Secure Solutions
Ensuring your peace of mind
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST at a glance</td>
<td>3</td>
</tr>
<tr>
<td>Where to find us</td>
<td>4</td>
</tr>
<tr>
<td>Secure application solutions</td>
<td>5</td>
</tr>
<tr>
<td>ST’s secure microcontrollers</td>
<td>6</td>
</tr>
<tr>
<td>Value chain</td>
<td>7</td>
</tr>
<tr>
<td>Technology</td>
<td>8</td>
</tr>
<tr>
<td>Contactless and NFC</td>
<td>8</td>
</tr>
<tr>
<td>ARM® core</td>
<td>8</td>
</tr>
<tr>
<td>Flash technology</td>
<td>8</td>
</tr>
<tr>
<td>Security &amp; certifications</td>
<td>9</td>
</tr>
<tr>
<td>Banking &amp; ID</td>
<td>12</td>
</tr>
<tr>
<td>Banking &amp; ID Solutions Offers</td>
<td>12</td>
</tr>
<tr>
<td>Secure Wearables</td>
<td>13</td>
</tr>
<tr>
<td>BoostedNFC™ opens new ways to pay</td>
<td>13</td>
</tr>
<tr>
<td>Mobile Security Consumer</td>
<td>14</td>
</tr>
<tr>
<td>ST’s solutions to build the most effective and secure mobile applications</td>
<td>14</td>
</tr>
<tr>
<td>Standalone solutions</td>
<td>15</td>
</tr>
<tr>
<td>Mobile security eSIM/NFC convergence integrated solutions</td>
<td>15</td>
</tr>
<tr>
<td>Authentication in IoT</td>
<td>16</td>
</tr>
<tr>
<td>IoT markets &amp; applications</td>
<td>16</td>
</tr>
<tr>
<td>STSAFE™ family, a scalable security offer</td>
<td>16</td>
</tr>
<tr>
<td>M2M Industrial &amp; IoT</td>
<td>18</td>
</tr>
<tr>
<td>Flexible cellular connectivity solution</td>
<td>18</td>
</tr>
<tr>
<td>Reliability and high-quality</td>
<td>18</td>
</tr>
<tr>
<td>Secure Automotive</td>
<td>19</td>
</tr>
<tr>
<td>Embedded secure solutions for connected cars</td>
<td>19</td>
</tr>
</tbody>
</table>
ST at a glance

ST is a global semiconductor leader delivering intelligent and energy-efficient products and solutions that power the electronics at the heart of everyday life. ST’s products are found everywhere today, and together with our customers, we are enabling smarter driving and smarter factories, cities and homes, along with the next generation of mobile and Internet of Things devices. By getting more from technology to get more from life, ST stands for life.augmented.

In 2018, the Company’s net revenues were $9.66 billion, serving more than 100,000 customers worldwide. Further information can be found at www.st.com.

- A global semiconductor leader
- The largest European semiconductor company
- 2018 net revenues of US$ 9.66B

- Approximately 46,000 employees worldwide
- 11 manufacturing sites

- Over 80 sales & marketing offices
- Listed on New York Stock Exchange, Euronext Paris and Borsa Italiana, Milano
Where to find us

Making driving safer, greener and more connected

Making homes & cities smarter, for better living, higher security, and to get more from available resources

Making everyday things smarter, connected and more aware of their surroundings

Enabling the evolution of industry towards smarter, safer and more efficient factories and workplaces

Smart Driving

Internet of Things
The market for secure applications based on «smartcard» technology has covered mainly banking, ID, SIM, transportation, and pay TV applications since 1995. The growing demand for strong security in consumer goods and the market’s evolution has enlarged the application scope by providing secure solutions such as public key infrastructure (PKI) for enterprises, Trusted Platform Module (TPM) as well as brand protection, anti-piracy, and anti-fraud mechanisms. Today, it is the ubiquitous use of mobile phones and wireless technology that mainly drives the evolution of this market with the embedded secure elements, eSIM and NFC devices as well as contactless cards. The connected world of the Internet of Things will influence the evolution of this technology by using securely-connected devices in smart grid, smart home, smart city, autonomous car and smart world applications.
ST’s secure microcontrollers and turnkey security solutions ensure your peace of mind by protecting your privacy in the fast growing connected digital world. From traditional smartcard applications such as SIM, banking or ID to the latest ones such as secure mobile transactions or Internet of Things, ST is able to deliver the right solution. ST’s secure MCUs are certified as per the latest security standards (Common Criteria, EMVCo and CUP) and cover a complete range of interfaces for both contact and contactless communication, including ISO/IEC 7816, ISO/IEC 14443 Type A & B, NFC, USB, SPI and I²C. By offering a complete solution ranging from a secure operating system embedded in the secure MCU, to full enablement and personalization services, ST offers seamless integration of security features to customers who might not be experts in secure systems.

ST’s secure microcontroller division portfolio focuses on several main vectors.

- Banking & ID solutions for traditional smartcard businesses such as payment, people identification, transport, and pay TV
- Secure Wearables covering secure transactions in handheld devices and wearables
- Mobile Security for consumer applications addressing SIM/eSIM solutions for cellular connectivity in mobile, wearable as well as secure solutions for near field communication (NFC & eSE)
- Authentication covering brand protection, TPMs and strong authentication solutions for IoT networks
- M2M Industrial addressing eSIM secure connectivity in IoT, industrial and networks infrastructures
- Secure Automotive enabling security in telematics (eSIM/eSE) and gateways (eSE)
Value chain

MAIN ACTIVITIES IN OUR VALUE CHAIN

Suppliers
We purchase silicon lingot, raw materials, equipment, energy, gas, chemicals and services from many suppliers and subcontractors.

R&D concept and design
New products are created in a multi-step process including architecture conception, electrical layout, electrical and logic simulation, chip layout and generation of the mask that will be used to etch the design in silicon.

Manufacturing front end (FE)
Manufacturing chips requires around 400 separate stages starting with a plain silicon wafer and resulting in the etching of several hundreds to thousands of dice.

Electrical wafer sorting, secure keys & data loading
Dice on a silicon wafer are electrically tested in step known as wafer sort or probe. Secure MCUs require embedded software, keys and data to be pre-loaded in a secure environment using a hardware security module (HSM).

Assembly line and final back end (BE)
Dice are cut from the silicon wafer before being assembled in a package. These chips are then tested prior to delivery.

Secure pre-personalization
Secure MCUs include customer keys and data that must be loaded in a secure environment.

Sustainable technology
ST works to improve our social and environmental footprint at every stage of the product life, from raw material extraction to end of life.

OUR CERTIFICATIONS

ST adheres to the Responsible Business Alliance (RBA) Code of Conduct in our supply chain and requires ISO and OHSAS certifications to address ethics, social, environmental, health and safety risks. We participate in the Responsible Minerals Initiative (RMI).

We design, manufacture and pre-personalize products to ensure their compliance with quality, environment, safety, and security standards and certifications:
• Continuity management systems
• ISO/TS 16949 quality management systems
• MasterCard Card Quality Management (CQM) certification
• ISO 50001 and ISO 14064 environmental management standards
• Common Criteria EAL5+/EAL6+ and FIPS 140-2 security evaluation
• ISO/IEC 15408 computer security certification
• OHSAS occupational health and safety management systems
• Business Continuity Management
• ISO 22301 business continuity standards
• GSMA SAS-UP eUICC personalization site certification
CONTACTLESS AND NFC
ST31 dual-interface secure microcontrollers are designed to enable secure and fast contactless transactions for banking, ID and transport applications. For NFC-based solutions in mobile devices or wearables, ST provides a complete portfolio from the ST21NFC NFC controller family to the ST53 / ST54 system-in-package platforms combining an ST31 or ST33 secure element with an STS392x booster or ST21NFC NFC controller embedding boostedNFC™ technology based on Active Load Modulation.

Multi-protocol
ST31 secure MCUs support various multi-protocol RF interfaces enhancing multi-application versatility. ISO/IEC 14443 Type A and B, NFC and ISO/IEC 18092 protocols are all available and Auto-detect mode allows automatic detection and dynamic adaptation of the device to the correct reader protocol. ST21NFC and ST54 families are able to cover all NFC modes (Reader/Writer, Card Emulation and Peer-to-Peer) to address all possible NFC use cases.

MIFARE®
To support multi-application solutions including MIFARE® applications, optional secure MIFARE® libraries (MIFARE Plus® and MIFARE® DESFire® EV1/EV2 libraries) are available on ST platforms.

ARM® CORE
ST31 and ST33 platforms embed the ARM® SecurCore® processors that deliver outstanding computing performance and low dynamic power consumption which enables fast and reliable transactions. Software engineers can benefit from the industry-recognized ARM® development environment and from best-in-class code density.

FLASH TECHNOLOGY
ST has been continuously investing in advanced technology R&D and is proud to control both R&D and production in-house. Based on 40nm Flash technology, our most recent secure MCUs deliver advanced features at an optimized cost.

Flexibility
Thanks to ST’s Flash technology, flexibility is improved all along the value chain, from development to manufacturing:
• time-to-market is significantly improved by avoiding ROM masking cycle time
• production lead times are shortened by software loading at a very late manufacturing stage
• inventory management is optimized

Performance and reliability
Fast programming speeds reach up to 10 μs/byte in a chained mode. ST Flash technology demonstrates excellent endurance and retention capabilities, up to 500,000 cycles of erase/program operations per page and 30 years’ data retention.
SECURITY & CERTIFICATIONS

With over 30 years’ experience in security, ST’s success is confirmed by its awards and certificates attributed by organizations such as EMVCo, Visa, Mastercard, NFC, MTPS, China Union Pay, FIPS and Common Criteria. On top of that, ST recently became the first electronic component manufacturer to receive the “GSMA SAS-UP Certification” for eSIM production, demonstrating the highest level of security given for these types of devices and the flexibility to address all markets. With its secure manufacturing chain, ST is able to provide a secure end-to-end solution. The security in ST’s secure MCU portfolio is also ensured by the high-level expertise of ST’s crypto experts, who have also designed the AES and Keccak cryptographic algorithms. The increasing number of connected objects gives criminals more opportunities to control a given asset by introducing malware or counterfeit software to control/harm the connected network. As such, there is a strong need for OEMs, utilities and network providers to be able to trust their connected objects by relying on the security of their assets or networks. Adding a tamper-proof secure element to one’s assets or IoT objects offers robust authentication, platform integrity and end-to-end security to ensure end-user privacy as well as data, IP and brand protection. Typical target applications for a secure element are printers, computers, gateways, IoT endpoints, and sensors.
Secure MCU solutions are driven by dynamics based on smartcards technologies, Mobile secure transactions and secure connected world.

Ensuring your peace of mind with ST’s secure microcontrollers

Secure MCU

Banking & ID

Hardware & Solutions for Banking, ID, PayTV, Transport

ST31
STPay

Mobile Security Consumer

Hardware & Solutions for Mobile transactions (Consumer)

ST33 eSIM, eSE
ST21NFC
ST54

Secure Wearables

Hardware & Solutions for contactless applications

ST31
ST53
ST54

Consumer Hardware & Solutions

for contactless applications

ST31
ST53
ST54
ST proposes a complete set of security features:
- In-house technology
- Hardware and software certified security
- Cryptography and architecture expertise
- Secure environment
- Strong security community involvement

Authentication in IoT
- STSAFE-A
- STSAFE-J
- STSAFE-TPM

M2M for Industrial & IoT
- ST32-M
- ST33-M
- M2M Solutions

Secure Automotive
- ST33-A eSIM, eSE
- ST33-A TPM

Solutions for Brand Protection, Computer, IoT

Hardware & Solutions for M2M connectivity solutions
ST’s Banking & ID product family offers a complete portfolio of contact, dual interface and contactless (ISO/IEC 14443 Types A and B & ISO/IEC 18092) secure microcontrollers to enable a wide range of banking or identify applications, from traditional smart cards to innovative wearable objects. Having sold more than 3.5 billion banking cards based on secure MCUs, ST has solid references in the banking industry and is present in banking and transport cards.

**BANKING & ID SOLUTIONS OFFERS**

The ST31 secure microcontroller family is designed to support identification, PayTV, transport, and SDA & DDA banking applications. With the ARM® SecurCore® SC000 processor and an architecture optimized for contactless performances, the ST31 offers a broad portfolio including MIFARE Plus®, MIFARE Classic® and MIFARE DESFire® libraries. The platform addresses the highest security standards such as Common Criteria, EMVCo and China Union Pay (CUP).

Our STPay system-on-chip solution offers a comprehensive range of “ready-to-use” banking solutions, including Static Java, Dynamic Java and Multos OS-based solutions, covering a wide range of payment applications such as Visa, Mastercard, CUP, Amex, Discover, JCB, CPA and many other domestic brands.

To ensure a quick set-up of the personalization line, STPay products are compliant with EMV® Card Personalization Specifications (CPS), which have been validated and supported by major personalization equipment suppliers such as Entrust Datacard (part of the CPV program), and support our certified libraries including MIFARE Classic®, MIFARE Plus® and MIFARE® DESFire®.

**STPAY: ST’S SECURE PAYMENT SOLUTION**

- Full range of payment applications (Visa, MasterCard, JCB, American Express, Discover, Interac Flash...)
- Contact and Dual interfaces
- Common Personalization Standard compliant (CPS)
- Entrust Datacard Card Validation Program (CVP)
- MIFARE® and MIFARE® DESFire® options

**ST31**

Banking, PayTV, transport and identification applications
- 32-bit ARM® SecurCore® SC000 CPU
- Multiprotocol (ISO7816, ISO14443 A/B/F)
- EMVCo & Common Criteria certified

**STPay**

Ready-to-use banking offer
- Based on ST31 Secure MCU
- Java, Advantis & Multos OS
- Contact & Dual interfaces products
- Dedicated solution for transport applications
ST's security platform includes a large choice of products and solutions for wearable applications such as payment, transport, and multiple contactless transactions answering challenges such as security certification, interoperability, power consumption, integration, and the highest NFC performance. ST offers a complete range of solutions from optimized passive (battery-less) ST31 secure microcontrollers and STPay solutions to full-scale NFC solutions based on state-of-the-art ST53 and ST54 systems-in-package integrating a Secure Element.

**BoostedNFC™ OPENS NEW WAYS TO PAY**

ST’s boostedNFC™ technology is ideal for applications that require a card emulation function, but are environmentally challenged or have limited space for the antenna. Our STS392x family of advanced analog front-ends implement Active Load Modulation technology and guarantee reliable NFC & contactless transactions on wearables in challenging metallic environments or that require a very small antenna.

**STPay-BOOST & FIDESMO**

The STPay product range integrates the boostedNFC™ technology under the STPay-I-Boost reference. Based on the STPay-Boost and personalization from Fidesmo, ST and Fidesmo have created a turnkey active solution for secure contactless payments integrated in Kronaby watch.

**Secure Wearables**

**ST31**
- Optimized Passive
- For payment and transport
- ARM® SecurCore® SC000 CPU
- Card Emulation, ISO14443 A/B/F
- MIFARE®
- Down to Class 6 antennas supported

**ST53**
- Optimized Active
- For high-end multi-applications
- For payment and transport
- Combined SE and transport
- Combined SE and RF booster
- Card Emulation, ISO 14443 type A
- MIFARE®
- Class 6 and below

**ST54**
- Advanced Active
- Combined SE and NFC Controller
- NFC Card Emulation, ISO14443 A/B/F
- MIFARE4Mobile® v2
- Typical antenna <100 mm² and metal cover
Mobile security is expanding from the largely deployed SIM technology in mobile phones to the growing NFC, embedded Secure Element (eSE) and embedded SIM (eSIM) technologies in smartphones, tablets, wearables, and laptop devices.

**ST’S SOLUTIONS TO BUILD THE MOST EFFECTIVE AND SECURE MOBILE APPLICATIONS**

ST provides an exhaustive offer of NFC and eSE/eSIM products and solutions to address secure mobile transaction applications: from the state-of-the-art ST21NFC NFC controller to the ST54 integrating the widely deployed ST33 Secure Element.

**ST33 / ST21NFC**

- Application processor
- SIM ST33
- NFC ST21
- eSE ST33

**ST33 / ST54**

- Application processor
- SIM ST33
- NFC ST21
- eSE ST33
- eSIM ST33

**ST54**

- Application processor
- SIM ST33
- NFC + eSIM + eSE ST54J

**Multiple chips**

- SIM + NFC + eSE

**eSIM emergence**

- [NFC + eSE] SiP

**eSIM / NFC Convergence**

- [eSIM + NFC + eSE] single die
STANDALONE SOLUTIONS

ST33 for eSIM and eSE applications

ST33 secure microcontrollers meet the advanced security and performance requirements for secure applications including embedded SIM, NFC-SIM, and embedded NFC secure elements with a large user Flash memory capability. Already integrated by major OEMs in tablets, wearables and notebooks, the eSIM continues to be largely deployed in smartphones. An eSIM is a surface-mounted device soldered directly on the PCB; enabling OEMs to design smaller and thinner mobile devices and end users to subscribe to the Mobile Network Operator of their choice. Remote provisioning of the SIM application inside the eSIM device is ensured by subscription management systems compliant with the GSMA Remote SIM provisioning specification. ST’s eSIM is available in multiple form factors such as WLCSP (Wafer Level Chip Scale Package), the smallest and thinnest package of its kind. It is fully compliant with the GSMA Remote SIM Provisioning specification and is fully interoperable with the major subscription management providers.

GSMA SAS-UP CERTIFICATION

In 2018, ST became the first chip maker accredited by the GSMA to personalize eSIMs for Mobiles and connected IoT devices delivering ready to use solution with no further programming required. The eSIMs, customized with connection credentials, enable smaller form factors, greater security, and increased flexibility.

ST21NFC for NFC Controller

The growth of contactless mobile transactions is driving the adoption of NFC and embedded Secure Element (eSE) solutions in consumer mobile devices such as smartphones and wearables. Tablets, gaming consoles, laptops and ultrabooks are also integrating NFC technology so they can read tags to interact with smart IoT objects or accept payment cards. ST21NFC is ST’s 4th generation NFC controller integrating a high-performance RF booster to provide the best user experience and ensure a high level of interoperability to ease integration and certification efforts for OEMs.

MOBILE SECURITY eSIM/NFC CONVERGENCE INTEGRATED SOLUTIONS

ST54 for Integrated Solutions

In order to manage the future of secure mobile transactions, ST provides a large range of ST54 integrated solutions merging our ST21NFC NFC Controller and the proven ST33 secure element. The first generation is a System-in-Package (ST54H) delivered in a BGA package while the new ST54J System-on-Chip (SoC), optimized to address convergence, is available as a single-die in a thin WLCSP package. The ST54J delivers performance-boosting integration for mobile and IoT devices with the added benefit of ST’s software-partner ecosystem for smoother user experiences in mobile payments and e-ticketing transactions, as well as more convenient, remote, mobile provisioning to support multiple operator subscriptions.

ST21NFC

NFC Controller

- For tiny and metal cover antennas
- Reduced bill of materials
- Low-power mode

ST33

eSE/eSIM

- GP2.2 Operating System
- Large user memory
- MIFARE®
- DFN, WLCSP or BGA stacked with NFC

ST54

NFC & eSE/eSIM

- Combined SE and NFC
- Multi-application and NFC
- MIFARE®
- WLCSP, BGA
To ensure that a company’s IoT platform can be trusted and protected against possible threats and vulnerabilities, all its key components, Network & Cloud, Gateways & Concentrators and Smart Things or nodes, must be able to exchange data and communicate in a secure manner, regardless of the field of application.

**IoT MARKETS & APPLICATIONS**

Today’s secure embedded systems are currently expanding from largely deployed brand protection, IT security and TPM solutions to now include connected devices for the Internet of Things (IoT). Data issued from connected devices involved in smart meters, smart cities, smart homes and smart industry including the industry 4.0 initiative must be trusted. More and more connected devices are now adopting solutions based on secure elements similar to those used in printers, PCs, game controller, phone accessories, batteries, and luxury goods.

**STSAFE™ FAMILY, A SCALABLE SECURITY OFFER**

Designed to ensure the security of the three main components of an IoT solution, STSAFE products are all evaluated by independent third-parties and have received best-in-class security certificates including Common Criteria, BSI, and FIPS as well as specific evaluation and validation schemes.

<table>
<thead>
<tr>
<th>STSAFE-A OPTIMIZED</th>
<th>STSAFE-J FLEXIBLE</th>
<th>STSAFE-TPM STANDARDIZED</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Brand Protection</td>
<td>• Utilities</td>
<td>• Computer</td>
</tr>
<tr>
<td>• Assets tracking</td>
<td>• Gateway</td>
<td>• Gateway</td>
</tr>
<tr>
<td>• Smart City</td>
<td>• Smart City</td>
<td>• Network equipment</td>
</tr>
<tr>
<td>• eHealth</td>
<td>• Servers</td>
<td>• Servers</td>
</tr>
<tr>
<td>• Industry 4.0</td>
<td>• Industry 4.0</td>
<td>• Industry 4.0</td>
</tr>
</tbody>
</table>
**STSAFE™-A OPTIMIZED SOLUTION FOR EMBEDDED SYSTEMS**

Designed for applications exposed to fraud or counterfeiting such as ink cartridges, accessories for phones or gaming, USB Type-C devices, IoT devices based on Wi-Fi, Bluetooth Low Energy (BLE) or low-power wide-area networks (LPWAN) or IoT objects that are part of critical credential management systems or other valuable services, STSAFE-A is the ideal solution for those wishing to build an ecosystem around their brand.

**STSAFE™-J FLEXIBLE SOLUTION WITH JAVA PLATFORM**

Focused on providing state-of-the-art security for connected objects, the STSAFE-J100 gives each object an unalterable identity that can be authenticated. Device designers can take advantage of the freedom of customizable applets to create their own security profiles, or to get to market faster using ST’s pre-certified profiles for German BSI and French Enedis smart-utilities specifications.

**STSAFE™-TPM STANDARDIZED SOLUTION FOR TRUSTED COMPUTING**

Fully compliant with TCG’s (Trusted Compliant Group) specifications covering Computer & IoT profiles, STSAFE-TPM products are Common Criteria EAL4+ as well as FIPS 140-2 certified. They offer the most comprehensive and cost-effective system-on-chip for trusted computing. Available in different packages and interfaces, this cost-effective system-on-chip provides a flexible solution for a wide range of connected devices.

---

**STSAFE-A100 OPEN DEVELOPMENT KIT**

- STSAFE-A100 datasheet
- STSAFE-A100 STM32 Nucleo Expansion board (X-NUCLEO-STSA100)
- Morpho and Arduino connectors
- STSAFE-A100 Software Package (STSW-STSA100)
- Driver and use case examples

Our STSAFE-A100 Evaluation Pack (STSW-STSA100) extends the rich STM32 Nucleo ecosystem to accelerate secure element integration, leveraging reusable source code that simplifies the creation of secure IoT devices, high-value consumables such as medical probes and accessories, and consumer products. Available for download at www.st.com/stsafe-a

---

**KEY APPLICATIONS**

- Consumer goods
- Sensitive & high-value consumables
- Smart Industry & Smart City
- Utilities & gateways
- Computers
- Network equipment & Servers
- IoT nodes
- Asset tracking
A connected device brings a lot of key benefits such as remote control and real-time asset management. Moreover, the emergence of cellular connectivity has made it easier to connect devices, enabling a greater diversity of devices. Then, these new opportunities require different specification. ST diversifies its connectivity offer and proposes a large range of products compatible with all cellular connectivity solutions.

**FLEXIBLE CELLULAR CONNECTIVITY SOLUTION**

There are 2 types of cellular connectivity designed for different markets. The first is the classic SIM that only includes cellular connectivity for Smart IoT devices. By being easy to deploy, it enables a fast go-to-market. The most recent is the emerging embedded SIM (eSIM) defined by the GSMA SGP02 specification. It is a scalable solution that makes possible to change over the air the network providers (profile) without impacting the eSIM itself. The eSIM is a flexible and cost optimized solution.

**For IoT SIM solution**
- Simple & Small
- Java Card framework environment with one Cellular connectivity (SIM)

**For industrial SIM solution**
- M2M industrial robustness (500Kcycles & temperature range -40 °C to + 105 °C)
- Cellular connectivity (SIM)

**For industrial eSIM solution**
- Scalable connectivity with eSIM (GSMA M2M compliant)
- GSMA SAS-UP certified (HW & OS)
- M2M industrial robustness

**RELIABILITY AND HIGH-QUALITY**

According to the environment, ST offers a dedicated range of products for M2M industrial and IoT applications compatible with a cellular connectivity solution. Low-end solutions, based on the ST32 family, target Smart IoT products for a simple, smaller and faster integration. This product is compatible with a SIM.

To address industrial applications, ST offers an ST33-based solution that supports extreme environmental conditions with high data retention and high temperature range. Moreover, the ST33G1M2M is CC EAL5+ and GSMA M2M certified.
With the growth of connected cars and the automotive industry’s roadmap towards autonomous driving, secure chips start to find their place in vehicle telematics, gateways and electronic control units (ECUs). Security being at the heart of such new challenges, ST is committed to the development of secure solutions to cover most requirements for the new era of digital technologies.

EMBEDDED SECURE SOLUTIONS FOR CONNECTED CARS

Secure elements and embedded SIMs in connected vehicles ensure many key functions to protect against theft of service, fraudulent network access, device cloning and counterfeiting as well as data eavesdropping and corruption:
- Secure V2X connectivity for eCall, diagnostics, SW upgrade, payment & Internet services, ADAS, and other sensitive services and systems
- In-car security communication & platform integrity
- User data storage to prevent physical and cyber attacks, to guarantee passenger safety and vehicle behavior and to ensure data privacy

To address these challenges, ST has developed the ST33G1M2A. Based on an ARM® SecureCore® SC300 32-bit RISC core, the ST33G1M2A secure microcontroller ensures high-quality security solutions for Automotive-grade applications.

ST33-A TPM

- Standardized for Automotive
- TPM 2.0 services
- User data and secure key storage
- In-car communication security and integrity

ST33-A Secure Element

- Secure Automotive solution
- User data and secure key storage
- Communication security and integrity

ST33-A eSIM

- Secure cellular connectivity for car
- Cellular connectivity
- Secure communication
- eCall