How to secure services based on connected objects with STSAFE-A

Contents

Overview of the connected devices' market

Security camera, water pump, heart monitor.
All these objects have in common is that they are now connected. Wherever we go, may it be at home, in the city or in industrial infrastructure, connected devices are all around us. Several factors fueled this wave of the "ever-more connected", among which a change
in the way we sell them.

FROM A TRADITIONAL BUSINESS MODEL...

In this former configuration, companies used to sell devices in shops. While bringing some advantages, drawbacks were also numerous. Among these, the most significant ones were that selling a device generates a one-time income, and that companies had a hard time getting feedback from customers' experience.

...TO A SERVICE-BASED APPROACH

From these observations, companies have expanded their business model to sell extra recurrent services. This approach brings the benefit of ensuring recurrent revenue for companies, to make customers more captive and finally, it was a way to get direct feedback from customers.

ENABLED BY THE SURGE OF NEW TECHNOLOGIES

This evolution in business models was made possible thanks to the emergence of new technologies, among which connected objects with sensors and actuators, data processing in the cloud and artificial intelligence (AI).

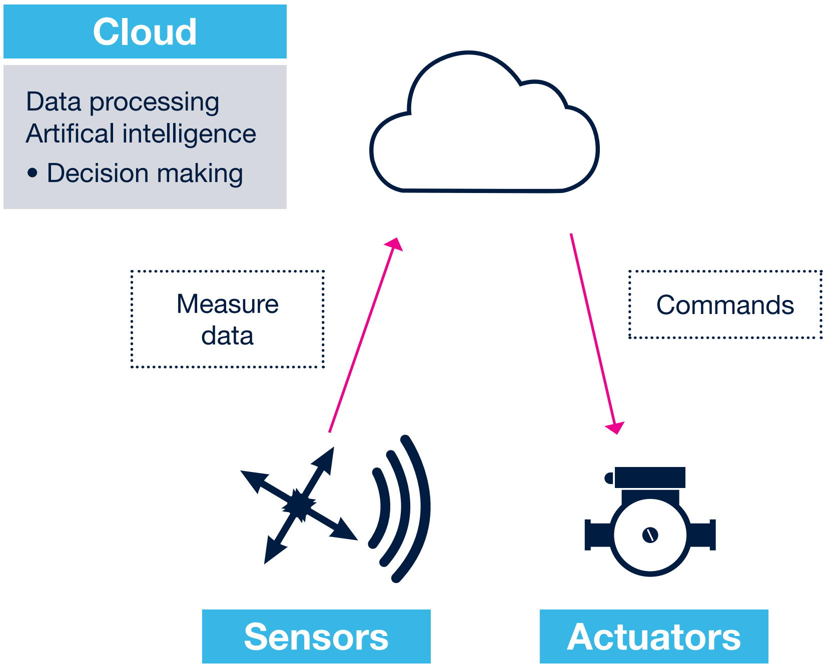
Introducing connected devices principles

CONDITIONS OF THIS SERVICE-BASED BUSINESS MODEL

For this business model to work, three conditions are required:

- The service must be available
- The service must be reliable
- The service must guarantee the privacy of the customer information

Note that in this specific setup, the customer pays for the service. Consequently, the quality expectation is higher.



Cloud

Data processing
Artifical intelligence
• Decision making

Measure data

Commands

Sensors

Actuators

Measurements must come from the **expected** sensors

Measurements **cannot be modified** between the sensors and the could

Commands are executed by the **expected** actuators

Commands **cannot be modified** between the cloud and the actuators

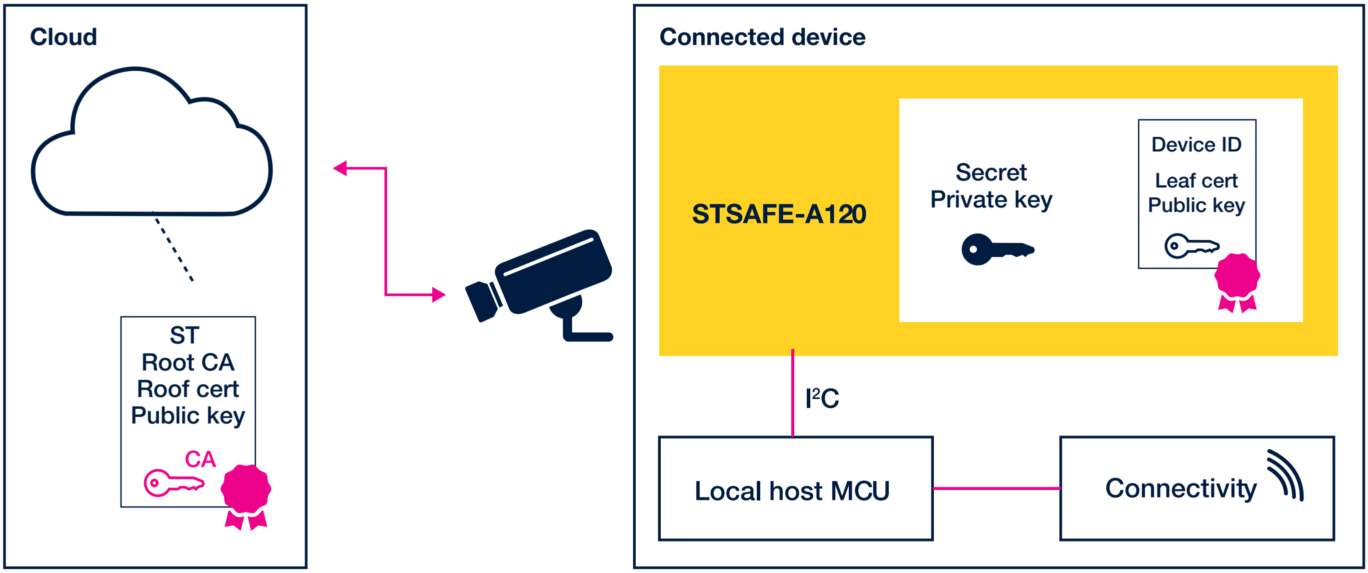
To ensure that these four requirements are fulfilled, two actions can be implemented:

- **Sensors & actuators authentication:** to ensure that measurements are coming from the expected sensors on one side, and that commands are executed by the expected actuators on the other side, the solution is to authenticate both devices.
- **Signature & ciphering of data and commands:** to ensure that measurements cannot be modified between the sensors and the cloud on one side, and that commands cannot be modified between the cloud and the actuators on the other side, the solution is to sign and cipher data and commands.

Providing an authentication solution STSAFE-A

INTRODUCING STSAFE-A

STSAFE-A is a solution allowing a secure authentication of objects. Based on a secure element certified by independent third parties, STSAFE-A has a command set that is customized to perform device authentication and monitor device usage.



Optimized System-on-Chip (SoC) for product authentication

STSAFE is preloaded with secrets and X509 certificates to enable strict object authentication. It also includes a basic API that implements security protocols for authentication purposes.

A companion chip of object local host MCU/MPU

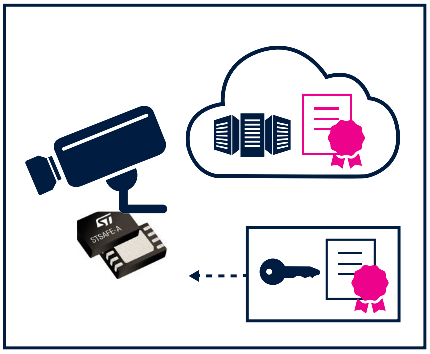
STSAFE-A is connected to the local host through a simple I²C interface.

Personalized at ST secure manufacturing site

STSAFE-A can be personalized with customer-specific object secrets and information at ST secure manufacturing sites.

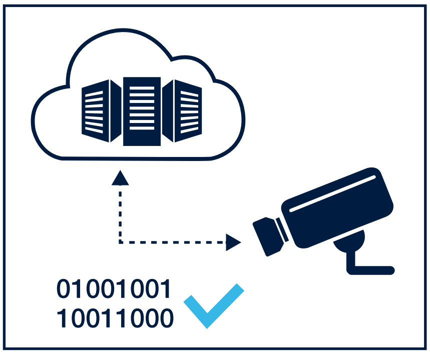
KEY PRODUCT FUNCTIONS

To ensure secure connections with the cloud, STSAFE-A is designed to perform four main tasks:



Authenticate a device

STSAFE-A is delivered with a pre-loaded X509 certificate and the security protocol that authenticate the device.

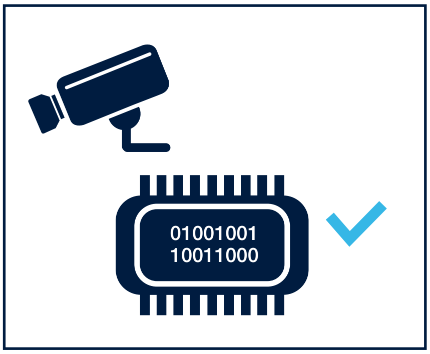


Create a secure connection with the cloud

STSAFE-A ensures the integrity and confidentiality of exchanged data by signing and/or encrypting them. For instance, the data exchanged between a security camera and a cloud-based server is signed and/or encrypted.

Securely store connectivity credentials and sensitive data

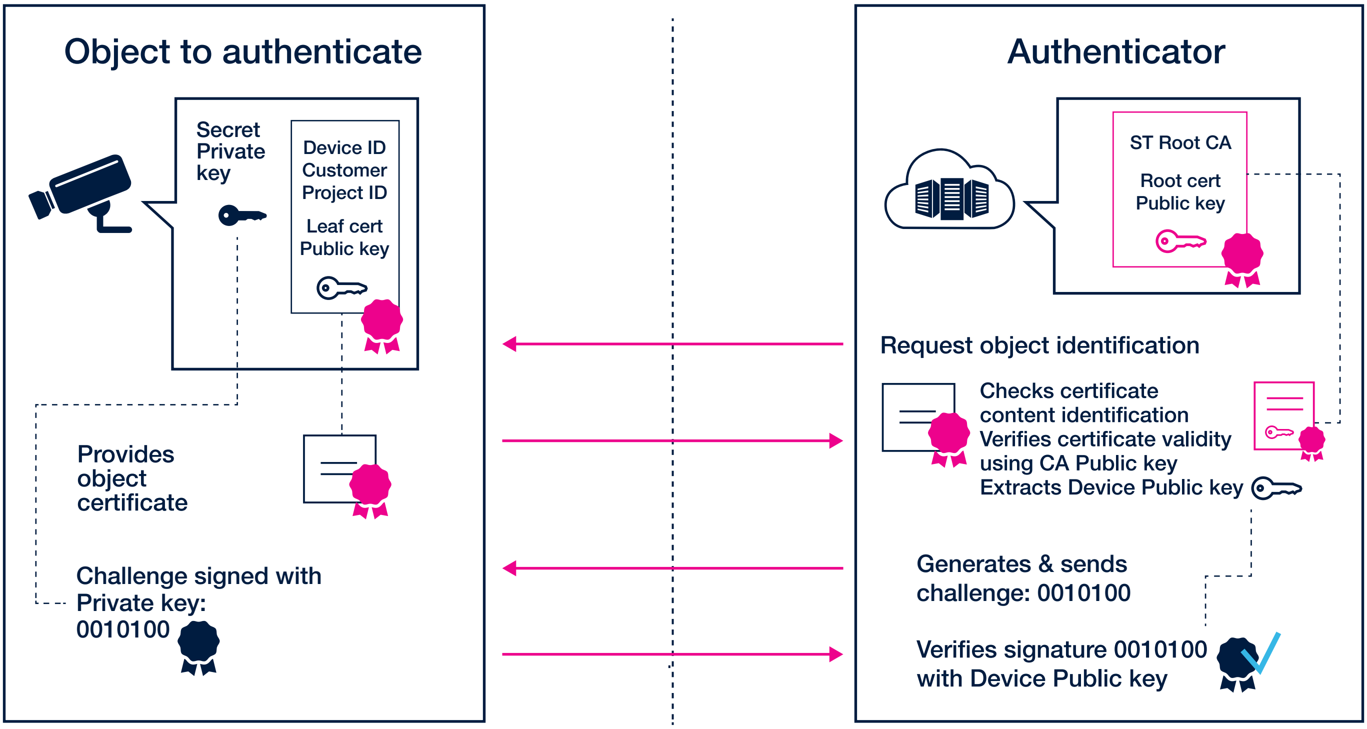
STSAFE-A ensures that credentials and sensitive data are securely stored in the Secure Element (SE) storage and in the non-volatile memory (NVM) of the device.



Verify the integrity of the device’s firmware and updates

STSAFE-A verifies the signature of the device's application firmware, at the initial start as well as when the firmware is updated.

Authentication process
How does it work?


Object to authenticate
Secret Private key
Device ID
Customer
Project ID
Leaf cert
Public key
Provides object certificate
Challenge signed with Private key:
0010100
Authenticator
ST Root CA
Root cert
Public key
Request object identification
Checks certificate content identification
Verifies certificate validity using CA Public key
Extracts Device Public key
Generates & sends challenge: 0010100
Verifies signature 0010100 with Device Public key

STSAFE-A is a secure element that is embedded into the object (in this case, the camera), which requires authentication. The secure element contains the battery certificate, which includes a Public key and a secret Private key. In contrast, the Cloud acts as the authenticator and contains the Certificate Authority (CA) with its Public key.

HOW DOES THE CLOUD AUTHENTICATE THE CAMERA?

1. The process starts with the Cloud requesting the object identification from the camera.
2. The camera provides its certificate to the Cloud
3. The Cloud then verifies the certificate validity using its own CA Public Key
4. When validity has been proven, the Cloud extracts the Public key from the camera certificate
5. The Cloud generates and sends a challenge to the camera.
6. This challenge is signed using the secret Private key and sent back to the Cloud
7. Finally, the Cloud verifies the signature of this challenge thanks to the Public key that was previously extracted from the camera certificate

Authentication completed
Expected camera

Ensuring security robustness STAFE-A

STATE-OF-THE-ART CERTIFIED SECURITY TO PROTECT SECRETS

STSAFE-A is based on the latest security technologies, similar to those used in banking cards and digital IDs. STSAFE-A is a secure element that incorporates sophisticated countermeasures to effectively fight against both physical and logical attacks.

Security countermeasures ❯

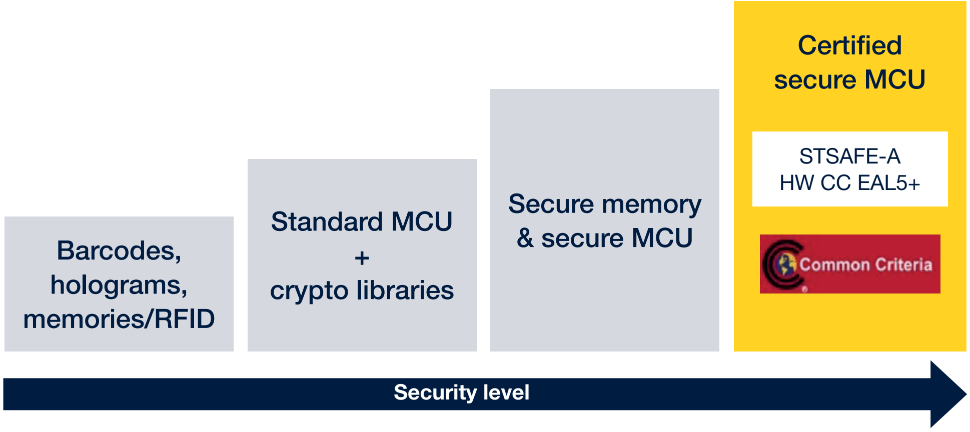
Protection against remote attacks

Protection against attacks on chip

Certified by recognized external authorities

ST secure elements, their development environment and their manufacturing processes are regularly audited and certified by external independent laboratories and certification bodies.

These independent organizations confirm that ST's solutions are compliant with the most demanding security standards. For instance, STSAFE-A110 is certified Common Criteria (CC) EAL5+ AVA_VAN5.



Barcodes, holograms, memories/RFID

Standard MCU + crypto libraries

Secure memory & secure MCU

Certified secure MCU

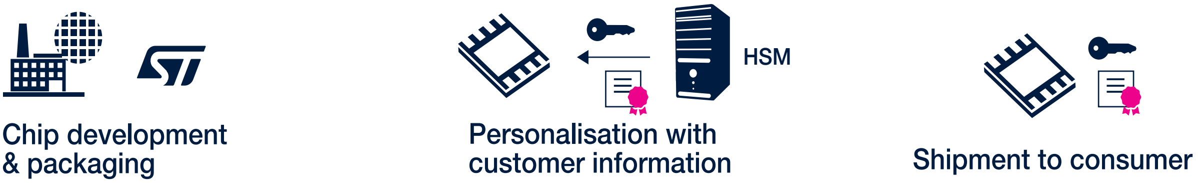
STSAFE-A HW CC EAL5+

Common Criteria

Security level

SECURE PROVISIONING AT ST

STSAFE can be personalized with device secrets and certificates at ST's secure manufacturing sites. This service is available for a minimum order quantity (MOQ) of 5 Ku.



Chip development & packaging

Personalisation with customer information

Shipment to consumer

Benefits for device and consumable manufacturers

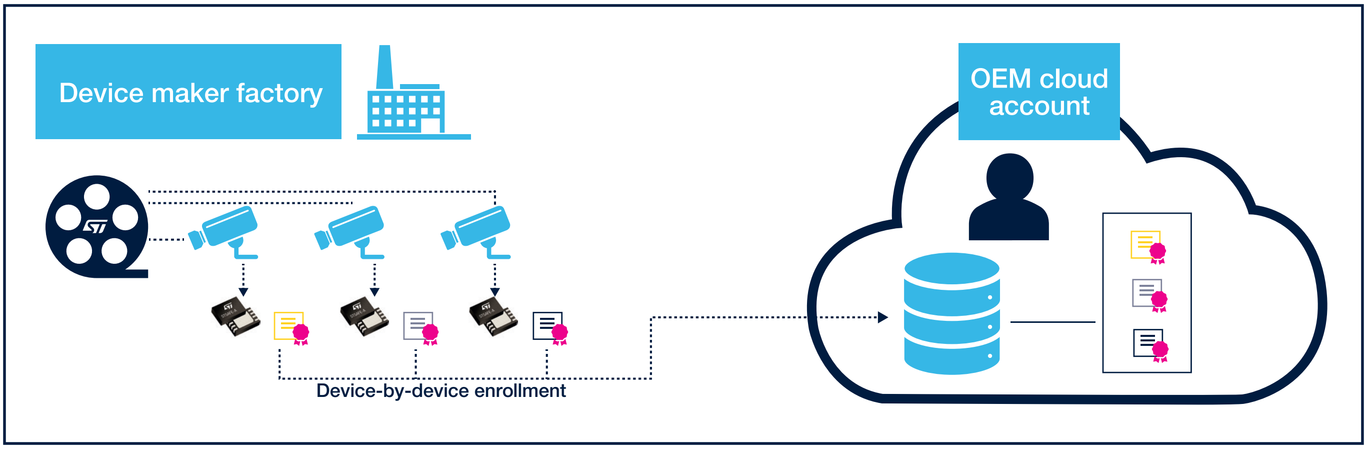
- No sensitive data or secret to manipulate
- No need for specific investments on customer production lines
- No need for specific investments in security skills
- No need for online data loading
- No risk of production stoppages
- Customers can select external partners or EMS without worrying about security concerns

Enroll connected objects to clouds account with STSAFE-A

The security of service based on connected object relies on a strict authentication of the objects by the service. This authentication requires that the objects are enrolled to the targeted service before they are put on the market by the OEM. Devices can be enrolled one by one, or a full family of devices can be pre-enrolled.

ENROLLING A SINGLE DEVICE TO A CLOUD ACCOUNT

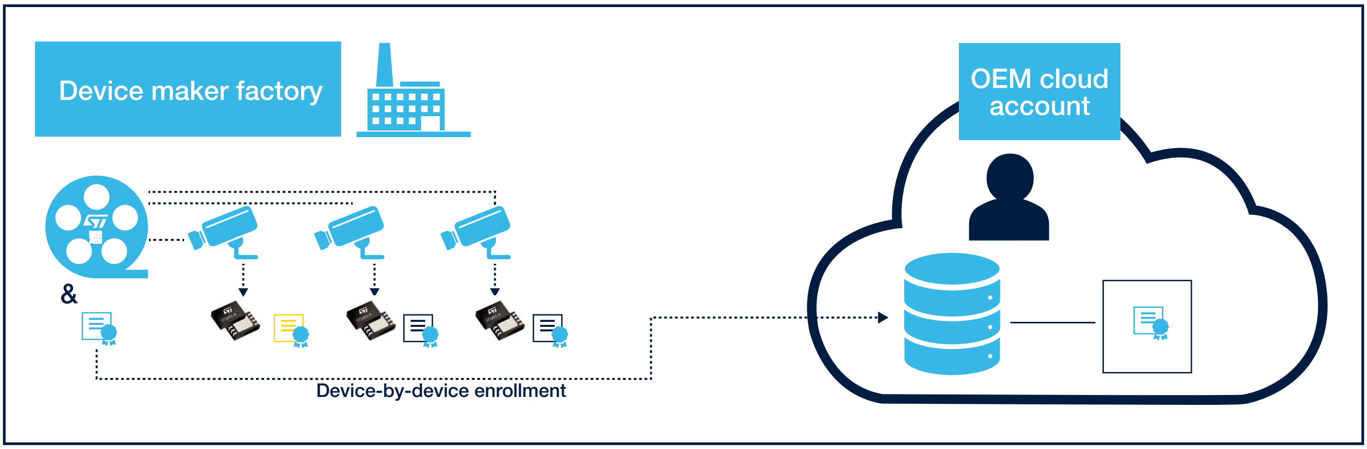
Each STSAFE-A comes loaded with a X509 certificate containing a unique ID and a key to be able to authenticate. A cloud account that has this X509 certificate can use it to strictly authenticate the connected device where the STSAFE-A is mounted. Each device can be enrolled to a cloud account by registering the X509 certificate to the cloud account.



ENROLLING A SINGLE DEVICE TO A CLOUD ACCOUNT

An entire family of devices can be registered to a cloud account by registering a single device family certificate.

A device maker can ask ST for this family certificate from a MOQ of 5Ku. It releases the device maker from reading each STSAFE-A X509 certificate.



Conclusion

An optimized system-on-chip (SoC) based on state-of-the-art certified hardware security, STSAFE-A is a secure element offering a simple solution for authenticating devices.

To maintain a high security level, STSAFE-A is personalized with device information (an X509 certificate) at ST secure manufacturing facility.

Moreover, it comes with a full hardware and software ecosystem to ease its integration by device makers that have no specific security knowledge.

WANT TO GO FURTHER?

Learn more about our products

Contact your local ST sales offices or find a distributor

At STMicroelectronics we create technology that starts with You

Order code: **BR2404STSAFEACDEV**

For more information on ST products and solutions, visit www.st.com