ST Automotive HW Secure Element for Digital Key

Marie Ando
STMicroelectronics
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

**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

---

*is a registered and/or unregistered trademark of STMicroelectronics International NV or its affiliates in the EU and/or elsewhere
### WHY eSE? – ST expertise

**a complete set of hardware and software countermeasures**

<table>
<thead>
<tr>
<th>Software attack</th>
<th>Board-level attack</th>
<th>Silicon-level attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Network protocols weakness (weak ciphers, short keys, mitm*)</td>
<td>• SPA / DPA Power analysis, emission analysis, timing analysis</td>
<td>• Device delayering, circuit reverse engineering, micro-probing</td>
</tr>
<tr>
<td>• Flaws in software design / implementation, buffer overflows</td>
<td>• Fault injection: glitches, laser, light, UV, X-rays</td>
<td>• Fault injection: Focused Ion Beam</td>
</tr>
<tr>
<td>• Debug interfaces, gaining admin rights</td>
<td>• Memory probing</td>
<td>• Advanced microscopy</td>
</tr>
<tr>
<td>More expensive, More time consuming</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• No external debug interface (Jtag)</td>
<td>• Randomization</td>
<td>• Physical Shield</td>
</tr>
<tr>
<td>• Hardware cryptography fast computing</td>
<td>• Secured crypto-engines</td>
<td>• Glue Logic Layout</td>
</tr>
<tr>
<td>• Enhanced security with physical isolation of security toolbox (secure key storage, secure &amp; trusted execution in secure element)</td>
<td>• Design Flow</td>
<td>• Bus &amp; Memory Scrambling</td>
</tr>
<tr>
<td></td>
<td>• Environment Sensors</td>
<td>• Bus &amp; Memory Encryption</td>
</tr>
<tr>
<td></td>
<td>• Integrity checkers</td>
<td>• Anti-reverse</td>
</tr>
<tr>
<td></td>
<td>• Code Signature</td>
<td>• Advanced Lithography</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Hardware and software countermeasures

- 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
Information is only made available to **authorized** entities.
Information is **fully protected** from unauthorized requests.

**Ensure Confidentiality**

Data **accuracy & completeness** are maintained over the life cycle.
Data **cannot be modified** in an unauthorized manner.

**Ensure Integrity**

Information is made available to authorized requestors whenever needed.

**Ensure Availability**
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
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)**

**ST25 NFC reader**

**ST33-A Hardware SE / eSIM**
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
Making driving smarter and safer

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

**Data privacy**

**INTEGRITY**
- Root of Trust
- Platform integrity
- Secure firmware update

**CONFIDENTIALITY**
- Secure communication
- Secure storage

**AUTHENTICATION**
- Genuine device
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+)

Prevent vulnerabilities in connect cars with in-vehicle secure elements

May 23
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)
Digital key system
Digital key system CCC v3

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

- 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

eSE required in vehicle, phone and cards
ST end-to-end digital key solution
ST is everywhere to ensure secure NFC car access

**In the digital key**

<table>
<thead>
<tr>
<th>ST54</th>
<th>ST31</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST54 combines an eSE and an NFC Controller in a Mobile Phone</td>
<td>ST31 eSE enables NFC-A card emulation and energy harvesting</td>
</tr>
</tbody>
</table>

**In the door-handle**

<table>
<thead>
<tr>
<th>ST25R3920B</th>
<th>STM8</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST25R3920B Automotive NFC Reader detects and communicates with the key</td>
<td>Information is transmitted to Automotive MCU</td>
</tr>
</tbody>
</table>

**In the car**

<table>
<thead>
<tr>
<th>SPC58</th>
<th>STSAFE-V500</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPC58 Automotive MCU receives information from the door-handle</td>
<td>STSAFE-V500 Secure Solution authenticates the user</td>
</tr>
<tr>
<td>ST25R3920B communicates with the key in the center console</td>
<td></td>
</tr>
</tbody>
</table>
STSAFE-V500 for digital key secure element in central console

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

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

Device OEM server
ST54
ST31
ST33K1M5A AEC-Q100 HW
Java® Card OS
STSAFE-V500
1
2
3
BLE
UWB
ST25R3920B NFC reader
Host MCU (SPC58)
G+D DK CCC Applet
Tier1 DK CCC Applet
Java® Card OS
ST33K1M5A AEC-Q100 HW
STSAFE-V500
SPI

Vehicle OEM server

STSAFE-V500 for digital key secure element in central console

SGP-TC-EVK (Smart Gateway Platform) evaluation kit
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)
Our technology starts with You

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