



life.augmented

Authentication & IoT secure solutions



Authentication market segments

Hardened security for a wide application range



Consumables, accessories
printer, computer

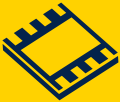



Environmental sensors, actuators,
factory automation



Gateway, base station,
utilities

Authentication threats and countermeasures

Threats	Security services	Benefits
Device cloning or counterfeiting	<ul style="list-style-type: none">• 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
	 <ul style="list-style-type: none">• EAL5+ CC certified secure MCU  <ul style="list-style-type: none">• Secure operating system, secure handling of cryptographic keys• Customer secure keys and certificates loading at ST in a security certified environment	

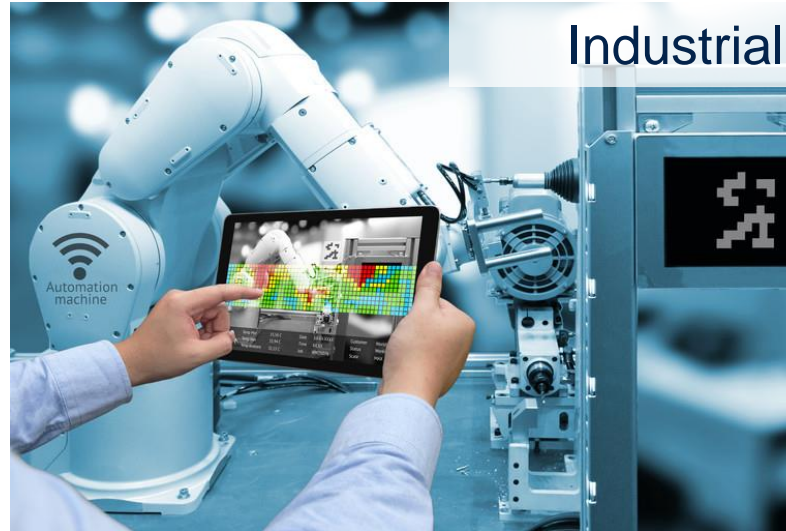
STSAFE* mapping in market segments

Consumer



Consumables, accessories
printers, computers

Industrial



Environmental 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 with optional default applet

Standardized (STSAFE-TPM)

TCG-standardized platform for trusted computing and crypto services

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

Secure your design with STSAFE-A110

STSAFE-A110

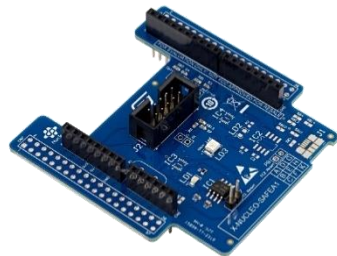
Secure Authentication

Unique ID
Authentication



STM32 Open Development Platform

X-NUCLEO-SAFEA1
X-CUBE-SAFEA1



Secure Provisioning

Customer credentials
LPWAN, USB Type-C,
Qi charging



Cloud Attachment

AWS, AZURE



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



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, CC EAL5+ certified platform

Generic ST applet:

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

Customer specific applet

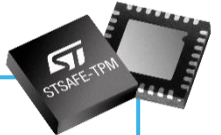
STSAFE-J100



- 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)

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

Under development

ST33GTPMI

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

Authentication takeaways

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

Thank you

© 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.

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



life.augmented