



life.augmented

Secure Solutions Ensuring your peace of mind



Contents

3	Secure Solutions
3	At a glance
4	Our value chain
5	Our offer
6	Where you find us
7	Our families
8	Smartcard applications
8	ST31
9	STPay
10	Mobile Security
11	ST33, ST21NFC, ST54
12	Authentication
12	STSAFE
14	M2M Connectivity
14	ST4SIM
15	Secure Automotive
15	ST33-A, ST4SIM-A

Secure solutions at a glance

With its STSECURE portfolio, STMicroelectronics offers a wide range of secure microcontrollers and turnkey solutions, answering the market need for advanced security.

The increasing number of connected devices gives criminals more opportunities to control a given asset by introducing malware or counterfeit software to control the connected network. Exposure to these threats is frequent and occurs in both private and professional environments.



STSECURE, ENSURING YOUR PEACE OF MIND

A complete portfolio dedicated to security

In the fast growing digital world, STSECURE products and solutions protect your privacy and your assets by ensuring their confidentiality, their integrity and their availability to authorized requesters where and when needed. We deliver hardware- and software-certified solutions, offer seamless integration of security features, and are experts in cryptography and device architecture.

Learn more at www.st.com/stsecure

Over 30 years' experience in security

More than
8 billion

Secure MCUs
shipped to date



Cryptography & architecture expertise



Strong involvement in the security community



In-house technology



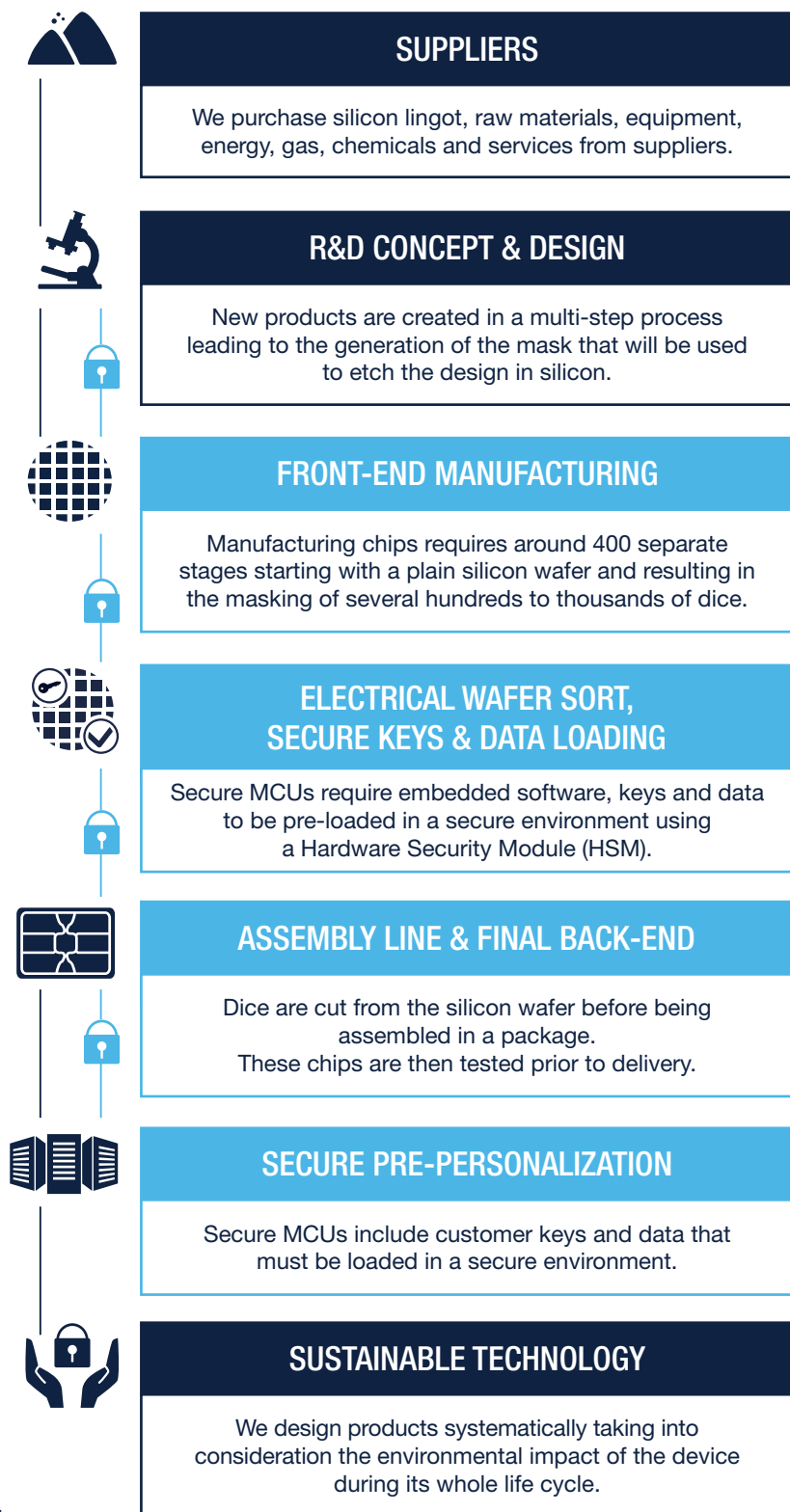
Hardware- & software-certified solutions



Secure environment (development, test, personalization)

Secure solutions our value chain

MAIN ACTIVITIES OF OUR VALUE CHAIN



STANDARDS

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

We are members of the Responsible Minerals Initiative (RMI).

We design, manufacture products and offer pre-personalization services to ensure device compliance with quality, environmental, safety, and security standards and certifications:

- Continuity in the 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 140-2/3 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 (Security Accreditation Scheme for UICC Production) eUICC personalization site certification.

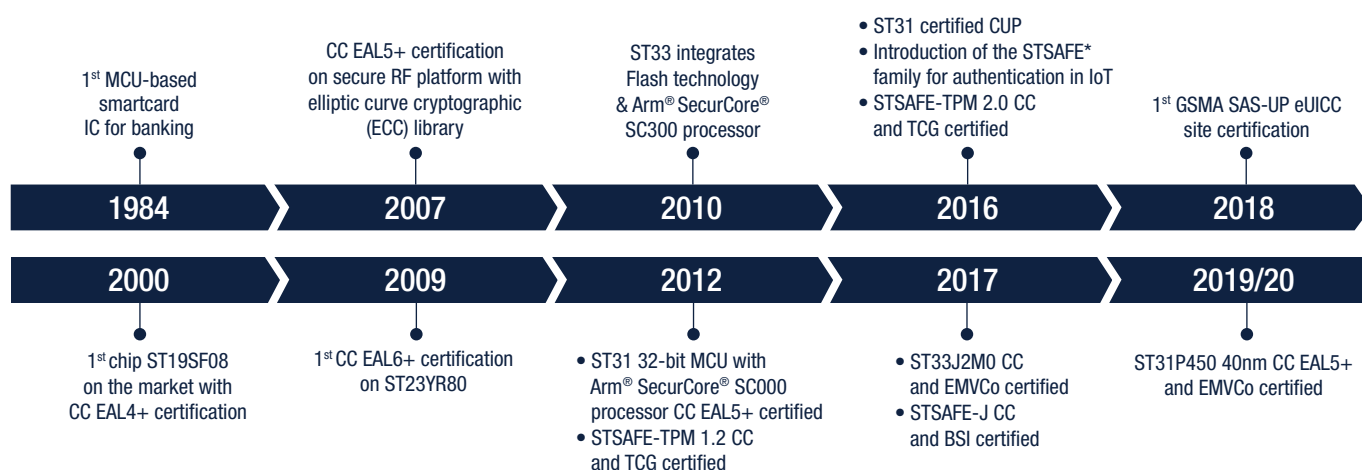


**ST provides secure
end-to-end solutions from
highest security lifecycle**

Secure solutions our offer

CERTIFICATIONS

ST's success is confirmed by its awards and certificates granted by organizations such as EMVCo, Visa, Mastercard, NFC, MTPS, China Union Pay (CUP), FIPS and Common Criteria (CC). On top of that, ST became the first electronic component manufacturer to receive the "GSMA SAS-UP Certification" for eSIM production, demonstrating the highest level of security possible for these types of devices and the flexibility to address all markets.



TECHNOLOGIES

The evolution of the secure market towards IoT, secure automotive, M2M, industrial and 5G applications fosters the development of advanced technology to design solutions in line with the latest requirements. These applications need cost-efficient products with a scalable eNVM cell and a high cycling capability, good retention and low power consumption on a wide temperature range.

40nm eSTM*, best-in-class 40nm Floating Gate Technology

The 40nm eSTM (embedded Select in Trench Memory) is a new embedded non-volatile memory designed, developed and industrialized by ST for general-purpose and secure microcontrollers in embedded applications. Thanks to its unique architecture, the 40nm eSTM cell offers the advantages of a conventional split-gate NVM cell in a smaller area than a typical Flash Memory cell, combined with very good scalability and reliable performance.

- Small cell area with very good scalability for a cost-efficient product
- One of the industry's highest endurance for increased end-product reliability
- Low current leakage technology to target low and ultra-low power applications
- Suitable for many applications: automotive, industrial, consumer, mobile transactions.

Notes

*Is a registered and/or unregistered trademark of STMicroelectronics International NV or its affiliates in the EU and/or elsewhere.

Secure solutions where you find us

SECURING ALL YOUR APPLICATIONS

Secure microcontroller solutions are driven by dynamics based on smartcard technologies, mobile transactions and the connected world. This is why, today, ST is securing all your applications from traditional applications, such as SIM, banking and ID, to the latest ones including contactless transactions and IoT connectivity.

With STSECURE portfolio, ST makes industries, cities, homes, cars and everyday things smarter and more connected in a safer way.



PERSONAL ELECTRONICS

BANKING, ID & TRANSPORT

ST31
STPay

SECURE WEARABLES

ST31
ST54

MOBILE SECURITY CONSUMER

ST33 eSIM, eSE
ST21NFC
ST54



COMPUTER & PERIPHERALS



INDUSTRIAL



AUTOMOTIVE

AUTHENTICATION

STSAFE-A
STSAFE-J
STSAFE-TPM

M2M CONNECTIVITY

ST32, ST32-M
ST33-M
ST4SIM-S / -M

SECURE AUTOMOTIVE

ST33-A
ST33GTPMA
ST4SIM-A

Secure solutions our families

SMARTCARD PACKAGING

Banking, ID and transport products are delivered in multiple packaging solutions thanks to a wide network of partners at global and local levels.

ST's offer allows you to either select a device from our wide range of modules, or benefit from a one-stop shop solution thanks to ST's collaboration with partners who can provide inlays and/or dual-interface modules.

OUR FAMILIES FOR BANKING, ID & TRANSPORT

ST31 for smartcard applications

ST31 hardware platform is designed to support smartcard applications such as banking, identification, PayTV and transport.

- **ST31P450** based on 40nm eSTM technology for faster transactions and a better user experience
- **ST31 for biometric system-on-cards** to enable advanced authentication technology for payment and ID

STPay, ST secure payment solution

Based on ST31 hardware, the STPay family is an independent offer for banking, transport smartcards and wearable payment. It allows card manufacturers to quickly address a variety of markets while saving software development effort and time.

- **STPay dual-interface solutions**
- **STPay contact solutions**
- **STPay for biometry**

OUR FAMILY FOR MOBILE SECURITY

ST33, ST21NFC & ST54 convergence in Mobile

ST provides an exhaustive offer of NFC, eSE and GSMA-certified eSIM products and solutions to address secure mobile transactions applications. Previously offered separately, they are now available as fully integrated solutions combining an NFC controller, eSE and eSIM, thereby enabling new design opportunities.

- **ST33 SIM, eSIM and eSE**
- **ST21NFC NFC Controller**
- **ST54 Integrated eSIM, eSE & NFC**

OUR FAMILY FOR AUTOMOTIVE

ST33-A & ST4SIM-A, the automotive-grade family

As cars become more connected, they are more vulnerable to attacks and ensuring security is increasingly challenging. This is why, based on ST33 hardware, ST offers a scalable portfolio of automotive-grade secure elements and eSIMs solutions dedicated to security and connectivity in the automotive ecosystem.

- **ST33G1M2A hardware**
- **ST33GTPMA SoC for eSE**
- **ST4SIM-A SoC for eSIM**

ST33, THE MULTI-APPLICATION FAMILY

ST33 is one of our main historical secure hardware platforms and can be found in multiple applications. With the latest 32-bit Arm® SecurCore® SC300, it offers a large memory capacity, multiple communication interfaces and certified cryptographic libraries in different form factors (wafers, SIM modules, DFN, WLCSP).

- **Mobile Security: SIM, eSIM & eSE**
- **Industrial & IoT: M2M eSIM & eSE**
- **Automotive: eSE & eSIM**
- **Trusted Computing: TPM solutions**

OUR FAMILIES FOR BRAND PROTECTION, INDUSTRIAL & IOT

STSAFE for authentication

The STSAFE family protects businesses by building secure and trusted embedded systems. STSAFE secure elements address IoT ecosystem products from embedded platforms to gateways and servers.

- **STSAFE-A** for embedded systems and brand protection
- **STSAFE-J** for gateways and IoT devices
- **STSAFE-TPM** for standardized and proven TPM services

ST4SIM for cellular connectivity

From removable SIMs to GSMA-certified eSIMs, ST4SIM is a flexible and scalable offer for cellular connectivity in multiple environments. High-quality and reliable, ST4SIM products are part of a complete ecosystem built with partners specialized in connectivity and subscription management platforms.

- **ST4SIM-S** for IoT
- **ST4SIM-M** for Industrial
- **ST4SIM-A** for Automotive

Smartcard applications

ST31

With over 4 million STSECURE MCUs for banking, ID and transport sold worldwide, ST has a strong expertise and solid references in the smartcard industry.

From traditional smart cards to innovative wearable devices and biometric solutions, ST offers a complete portfolio of contact and dual-interface secure microcontrollers.

The latest ST31 products answer the challenges of contactless applications by creating ultra-small dies thanks to 40nm eSTM technologies and advanced contactless IPs.

Over
4 billion
STSECURE MCUs
embedded in
smartcards



ST31, HIGHLY SECURE MICROCONTROLLERS

The hardware platform for smartcard applications

ST31 hardware platform ensures a proven level of security as it addresses the highest security standards and certifications. With its full range of contact and multiprotocol communication interfaces, you are sure to find the perfect fit for a broad range of smartcard applications.

Product portfolio

ST31P450

- Latest 40nm eSTM technology
- Best-in-class RF performance and low-power design
- Compliant with MIFARE® and Calypso® for transport applications

ST31 for Biometry

- Biometric system-on-card solution
- Development of advanced authentication technology for payment or ID cards with an embedded power management system.

KEY FEATURES

- 32-bit Arm® SecurCore® SC000 CPU
- Enhanced hardware security features
- Multiprotocol (ISO7816, ISO14443 A/B, ISO18092, VHBR)
- EMVCo, CC up to EAL6+ and CUP certified
- MIFARE Plus®, MIFARE Classic® and MIFARE® DESFire® libraries

Learn more at www.st.com/st31

Smartcard applications

STPay



The increasing need for trusted payment transactions has been driving the banking card market towards EMV chip-and-pin solution. Dual-interface cards already represent about half of the worldwide yearly chip-and-pin issuance. Innovative form factors allow the contactless payment functionality to be included in biometric cards and wearable objects, maximizing ease-of-use and user experience. The STPay family offers a comprehensive range of Java OS-based banking solutions, covering a wide range of payment applications.

Ready-to-use

for banking and transport applications

STPAY, ST SECURE PAYMENT SOLUTION

The most extended offer for payment and transport applications

STPay secure payment portfolio is among the best ready-to-use and independent solutions in the industry including all major international and regional payment schemes.

Product portfolio

STPay Dual Interface

- Certified by payment schemes based on reference antennas
- STPay-Topaz-1 with Java platform for flexible applet implementation

STPay Contact

- International schemes White label payment (CPA, ELO)

STPay for Biometry

- Biometric system-on-card solution for payment.

KEY FEATURES

- Multiple international and regional payment schemes (Visa, MasterCard, JCB, American Express, Discover, Interac Flash, CUP, Rupay,...)
- Certified from hardware (EMVCo, CC EAL5+) up to operating system and application software
- Contact and dual interfaces (ISO7816, ISO14443 A/B)
- Compliant with the CPS (Common Personalization Standard)
- Datacard EMV Chip Vendor Program
- Delivered in multiple form factors (wafer, micromodules)

Learn more at www.st.com/stpay

Mobile Security

ST33, ST21NFC, ST54

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 laptops devices.

ST provides an exhaustive offer of NFC and eSE/ eSIM products to address secure mobile transaction applications (secure connectivity, payment, wireless charging, digital car key): from the state-of-the-art ST21NFC to the ST54 integrating the widely deployed ST33.

ST54, the NFC and ST33 eSE & eSIM

integrated
solution for
mobile devices



MOBILE CONVERGENCE, SECURING YOUR APPLICATIONS

Building the most effective and secure mobile solutions

ST54 System-in-Package integrates an NFC controller and an eSE solution, and has reached a new step by merging NFC, eSE and eSIM technologies into ST54J, a single-die solution in a small WLCSP package (Wafer-Level Chip Scale Package).

BoostedNFC for better contactless transactions

ST's boostedNFC technology is ideal for space-constrained applications that require a card emulation function. Advanced analog front-ends, implementing Active Load Modulation technology, guarantee reliable

NFC and contactless transactions in challenging environments or in applications that require a very small antenna.

ST's eSIM leadership

With hundred millions of units sold to date, ST33 positions itself as the industry standard at major OEMs to deploy new eSIM-based devices, taking advantage of a smaller and thinner WLCSP and GSMA-compliant Personalization-on-Wafer industrial flow.

In 2018, ST became the first chip manufacturer to reach the GSMA SAS-UP certification to personalize ST33 eSIMs for mobiles and connected devices, enabling a seamless hardware and software integration at OEMs.

Learn more at www.st.com/sim-esim and www.st.com/secure-nfc

STANDALONE SOLUTIONS

ST33 for eSIM and eSE applications

ST33 secure microcontrollers meet the advanced security and performance requirements for secure applications including embedded SIM and embedded NFC secure elements with a large user Flash memory capability.

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.

ST21NFC for NFC Controller

The growth of contactless mobile transactions is driving the adoption of NFC and 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.

ST21NFCD is ST's fourth generation of NFC controllers with 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.

KEY FEATURES

ST33

- Up to 2 Mbytes Flash
- Delivered in multiple packages (WLCSP, MFF2, DFN8)
- GSMA SAS-UP certified flow
- EMVCo, CC EAL5+, MTPS certified

ST21NFC

- BoostedNFC for tiny and metal cover antenna
- Reduced BOM
- Low power mode
- Card emulation, Reader and P2P

ST54

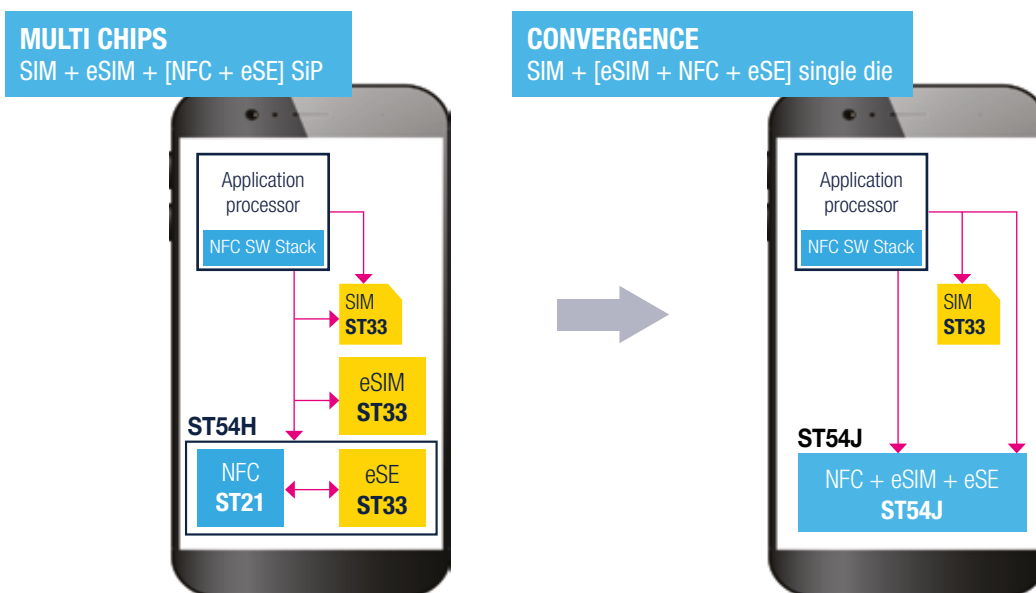
- ST33 eSE, eSIM and ST21NFC
- BGA System-in-Package and WLCSP single-die
- GSMA SAS-UP certified flow
- EMVCo, CC EAL5+, MTPS certified
- MIFARE® and FeliCa®

INTEGRATED SOLUTIONS

ST54H & ST54J

In order to manage the future of secure mobile transactions, ST provides a large range of ST54 integrated solutions. 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 user-friendly and remote mobile provisioning to support multiple operator subscriptions.



Authentication

STSAFE

STSAFE is a secure element product range providing authentication, confidentiality and platform integrity services to protect OEMs against cloning, counterfeiting, malware injection and unauthorized production. In compliance with the most demanding security certifications, STSAFE secure elements come as turnkey solutions through a trusted supply chain with pre-provisioned secrets and certificates, and a set of software libraries and drivers for secure seamless integration.



**Scalable
security
offer**
for brand
protection
and embedded
systems

STSAFE, ENABLING END-TO-END SECURITY

Building secure and trusted systems

ST offers a full range of secure elements addressing multiple applications ranging from embedded platforms to gateways and servers.

Integrated into device design and connected to its processing unit, STSAFE secure elements help authenticate devices, ensure platform integrity and data confidentiality.

Product portfolio

STSAFE-A optimized for embedded systems

STSAFE-A is an optimized solution ensuring strong authentication, secure channel establishment and secure storage for applications exposed to fraud or counterfeiting. These products are key enablers for companies looking to build an ecosystem around their brand.

STSAFE-J flexible with Java platform

STSAFE-J is a flexible solution based on GlobalPlatform®, Java Card™ and dedicated applets. It offers a wide range of secure services which meet the requirements of custom applications.

STSAFE-TPM standardized computing services

STSAFE-TPM is a proven solution offering standardized trusted computing services (ISO / IEC 11889) ideal for Windows or Linux-based platforms. This family is available for consumer, industrial and automotive qualifications.

Learn more at www.st.com/stsafe

STSAFE MAPPING IN MARKET SEGMENTS



CONSUMER
Consumables, accessories,
printers, computers



INDUSTRIAL
Environmental sensors, actuators,
factory automation



INFRASTRUCTURE
Gateway, base station,
utilities

STSAFE-A Optimized
Tuned for brand protection and secure connection

STSAFE-J Flexible
Flexible Java™ platform with optional default applet

STSAFE-TPM Standardized
TCG standardized platform for trusted computing and crypto services

STSAFE-A110 ECOSYSTEM FOR SEAMLESS SECURITY

STSAFE-A110 is the latest STSAFE-A secure element with state-of-the-art security features that prevent the counterfeiting of genuine peripherals and IoT devices. Its ecosystem contains a complete set of tools for seamless integration:

- ODE STM32 Expansion board (X-NUCLEO-SAFEA1)
- STM32 Cube development ecosystem (X-CUBE-SAFEA1 software package)
- Pre-personalized STSAFE-A110 for secure key provisioning
- Arduino™ interfaces, drivers and source code examples.

Order your X-NUCLEO-SAFEA1 online at www.st.com/stsafe-a110

KEY FEATURES

- Secure TLS session establishment
- State-of-the-art security relying on a CC EAL5+ hardware
- USB Type-C standard and LPWAN authentication compliant
- Secure personalization according to customer needs



STSAFE-A110 packages



X-NUCLEO-SAFEA1

STPM4RasPI TPM expansion board



KEY FEATURES

- Measured boot and platform integrity
- Authentication and secure storage
- Cryptographic toolbox
- Firmware upgradable
- Linux ecosystem availability
- CC EAL4+, TCG and FIPS 140-2 certified
- Available in multiple packages (QFN32, WLCSP, TSSOP20)

STSAFE-TPM TRUSTED SOLUTION ENVIRONMENT

STSAFE-TPM is a TPM certified product family qualified to operate under an extended temperature range. A full development kit is available to offer easy integration.

- Expansion board (STPM4RasPI) for Raspberry Pi® and STM32MP1 available for both SPI and I²C interfaces
- Software package with driver and utilities (communication driver and firmware upgrade)
- Smooth system integration thanks to open source TPM software stacks and ST Partner network.

More information at www.st.com/stsafe-tpm

M2M Connectivity

ST4SIM

Cellular connectivity is a key enabler of connected devices. Leading to a greater diversity of smart objects, it paves the way to new market opportunities.

In order to answer market needs, ST offers a tailored, diversified connectivity portfolio with ST4SIM solutions, a wide range of SIMs and eSIMs compatible with IoT, industrial- and automotive-grade applications.

The ST4SIM product family is part of a complete ecosystem, built with trusted partners that provide and operate device-onboarding and service-provisioning platforms.

SIM
& **eSIM**
for cellular connectivity in industrial & automotive applications



ST4SIM, CONNECTING EVERYTHING EVERYWHERE

Always connected, always under control with SIM & eSIM

ST4SIM portfolio of SIMs and eSIMs is based on basic, cryptographic and GSMA SGP.02 configurations. Our solutions allow devices to be connected at all times and everywhere, while ensuring asset security. They simplify use cases such as remote condition monitoring and predictive maintenance as well as connected-driving services like emergency assistance.

Product portfolio

ST4SIM-S for IoT

- Basic & Crypto SIM/eSIM
- Configurable and customizable

ST4SIM-M for Industrial

- Basic, Crypto & GSMA SIM/eSIM
- Industrial-grade (JEDEC JESD47)

ST4SIM-A for Automotive

- Crypto & GSMA eSIM
- Automotive-grade (AEC-Q100 grade 2).

KEY FEATURES

- Scalable offer from removable SIM to GSMA-certified eSIM
- Java Card OS / Global Platform compliant
- Connectivity and platforms from a large panel of trusted partners
- High-quality and reliable ready-to-use solutions
- Delivered in multiple form factors (Card plug-in, MFF2, WLCSP, TSSOP20)

Learn more at www.st.com/st4sim

Secure Automotive ST33-A, ST4SIM-A

Around 80% of all innovations in the automotive industry today are directly or indirectly enabled by electronics.

With the growth of connected cars and the automotive industry's roadmap towards autonomous driving, secure microcontrollers are embedded in vehicle telematics, gateways and ECUs (electronic control units).

With security at the heart of these trends, ST is committed to the development of secure solutions to cover the requirements for the new era of digital technologies.

**Securing
gateways
& telematics**
for safer driving



ST33-A & ST4SIM-A, CONNECTING & SECURING CARS

Secure solutions embedded in the automotive ecosystem

Secure elements and embedded SIMs in connected vehicles are developed to fight against service and network access corruption, device cloning, counterfeiting and data eavesdropping and corruption. They cover main V2X and in-car functions (software upgrade, ADAS, platform integrity, secure data storage,...) to guarantee passenger safety, vehicle behavior and data privacy.

Product portfolio

ST33G1M2A HW for eSE and eSIM

- Ensuring on-board security in gateways, immobilizers and telematics
- AEC-Q100 and CC EAL5+ certified

ST33GTPMA SoC for eSE

- Ensuring platform integrity
- Based on latest TPM 2.0 firmware
- FIPS 140-2 and CC EAL4+ certified

KEY FEATURES

- Scalable offer from hardware to ready-to-use solutions
- Automotive-grade solutions
- Robust and reliable products

ST4SIM-A SoC for eSIM

- Based on ST33G1M2A HW compliant with GSMA SGP.02 specification
- Complete solution for in-car connectivity
- Ideal for eCall devices (emergency calls).

Learn more at www.st.com/secure-auto

life.augmented



Order code: BRSMCU0620

For more information on ST products and solutions, visit www.st.com

© STMicroelectronics - June 2020 - Printed in United Kingdom - All rights reserved
ST and ST logo are trademarks or registered trademarks of STMicroelectronics International NV or its affiliates in the EU and/or other countries. For additional information about ST trademarks, please refer to www.st.com/trademarks.

All other product or service names are the property of their respective owners.
MIFARE, MIFARE DESFire and MIFARE Plus are trademarks of NXP B.V and are used under license.



life.augmented