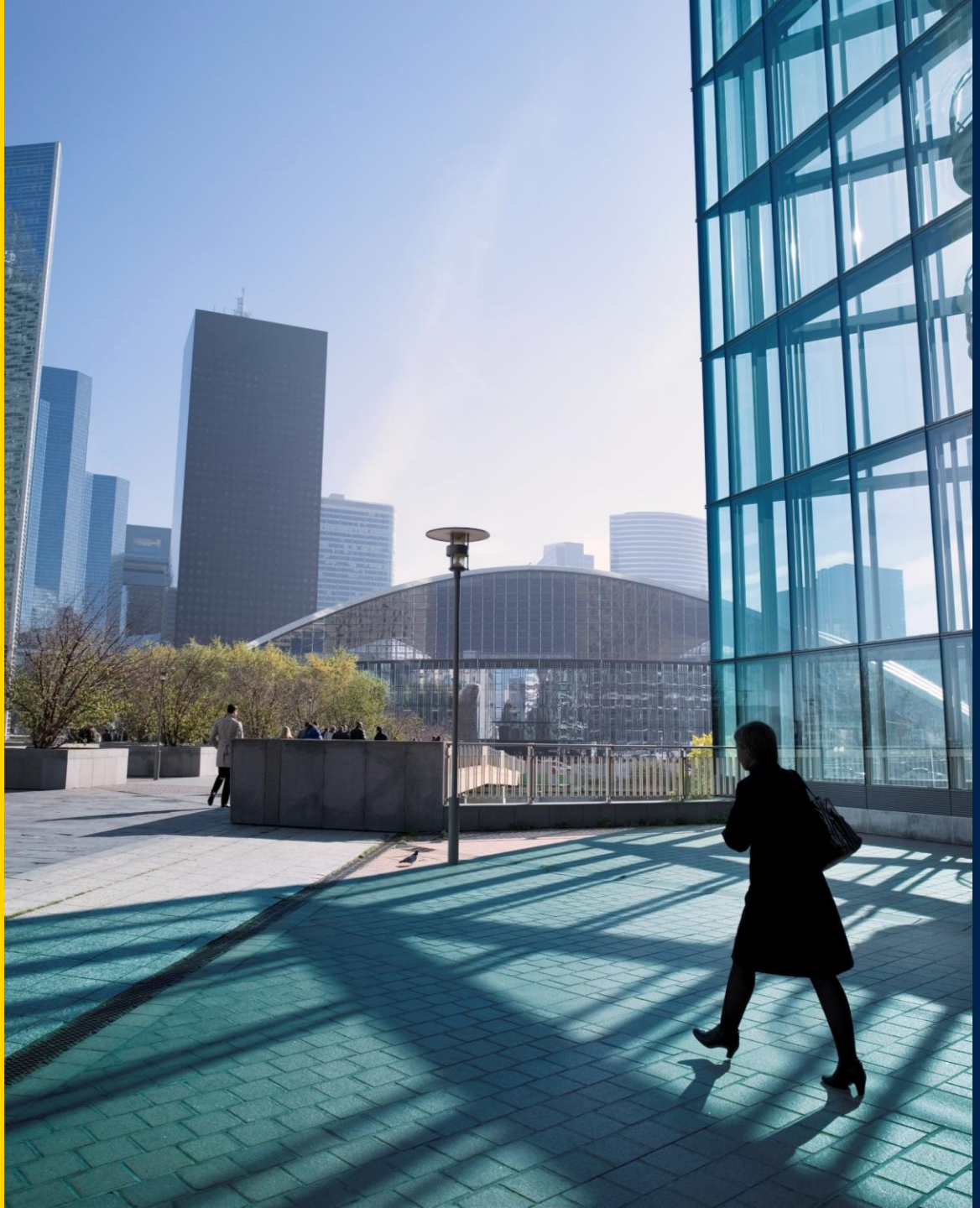


# How STSAFE contributes to CRA compliance

# CRA overview

# Cyber Resilience Act (CRA)

## Scope & purpose

Regulatory framework to improve the security of "**all products with digital elements**" (HW/SW) put on the EU market.

- Product divided into 4 categories with different conformity assessments

## Timeline

- Sept. 2026: Vulnerabilities and incident reporting
- Dec. 2027: Full enforcement of the regulation

## Requirements for device & SW/HW component manufacturers

- Device security risk assessment and security policy definition
- Device security update policy definition for at least 5 years
- Device vulnerabilities and incidents public reporting

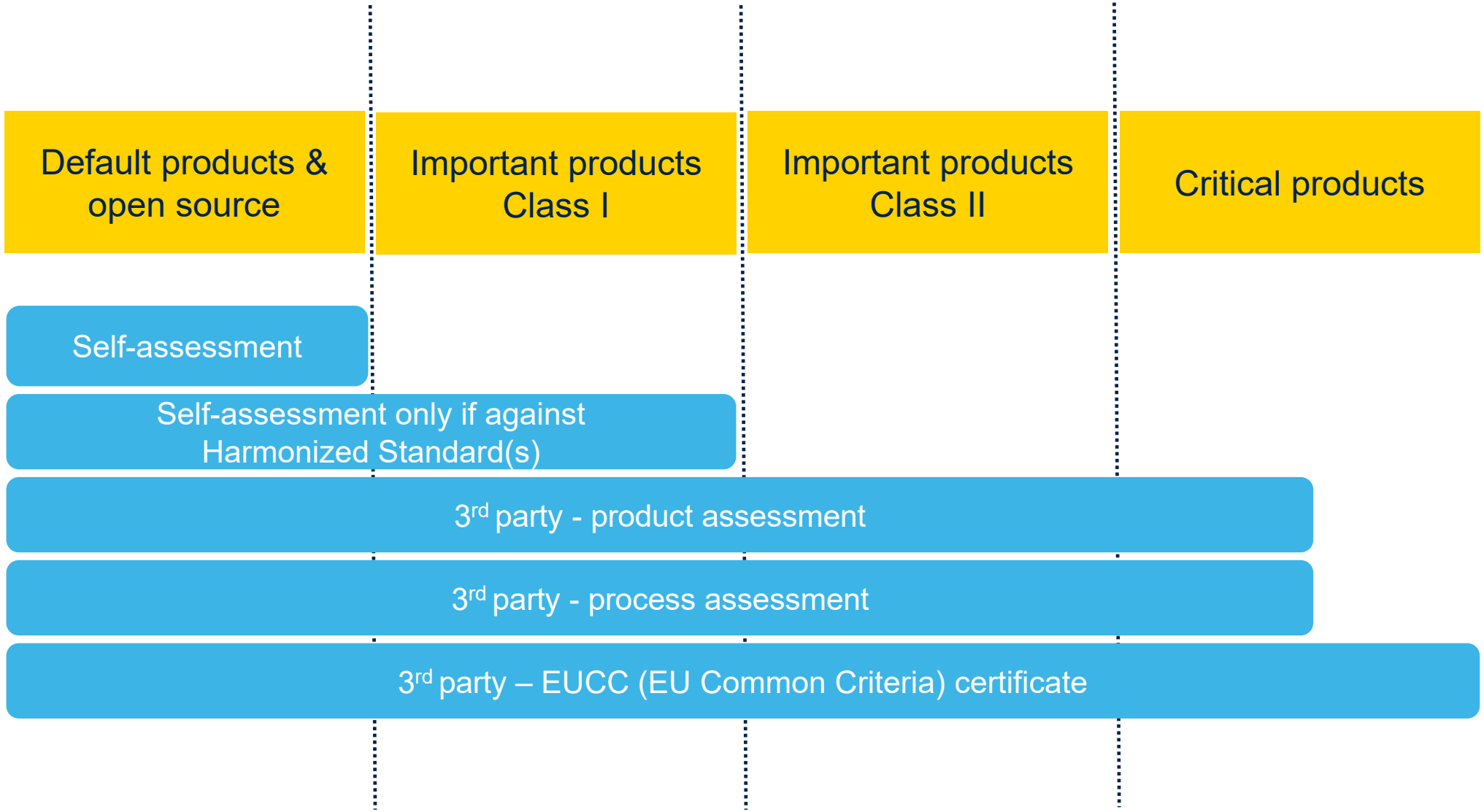
# Device manufacturer obligations under CRA over the product lifecycle

**Device specification phase:**
- Assess device security risks over its whole lifecycle
- Set and document **security policy** to put countermeasures against risks and threats identified

Security Policy

| Device development & manufacturing | Device maintenance in the field | Obligations post-maintenance |
|---|---|---|
| Develop and manufacture the object applying the countermeasures defined in the security policy:<br>• Integrate in object development the security countermeasures adequate to the object threats<br>• Manufacture the object with protection against the threats | • Report publicly security incident related to the object<br>• Report to CSIRT and ENISA exploited vulnerabilities and severe incident<br>• Ensure device security update (for at least 5 years) | Ensure security updates to remain available 10 years after publication |

# Product categories & conformity assessment

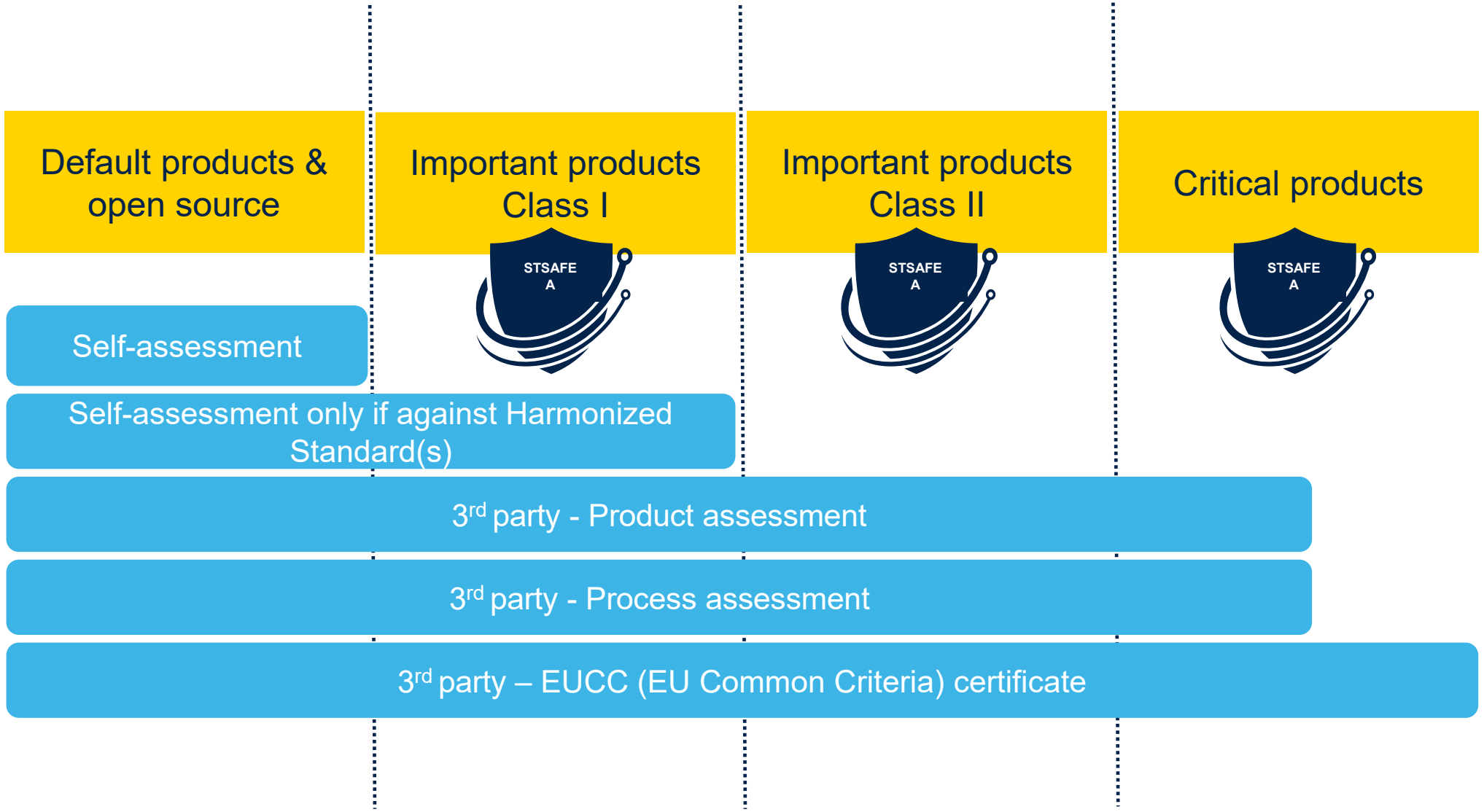


# STSAFE-A secure element contribution

# How STSAFE helps comply with CRA

| Steps | CRA obligations | STSAFE contribution |
|---|---|---|
| **Security policy specification** | • Assess device security risks over its whole lifecycle<br>• Set and document security policy to put countermeasures against risks and threats identified | • Best-in-class security **authentication companion chip** for connected devices<br>• **Common Criteria Certified** by recognized external body<br>✓ **STSAFE brings security credibility** |
| **Device development** | • Integrate in device development the security countermeasures adequate to the device threats | • Secure, seamless solution to identify and strictly authenticate devices and/or attach to Cloud / run services<br>• Secure storage of device credentials<br>✓ **Protection against attacks & on-chip data manipulation** |
| **Device manufacturing** | • Manufacture the device with protection against the threats | • Device maker keys and credential loading at ST secure certified factory site. No need to invest in complex security setup.<br>✓ **Piece of mind with secure configuration at ST certified manufacturing site** |
| **Device security maintenance** | • Publicly report security incident related to the device<br>• Report to CSIRT and ENISA exploited vulnerabilities and severe incident<br>• Ensure device security update (for at least 5 years) | • STSAFE is part of the ST PSIRT program for incident and vulnerability management.<br>• STSAFE supports in-field security updates through dedicated patches.<br>✓ **Device security incident and vulnerability reporting partially supported by STSAFE's PSIRT coverage**<br>✓ **Device security updatability can partially rely on STSAFE's security update capability** |
| **Post-maintenance** | • Ensure security updates to remain available 10 years after publication | • STSAFE security patches are free to be deployed by customers for the period of their choice |

# STSAFE-A authentication for devices in class I, II and critical



# Do not take risks with CRA compliance

**STSAFE-A is the ideal companion chip. Here is why:**

- Device authentication and credential secure storage with best-in-class, on-chip protection against manipulations
- Best-in-class secure personalization and configuration to secure end-device manufacturing
- Incident and vulnerability reporting (STSAFE-A is part of ST PSIRT program)
- STSAFE-A updatability over the time

1. Secure device implementation & ease security justification
2. Secure device configuration at manufacturing

**STSAFE-A brings best-in-class security credibility and CRA justification.**

# Secure connected devices with STSAFE-A120

## Best-in-class embedded Secure Element (eSE)

**HW CC EAL5+ certified**

### Key applications

- Consumer & Industrial IoT
- Smart Home (Matter ready)
- Healthcare
- Power supply (Open Compute Project)
- Wireless charging (Qi)
- Cordless Kitchen (Ki)

### Rich feature set

- Authentication with personalized X509 certificate
- Secure connection establishment
- Secure data storage
- Data hashing
- Signature verification

### Best-in-class hardware

- Highly secure MCU, CC EAL5+ AVA_VAN5 certified
  - ECC NIST1brainpool up 521Bits
  - AES128/256
- 16kBytes EEPROM
- 30 years data retention, 500kcycles
- Temperature range: -40C to 105C
- SO8N, DFN8 2x3



### Personalization

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

# STSAFE-A120
# Benefits for CRA compliance

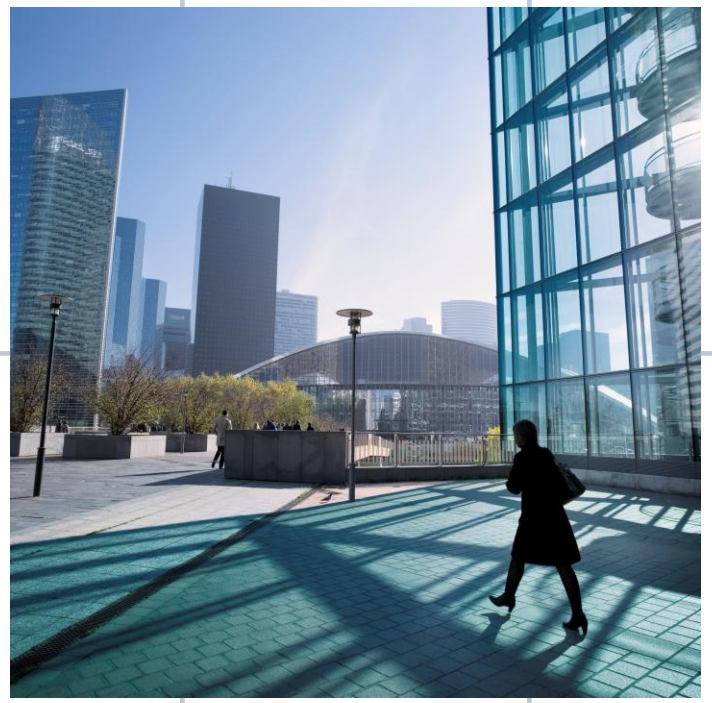
| | STSAFE-A features | Direct benefits for CRA compliant device |
|---|---|---|
| **STSAFE-A** provides certified security by default.<br><br>It supports device security implementation | A secure companion chip that manages the critical device identity (X.509 certificate private key) | Identity allowing distinction between genuine device and malicious device |
| | Best-in-class tamper-proof protection of private key | Prevent identity cloning from attacks on-chip or side-channel attacks |
| | Offer security protocol for device attestation and secure connection establishment | Ensure data protection transiting from device to service (Cloud) |
| | Offer secure storage with counters and immutable sections | Offer a secure storage for credentials or attestation keys |
| | Secure loading of device identity credentials at ST secure manufacturing sites | Prevent identity cloning through leakage at manufacturing or configuration |
| | Common Criteria certified (EU CC EAL5+ AVA_VAN5) | Ease device conformity (up to CRA Class CRITICAL) |
| | In-the-field updatability | Ease device security function updatability |
| | PSIRT vulnerabilities public reporting | Ease device vulnerability public reporting |

# Useful resources

Product page
Visit here

STSAFE personalization services
Discover now

STSAFE & CRA webinar
Watch here



Product presentation
Download

Q&A on CRA
Visit here

CRA webpage
Visit here

# Our technology starts with You

Find out more at st.com