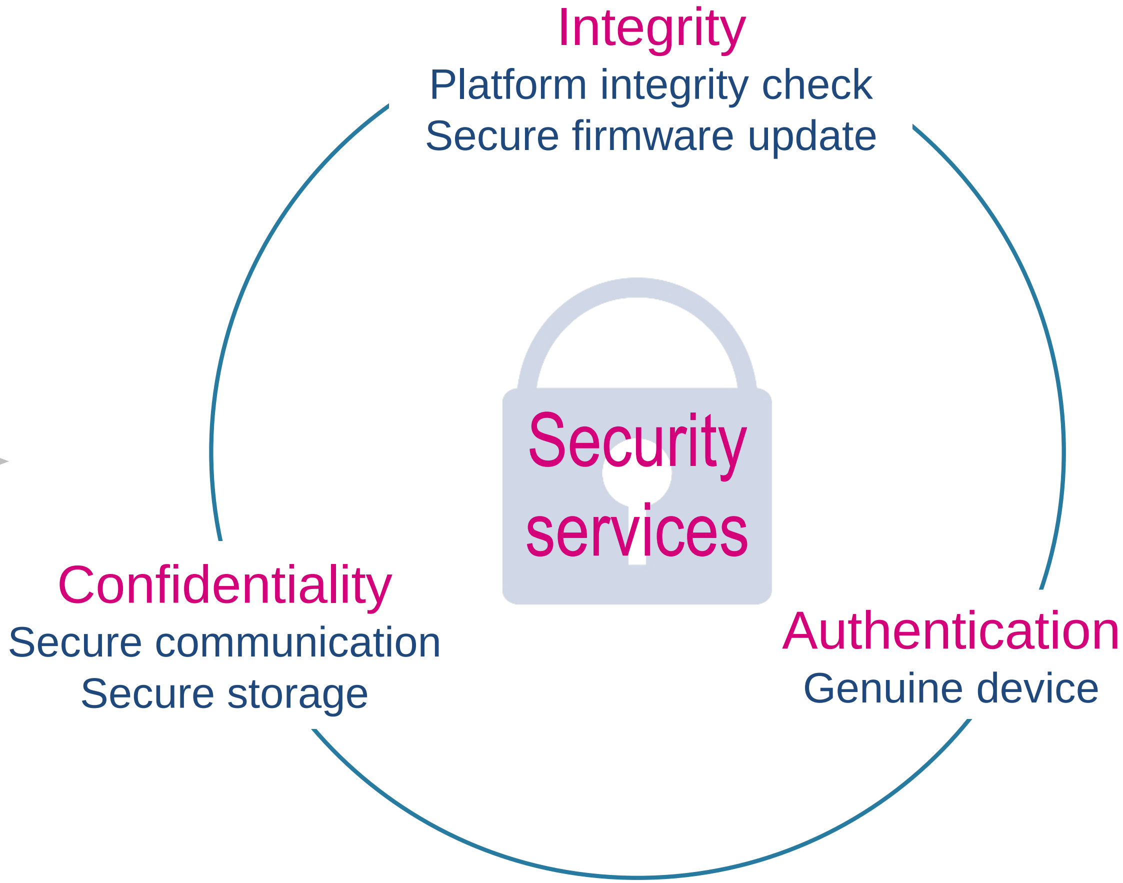
Guarantee vehicle behavior

(prevent device cloning, ensure device integrity)

Data privacy

Guarantee sensitive data and keys are not manipulated

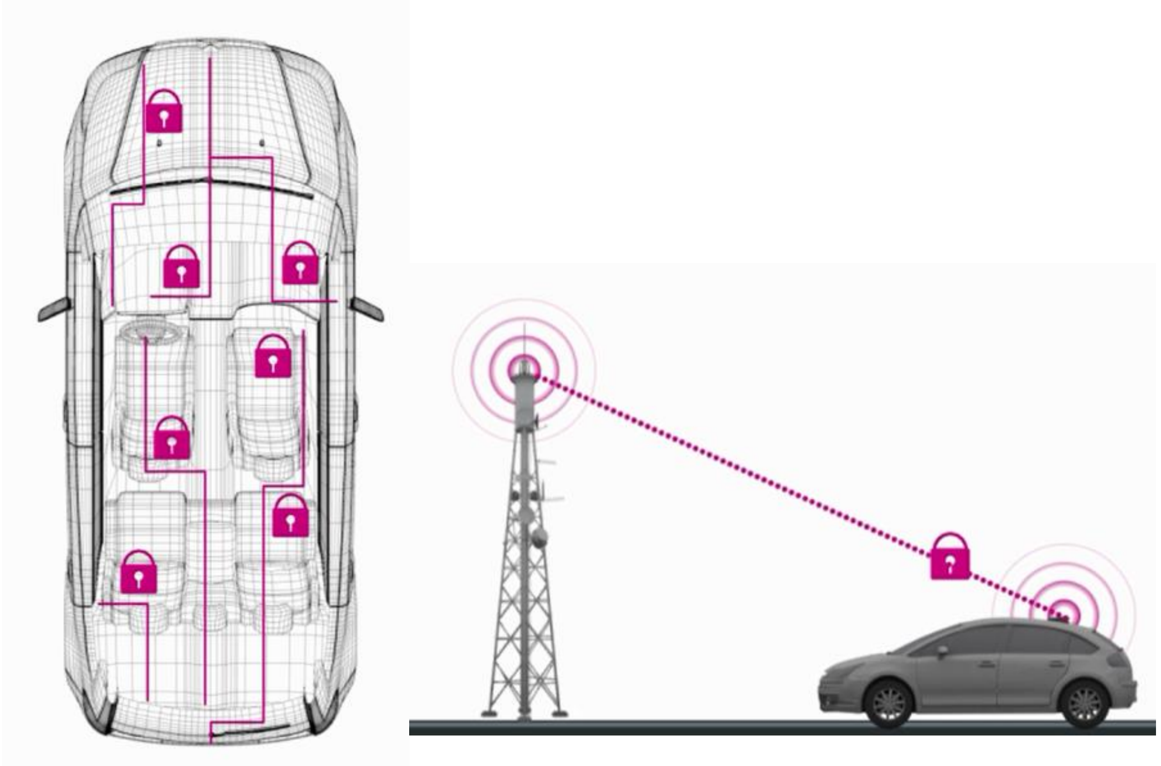
(prevent data corruption or eavesdropping)



ST : Uniquely Positioned

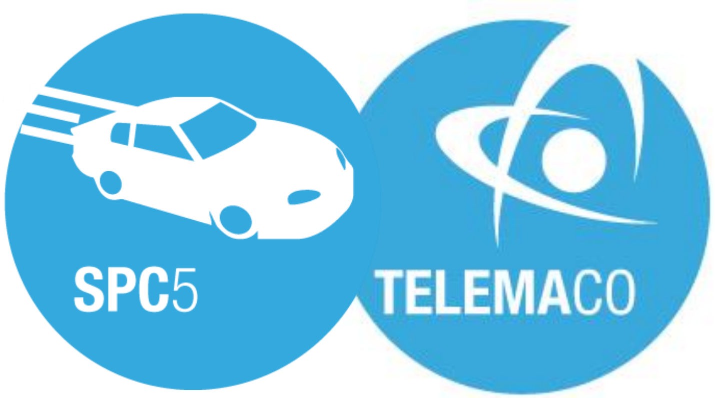
ST has a unique position – 30 years of Automotive and Secure MCUs experience

- End-to-end vehicle security depends on securing all the electronic networks and components
- This requires in depth security knowledge combined with a complete automotive offer
- ST has a unique position in having over 30 years of Automotive and Secure MCU experience, with an offer covering every vehicle component from body to infotainment to ADAS



ST is making Driving More Connected and More Secure

ST Offer



- Automotive MCUs with eHSM for Secure Gateway, Body, Powertrain, ADAS applications
- Dedicated Telematics Processors with eHSM
- Automotive Grade

- V2X Partnership
- Leading V2X technology
- Embedded Security
- Automotive Grade

- ST33 Secure Element
- Platform integrity and TPM
- Protection against physical and logical attacks
- Automotive Grade

Secure Vehicle Solutions

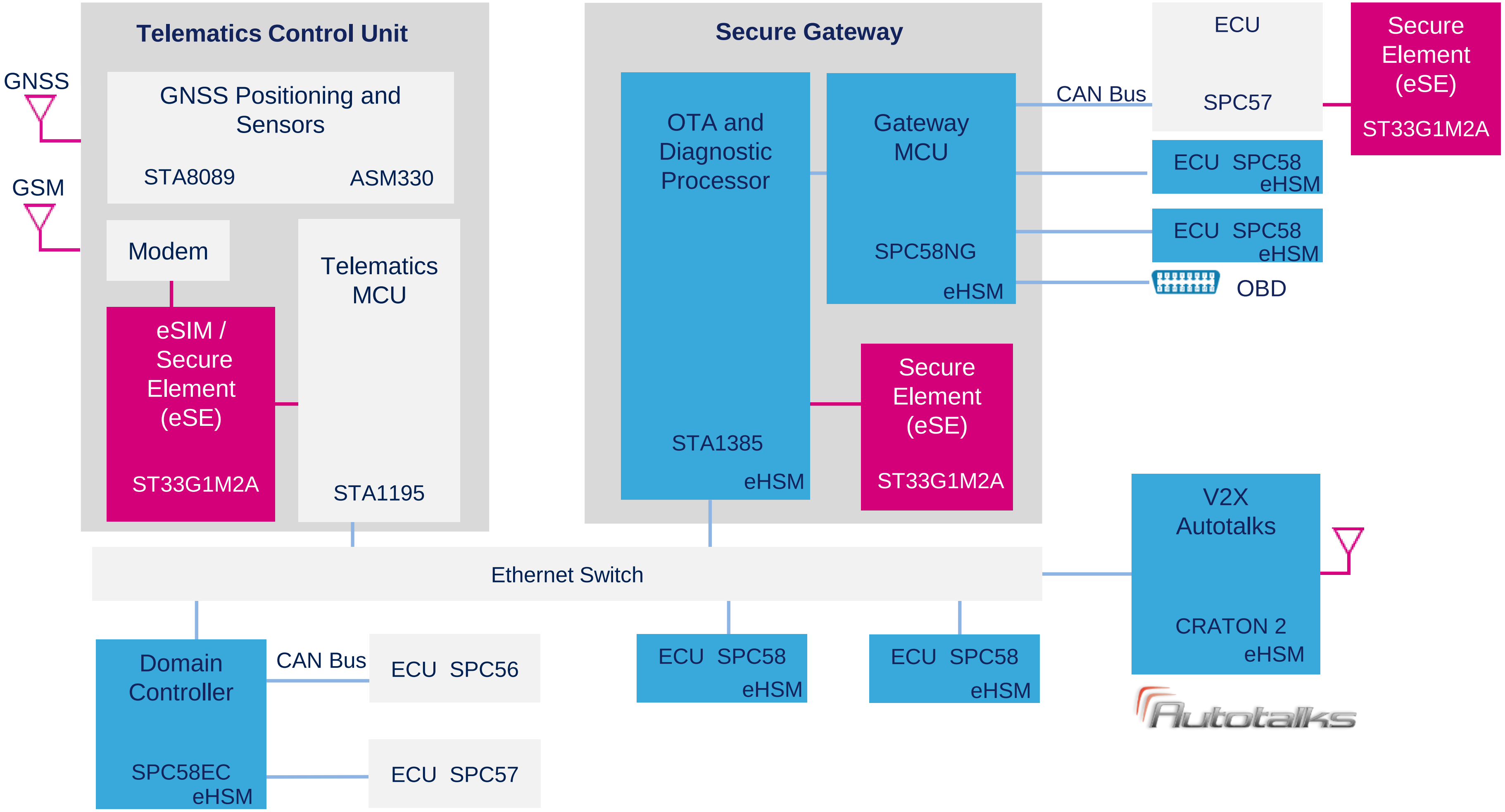
ST Global Security Offer

SPC5

Teseo

TELEMACO

Secure MCU



Telematics Control Unit

GNSS

GSM

GNSS Positioning and Sensors: STA8089, ASM330

Modem

eSIM / Secure Element (eSE): ST33G1M2A

Telematics MCU: STA1195

Secure Gateway

OTA and Diagnostic Processor: STA1385, eHSM

Gateway MCU: SPC58NG, eHSM

Secure Element (eSE): ST33G1M2A

CAN Bus

ECU: SPC57

Secure Element (eSE): ST33G1M2A

ECU SPC58 eHSM

ECU SPC58 eHSM

OBD

Ethernet Switch

V2X Autotalks: CRATON 2, eHSM

Autotalks

Domain Controller: SPC58EC, eHSM

CAN Bus

ECU SPC56

ECU SPC57

ECU SPC58 eHSM

ECU SPC58 eHSM

eHSM : embedded hardware security module

life.augmented

Global Secure Solutions for Automotive

ST key strengths to secure the connected cars

Multiple offers **from Hardware to Standardized SoC**

Unified and **scalable offer with SPC5x and TC3P** products from ST

Certified Highest **Security level Common Criteria EAL5+**

Full range of **hardware Automotive grade** products

SPC5
TELEMACO
Secure
MCU

life.augmented