STSAFE-A110 Authentication solution

STSECURE

Authentication market

STSAFE
Protect businesses & connected services

Prevent product cloning

- Protect business model revenues
- Keep control over products’ image

Protect brand reputation

Prevent services from being hacked

- Keep information and data confidential
- Maintain proper behavior and service quality

Protect service performance and quality

Authentication applications — Examples

Consumables

- Ink cartridges
- Medical consumables
- And more…

Peripherals and accessories

- Batteries
- Game console accessories
- Scooter / e-bike parts and motors
- And more…

Security for connected objects — Examples

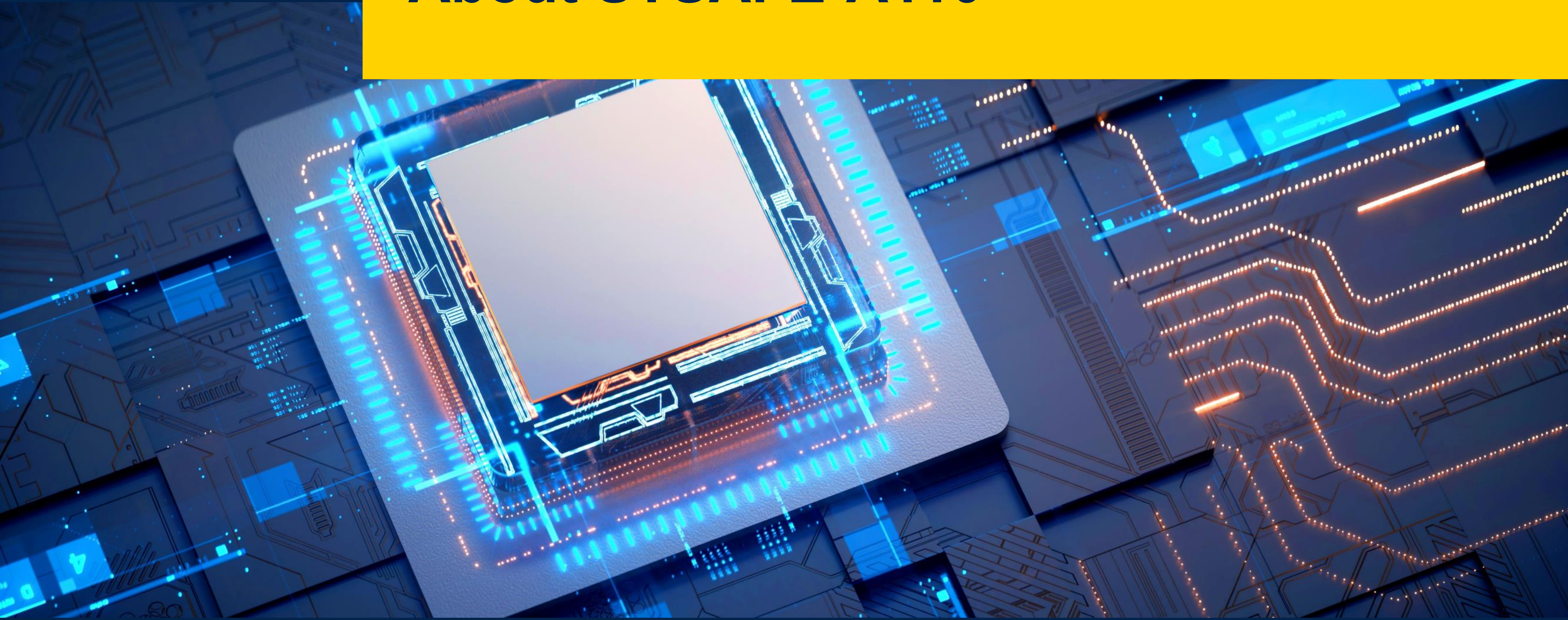
Edge connected objects

- Sensors & detectors
- Actuators (pumps, valves)
- Connected bikes/scooters
- Smart lock
- Renting car controller
- Camera
- EV chargers
- And more…

Gateways / Data concentrators / Smart meters

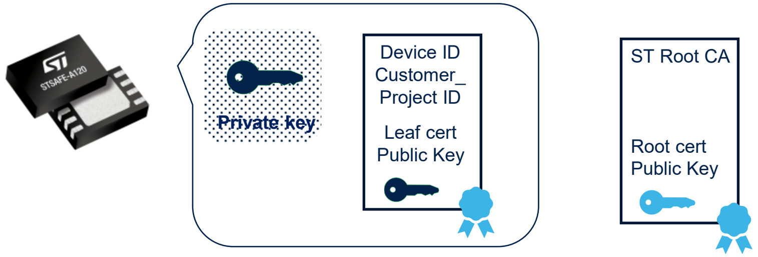
- Connectivity gateways (e.g., Matter gateways)
- Data concentrators
- Smart meters
- And more…

About STSAFE-A110



STSAFE-A110
Optimized secure solution for **connected devices**

Deliverable



Private key

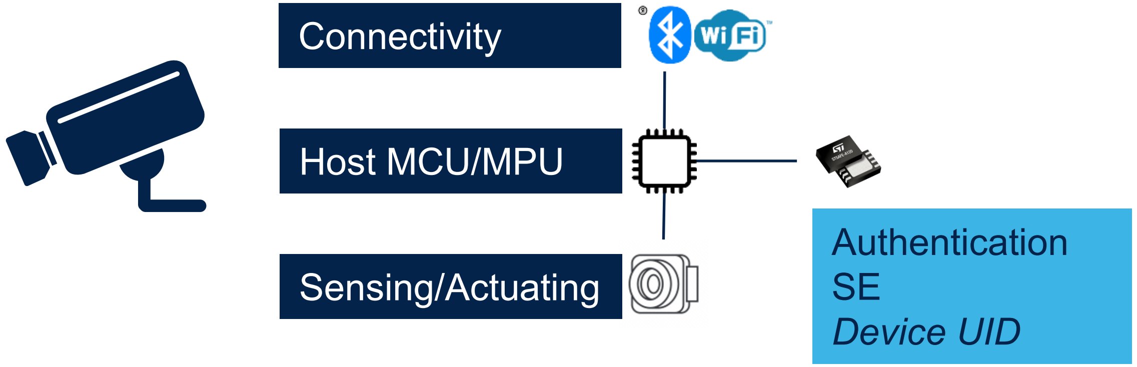
Device ID
Customer_
Project ID

Leaf cert
Public Key

ST Root CA

Root cert
Public Key

Integration in object



Connectivity

Host MCU/MPU

Sensing/Actuating

Authentication
SE
Device UID

Authentication with personalized certificate

Main features:

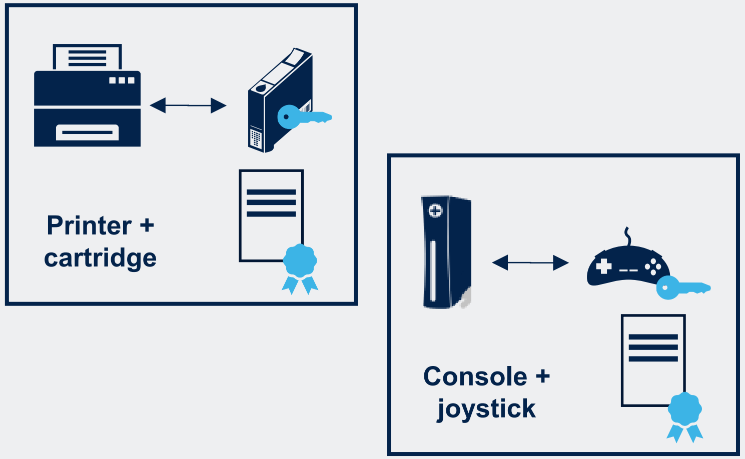
- Authentication with personalized certificate(s)
- Secure connection establishment (TLS)
- Encryption/decryption
- Secure data storage
- Signature verification

EAL5+ Common Criteria certified chip

Personalization at ST certified manufacturing site

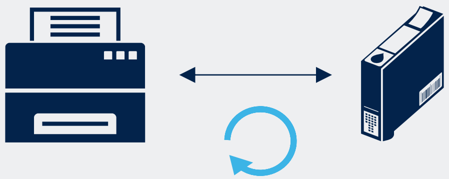
Functionalities for consumables and peripherals anticloning

Checks genuine objects



Verify that a consumable or a peripheral is genuine

Tracks number of usages



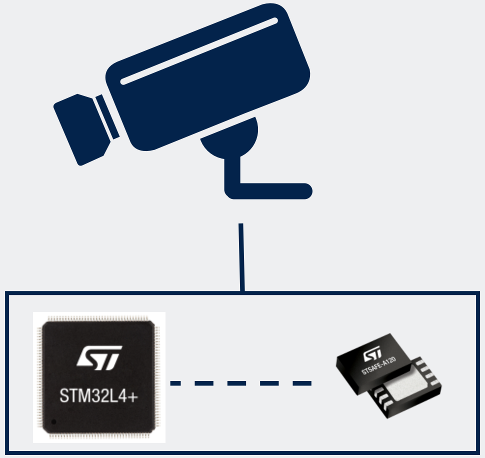
Track and control the number of usages

Stores data securely

Securely store object data such as configuration files, maintenance reports, etc.

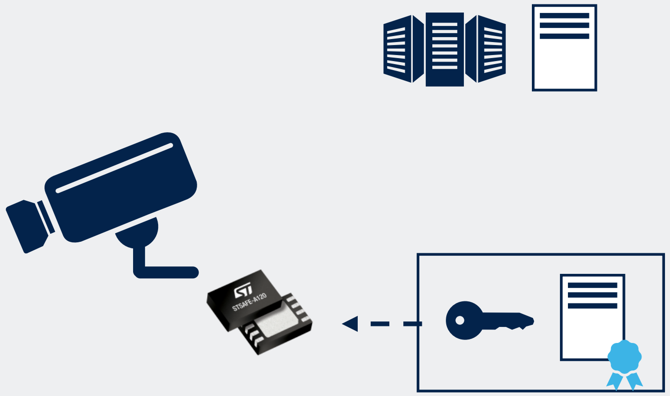
Functionalities to secure ecosystems based on connected objects

SE companion of the device MCU/MPU



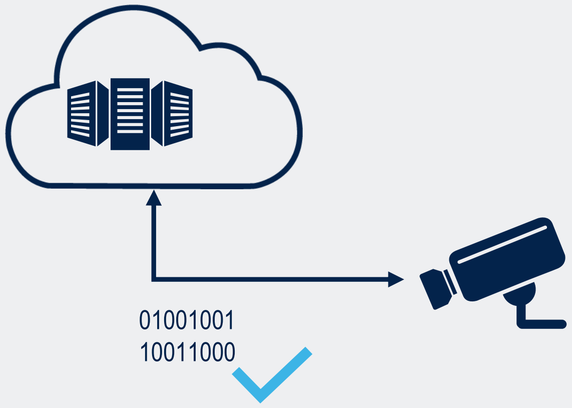
STSAFE-A is embedded into the object to authenticate, connected to local host MCU/MPU

Strictly authenticates the device



STSAFE-A contains the certificate and secret key, and the cryptography to authenticate the object by the cloud

Assists device secure connection



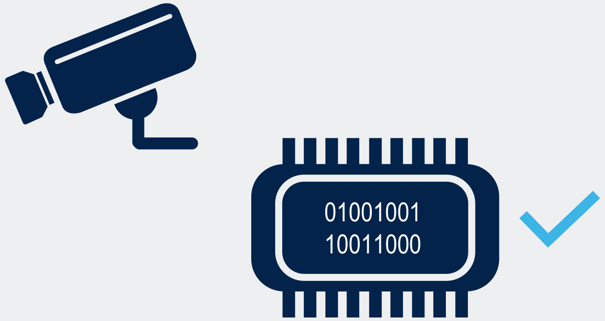
STSAFE-A ensures the integrity and confidentiality of exchanged data by ciphering and/or signing data

Additional security services

Securely stores connectivity credentials and sensitive data

STSAFE-A ensures the secure storage of credentials and sensitive data both in SE storage and in device NVM

Assists device applicative FMW integrity check



STSAFE-A can perform a device applicative firmware signature verification at initial start and when firmware is updated

STSAFE-A110 security robustness

Certified security to protect secrets’ privacy

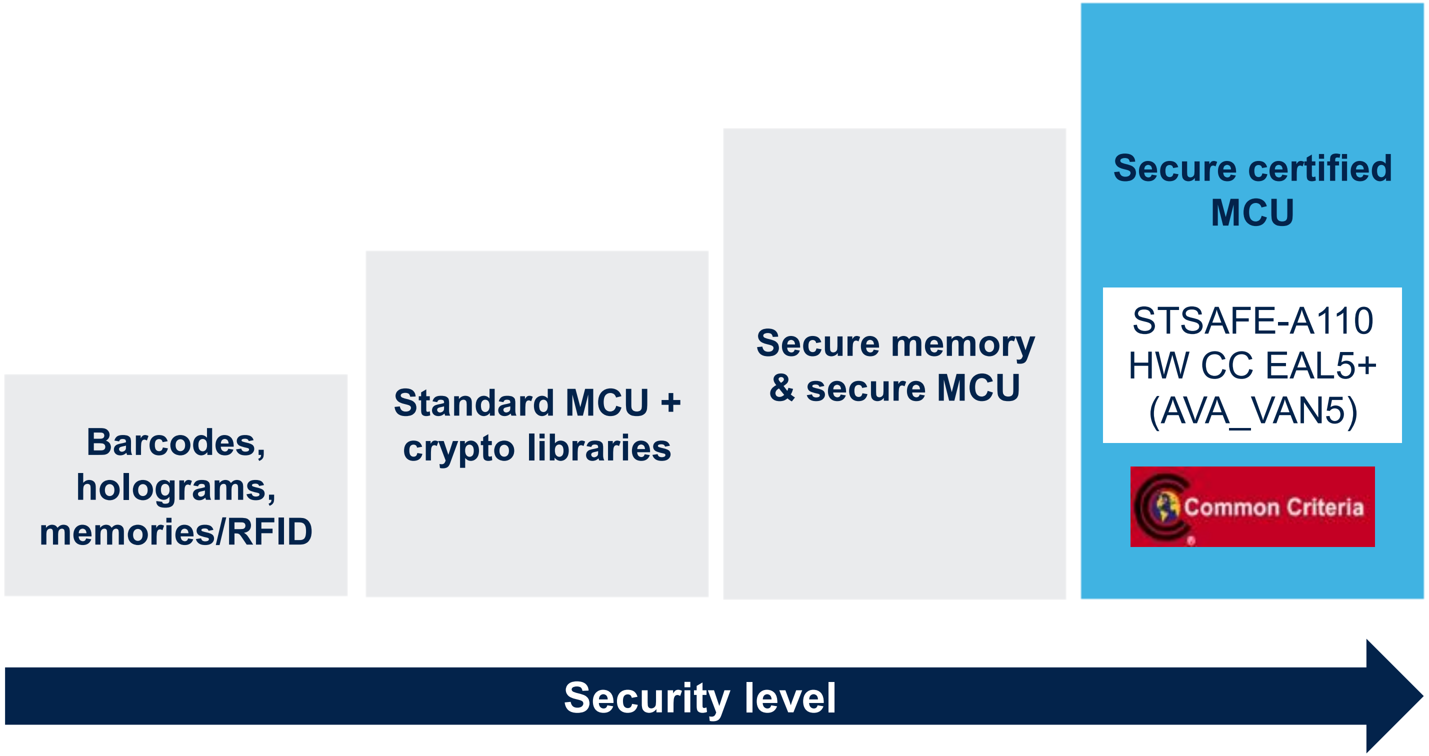
Security countermeasures

Protection against side-channels attacks

Protection against attacks on chip

Secure development environment

Certified by recognized external authorities



Barcodes, holograms, memories/RFID

Standard MCU + crypto libraries

Secure memory & secure MCU

Secure certified MCU

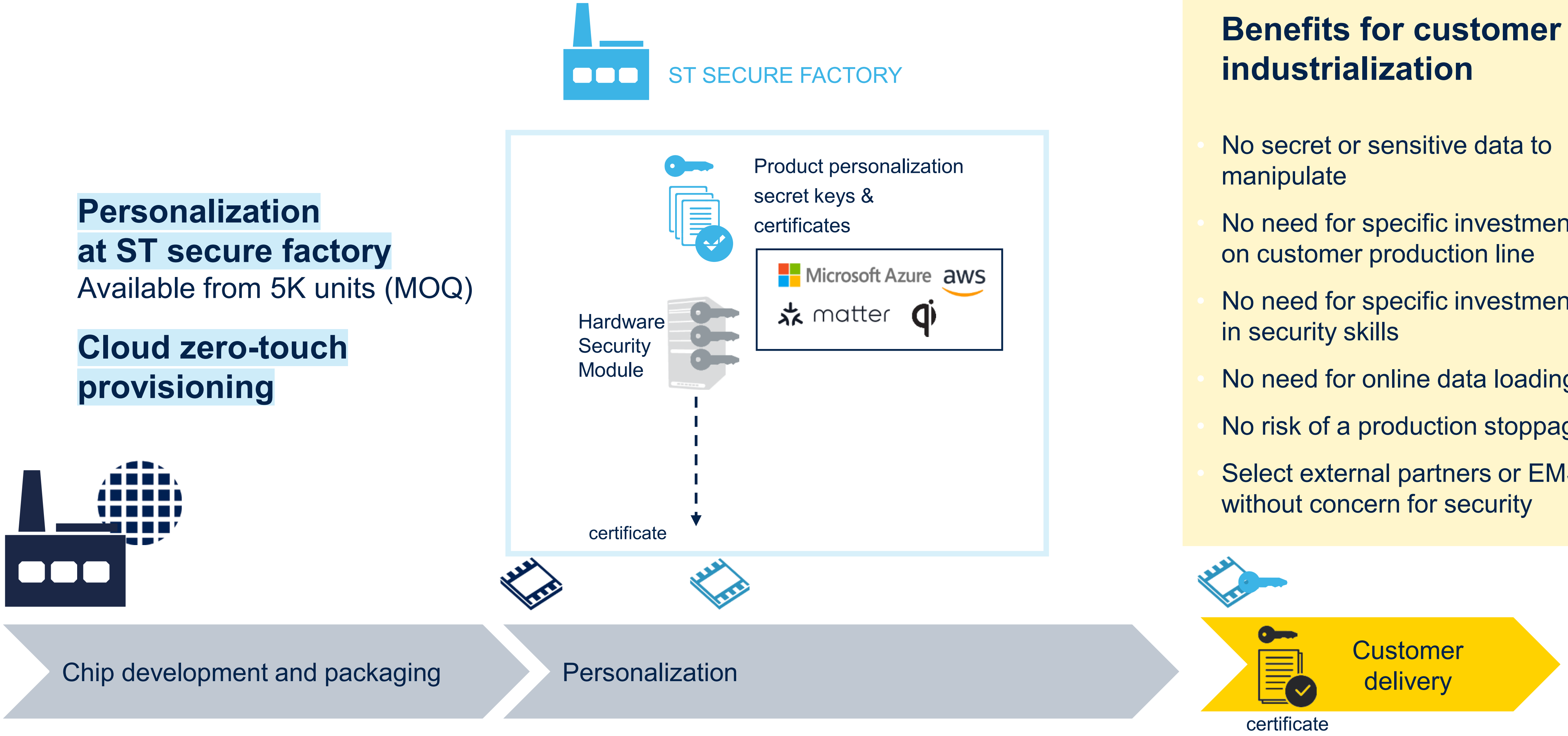
STSAFE-A110 HW CC EAL5+ (AVA_VAN5)

STSAFE-A provisioning at ST factory

Personalization at ST secure factory

Available from 5K units (MOQ)

Cloud zero-touch provisioning



Benefits for customer industrialization

- No secret or sensitive data to manipulate
- No need for specific investment on customer production line
- No need for specific investment in security skills
- No need for online data loading
- No risk of a production stoppage
- Select external partners or EMS without concern for security

STSAFE-A110 takeaways

STSAFE-A110 is an appropriate solution for brand protection and connected devices

- Support 1.8 V power supply
- Support hibernate mode at 1.1 µA (Typ.)

Best-in-class security with hardware certified

- Protected against attacks on chip

Personalized at ST secure manufacturing site

- Starting with small MOQ 5Ku

STSAFE-A110 features & applications

Best-in-class embedded Secure Element (eSE)

HW CC EAL5+ certified

Key applications

- Consumables and accessories anticloning
- Smart home (Matter ready)
- Healthcare
- Power supply (Open Compute Project)
- Metering & industrial equipment
- Wireless charging (Qi)

Rich feature set

- Authentication with personalized certificate
- Secure connection establishment
- Secure data storage
- Encryption / decryption
- Signature verification

Best-in-class hardware

- Highly secure MCU, CC EAL5+ AVA_VAN5 certified
- 6kBytes non-volatile memory
- 30 years of data retention, 500k cycles
- Temperature range: -40℃ to 105℃
- 1.62-5.5 V power supply
- Hibernate mode at 1.1 µA (Typ.)

Personalization

- Customer certificate and keys personalization at ST secure factory
- MOQ 5Ku

Our technology starts with You

Find out more at st.com/stsafe-a120