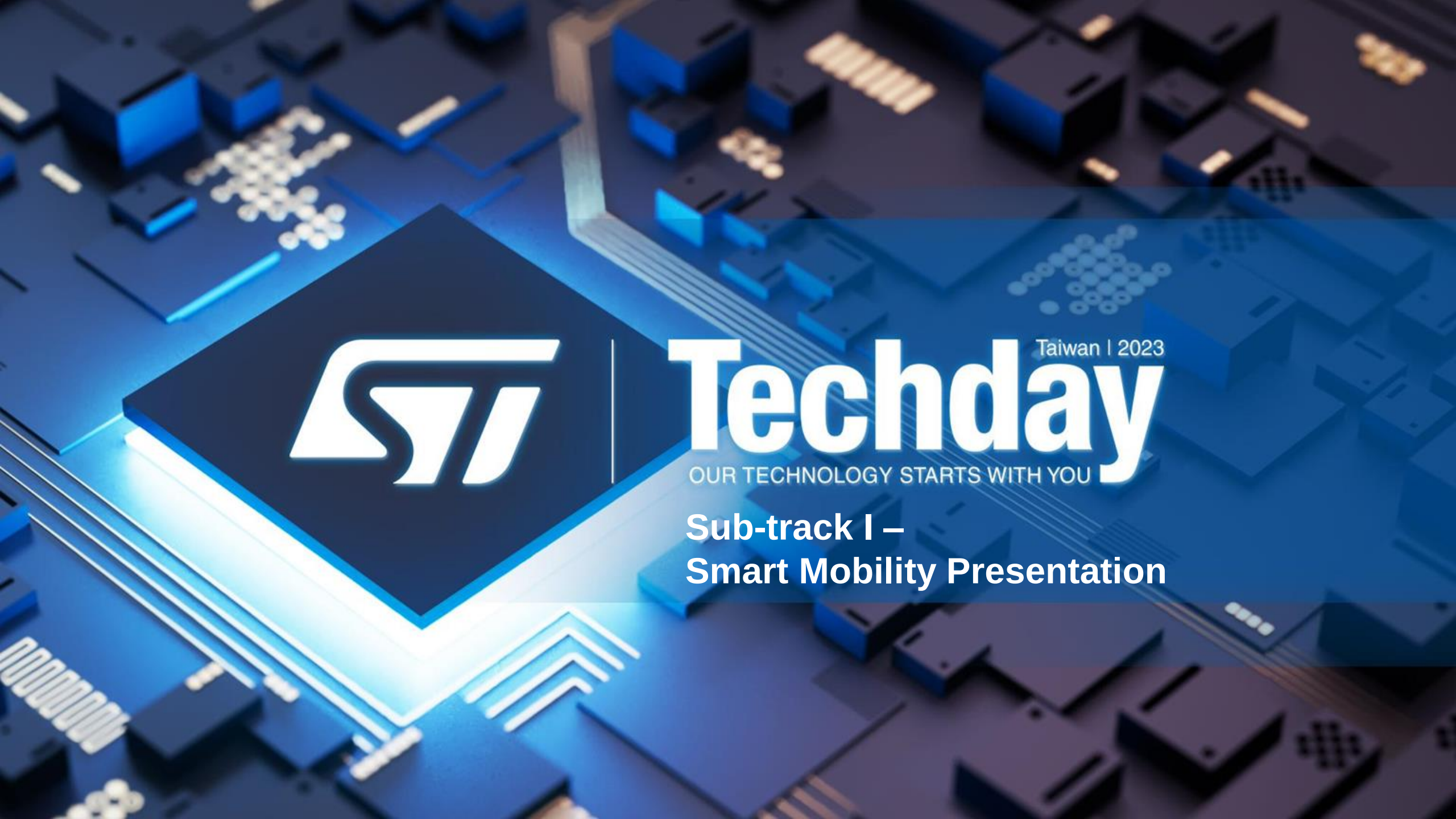


Sub-track I –
Smart Mobility Presentation

life.augmented

ST Automotive HW Secure Element for Digital Key

Marie Ando

STMicroelectronics

STSECURE

Trusted & connected cars overview

Challenges

- Compliancy Automotive-grade and highest level of security requirements
- Security vulnerability in all the supply chain
- Long term life cycle
- Large interaction range with lowest power

Major players

- IC vendors
- Tier-one integrators / Car Makers
- Device Makers

Market

- Growing automotive secure MCUs market (CAGR > 15% 2021-24)**
- Multiple applications
  - Digital Key System (DKS)
  - Electrical Vehicle (EV) Charging
  - Smart Audio / Infotainment
  - Wireless Qi Charging WPC 1.3
  - Secure Gateway
  - Open Java Card Open Platform for custom Applet
  - Autonomous Driving (ADAS)
  - Sensor & Camera Management
  - Accessory detection

Connected Security

- Complete STSAFE* Vehicle solutions
  - Scalable offer from hardware to system on chip solution
  - AEC-Q100 & CC EAL6+ certified
- 20+ years of in-house secure personalization
- STSAFE-V family from dedicated product to open solution
- Automotive HW selected by Major eSIM supplier
- Dedicated support team

WHY eSE ? – ST expertise
a complete set of hardware and software countermeasures

Software attack	Board-level attack	Silicon-level attack
• Network protocols weakness (weak ciphers, short keys, mitm*) • Flaws in software design / implementation, buffer overflows • Debug interfaces, gaining admin rights	• SPA / DPA Power analysis, emission analysis, timing analysis • Fault injection: glitches, laser, light, UV, X-rays • Memory probing	• Device delayering, circuit reverse engineering, micro-probing • Fault injection: Focused Ion Beam • Advanced microscopy

More expensive, More time consuming

• No external debug interface (Jtag) • Hardware cryptography fast computing • Enhanced security with physical isolation of security toolbox (secure key storage, secure & trusted execution in secure element)	• Randomization • Secured crypto-engines • Design Flow • Environment Sensors • Integrity checkers • Code Signature • Internal Clock Integrity • OS features (MPU) • Jittered Clocks • Data whitening	• Physical Shield • Glue Logic Layout • Bus & Memory Scrambling • Bus & Memory Encryption • Anti-reverse • Advanced Lithography

Hardware and software countermeasures

life.augmented

Securing assets & exchanges

Ensure
Confidentiality

Information is only made available to **authorized** entities

Information is **fully protected** from unauthorized requests

Ensure
Integrity

Data **accuracy & completeness** are maintained over the life cycle

Data **cannot be modified** in an unauthorized manner

Ensure
Availability

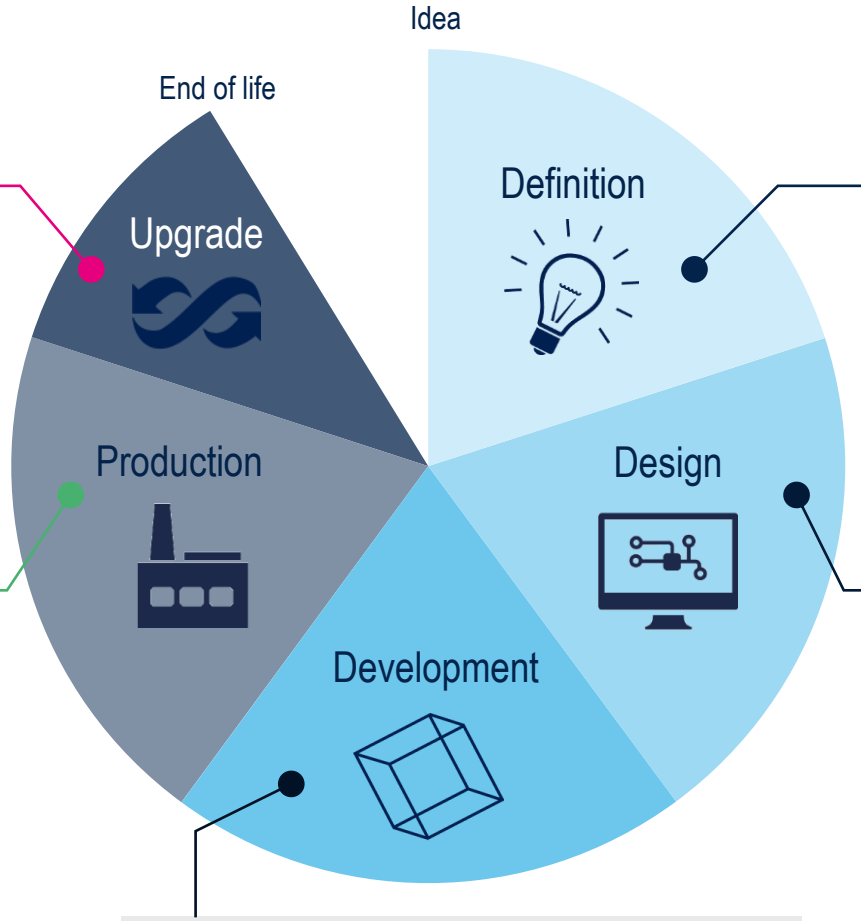
Information is made available to authorized requestors whenever needed

life.augmented

Supporting the security process security along the product life cycle

Secure firmware upgrade, secure end-to-end communication

Secure production environment, secure firmware installation, certifications



Support in defining the appropriate level of security

Leveraging on ST's security ecosystem and strong know-how

Selection of secure components & processes solving customer security needs

life.augmented

Connected security offers for various applications

Qi wireless charging

- Safe phone charging
- Trusted authentication
- NFC Cards protection
- WPC1.3 & 2.0 implementation

Digital Key System

- Secure car access
- In-vehicle SE
- CCC R2.0 & R3.1 implementation
- NFC door & console readers

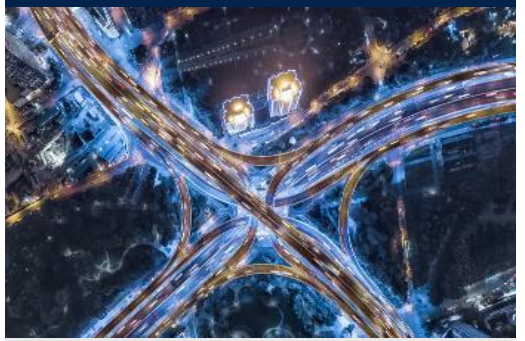
Electric vehicle charging

- EV Plug & Charge
- Trusted authentication
- ISO15118 implementation

Secure Infotainment

- Automotive OS
- Store passwords
- Verify applets

Secure gateway / Connectivity



- Secure boot
- Secure storage
- Authentication
- CC EAL6+ compliant
- eSIM

STSAFE-V System-on-chip (SoC)

ST33-A Hardware SE / eSIM

ST25 NFC reader

life.augmented

Connected security automotive solutions

ST33-A
Tamper-resistant hardware

- Hardware Secure MCU
- Set of software libraries
- AEC-Q100 & CC EAL6+ certified
- User guide support
- Secure Element & eSIM

STSAFE-V
SoC solution based on ST33-A

- Digital key access
- Strongbox SE
- Secure network connectivity
- Secure autonomous driving
- New services (Qi, EV charging)

ST25 NFC Reader
for convenience

- Digital key access
- NFC card protection for WPC
- NFC Forum compliant
- Supporting requirements of major phone OEM

life.augmented

Making driving smarter and safer

Passenger security

Data privacy

- Guarantee vehicle behavior
- Ensure secure car access
- Prevent device cloning
- Ensure secure connectivity
- Guarantee sensitive data remains confidential
- Prevent data corruption & eavesdropping

INTEGRITY

- Root of Trust
- Platform integrity
- Secure firmware update

CONFIDENTIALITY

- Secure communication
- Secure storage

AUTHENTICATION

- Genuine device

Prevent vulnerabilities in connect cars with in-vehicle secure elements

ST offers a full portfolio to secure your vehicle with secure solution

Secure Infotainment
In-vehicle infotainment & cockpit security
App security & password storage

Digital Key System
Secure car access

In-car services
Qi charging for smartphones, tablets

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

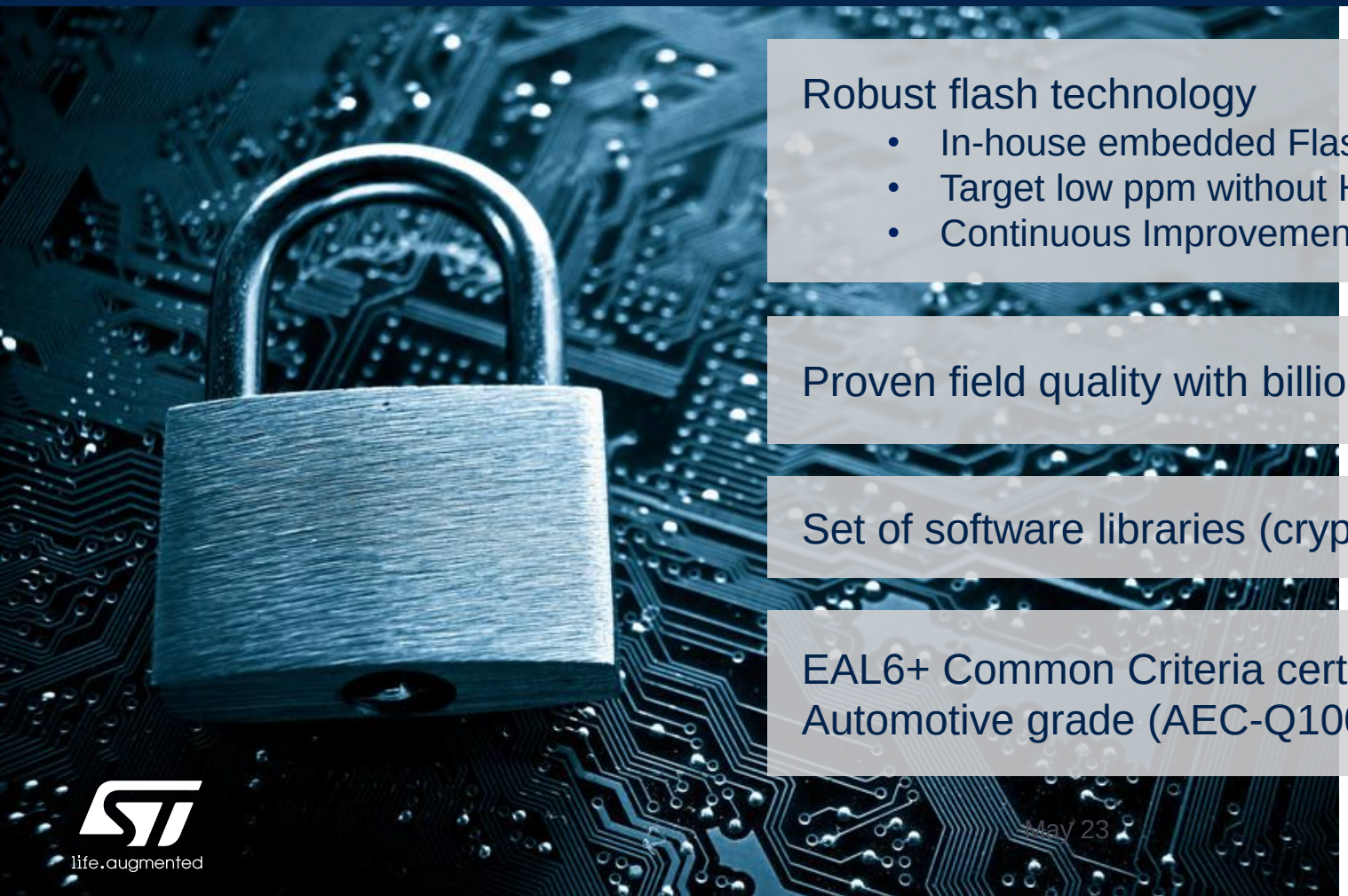
EV Charging
Secure plug & charge

Sensors
In-car data sensor privacy

In-car security
Secure Gateways
Software upgrade
V2X (PP EAL4+)

ST33-A hardware secure MCU overview

A certified secure element



Robust flash technology
- In-house embedded Flash 80 & 40nm
- Target low ppm without HW wear leveling
- Continuous Improvement Program (CIP) strategy

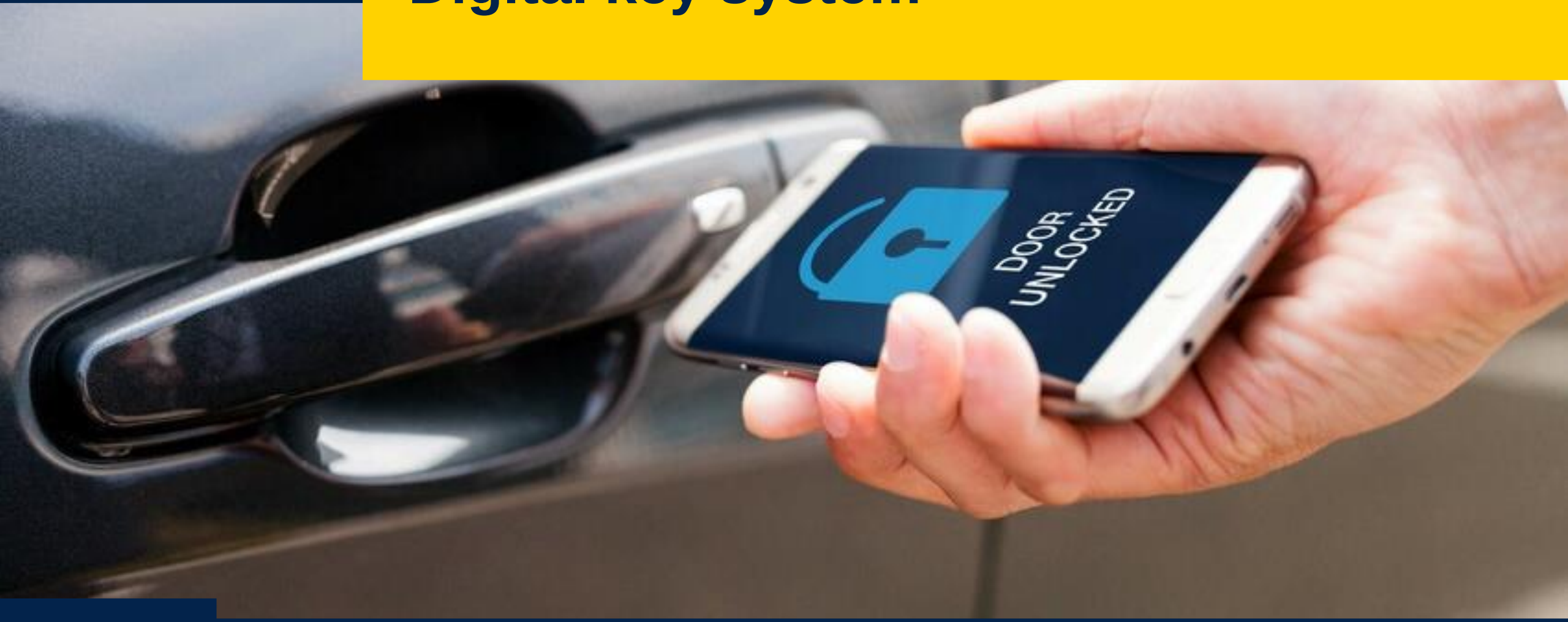
Proven field quality with billions of ST33 hardware secure MCU deployed

Set of software libraries (cryptography & flash management)

EAL6+ Common Criteria certified
Automotive grade (AEC-Q100 grade 2 and 0)

life.augmented

Digital key system



life.augmented

Digital key system CCC v3

A full ecosystem for an end-to-end digital key system

eSE required in vehicle, phone and cards

- CCC Digital Key is a standardized ecosystem that enables mobile devices on any operating system to securely store, authenticate and share Digital Keys for smart vehicles
- CCC v2 NFC based
- CCC v3 BLE/UWB based, NFC as mandatory backup

ST end-to-end digital key solution
ST is everywhere to ensure secure NFC car access

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

ST31 eSE enables NFC-A card
emulation and energy harvesting

In the digital key

ST25R3920B Automotive NFC Reader
detects and communicates with the key

Information is transmitted to
Automotive MCU

In the door-handle

SPC58 Automotive MCU receives
information from the door-handle

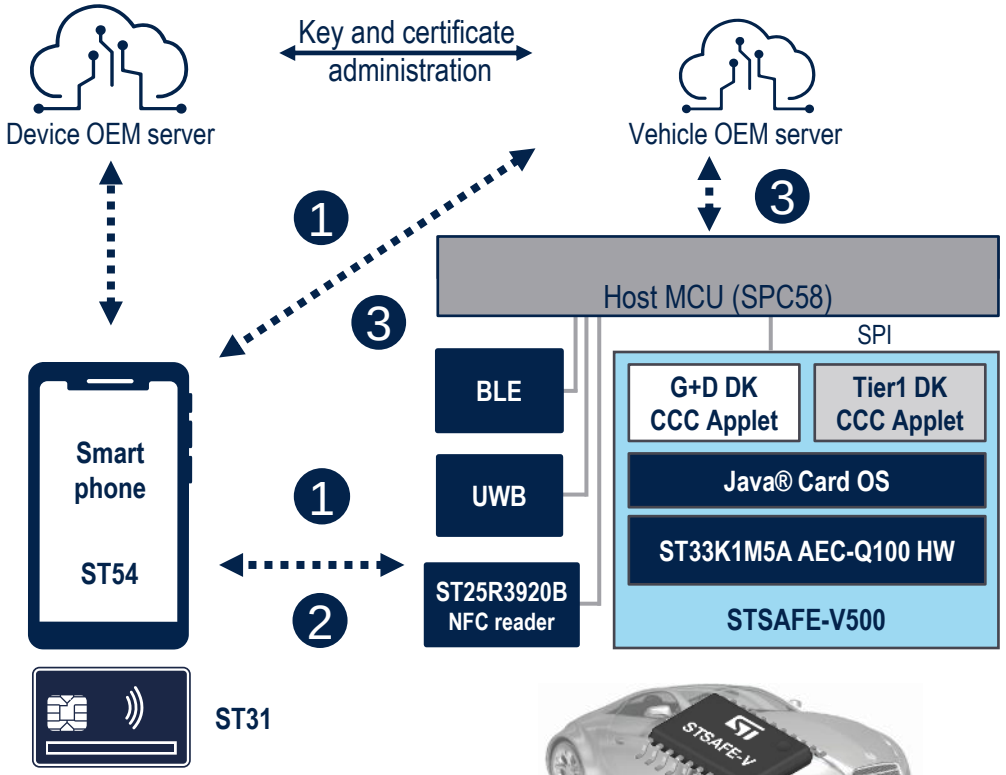
STSAFE-V500
Secure Solution authenticates the user

ST25R3920B communicates with the key
in the center console

In the car

life.augmented

STSAFE-V500 for digital key secure element in central console



1. Password management for 1st car access and owner pairing
2. Car access: Secure localization (UWB) + Digital Key check (BLE and NFC)
3. Management of owner Key sharing with family and friends

A discrete eSE in the console

- Java card-based SoC solution (v3.0.5 classic edition, GP 2.3)
- CCC v3.0 specification compliant
- Based on ST33-A Hardware / AEC-Q100 Grade 2, CC EAL6+ certified
- Password verifiers and digital key secure storage
- Owner pairing secure protocol / Mutual authentication car to phone
- Secure OTA SW update following SCP03 or SCP11.c protocol

A scalable offer

- STSAFE-VJ100-CCC : ST JCOS + ST Partner applet
- STSAFE-V500 : JCOS multi-application platform + customer DK applet

Integration at system level CCC v2 to v3

- CCC v2 validated based on ST33A, SPC58, ST25 NFC
- BLE and UWB integration, strategy under definition over 2023

SGP-TC-EVK (Smart Gateway Platform) evaluation kit

life.augmented

STSAFE-V500
Java® card open platform

Java card open platform supporting various and multiple use cases

- Support of Java® Card v3.0.5 classic edition
- Based on GlobalPlatform® specification (version 2.3.0)
- Secure OTA SW update following SCP03 or SCP11.c protocol
- Supports of Java ® Card-based applets integration
  - to store credentials and sensitive information
  - to execute cryptographic operations required for each use case
- Supports of all mandatory features for automotive application such as:
  - Digital Key (discrete eSE in the console)
    - Strongbox application (Google specification)
    - Qi charging application (WPC1.3/2.0)

life.augmented

Our technology starts with You

Find out more at www.st.com/secure-auto

life.augmented