



life.augmented

# Certified IC solution for security, STSAFE™ family & ecosystem

STMicroelectronics

조경민 차장

[stsafe-korea@st.com](mailto:stsafe-korea@st.com)



# Agenda

#1 STSAFE product portfolio

#2 STSAFE-A110 evaluation demo

#3 STSAFE-A Smart city demo

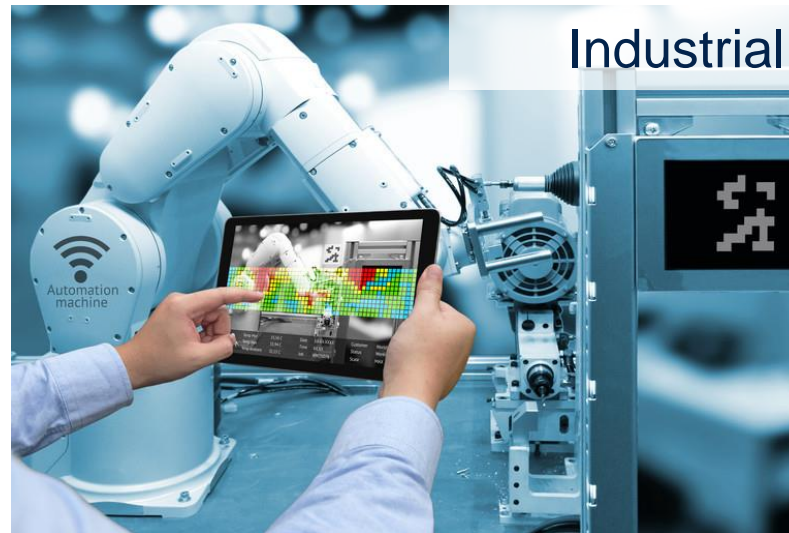
# Authentication market segments

Hardened security for a wide application range



Consumer

Consumables, accessories  
printer, computer



Industrial

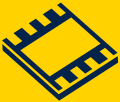

Environmental sensors, actuators,  
factory automation



Infrastructure

Gateway, base station,  
utilities

# Authentication 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™ mapping in market segments



Consumables, accessories  
printer, computer



Environmental sensors, actuators,  
factory automation



Gateway, base station,  
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 of Secure Element

## Security certified solutions

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+

### Flexible

#### STSAFE-J

- Javacard based OS
- Applets 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

- Measured Boot & Platform integrity
- Authentication & Secure storage
- Cryptographic toolbox
- Firmware upgradable
- Linux ecosystem availability
- Linux based MPU Development kit
- Third Party Partners for integration

# Secure your design with STSAFE-A110

## STSAFE-A110

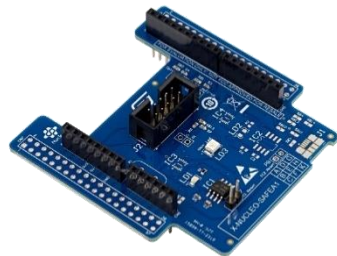
### Secure Authentication

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
- Secure connection establishment (TLS)
- Secure data storage
- Signature verification
- Personalization @ ST factory
- EAL5+ Common Criteria certified

Samples and STM32 Nucleo expansion board available @ distribution [www.st.com/STSAFE-A](http://www.st.com/STSAFE-A)

## STSAFE-A110

Enriched secure connection & LPWAN

- Customer certificate & keys personalization in an ST secure environment
- **Seamless integration** with **STM32 Nucleo** Expansion board and **CUBE** Software package

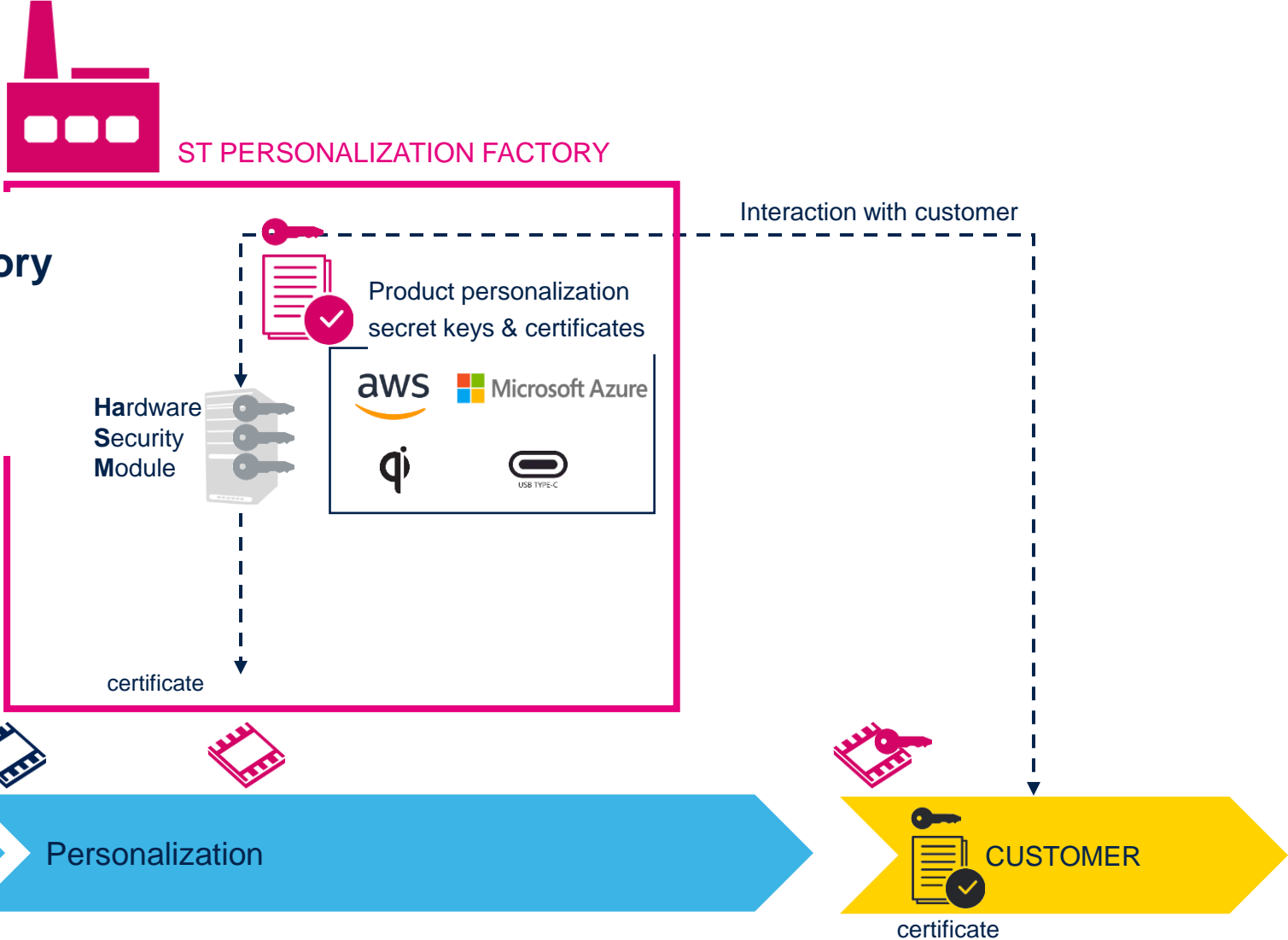




# STSAFE-A secure provisioning

Personalization @ST secure factory available

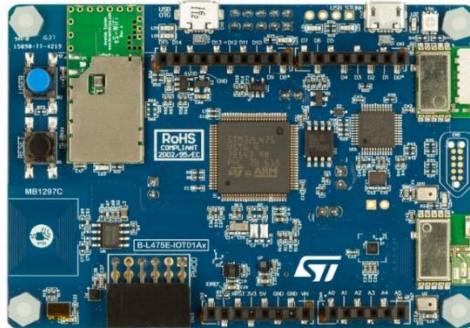
Cloud zero-touch provisioning



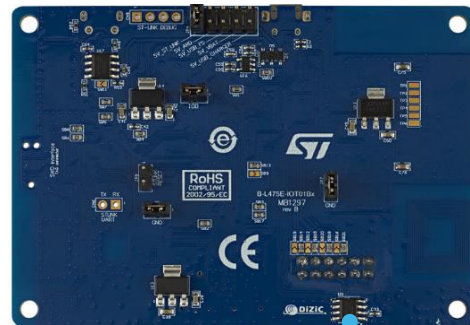
# Secure solution for AWS cloud

## Zero touch provisioning & registration to Amazon Web Services

STM32 B-L475 Discovery board



Recto



Verso

STSAFE-A110

Device by device registration with STSAFE-A110 standard personalization

STSAFE-A110 pre-attachment (Just In Time) to the AWS cloud  
Devices Registration by batch, no need device by device registration

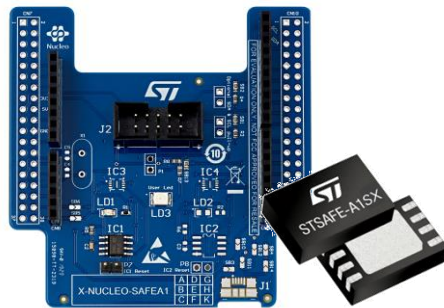
STSAFE-A110 secure TLS connection establishment

## Secured by STSAFE-A1SX



X-NUCLEO-S2868A1  
X-NUCLEO-S2915A

STSAFE-A optimized  
secure element



X-NUCLEO-STSAFE-A1SX

Ease Sigfox IoT device manufacturing

STSAFE-A1SX is preloaded with Sigfox IDs and network keys. No extra configuration required at manufacturing time

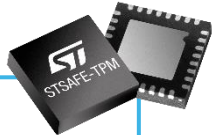
Secure Sigfox data exchanges

STSAFE-A1SX authenticates and encrypts (optional) Sigfox payloads

Ease your IoT devices developments

STSAFE-A1SX along with its driver is certified by Sigfox

## 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

# STSAFE-TPM products – Key benefits

A wide offer range for a variety of uses cases

## ST33TPHF2E

- ST33TPHF2E: support of TPM 2.0 and TPM 1.2 for legacy systems

## ST33TPHF20

- ST33TPHF20: support of TPM 2.0 and 110kB Non-volatile memory for specific use cases (Biometric)

### Common Key Features

- Support of extended cryptography for long lifecycle devices (ECC384, SHA2-384, SHA3, AES 256)
- Fault tolerant firmware upgrade without reduced mode
- TPM firmware and critical data self recovery (NIST SP800-193)
- Resistant to high potential attacks (AVA\_VAN.5)
- Available with SPI or I<sup>2</sup>C interface
- Temperature range -40°C/+105°C

## ST33TPHF2X

Available

- Consumer qualification – Available in QFN32 package

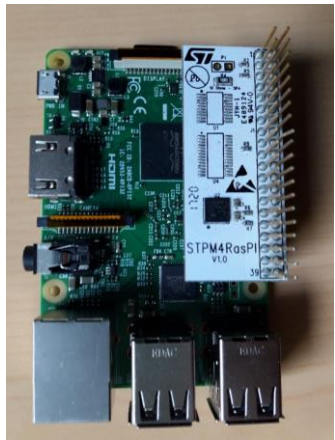
## ST33GTPMA

Available

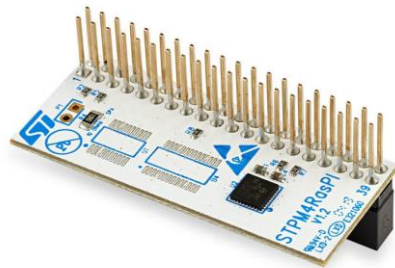
- AEC-Q100 qualification - Available in TSSOP20 package

# STSAFE-TPM expansion board

For a seamless integration



Raspberry Pi® & STM4RasPI expansion board



- STPM4RasPI expansion board for Raspberry PI® and STM32-MP1 (I<sup>2</sup>C, SPI TPM compatible serial interface / 40-pin female connector)
- Software package with driver and examples (ST Drivers SPI & I<sup>2</sup>C, Plug & Play 3rd party TPM Software Stacks)
- [STPM4RAasPI Databrief](#) available on st.com

# STSAFE-A110 evaluation demo

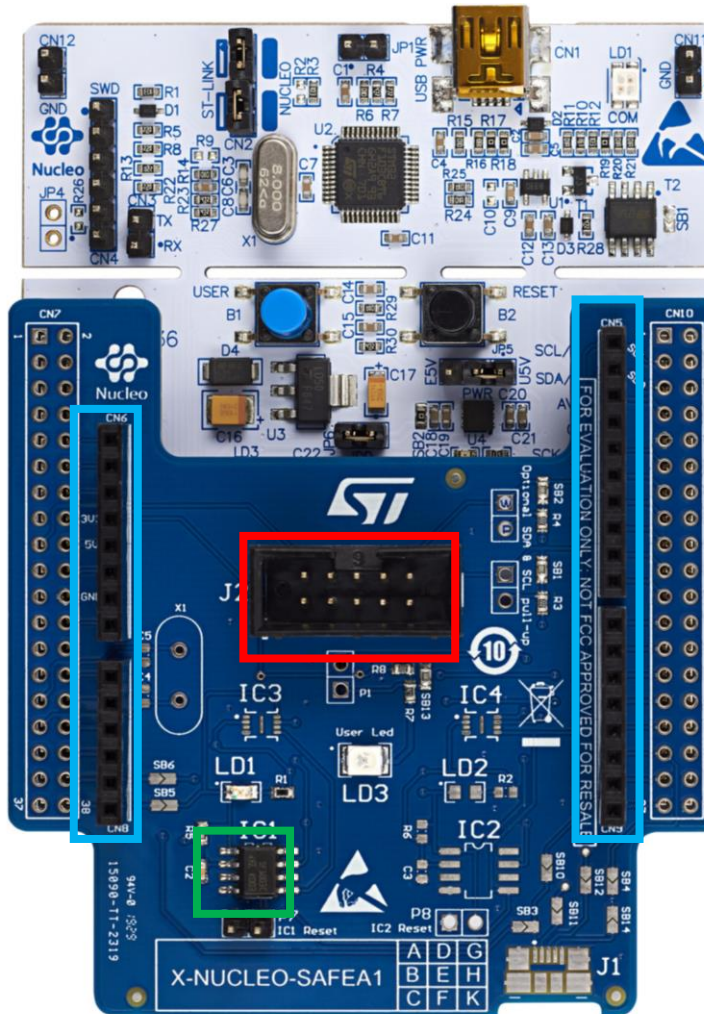
# H/W tool




- NUCLEO-L476RG

- <https://www.st.com/en/evaluation-tools/nucleo-l476rg.html>

- X-NUCLEO-SAFEA1

- On-board STSAFE-A110 customized with a standard evaluation profile
- HE10 extension connector to mount additional STSAFE devices
- Arduino UNO R3 connector
- Free drivers, middleware and software samples compatible with the STM32 ODE
- More information:
  - <https://www.st.com/en/ecosystems/x-nucleo-safea1.html>
  - [https://www.st.com/resource/en/data\\_brief/x-nucleo-safea1.pdf](https://www.st.com/resource/en/data_brief/x-nucleo-safea1.pdf)



-  Arduino connector
-  HE10 connector
-  STSAFE-A SO8N



# S/W tool #1 STM32CubeIDE

- Advanced C/C++ development platform with peripheral configuration, code generation, code compilation, and debug features for STM32
- IDE to build & run X-CUBE-SAFEA1 sample projects
- More info & download
  - <https://www.st.com/en/development-tools/stm32cubeide.html>
  - [https://www.st.com/resource/en/data\\_brief/stm32cubeide.pdf](https://www.st.com/resource/en/data_brief/stm32cubeide.pdf)

STM32CubeIDE  
All-in-one STM32 development tool

TrueSTUDIO<sup>®</sup> for STM32



+

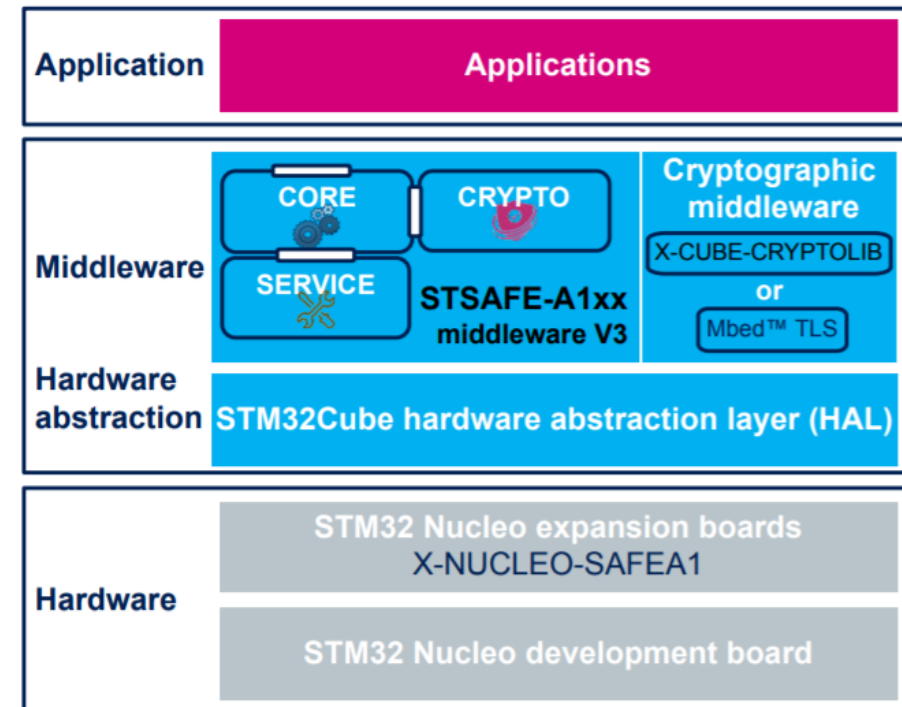


# S/W tool #2

## X-CUBE-SAFE1



- STSAFE-A110 software package
  - STSAFE-A110 middleware application programming interface
  - Embedded sample demonstrations provided
  - Support for NUCLEO-L476RG and X-NUCLEO-SAFE1 boards
  - STM32L4 Series HAL driver (STM32Cube)
  - More information:
    - <https://www.st.com/en/embedded-software/x-cube-safea1.html>
    - [https://www.st.com/resource/en/data\\_brief/x-cube-safea1.pdf](https://www.st.com/resource/en/data_brief/x-cube-safea1.pdf)

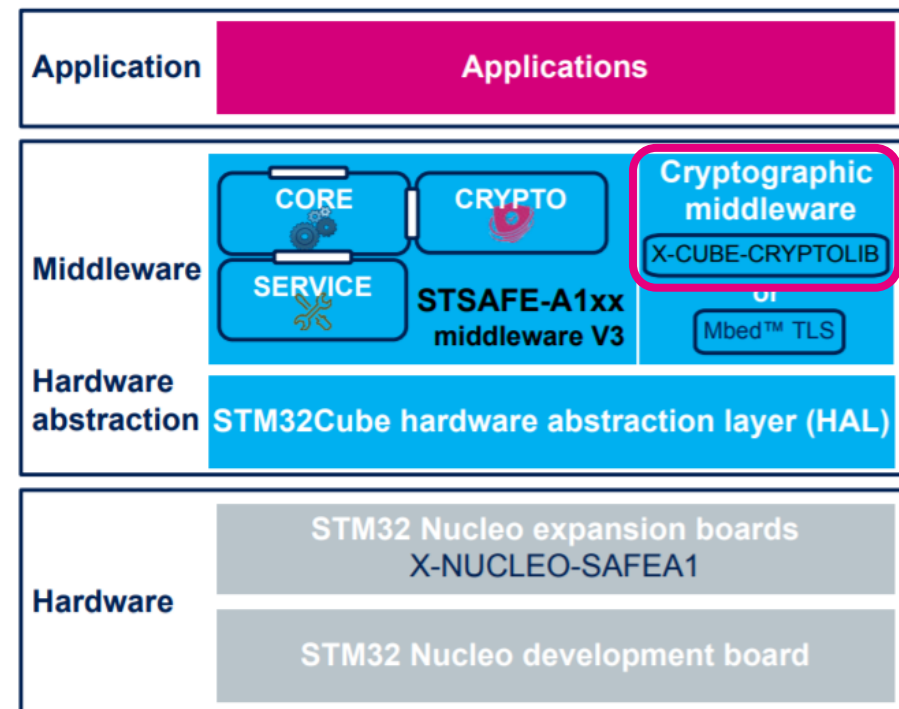


# S/W tool #3

## X-CUBE-CRYPTOLIB



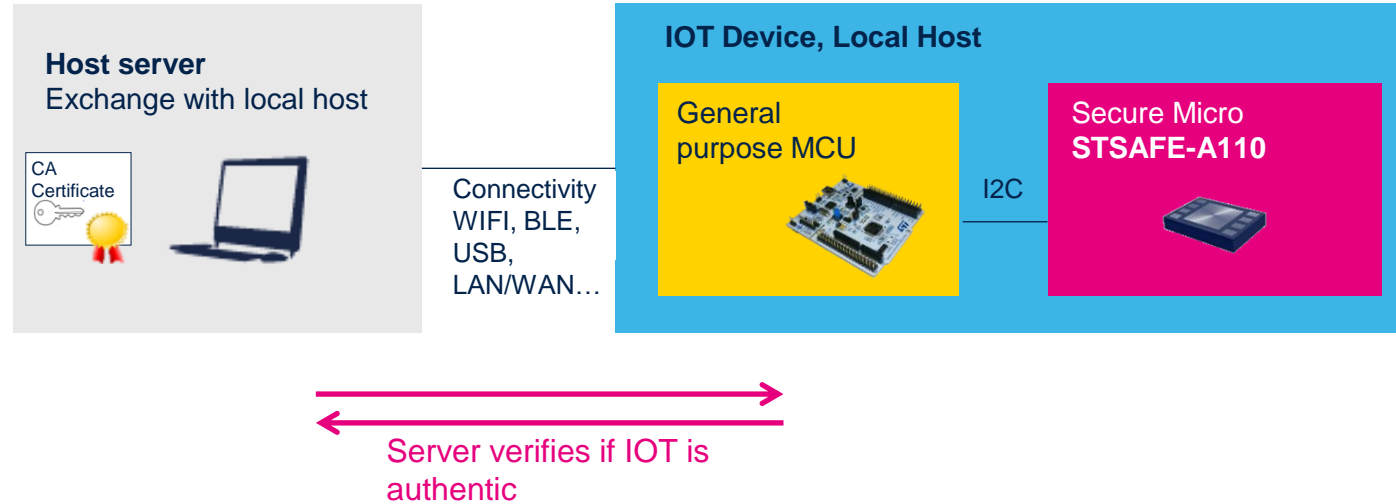
- STM32 crypto library package (X-CUBE-CRYPTOLIB) is based on STM32Cube architecture package and includes a set of crypto algorithms
- Crypto library to run X-CUBE-SAFE1 sample projects
- More info & download
  - <https://www.st.com/en/embedded-software/x-cube-cryptolib.html>



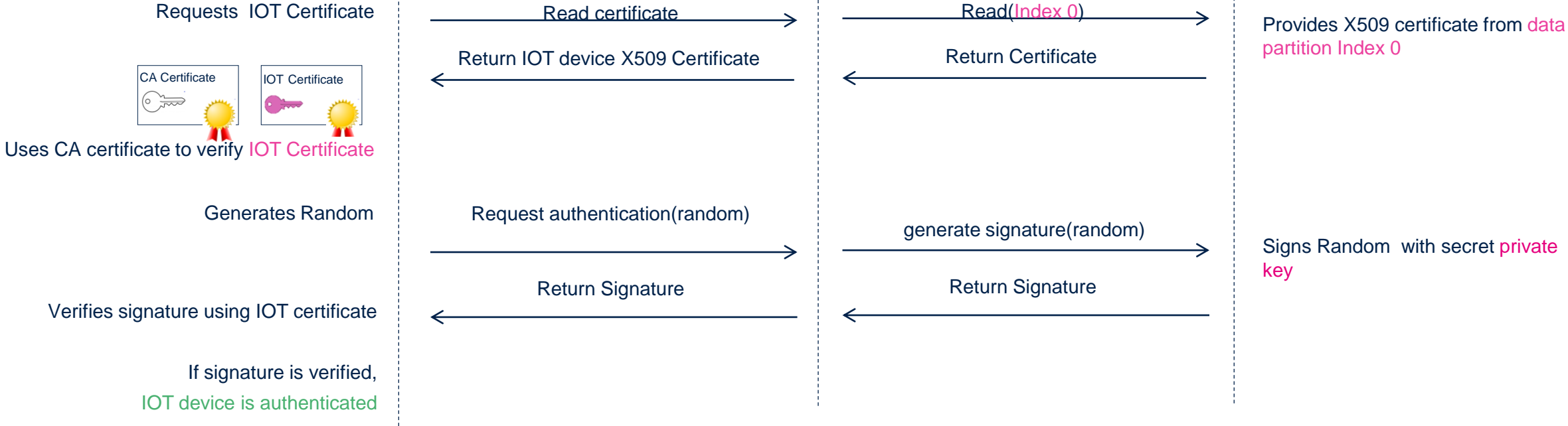
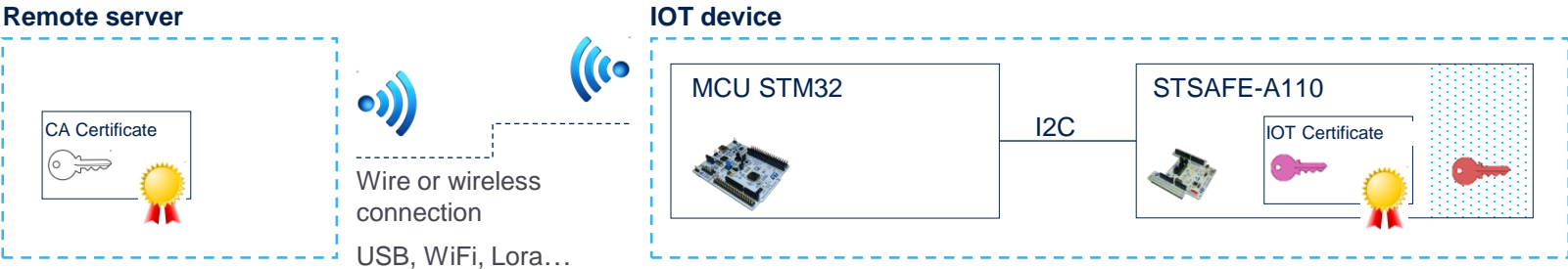
# Use Case 1

## Peripheral authentication

- Host server verifies IOT device is an authentic one
  - STSAFE-A110 contains IOT key pair: private key and certificate
  - Host server must have access to CA certificate allowing verify IOT certificate
- Ex. anti-counterfeiting



# Use Case 1 Peripheral authentication



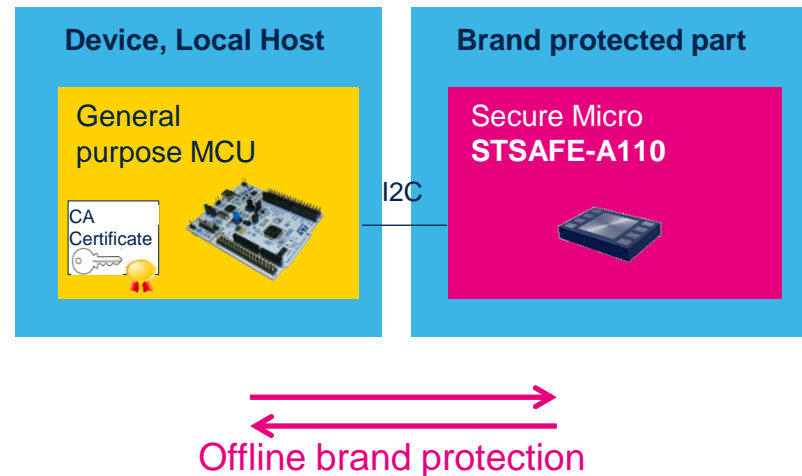
# Use Case 1bis

## Peripheral authentication & Brand protection

Local host verifies if STSAFE-A110 is present and is an authentic one

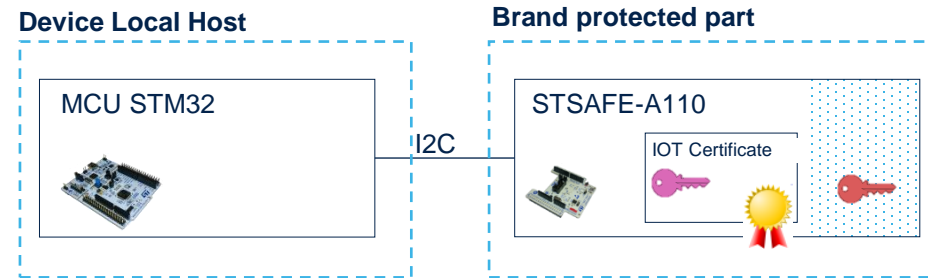
- STSAFE-A110 contains IOT key pair: **private key** and **certificate**
- Device must have access to CA certificate allowing verify IOT certificate

Ex. anti-counterfeiting



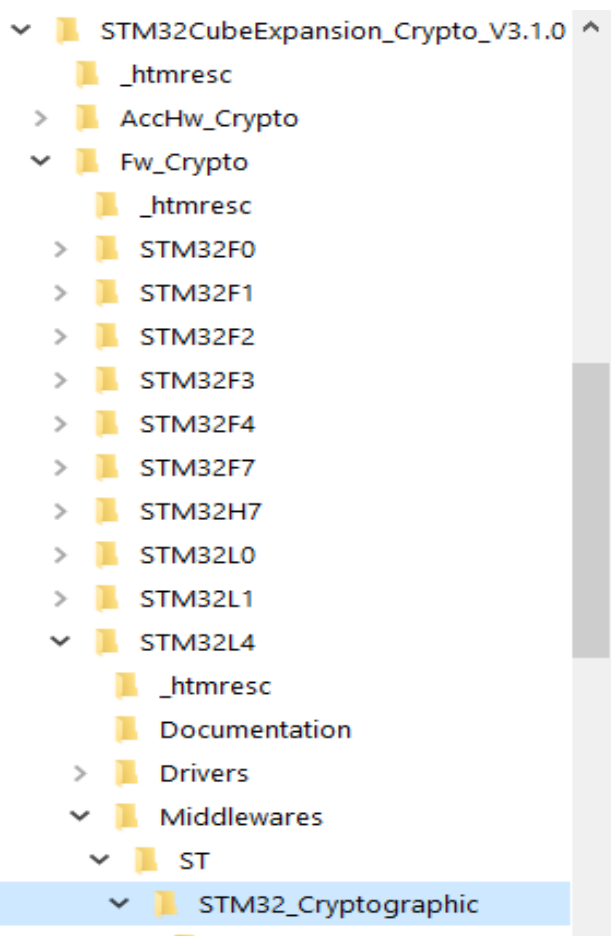
# Use Case 1bis

## Peripheral authentication & Brand protection

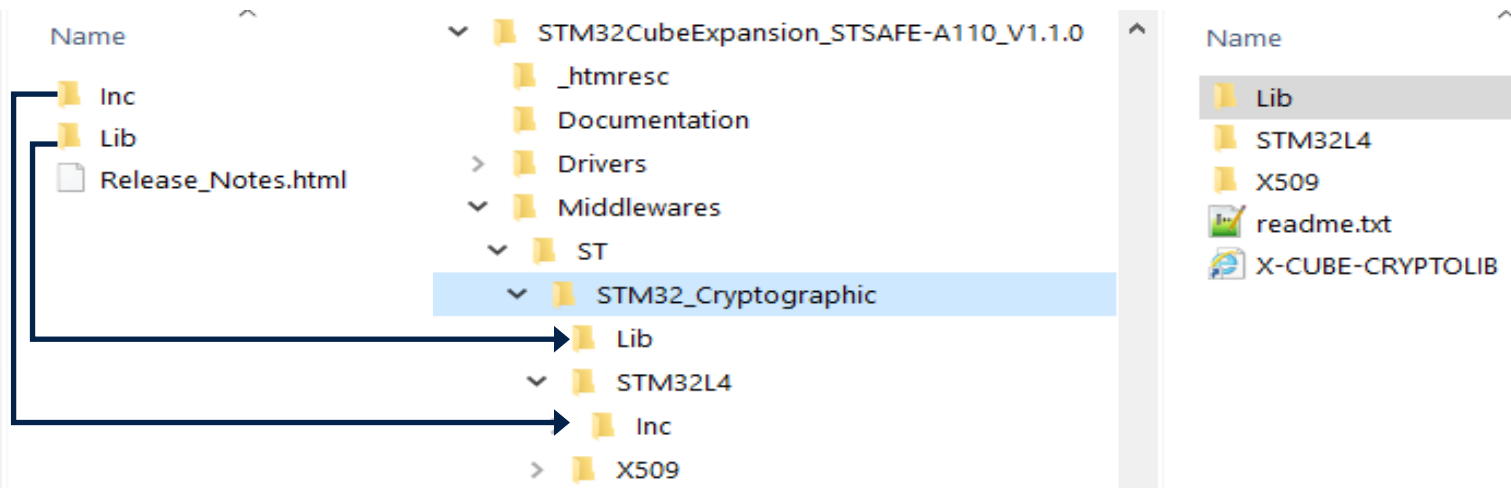


# Copy X-CUBE-CRYPTOLIB Inc & Lib folder to X-CUBE-SAFEA1

- STM32L4 Inc & Lib path in X-CUBE-CRYPTOLIB



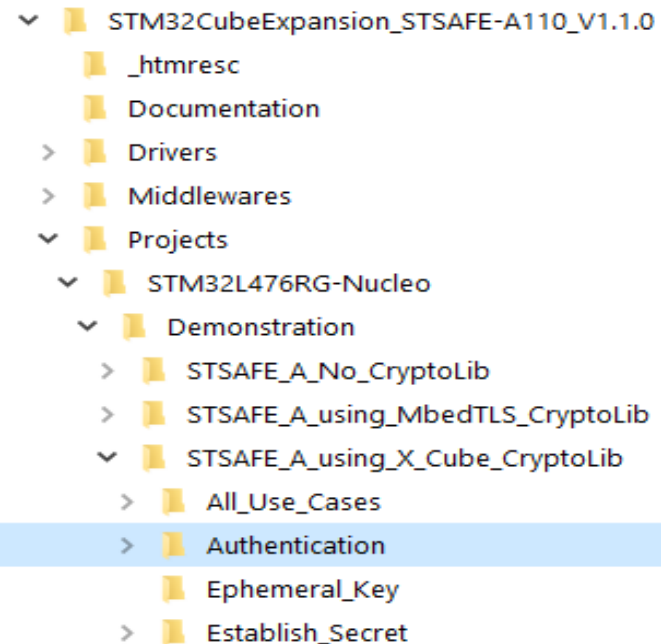
- Path in X-CUBE-SAFEA1





# X-CUBE-SAFE1 authentication demo project path

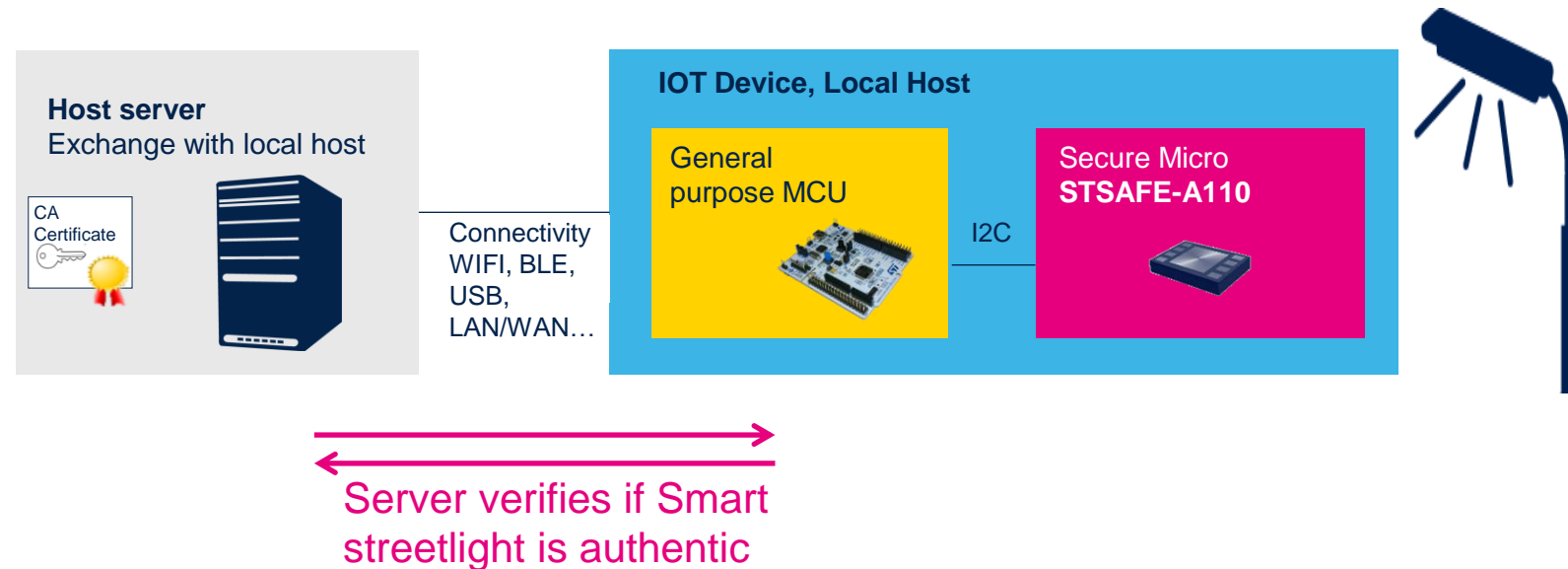
- Target project: Authentication of STSAFE\_A\_using\_X\_Cube\_CryptoLib
- If MbedTLS library is preferred, select Authentication in STSAFE\_A\_using\_MbedTLS\_CryptoLib



# STSAFE-A smart city demo

# STSAFE-A Smart city demo

- Host server verifies smart streetlight is an authentic one
  - STSAFE-A110 of Smart streetlight contains IOT key pair: private key and certificate
  - Host server must have access to CA certificate allowing verify IOT certificate
- Ex. anti-counterfeiting



# Thank you

Email: [stsafe-korea@st.com](mailto:stsafe-korea@st.com)

© STMicroelectronics - All rights reserved.

The STMicroelectronics corporate logo is a registered trademark of the STMicroelectronics group of companies. All other names are the property of their respective owners.



life.augmented