Secure Solutions
Ensuring your peace of mind
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 2016, the Company’s net revenues were $6.97 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
- 2016 net revenues of US$ 6.97B
- Approximately 43,500 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 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, 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 EAL6+, 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 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.
### MAIN STEPS IN OUR VALUE CHAIN

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppliers</td>
<td>We purchase silicon ingot, raw materials, equipment, energy, gas, chemicals and services from many suppliers and subcontractors.</td>
</tr>
<tr>
<td>R&amp;D concept and design</td>
<td>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.</td>
</tr>
<tr>
<td>Manufacturing Front end (FE)</td>
<td>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.</td>
</tr>
<tr>
<td>Electrical Wafer Sorting</td>
<td>Dies on the wafer are electrically tested. This step is known as wafer sort or probe. Secure MCU requires pre-loading of embedded software, keys and data in a secure environment using HSM.</td>
</tr>
<tr>
<td>Assembly line and final Back end (BE)</td>
<td>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.</td>
</tr>
<tr>
<td>Secure Pre-Personalization</td>
<td>Secure MCU will be loaded with customer keys and data in a secure environment.</td>
</tr>
<tr>
<td>Product use and end of life</td>
<td>We offer a large portfolio of products for a wide range of applications.</td>
</tr>
</tbody>
</table>

### OUR CERTIFICATIONS

- 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, manufactured and pre-personalized products systematically taking into consideration to obtain certifications in Quality, Environment, Safety, Security and Site Business:
  - Continuity management system domains
  - Quality System certification ISO TS 16949
  - Quality CQM/Mastercard
  - Environment certifications ISO 50001 and ISO 14064
  - Security certification Common Criteria EAL5+/EAL6+
  - Safety certifications ISO 15408 and OHSAS
  - Site Business Continuity Management
  - System ISO 22301

- We participate in the Conflict Free initiative.

- We purchase silicon ingot, raw materials, energy, gas, chemicals and services from many suppliers and subcontractors.

- We design, manufactured and pre-personalized products systematically taking into consideration to obtain certifications in Quality, Environment, Safety, Security and Site Business:
  - Quality System certification ISO TS 16949
  - Quality CQM/Mastercard
  - Environment certifications ISO 50001 and ISO 14064
  - Security certification Common Criteria EAL5+/EAL6+
  - Safety certifications ISO 15408 and OHSAS
  - Site Business Continuity Management
  - System ISO 22301

- We offer a large portfolio of products for a wide range of applications.
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 a 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, 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 respectively embed 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.
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

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 identity applications, from traditional smart cards to innovative wearable objects.

Having sold more than 3 billion banking cards based on secure MCUs, 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®.

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

BoostedNFC OPENS NEW WAYS TO PAY

The boostedNFC technology opens new ways to pay with an infinite number of everyday-life form factors including wristbands and watches. Combining a secure MCU with a boostedNFC IC, the ST53 family offers an unique solution that makes contactless payment transactions faster and more robust, while using tiny antennas that are easy to integrate with any wearable form factor.

The boostedNFC technology is also available in the STPay product range under the STPay-I-Boost reference.
TOWARDS FUTURE ID DOCUMENTS
Future LDS2 ePassport and ID documents are being designed to securely embed an increasing volume of personal data, to further secure authentications, and significantly accelerate transactions.

ST is preparing this major evolution by proposing large Flash memory secure microcontrollers, combining advanced cryptographic mechanisms and high processing speed.

IDENTIFICATION
ST’s products dedicated to Identity and e-Government applications meet the growing demand for secure cryptographic ICs with high-speed interfaces and large memory capacity. They integrate an enhanced crypto coprocessor 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.

ePASSPORT & ID OPERATING SYSTEM PARTNERSHIP
A wide range of ST-based certified eID and ePassport solutions are available from our software development partners such as Masktech. Please contact your ST Sales representative for more details.

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 EAL5+, EMVCo, and China UnionPay (CUP).

ST31 KEY FEATURES
- Supply chain flexibility: Advanced Flash technology
- Development efficiency: 32-bit ARM® SC000 core
- Certified security: CC EAL5+, EMVCo, and CUP
- Interoperability: multiprotocol interfaces (ISO/IEC 7816, ISO/IEC 14443 A & B, and VHBR)
Mobile security

The mobile security market 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, laptop devices and connected cars.

NFC & eSE

The growth of contactless mobile transaction is driving the adoption of NFC and embedded Secure Element (eSE) solutions in consumer mobile devices such as smartphones and wearables. Increasingly popular, payment and transport wallets are currently being deployed by OEMs and MNOs throughout the world allowing consumers to use their favorite payment and transport schemes directly on their mobile devices. 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. ST’s large portfolio of NFC Controller and Secure Element products lets OEMs develop and manufacture cost-effective and high-performance NFC solutions.

ST21NFCD is ST’s 3rd 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. ST’s eSIM solution is based on ST33 Secure Element platform and 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.

eSIM FOR CONSUMER

The use of embedded SIM (eSIM) solutions is at the very beginning of its success. Currently deployed by large OEMs in mobile consumer devices such as tablets, wearables, laptops, and ultrabooks, the key growth driver will be development of eSIM applications for smartphones and feature phones.

An eSIM is a surface-mounted device soldered directly on the PCB; enabling OEMs to design smaller and thinner mobile devices and end user to subscribe to the Mobile Network Operator of his 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 solution is based on ST33 Secure Element platform and 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.

The ST54 system-in-package family integrates an ST21NFCD NFC Controller and ST33 Secure Element embedding a Java Card operating system to host a large number of payment and transport applications.
eSIM & eSE FOR AUTOMOTIVE

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).

They provide wireless connectivity based on eSIM technology and increase the level of security of in-car-communications and over-the-air firmware updates through the use of tamper-resistant Secure Elements.

To provide the security required in automotive applications, ST’s widely deployed ST33-A Secure Element is available in a fully automotive-qualified version (AEC-Q-100) and can operate from -40 up to 105 °C.

ST’s ST33-A automotive platform can be used as an eSIM fully compliant with the GSMA Remote SIM Provisioning specification and is fully interoperable with the major subscription management providers.

Used as an embedded Secure Element with a Trusted Platform Module (TPM) or a Java Card operating system, the ST33-A becomes a companion chip to the automotive MCU/MPU providing roots of trust services, ciphering and deciphering in a tamper-proof and certified environment to secure OTA firmware updates or store secret keys and credentials.

FOCUS ON ST54

ST’s latest generation of the ST54 System-in-Package integrates the 3rd generation ST21NFCD NFC controller embedding ST’s widely deployed RF booster and the most recognized ST33 Secure Element allowing OEMs to develop high-performance, cost-effective NFC solutions. The ST54’s embedded ST21NFCD NFC controller features a high output power TX driver and an Active Load Modulation IP as well as an RX stage with high sensitivity and high immunity to noise, allowing for a greater user experience and improved interoperability test coverage for mobile device manufacturers. Secure applications such as transport and payment cards are loaded into the ST54’s ST33 Secure Element. The ST33 series includes a family of Secure Element embedding an ARM® SecureCore® SC300 running a Java Card operating system. The ST33 is available with different memory sizes, CPU performance and interfaces. The ST33G1M2 in 80 nm ST technology integrates 1.28 Mbytes of eFlash memory and can operate at up to 33 MHz. It simultaneously supports ISO/IEC 7816, SWP and SPI master/slave interfaces. Designed for the convergence of applications such as embedded Secure Element and eSIM, the ST33J2M0 in 40 nm ST technology integrates 2 Mbytes of eFlash memory, operates at up to 60 MHz and supports simultaneously supports ISO/IEC 7816, SWP, SPI master/slave and I2C interfaces. Multiple GPIOs can be configured for both ST33 products.

MOBILE SECURITY SOLUTIONS

- ST33G1M2/ST33J2M0
  - eSIM for smartphones, tablets, wearables, and connected PCs
  - NFC for smartphones
- ST33G1M2A
  - eSIM for connected cars
  - eSE for automotive gateways and ECUs
- ST21NFC
  - NFC controller for smartphones, tablets, wearables and connected PCs
- ST54
  - NFC and eSE for smartphones, tablets, wearables, and connected PCs
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**
  - Brand Protection
  - Utilities
  - Smart City
  - Smart Agriculture
  - Assets tracking
  - Industry 4.0
  - eHealth

- **STSAFE-J flexible**
  - Utilities
  - Smart City
  - Industry 4.0

- **STSAFE-TPM standardized**
  - Computer
  - Gateway
  - Network equipment
  - 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**

STSAFE-J is a flexible secure solution based on Global Platform, Java 3.0.4 and a dedicated Java Card modular application. It offers a wide range of cryptographic and secure services meeting requirements for custom applications. Moreover, its common Criteria EAL5+ certificate enables it to serve the smart grid market as well as the markets requiring certified security in concentrators, gateways, and IoT devices.

**STSAFE-A**

Running on a Common Criteria EAL5+ platform, STSAFE-A is a highly secure authentication solution. 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 and to secure IoT devices based on Wi-Fi, BLE and LPWAN communication networks.
TURNKEY SOLUTION

Host library
Set of software libraries

System on Chip
Hardware
Embedded software
Pre-personalization

Tools & demo kit
STM32 Nucleo and Raspberry Pi extension boards compatible
Software libraries

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.