Secure Automotive solutions
Ensuring security in all automotive connected services

- Vehicle to cloud
- Vehicle to Infrastructure
- Vehicle to Vehicle
- Vehicle access
Connected services threats

Connected vehicles become more vulnerable to attacks

Vehicle-to-Cloud
- Diagnostics
- Software Upgrades
- Traffic information
- Infotainment
- Payment services
- Internet services
- Emergency Call (eCall)

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

Vehicle-to-Infrastructure
- Real-time traffic information

Vehicle-to-Vehicle
- Advanced Driver Assistance System (ADAS)

Consumer device integration
- Smartphones
- Tablets

Life augmented
Implementing security in connected vehicles

Security 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)
Secure connectivity in telematics
- eCall
- Diagnostics
- Software upgrades (FOTA)
- Payment & internet services
- Real-time traffic information
- V2X

In-car security and integrity
- Gateways
- Authentication units & immobilizer
- DKS: Digital Key Devices
- Sensor integrity: camera, radars

eSE secure storage and services
- Secure boot
- EAL5+ secure storage of confidential data
- Cryptographic services
- EAL5+ Common Criteria

ST33-A secure element
CC EAL5+-certified eSE for Automotive applications
ST33-A secure element benefits

ST33-A, a proven and deployed solution for secure car

- **Proven**: More than 1Bu ST33 sold
- **Selected**: ST33-A adopted by Tier-One car makers
- **Quality**: 10ppm target without wear leveling
- **Certified**: Common Criteria EAL5+

**Certification**: ST33 secure MC2 sold.
End-to-end digital key system

ST is everywhere to ensure Secure NFC Car Access

In the digital key

ST54 combines an eSE and an NFC Controller in a Mobile Phone

ST31 eSE enables NFC-A card emulation and energy harvesting

In the door-handle

ST25R3920 Automotive NFC Reader detects and communicates with the key

Information is transmitted to STM8-A Automotive MCU

In the car

SPC58 Automotive MCU receives information from the door-handle

ST33-A Secure Element authenticates the user to enable car access
ST4SIM Overview

Cellular connectivity solutions

- **Wide range SIM/eSIM solutions based on Cryptographic and GSMA SGP.02 configurations**
- **GSMA eSIM certified and interoperable with MNOs & Subscription Management platform**
- **Complete ecosystem with trusted partners for connectivity & Subscription Management Platform**
- **Automotive grade solutions (T° & reliability)**
- **Multiple packages format (MFF2, TSSOP20)**
Secure connectivity solution

ST’s eSIM solution strengthens its positioning in Automotive market

Cellular Connectivity secure solution Leader
- SIM / eSIM for consumer or IoT devices (GP / GSMA-certified)
- Proven field quality with more than 1.5 billion ST33 family cards deployed

Strong reliability and security in Automotive markets
- Automotive-grade qualification AEC-Q100 grade 2 [-40°C / +105°C]
- Certified Common Criteria solutions EAL5+

State-of-the-art secure product
- State-of-the-art, secure and flexible embedded OS (including certified cryptographic algorithms)
- Java Card applet development (Extended OS features and added services)
- Standard involvement (GSMA / SIMalliance / Global Platform / 3GPP / ETSI / Car Connectivity Consortium)
Secure automotive takeaways

• Scalable ST security offers (from eHSM to certified secure element)

• Hardware and System-on-chip solution

• Complete cellular connectivity solution with trusted partners
Thank you