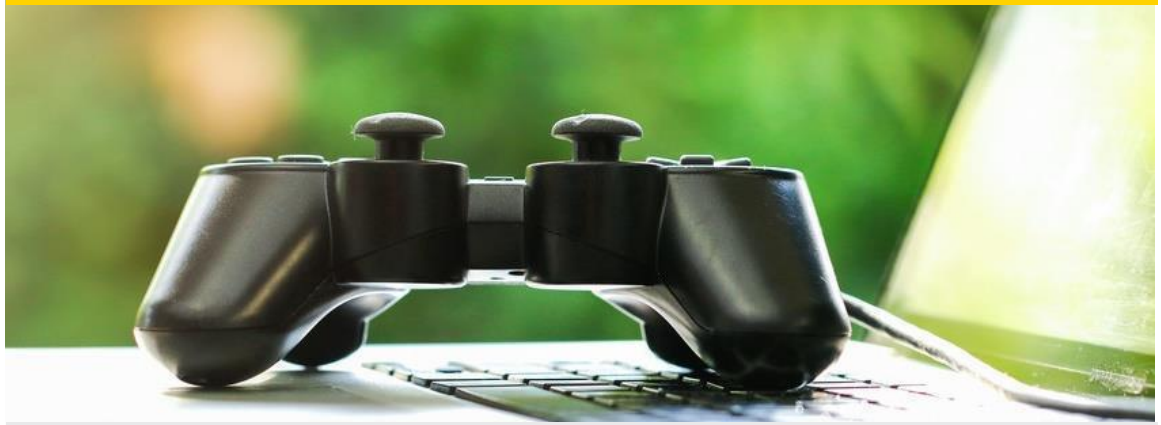
life.augmented

Secure authentication solutions for consumer & industrial

STSECURE

Consumer & Industrial market segments
Security hardening

Consumer



- Consumables, printers
- Various consumer goods and accessories
- Batteries
- Qi wireless chargers
- EV chargers
- Connected objects

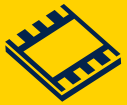
Industrial & infrastructure

- Factory automation
- Environmental sensors, actuators
- 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

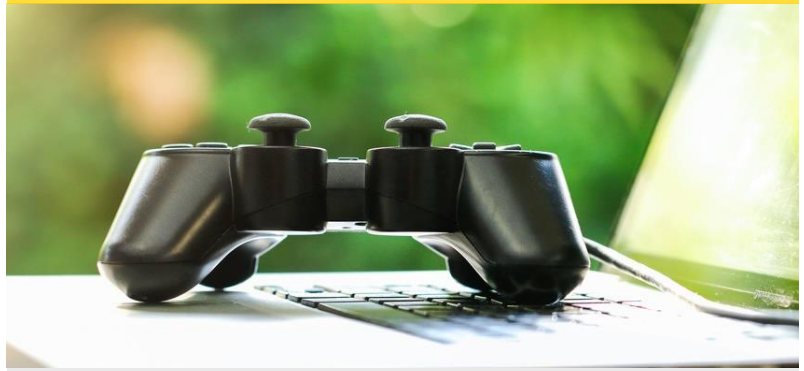
A scalable secure solution for consumer & industrial devices

- 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 market segments

Consumer



Consumables, printers, computers

Industrial

Sensors, actuators, factory automation

Infrastructure

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

STSAFE family

Certified security solutions from nodes to infrastructure

STSAFE-A
Optimized

- Fixed features set:
  - Authentication
  - Secure connection establishment
  - Secure storage
- Personalization services
- Seamless integration with STM32 ODE package
- HW CC EAL5+ certified

STSAFE-J
Flexible

- JavaCard™-based OS
- Applet specific features set:
  - Authentication
  - Secure connection establishment
  - Secure storage
- Personalization services
- HW CC EAL5+ certified

STSAFE-TPM
Standardized

- Platform integrity
  - Secure Boot
  - Secure Firmware upgrade
- Trusted network access
- Secure storage
- Linux-based MPU Development kit
- SoC CC EAL4+, TCG 2.0, FIPS140-2 certified

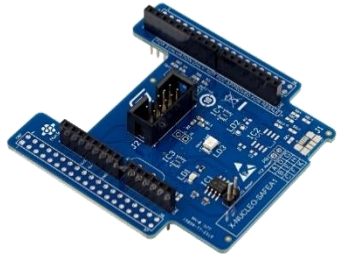
life.augmented

STSAFE-A110 services

Secure authentication

- Unique ID
- Authentication with asymmetric cryptography
- Attestation based on X509 certificates

Ecosystem



- X-NUCLEO-SAFEA1
- X-CUBE-SAFEA1

Secure Provisioning

- Customer certificates
- WPC 1.3 QI charging

Cloud Attachment

- Amazon Web service
- Microsoft Azure
- Private Clouds

life.augmented

STSAFE-A110 overview

Secure solution for brand protection & connected devices

Optimized and certified

Provisioning services

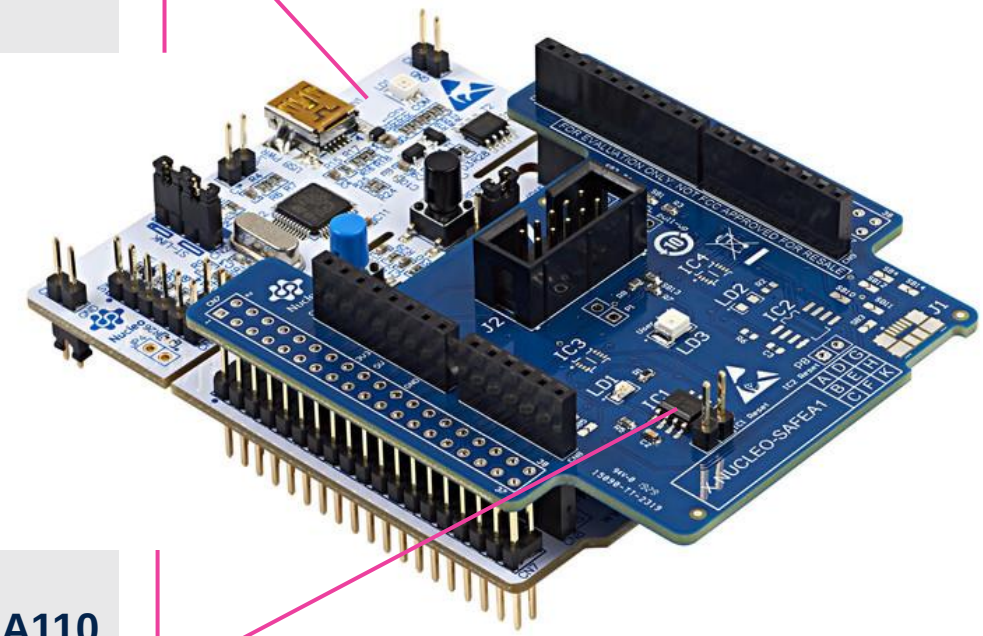
Seamless integration

- Strong authentication
- Secure channel establishment (TLS)
- Signature verification
- Decrement counter
- Secure data storage
- Amazon AWS JIT and Microsoft Azure DPS device enrollment
- WPC 1.3 Qi authentication compliant
- Based on CC EAL5+ platform

life.augmented

STSAFE-A110 evaluation tools & software

STM32 Nucleo board



STSAFE-A110

[X-NUCLEO-SAFEA1](#)

- ODE STM32 expansion board
- Pre-personalized STSAFE-A110
- Arduino™ interface

- A complete software package STM32 cube compliant
  - [X-CUBE-SAFEA1](#)
  - [STSW-SAFEA1-MW](#)
- An openSSL security stack
  - [STSW-STSA110-SSL](#)

life.augmented

STSAFE-J overview

A secure platform for industrial devices and infrastructure

Flexible and certified

Provisioning services

Complete ecosystem

- Java based platform Java 3.0.4, GP 2.1.1, HW CC EAL5+ certified
- A Java Card™ applet for
  - Authentication
  - Secure connection
  - Secure data storage
  - Personalization service
- Customer specific applet
- Arduino-compliant expansion board
- PKCS11 Software package
  (driver and code examples)

life.augmented

STSAFE-TPM overview

Expanding standardized trust from personal computing to connected devices

Standardized & certified

Provisioning

Complete ecosystem

- Ensure platform integrity
- Secure connected devices
- TPM 2.0 r1.38 or r1.59
- 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

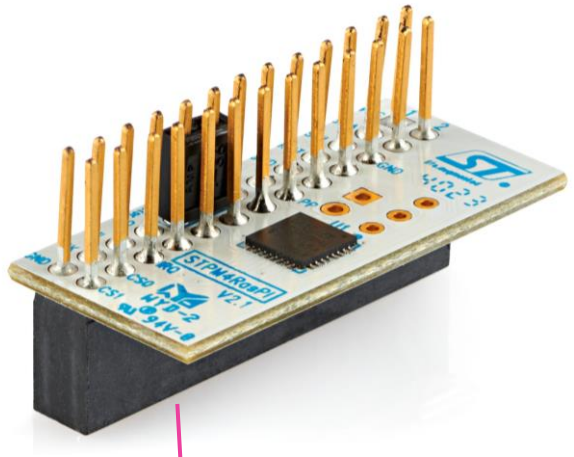
life.augmented

STSAFE-TPM evaluation tools & software

new STPM4RasPIV21 dedicated for ST33KTPM family

- **STPM4RasPIV21** expansion board for Raspberry PI® and STM32 microprocessor with **Consumer & Industrial** TPM supporting I2C or SPI interfaces

- Application notes, software drivers
  - ST Github / STSAFE-TPM
  - TPM Linux integration application note (AN5714)
- Board databrief
  - STPM4RasPiV21



STSAFE-TPM
Consumer & Industrial
(ST33KTPM2X, ST33KTPM2XSPI, ST33KTPM2I)

life.augmented

STSAFE solution takeaways

Product family addressing end-to-end security

STSAFE-A & STSAFE-TPM offer a comprehensive ecosystem

In-house personalization services

life.augmented

Our technology starts with You

Find out more at www.st.com/stsafe

life.augmented