life.augmented

Authentication & IoT secure solutions

STSECURE

Consumer & Industrial market segments

Hardened security your product and business

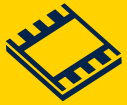
Consumables, printers, accessories,
computers, connected objects

Environmental sensors, actuators, factory automation,
Gateway, base station, utilities

life.augmented

Threats and countermeasures

Threats	Security services	Benefits
Device cloning or counterfeiting	• Authentication, unique ID • Secure communication • Platform integrity • Usage monitoring • Secure storage	Brand protection
Device integrity or Data corruption		Trusted Device
Loss of confidential information		Privacy



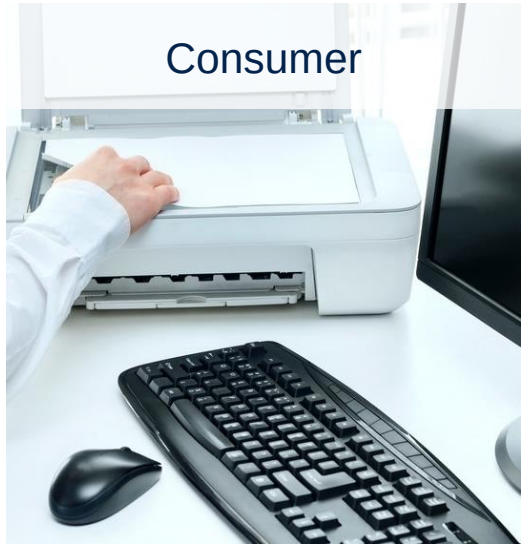
- EAL5+ CC certified secure MCU
- Secure operating system, secure handling of cryptographic keys

- Customer secure keys and certificates loading at ST in a security certified environment

life.augmented

STSAFE* solution overview

A scalable secure solution for consumer & industrial devices



STSAFE

- Developed to ensure devices authentication, platform integrity, data confidentiality and availability
- Scalable STSAFE family from optimized to flexible and standardized TPM solutions
- Based on proven CC EAL5+ hardware Secure Element
- Provided within a complete ecosystem
- With in-house pre-personalized secrets and certificates

life.augmented

STSAFE* mapping in market segments

Consumables, accessories, printers, computers

Sensors, actuators, factory automation

Gateways, base stations, utilities

Optimized (**STSAFE-A**)

Tuned for brand protection and secure connection

Flexible (**STSAFE-J**)

Flexible Java™ platform

Standardized (**STSAFE-TPM**)

TCG-standardized platform

life.augmented

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

STSAFE* family secure element

Security-certified solutions from IoT nodes to IoT infrastructure

HW CERTIFIED CC EAL5+

Optimized

STSAFE-A

- Fixed features set:
  - Authentication
  - Secure connection establishment
  - Secure storage
  - LPWAN LoRa / Sigfox compliant
- Personalization services
- Seamless integration with STM32 ODE package

CERTIFIED CC EAL5+, BSI

Flexible

STSAFE-J

- Javacard-based OS
- Applet specific features set:
  - Authentication
  - Secure connection establishment
  - Secure storage
- Personalization services
- Linux-based MPU Development kit

CERTIFIED CC EAL4+, TCG 2.0, FIPS140-2

Standardized

STSAFE-TPM

- Platform integrity
  - Secure Boot
  - Secure Firmware upgrade
- Trusted network access
- Secure storage
- Linux-based MPU Development kit

life.augmented

Secure your design with STSAFE-A110

STSAFE-**A110**

Secure Authentication

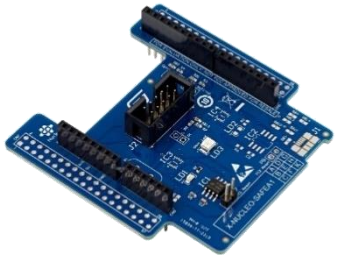
Unique ID

Authentication

Ecosystem

X-NUCLEO-SAFEA1

X-CUBE-SAFEA1



Secure Provisioning

Customer credentials

LPWAN, USB Type-C,
QI charging

Cloud Attachment

AWS, AZURE

aws

Microsoft Azure

STSAFE-A110

Secure Element for Brand Protection & IoT

Protect your brand
consumables / peripherals

Secure the connected devices
IoT nodes / gateways

- Authentication with personalized certificate
- Secure connection establishment (TLS)
- Secure data storage
- Signature verification
- EAL5+ Common Criteria certified

Available @ distribution www.st.com/STSAFE-A

STSAFE-A110
Enriched secure connection & LPWAN

- Customer certificate & keys personalization at ST secure factory
- **Seamless integration** with GP MCU
  - **STM32 ODE Nucleo** expansion board
  - **STM32Cube** Software package

STM32 Open Development Environment

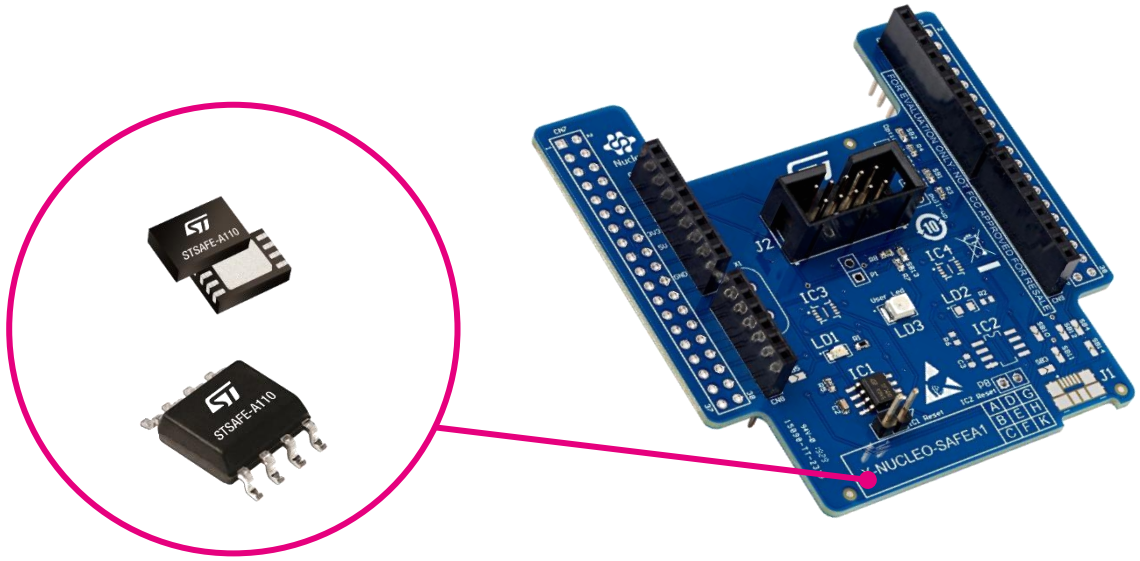
STM32 Cube

STSECURE

life.augmented

STSAFE-A110 evaluation tools

Complete set of tools for a seamless integration



- ODE STM32 expansion board
- Pre-personalized STSAFE-A110
- Arduino™ interface
- STM32 Cube development ecosystem
- Drivers and examples source codes

STSAFE-J

Flexible Java Card platform solution

ST generic or customer specific applet

Secure the connected devices
IoT nodes / Connected equipment / Gateways

Java 3.0.4, GP 2.1.1, HW CC EAL5+ certified

Generic ST applet:

- Authentication
- Secure connection
- Secure data storage
- Personalization service

Customer specific applet

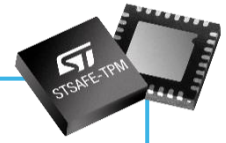
STSAFE-J110

- STSAFE-J100 JavaCard OS for customer-specific applet
- STSAFE-J100 with Spinel generic applet
- Arduino-compliant expansion board
- PKCS11 Software package (driver and code examples)

life.augmented

STSAFE-TPM

Expanding standardized trust from personal computing to connected devices



Ensure platform integrity
computer, connected devices

Secure the connected devices
IoT nodes / gateways

- TCG TPM 1.2 and TPM 2.0 rev1.38
- Available in consumer, automotive and industrial qualifications
- Upgradable firmware
- Linux Open source ecosystem (driver, Software stacks, Linux open source)
- Provisioning service
- Common criteria EAL4+ & FIPS 140-2 level 2 certified

Available

ST33TPHF20/2E

- Consumer equipment
- 2E: TCG TPM 1.2 / TPM 2.0
- 20: TCG TPM 2.0

Available

ST33TPHF2X

- Consumer equipment
- TCG TPM 2.0
- Extended cryptography
- Enhanced security support

Available

ST33GTPMA

- Automotive environment (AEC-Q100)
- TCG TPM 2.0
- Enhanced cryptography
- Enhanced security support

Available

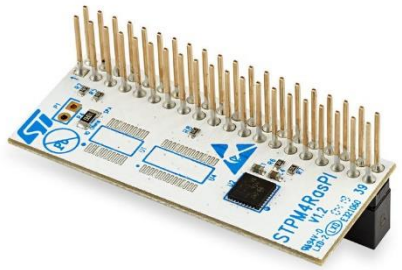
ST33GTPMI

- Industrial environment (JEDEC)
- TCG TPM 2.0
- Enhanced cryptography
- Enhanced security support

life.augmented

STSAFE-TPM expansion board

For seamless integration



Raspberry PI ® & STM4RasPI expansion board

- STPM4RasPI expansion board for Raspberry PI ® and STM32-MP1
  (I²C, SPI TPM compatible serial interface / 40-pin female connector)
- Software package with driver and examples
  (ST Drivers SPI & I²C, Plug & Play 3rd party TPM Software Stacks)
- Databrief on st.com

life.augmented

Consumer & Industrial authentication takeaways

- Product family covering end-to-end security
- STSAFE-A & STSAFE-TPM full ecosystem available
- In-house personalization services

Learn more at www.st.com/stsafe

life.augmented

Our technology starts with You

Find out more at www.st.com/stsafe

life.augmented