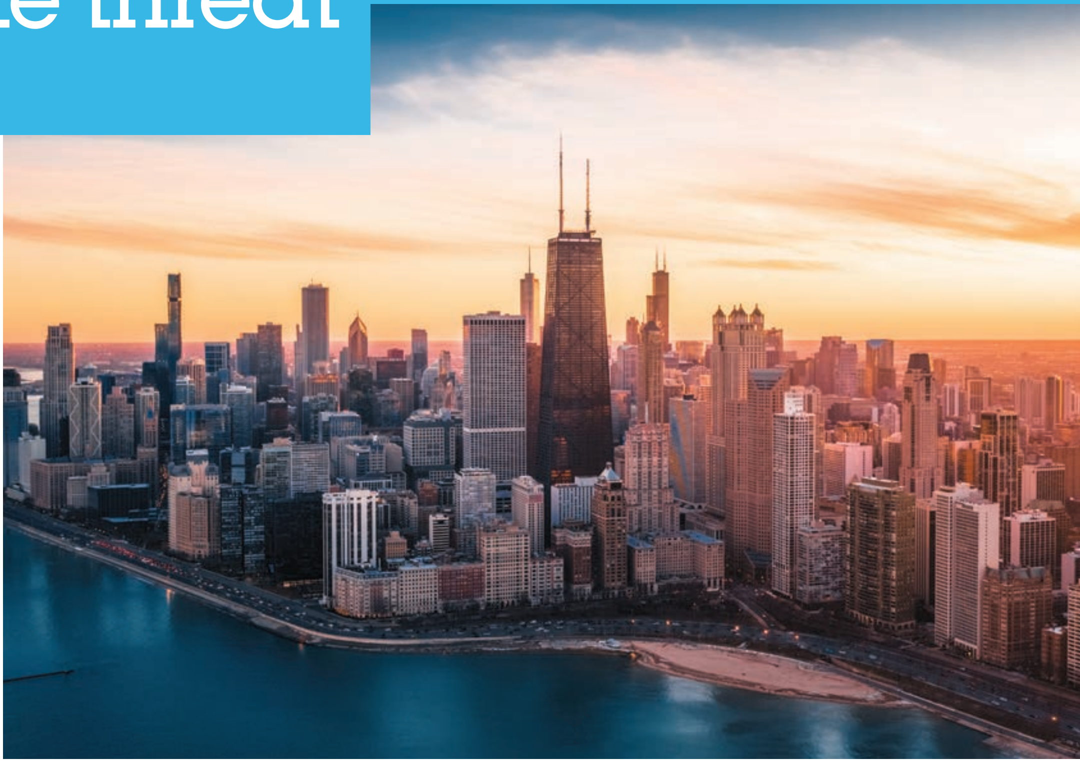
How to protect objects against cloning & counterfeiting with STSAFE-A

Contents

Counterfeiting: a concrete threat



Counterfeiting has been affecting companies for years. While commonly associated with luxury goods, counterfeiting also extends to electronic devices, including consumables, accessories, and peripherals.

ALL OBJECTS ARE EXPOSED TO COUNTERFEITING...

Ink cartridges, batteries, medical consumables, and electronic device accessories are ubiquitous in our daily lives. Although these items may seem basic and require periodic replacement, they are critical components of many companies' business models and essential to the quality of their solutions.

$464B

Volume of international trade in counterfeit products in 2019[1]

... GENERATING SERIOUS CONSEQUENCES

Using copies or clones of consumables in devices or solutions can have various negative consequences. The impact can be significant in terms of revenue loss, safety and brand image.

IS THERE A SOLUTION?

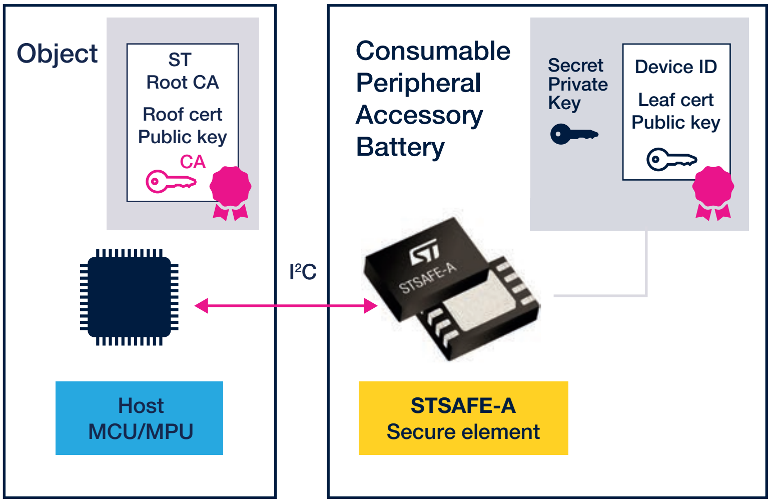
What if device manufacturers could embed a reliable authentication solution in their products to quickly and accurately distinguish genuine objects from counterfeits?

Source 1: https://www.oecd-ilibrary.org/sites/74c81154-en/index.html?itemId=/content/publication/74c81154-en

Providing an authentication solution STSAFE-A

ABOUT STSAFE-A

STSAFE-A is a solution that enables strict 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 an X.509 certificate 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

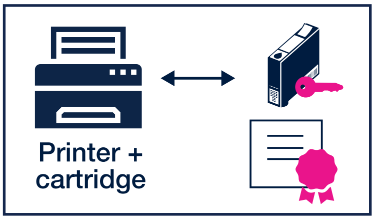
STSAFE-A is connected to the local host through a simple I²C interface.

Personalized at ST secure manufacturing site

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

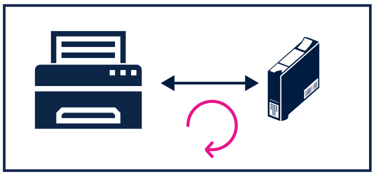
PRODUCT FUNCTIONALITIES

In order to ensure the end-product authenticity, STSAFE-A offers three main functionalities:



Verify genuine objects

STSAFE-A comes with an authentication protocol based on asymmetric ECDSA protocol and X509 certificates. It embeds a device leaf certificate containing the device Unique Identity. ST also acts as Certificate Authority (CA) and offers the Root certificate to attest of the authenticity of STSAFE-A leaf certificates. Concretely, in the case of a printer and its ink cartridges, the printer will be able to verify that the cartridge is genuine.



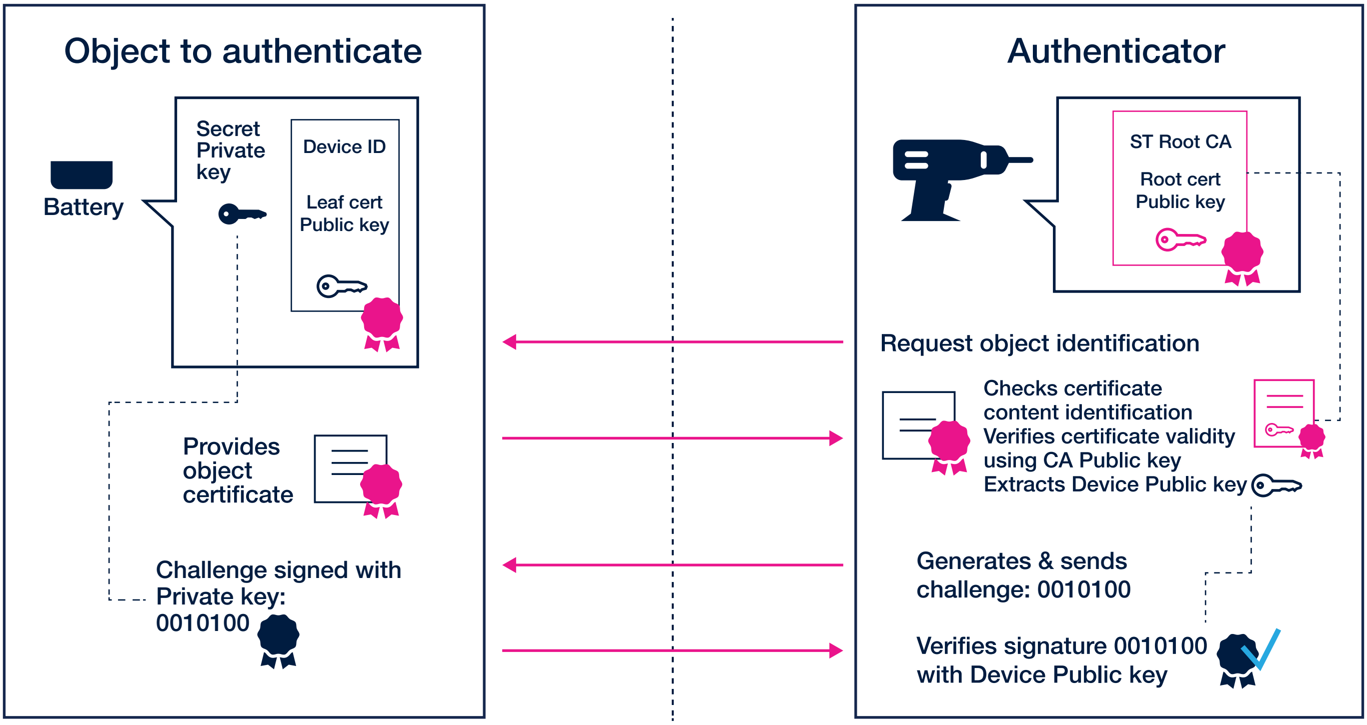
Track number of usages

STSAFE-A offers secure counters allowing to track the number of usages of a device. For instance, the printer can keep track of how many times an ink cartridge has been used.

Store data securely

Additionally, STSAFE-A embedds a nonvolatile memory that stores device information and secrets. This memory can be partitioned, and access conditions can be set to ensure the secure storage of data.

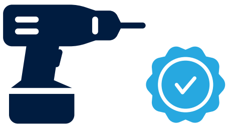
Authentication process How does it work?


Object to authenticate
Battery
Secret Private key
Device 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 battery), which requires authentication. The secure element contains the battery certificate, which includes a Public key and a secret Private key. In contrast, the power drill acts as the authenticator and contains the Certificate Authority (CA) with its Public key.

HOW DOES THE POWER DRILL AUTHENTICATE ITS BATTERY?

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



Authentication completed
Genuine battery

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 ❯

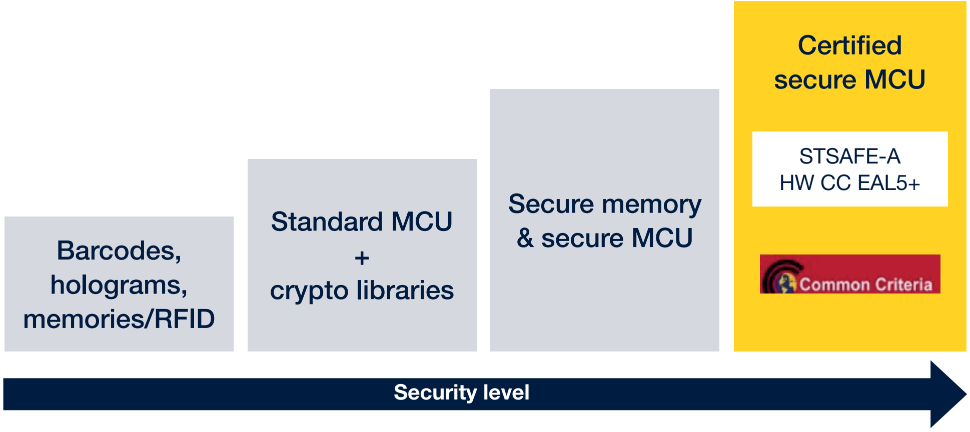
Protection against remote attacks

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

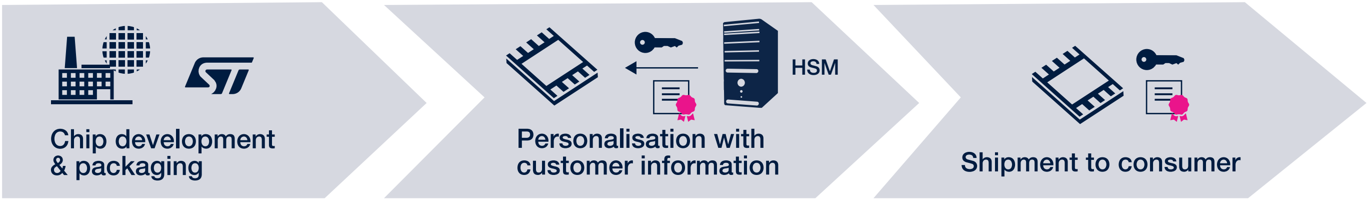
Certified secure MCU

STSAFE-A HW CC EAL5+

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

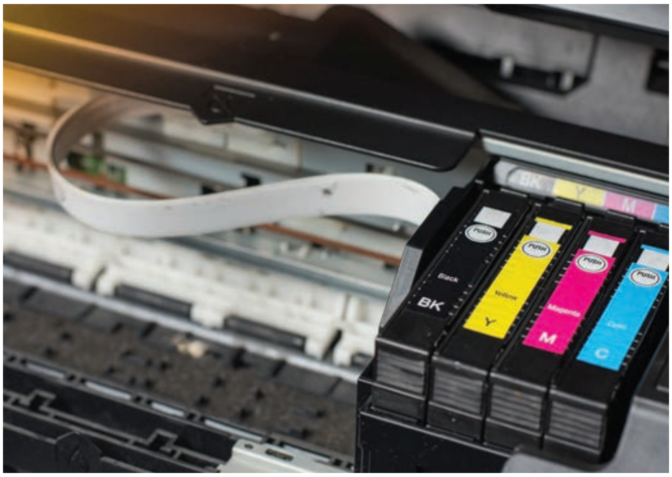
Benefits for device and consumable manufacturers

- 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

Conclusion

STSAFE-A is a System-on-Chip (SoC) solution that utilizes state-of-the-art hardware security to provide a simple and reliable authentication solution for a wide range of objects.

To simplify and secure object manufacturing, STSAFE-A can be personalized with customer-specific information at ST's secure manufacturing sites. Finally, STSAFE-A comes with a comprehensive 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: **BR2403STSAFEA**

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