Secure Solutions
Ensuring your peace of mind
Content

ST at a glance ................................................................. 3
Value chain ........................................................................ 4
Where to find us ............................................................. 5
Secure application market .................................................. 6
ST’s secure microcontrollers .............................................. 7
Technology ........................................................................ 8
Contactless and NFC ....................................................... 8
ARM® core ......................................................................... 8
Flash technology .............................................................. 8
Manufacturing ..................................................................... 8
Security & certifications ...................................................... 9
Banking & ID ....................................................................... 10
Banking .............................................................................. 10
Banking market ................................................................. 10
Identification ....................................................................... 11
Government and identity market ......................................... 11
Focus on ST31 ..................................................................... 11
Mobile security ..................................................................... 12
eSIM for consumer ............................................................ 12
Focus on NFC components and architecture ....................... 12
Embedded SIM for M2M industrial & automotive ................ 13
Focus on ST33 ................................................................. 13
Authentication ...................................................................... 14
Focus on authentication and IOT solutions ......................... 14
Turnkey solution ............................................................... 15
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 2015, the Company’s net revenues were $6.90 billion, serving more than 100,000 customers worldwide. Further information can be found at www.st.com.
**Value chain**

**MAIN STEPS 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 separated stages, starting with a plain silicon wafer, and resulting in the etching of several hundreds to thousands of die.

**Electrical Wafer Sorting**
Dies on the wafer are electrically tested. This step is known as wafer sort or probe.

**Assembly line and final Back end (BE)**
The dies are cut from the silicon wafer before being assembled in a package the chips are then tested prior to delivery to the customer.

**Product use and end of life**
We offer a large portfolio of products for a wide range of applications. Which are developed by our customers.

**MANAGEMENT OF OUR IMPACTS**

- We implement the EICC standards in our supply chain and require ISO and OHSAS certifications to address ethics, social, environmental, health and safety risks. We participate to the Conflict Free initiative.

- We design products systematically taking into consideration the environmental impact of the device during its whole life cycle, including raw materials, transportation, manufacturing, usage and end of life.

- FE manufacturing requires large quantities of water and some ST sites are located in water scarce regions. Through our water management programs we are continuously reducing our water footprint through reuse and recycling.

- We implement our Code of Conduct and the EICC standards in all our sites to mitigate our ethics and labor and human rights risks. Although most of our FE production is based in Europe, we also have FE and BE manufacturing located in Asia where risks can be higher. We do regular assessments of our production sites. We ensure the health and safety of our employees through advanced management systems and certification.

- We manage our direct and indirect greenhouse gas emissions from all our operations, including Perfluorinated Compounds (PFCs) which have a very long atmospheric lifetime and high Global Warming Potential. Consequently, even if our consumption of PFCs is relatively low, their impact is significant and requires actions to reduce the CO2-equivalent emissions that they produce.

- We minimize the environmental, health and safety risks related to the chemicals and materials used in the manufacturing process, by basing the selection, handling and substitution on the precautionary principles.

- Our products are designed to minimize the carbon footprint and consume as little energy as possible in the end-application. We also develop innovative products to help our customers develop new energy saving applications. ST products are not subject to WEEE but our management of hazardous substances minimizes the impact of disposal and facilitates recycling.
Where to find us

Making driving safer, greener and more connected

Making homes smarter, for better living, higher security, and less waste

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

Enabling cities to make more of available resources

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 and the Trusted Platform Module (TPM) standard for computers, 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 introduction of embedded secure elements, eSIM devices, M2M devices and NFC enable devices as well as contactless cards.

Tomorrow 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, and smart world applications.
Among its large portfolio serving all electronics segments, STMicroelectronics offers a complete secure microcontroller product line, enabling security in mobile, banking & ID, and IoT-connected devices. Throughout its 20-year presence in security, ST has supplied the market’s most advanced technologies and solutions, with a continuous focus on innovation and the highest levels of security certification. ST’s secure microcontrollers contribute to a smarter and more secure connected world. By getting more from technology to get more from life, ST stands for life.augmented.

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

- **Banking & ID solutions** for traditional smartcard businesses such as payment, people identification, transport, and pay TV.
- **Mobile security** addressing SIM solutions for cellular connectivity in mobile, wearable and machine-to-machine (M2M) products, as well as secure solutions for near field communication (NFC & eSE) and Secure Driving in automotive applications.
- **Authentication covering** brand protection, TPMS and strong authentication solutions for IoT networks.
CONTACTLESS AND NFC
ST31 dual interface secure microcontrollers are designed to enable secure and fast contactless transactions for banking, ID and transport applications. To cover NFC technology in secure mobile connectivity, ST provides a complete product portfolio from the ST21NFC NFC controller family to the NFC system-in-package ST54 platform combining a ST33 secure element with a ST21NFC NFC controller.

Multi-protocol
ST31 secure MCUs support various multi-protocol RF interfaces enhancing multi-application versatility. ISO/IEC 14443 Type A, B and B’, NFC, ISO/IEC 18092 and Very High Bit Rate 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 the NFC modes as Reader/writer, Card emulation and Peer to Peer to address all the 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 respectively the ARM® SecurCore® SC000 and SC300 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. The latest ST’s Secure MCUs are based upon 40nm Flash technology, allowing to deliver advanced feature products at optimized cost to its customers.

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.

MANUFACTURING
In order to provide a complete end-to-end secure solution, ST has put in place a strong security manufacturing chain from hardware and firmware development to the pre-personalization stage for the end solution. Thanks to its large manufacturing capacity, ST is able to provide a Common Criteria certified process from the development to the shipment to customer facilities.

ST process & shipment

<table>
<thead>
<tr>
<th>Development</th>
<th>Fabrication &amp; pre-personalization</th>
<th>Customers</th>
</tr>
</thead>
</table>

Customer process
Security & certifications

With over 20 years’ experience in security, ST’s success is confirmed by its awards and certificates attributed by organizations such as EMVCo, Visa, Mastercard, EMVCo, China Union Pay, FIPS and Common Criteria.

On top of that, ST recently became the first electronic component manufacturer to receive the “Label France Cybersecurity” for its secure microcontroller solutions, demonstrating the highest level of security given by these kind of products and the flexibility to address all markets. With its secure manufacturing chain, ST is able to provide a secure end-to-end solution for its customers.

The security in ST’s secure MCU portfolio is also ensured by the high level expertize 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.
Banking & ID

Banking

STMicroelectronics’ banking product family offers a complete portfolio of contact, dual interface and contactless (ISO14443, Types A, B and B’, ISO18092) secure microcontrollers to support SDA or DDA markets.

Having sold more than 2 billion secure MCU-based banking cards, ST has solid references in the banking industry and is present in banking smartcards all around the world.

Multi-application banking and transport cards support MIFARE Plus® (including MIFARE® Classic) and MIFARE® DESFire®.

Banking Market

The increasing need for highly secure payment transactions drives the banking card market towards chip-and-PIN solutions. The US, China, Russia and India are now joining Europe and adopting chip card solutions. The contactless/dual interface trend is being confirmed and should be reinforced in the coming years: contactless payments facilitate small payment transactions and maximize adoption and user experience.

Key Benefits

- ST’s proven experience: with more than 2 billion banking secure MCUs shipped around the world, ST is a reference in Banking card ICs
- All solutions to support the traditional contact SDA, contact DDA and dual interface cards and to enable the emerging wearable applications
- Banking & Transport multi-application cards can rely on our certified libraries including MIFARE Plus® and MIFARE® DESFire®
- Our STPay system-on-chip solution is among the best ready-to-use and independent offer in the industry including Visa, Mastercard, Amex, Discover, JCB, CUP.
**IDENTIFICATION**

STMicroelectronics offers the optimum combination of security, portability and functionality for governments and industry partners in each country. In areas such as international passports, national ID cards, driving licenses and health or industrial PKCS, major programs are in progress to upgrade existing solutions with ST’s secure MCU technology. ST’s products dedicated to e-government applications meet the growing demand for secure cryptographic ICs with high-speed interfaces and large memory capacity. They integrate an enhanced crypto co-processor that supports the BAC, SAC, EAC, and AA security features required by ICAO standards and allow very fast e-passport transactions. The platform also supports all European standards related to electronic signatures and the European Citizen Card. ST developed the world’s first secure microcontroller to achieve Common Criteria EAL6+ (AVA V5) certification.

**GOVERNMENT AND IDENTITY MARKET**

Today, governments across the world recognize secure MCUs as a key tool in protecting sensitive and personal data, reducing fraud, and improving services and information for citizens. STMicroelectronics offers the optimum combination of security and functionality to governments and industry partners. With the ePassport market firmly established, growth is expected from eID applications: eVoting, eDriving License, eHealth, or digital signature are making an ordinary citizen an eCitizen.

**FOCUS ON ST31**

The ST31 secure microcontroller family is the platform for highly-secure applications including banking, identification, pay TV, and transport. With the ARM® SecurCore® SC000 processor and an architecture optimized for contactless performances, the ST31 offers a broad portfolio including MIFARE Plus® and MIFARE® DESFire® libraries, multiple interfaces, and certified cryptographic libraries. The platform addresses the highest security standards including Common Criteria up to EAL6+, EMVCo, and CUP.

**KEY BENEFITS**

- ST’s proven experience: over 20 years, more than 40 government institutions have adopted ST solutions to secure large-scale government programs representing more than 400 million Gov & ID secure ICs delivered to date
- High reliability guaranteed over the entire ID card life cycle (30 year data retention and 500 Kcycles endurance)
- Complete ID solutions through independent OS partners
- Native & Java platforms allowing flexibility for customer development

**KEY FEATURES**

- Supply chain flexibility: Advanced Flash technology
- Development efficiency: 32 bit ARM® SC000
- Certified security: CC EAL6+, EMVCo, CUP
- Interoperability: multiprotocol interfaces (ISO 7816, ISO 14443 A & B, B’)
Mobile security

The mobile security market is expanding from the largely deployed UICC technology in mobile phones to the growing embedded SIM (eSIM) technology in tablets, wearables, and M2M devices. The most promising growth in mobile security is driven by the NFC technology including NFC controllers and secure elements such as NFC-SIM and embedded Secure Element (eSE) chips for contactless transactions in mobile devices.

**eSIM FOR CONSUMER**

Embedded-SIM, or eSIM, ICs are at the heart of an expanding spectrum of the consumer market for easy-to-use, intuitive and user-friendly mobile applications. They target a broad range of electronic devices such as wearables, tablets and handsets with the aim to provide the best possible cellular connectivity experience. As mobile devices become smaller and more integrated, OEMs will greatly benefit from ST’s eSIM ICs that are available in very small form factors such as WLCSP. ST’s eSIM solutions are based on the widely deployed ST33 Secure Element platform providing a high level of security, large amount of memory and high performance for OTA data transfers and secure storage of new Mobile Network Operator subscriptions.

**FOCUS ON NFC COMPONENTS AND ARCHITECTURE**

The ST21NFC product line is a family of NFC controllers based on a microcontroller architecture with embedded non volatile memory and multiple connectivity channels. The devices comply with all relevant standards, and are perfectly suited to address all possible NFC use cases. The ST33 platform is a family of secure elements designed to meet the advanced EAL6+ / EMVCo/CUP security and performance requirements, combining the latest Flash technologies with the highest security levels on the secure ARM® SecurCore® SC300 core. The ST54 product family is a system-in-package platform combining an ST21NFC NFC controller with an ST33 secure element as part of ST’s global NFC offer.
EMBEDDED SIM FOR M2M INDUSTRIAL & AUTOMOTIVE

With the growth of connected things, more and more objects, devices, machines, and automotive systems are being connected applications, embedded SIM chips communicate through cellular networks using 2G, 3G, and 4G technologies.

To enable communication with cellular networks, SIM technology plays a key role in M2M (machine-to-machine) applications. SIM chips for M2M applications are based on traditional SIM technology which is reinforced to operate in harsh conditions and enhanced with state-of-the-art security and larger memory capacity. Such applications require the use of advanced secure microcontrollers including a comprehensive set of surface-mount device (SMD) packages. As more and more assets such as private data, sensitive user information, and secret keys are stored in machines, devices, and automotive systems, they need to be protected from malicious attacks; secure microcontrollers play a key role in these kinds of applications.

FOCUS ON ST33

The ST33 secure microcontroller family is designed to meet advanced security and performance requirements for applications including NFC-SIM secure element, NFC embedded secure element, embedded SIM for consumer, and machine-to-machine industrial & automotive segments.

With the latest ARM® SecurCore® SC300 32-bit RISC processor and an architecture optimized for high performance, the ST33 platform offers large memory capacity, multiple communication interfaces and certified cryptographic libraries in different form factors including wafers, SIM modules, DFN, and WLCSP packages.

The ST33 platform addresses the highest security standards including Common Criteria up to EAL6+, EMVCo and CUP.

To support MIFARE® technology on secure element applications, optional MIFARE® libraries (MIFARE® Classic and MIFARE® DESFire® EV1 libraries) are available on ST33 secure microcontrollers and are certified up to Common Criteria EAL6+.

MOBILE SECURITY SOLUTIONS

- ST33G1M2/ST33J2M0
  - eSIM Consumer
  - SWP SIM
  - eSE
- ST33G1M2A/J2M0A
  - M2M Industrial and Automotive
  - eSE Automotive
- ST32G512A
  - M2M Industrial and Automotive
- ST21NFC
  - NFC controller
- ST54
  - NFC SiP (System-in-Package)
  - ST21 + ST33
Authentication

The authentication market is currently expanding from largely deployed brand protection, IT security and TPM solutions to now include the Internet of Things market. Data issued from Objects involved in smart grids, smart cities, smart homes, smart industry, with Industry 4.0 initiative, must be trusted, and more and more connected devices are now adopting solutions based on secure elements similar to those used in printers, PCs, game controllers, phone accessories, batteries, and luxury goods.

STSAFE AUTHENTICATION SOLUTION

ST secure element STSAFE family ranges from optimized, to flexible Java based and TCG compliant TPM solutions

STSAFE-A optimized
- Printers
- Games
- PCB components
- Smart Home, Smart City
- Docking stations

STSAFE-J flexible
- Utilities
- Lighting
- Vehicle-to-grid
- Smart Home
- Healthcare

STSAFE-TPM standardised
- Computer
- Gateway
- Networks
- Servers
- Automotive

STSAFE-TPM
ST’s Trusted Platform Module is an EAL4+ Common Criteria-certified solution compliant and certified TPM 1.2 & 2.0 TCG (Trusted Computing Group) standard, which protects users’ assets by monitoring platform integrity from boot phase. Used in devices where firmware integrity is a must, TPMs are largely deployed in desktops, notebooks, tablets, and servers and continue to spread into today’s connected world, expanding from PCs to phones to home gateways to cars to infrastructures and more.

STSAFE-J
With a flexible Global Platform and Java 3.0.4-compliant command set, STSAFE-J is the new generation of KERKEY™ versatile secure solution offering a wide range of cryptographic and secure services for applications which need to comply with a pre-defined scheme. Moreover, its common Criteria EAL4+ certificate enables it to serve the smart grid market as well as those requiring strong security in concentrators, gateways, and IoT devices.

STSAFE-A
Running on a Common Criteria EAL5+ platform, STSAFE-A is a highly secure authentication solution whose security is certified by independent parties. Its command set is tailored to address strong authentication, establish a secure channel in the scope of a TLS session, verify signatures, and offer secure storage as well as decrement counters for usage monitoring. It is particularly well suited for applications heavily exposed to fraud and counterfeiting attacks, such as printers, game controllers, phone accessories, and IoT networks.
TURNKEY SOLUTION

ST’s turnkey solutions for the authentication market rely on highly secure MCUs whose security is certified by independent labs and achieve top-level Common Criteria EAL5+ certification.

By offering a complete solution ranging from an internally-developed secure operating system embedded in the secure MCU, example code for integration of the solutions in the applicative environment, and personalization services for the storage of confidential customer data in the secure MCU, ST offers seamless integration of security measures for customers who might not be experts in secure system.