



life.augmented

# Secure authentication solutions for consumer & industrial



# Consumer & Industrial market segments

## Hardened security your product and business

### Consumer





- Consumables, printers
- Accessories
- Batteries
- Computers
- Connected objects

### Industrial & Infrastructure



- Factory automation
- Environmental sensors, actuators
- Gateway, base station
- Utilities

# Threats and countermeasures

Threats	Security services	Benefits
Device cloning or counterfeiting	<ul style="list-style-type: none"><li>• Authentication, unique ID</li><li>• Secure communication</li><li>• Platform integrity</li><li>• Usage monitoring</li><li>• Secure storage</li></ul>	Brand protection
Device integrity or Data corruption		Trusted Device
Loss of confidential information		Privacy
 <ul style="list-style-type: none"><li>• EAL5+ CC certified secure MCU</li><li>• Secure operating system, secure handling of cryptographic keys</li></ul>  <ul style="list-style-type: none"><li>• Customer secure keys and certificates loading at ST in a security certified environment</li></ul>		

# 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



# STSAFE mapping in market segments

## Consumer



Consumables, printers, computers

### Optimized (STSAFE-A)

Tuned for brand protection and secure connection

## Industrial



Sensors, actuators, factory automation

### Flexible (STSAFE-J)

Flexible Java™ platform

## Infrastructure



Gateways, base stations, utilities

### Standardized (STSAFE-TPM)

TCG-standardized platform

# STSAFE family

Certified security solutions from nodes to infrastructure

## STSAFE-A Optimized

- Fixed features set:
  - Authentication
  - Secure connection establishment
  - Secure storage
  - LPWAN LoRa / Sigfox compliant
- 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

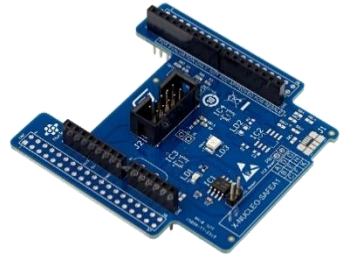
# STSAFE-A110 services

## Secure Authentication



- Unique ID
- Authentication

## Ecosystem



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

## Secure Provisioning



- Customer credentials
- LPWAN
- USB Type-C Power Delivery
- WPC 1.3 Qi charging

## Cloud Attachment



- Amazon Web service
- Microsoft Azure
- Private Cloud

# STSAFE-A110 overview

## Secure solution for Brand Protection & connected devices

Optimized and certified

Provisioning services

Seamless integration

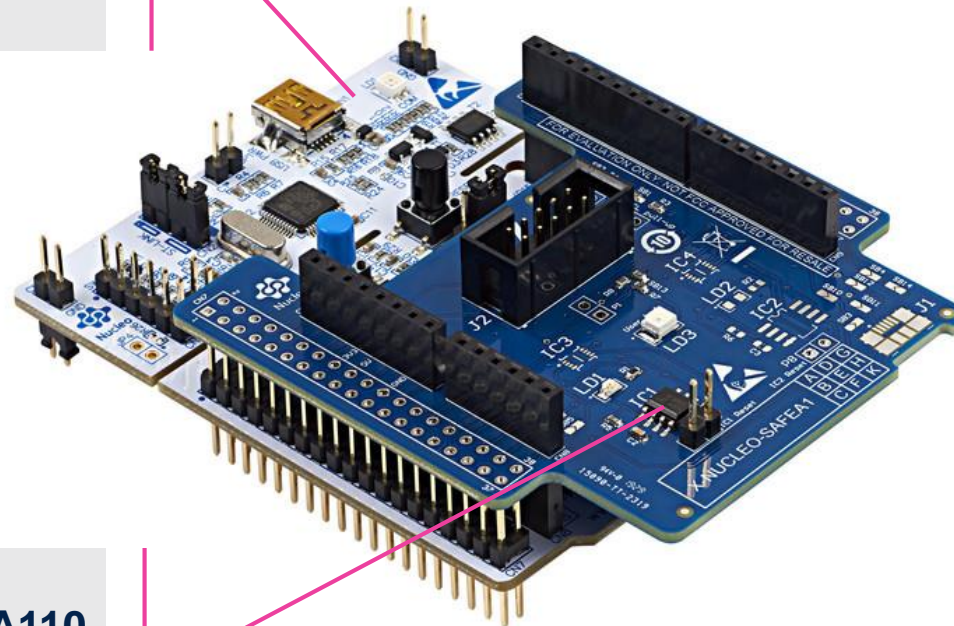
- Strong authentication (USB-C and Qi compliant)
- Secure channel establishment (TLS)
- Signature verification
- Decrement counter
- Secure data storage
- Amazon AWS JIT and Microsoft Azure DPS device enrollment
- WPC 1.3 Qi authentication-compliant
- LoRa- and Sigfox-compliant
- Based on CC EAL5+ platform





# STSAFE-A110 evaluation tools & software

STM32 Nucleo board



STSAFE-A110

## [X-NUCLEO-SAFE1](#)

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

- A complete software package STM32 cube compliant

- [X-CUBE-SAFE1](#)
- [STSW-SAFE1-MW](#)

- An openSSL security stack
  - [STSW-STSA110-SSL](#)



# 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 Javacard applet for
  - Authentication
  - Secure connection
  - Secure data storage
  - Personalization services
- Customer specific applet
- Arduino-compliant expansion board
- PKCS11 Software package (driver and code examples)

# STSAFE-TPM overview

## Expanding standardized trust from personal computing to connected devices



Standardized & certified

Provisioning

Complete ecosystem

- Ensures platform integrity
- Secure connected devices
- TCG TPM 1.2 and 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

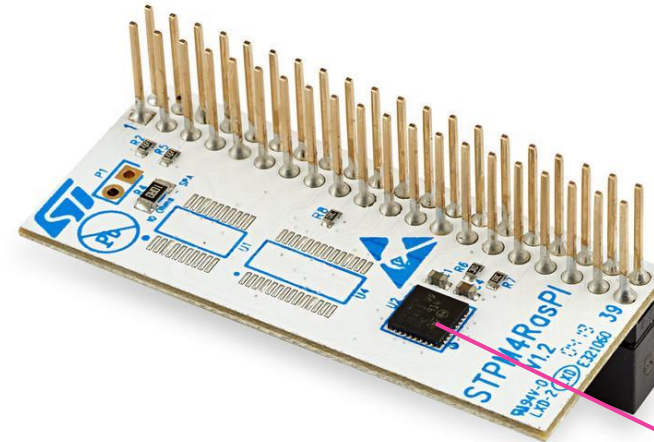


# STSAFE-TPM evaluation tools & software

## STPM4RasPI

- **STPM4RasPI** expansion board for Raspberry PI<sup>®</sup> and STM32-MP1 with I<sup>2</sup>C, SPI TPM compatible serial interface

- TPM Linux integration application note
  - [AN5714](#)
- ST Github Linux I<sup>2</sup>C driver TCG-compliant
  - [TCG-TPM-I2C-DRV](#)
- Software user guide
  - [STPM4RasPi databrief](#)



Raspberry PI<sup>®</sup>  
40-pin connector

STSAFE-TPM  
(ST33TPHFxx)

# STSAFE solution takeaways



Product family addressing end-to-end security

STSAFE-A & STSAFE-TPM offer a comprehensive ecosystem

In-house personalization services

# Our technology starts with You



Find out more at [www.st.com/stsafe](http://www.st.com/stsafe)

© STMicroelectronics - All rights reserved.

ST logo is a trademark or a registered trademark 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](http://www.st.com/trademarks).

All other product or service names are the property of their respective owners.



life.augmented