



TECHNICAL BRIEF · STM32H5 × EU CYBER RESILIENCE ACT

STM32H5

as a CRA-ready foundation

How the STMicroelectronics STM32H5 family's built-in security — TrustZone, immutable Root of Trust, cryptographic accelerators, MCE, OTFDEC, Debug Authentication — maps to the essential requirements of Regulation (EU) 2024/2847 Annex I § 1 and § 2.

Cortex-M33

with Arm TrustZone

PSA L3 / SESIP L3

certification target

AES / SHA / PKA / TRNG

on-chip crypto accelerators

STiRoT + OEMiRoT

immutable Root of Trust

PREPARED BY

BlackIoT Sagl — redesigning electronic products for EU CRA compliance.

01 · CONTEXT

The question manufacturers face

The CRA demands secure products. Silicon choice decides how hard — or easy — compliance becomes.

ANNEX I § 1

Product properties

Hardware must provide root of trust, isolation between trusted and untrusted code, cryptographic services, memory and code protection, and secure firmware update mechanisms. None of these can be bolted on after fabrication.

ANNEX I § 2

Vulnerability handling

Manufacturers must ship signed firmware updates for the declared support period, operate a PSIRT with coordinated disclosure, and produce a machine-readable SBOM. The silicon vendor's own security hygiene matters here too.

THE MCU CHOICE

Feasibility gate

Choosing an MCU without a TrustZone-capable core, no hardware root of trust, no crypto accelerators, or no supported secure-update stack forces CRA compliance onto software — expensive and brittle. A security-first MCU shifts the burden to hardware.

STM32H5 POSITION

Designed for this

ST released STM32H5 in 2023 with CRA, PSA Certified Level 3, and SESIP Level 3 explicitly in scope. Its security feature set directly addresses the Annex I requirements — and ST provides the tooling to operationalise them.

02 · STM32H5 FAMILY

STM32H5 at a glance

Arm Cortex-M33 mainstream MCUs with a security-first architecture.

CORE SPECIFICATIONS

| | |
|---------------|---|
| CPU | Arm Cortex-M33 @ up to 250 MHz |
| TrustZone | Armv8-M Security Extension (SAU, IDAU) |
| Flash | Up to 2 MB dual-bank, ECC, PCROP, WRP |
| SRAM | Up to 640 KB, MPU + GTZC protection |
| Crypto | AES, SAES, HASH (SHA-1/2), PKA (RSA, ECDSA), TRNG |
| Memory cipher | MCE (internal) · OTFDEC (external QSPI/OCTOSPI) |
| Debug | SWD + JTAG with Debug Authentication |
| Tamper | TAMP peripheral + backup register erase |

VARIANTS

Security feature matrix

| | |
|--------------------|--|
| H503 | entry — crypto accel, RDP, TrustZone |
| H523 / H533 | mid-range — adds OTFDEC, OBK |
| H562 / H563 | high-perf — adds STiRoT, MCE |
| H573 | top tier — adds OEMiRoT, SAES, full Debug Auth |

This brief focuses on H573 because it enables the full security stack; most features are also available on H56x.

03 · ARCHITECTURE

The six security layers

STM32H5 combines hardware primitives into a defence-in-depth stack. Each layer supports specific CRA requirements.

LAYER 1

Root of Trust

STiRoT (ST-provisioned, immutable in ROM) and OEMiRoT (manufacturer-provisioned, in protected flash). Verify every image in the boot chain via ECDSA P-256 or RSA-3072 before execution.

LAYER 2

Isolation

Cortex-M33 TrustZone partitions memory and peripherals. GTZC (TZIC + TZSC + MPCBB) extends secure/non-secure attribution to RAM blocks and peripherals.

LAYER 3

Cryptographic services

Hardware AES, SAES (key-never-in-software variant), SHA-1/256/384/512, HMAC, PKA (RSA up to 4096, ECDSA up to P-521, Curve25519), and NIST SP800-90B TRNG.

LAYER 4

Memory & code protection

RDP levels 0–2, WRP, PCROP, HDP, MCE (AES-GCM for internal memory), OTFDEC (AES-CTR for external QSPI/OCTOSPI), Option Byte Keys (OBK) for secure provisioning.

LAYER 5

Secure boot & update

Built-in secure boot via STiRoT/OEMiRoT eliminates X-CUBE-SBSFU dependency. Dual-bank flash supports A/B update. Anti-rollback via NVCOUNTER in OTP.

LAYER 6

Debug, tamper, life-cycle

Debug Authentication (ECDSA-P256 challenge/response, tokenised permissions). TAMP peripheral with active/passive anti-tamper I/Os. Closed / Closed-Locked life-cycle states.

04 · ISOLATION

TrustZone + GTZC — hardware partitioning

Enforce secure/non-secure separation at the CPU bus level, without relying on software discipline alone.

CPU-LEVEL

- Armv8-M Security Extension — two execution states (S / NS) per core.
- SAU (Security Attribution Unit): up to 8 regions mark memory S / NS / NSC.
- IDAU: fixed hardware default map that the SAU can override.
- NSC regions hold veneer functions — the only callable entry points from NS into S.
- Banked SP_S / SP_NS stack pointers and SysTick timers isolate context.

SYSTEM-LEVEL – GTZC

- TZSC: TrustZone Security Controller — peripherals can be set S or NS.
- TZIC: TrustZone Illegal Access Controller — traps every unauthorised access and raises a secure interrupt.
- MPCBB: Memory Protection Controller Block-Based — assigns each 512-byte SRAM block to S or NS.
- MPCWM: Memory Protection Controller Watermark — protects external QSPI/OCTOSPI memory regions.
- Writable lock-until-reboot: attacks that flip TrustZone attribution post-boot are blocked.

CRA MAPPING

Satisfies Annex I § 1(c) "protection from unauthorised access", § 1(h) "limitation of attack surfaces", § 1(i) "reduce the impact of an incident".

05 · ROOT OF TRUST

STiRoT and OEMiRoT — anchoring the boot chain

Every byte of code executed on the device is verified before execution, anchored in immutable ROM.

STiRoT

ST immutable RoT

Stored in masked ROM. Always trusted. Verifies the first customer image (OEMuRoT or application) using an ECDSA P-256 or RSA-3072 public key programmed by ST. Cannot be updated or bypassed; it is the silicon root.

OEMiRoT

OEM immutable RoT

Optional customer-provisioned RoT loaded into protected flash. Once installed and locked, it becomes immutable within the silicon life-cycle. Gives the manufacturer control over the first mutable stage while keeping silicon trust.

CHAIN

Boot chain

ROM → STiRoT → OEMiRoT → Secure application (S) → Non-Secure application (NS). Each stage verifies the next. Signatures use ECDSA P-256 or RSA-3072. Anti-rollback via NVCOUNTER monotonic counter in OTP.

CRA MAPPING

Satisfies Annex I § 1(a) "secure-by-design", § 1(f) "availability", § 1(j) "secure update path", § 2(2-c) "security updates without delay".

06 · CRYPTOGRAPHY

Hardware cryptographic services

On-chip accelerators remove the performance and side-channel penalty of software crypto.

AES · SAES

Symmetric

AES-128/192/256 with ECB/CBC/CTR/GCM/CCM. SAES variant loads keys from OBK or hardware only — keys never become visible to software. DPA-countermeasure hardened.

HASH · HMAC

Hashing

SHA-1, SHA-224, SHA-256, SHA-384, SHA-512. HMAC with any of those. Used for SBOM integrity, firmware signatures, log attestation, CRA-aligned integrity mechanisms.

PKA

Public key

RSA encryption, signature, key-pair up to 4096-bit. ECDSA and ECDH on P-256, P-384, P-521 and Curve25519. Side-channel hardened. Used by STiRoT / OEMiRoT and TLS handshakes.

TRNG

True RNG

NIST SP800-90B compliant entropy source with AIS-31 health tests. Feeds cryptographic key generation, nonces, and challenge-response protocols. A weak RNG breaks everything above it.

07 · MEMORY PROTECTION

Protecting code and data at rest

Multiple independent controls. Each addresses a different class of attack — readback, rollback, side-channel, cold-boot.

RDP

Read-out Protection

Level 0 (open) → 0.5 (debug off, update allowed) → 1 (memory read blocked, debug off) → 2 (irreversible lock). Regression from 1 erases flash — secure factory reset.

WRP · PCROP

Write & code protection

WRP: per-sector flash write protection. PCROP: executable-only region — code runs but cannot be read out even when other protections are lowered.

HDP

Hide Protection

Portions of flash become inaccessible after secure boot completes. Keys, vendor IP, measurement values vanish from the accessible address space before untrusted code runs.

MCE · OTFDEC

Transparent memory cipher

MCE: AES-GCM over internal SRAM / flash, keys in hardware only. OTFDEC: AES-CTR decrypts external QSPI / OCTOSPI memory on the fly — ships firmware encrypted on the external chip.

OBK

Option Byte Keys

Dedicated OTP-like flash pages for key material, provisioned at factory. Hardware enforces that only the crypto engines can read them — software, even secure software, cannot.

UNIQUE ID

Device identity

96-bit factory-programmed unique identifier. Basis for device-bound cryptographic keys (HKDF-derived) and attestation. Underpins per-device vulnerability reporting and revocation.

08 · BOOT & UPDATE

Secure boot and secure firmware update

The end-to-end flow the CRA expects — delivered by the silicon, not bolted on by the application.

AT BOOT

- Silicon always starts executing STiRoT from ROM — no branch possible.
- STiRoT verifies OEMiRoT signature (ECDSA-P256 or RSA-3072).
- OEMiRoT verifies active firmware image against its anti-rollback counter.
- Only verified images are allowed to execute; mismatch triggers failsafe boot.
- TrustZone attribution is locked and HDP regions become inaccessible.

DURING UPDATE

- Download signed + encrypted image (AES-CTR or AES-GCM) into inactive bank.
- Verify signature against OEMiRoT public key and check anti-rollback counter.
- Swap active bank on next reset (dual-bank A/B); revert automatically on boot failure.
- Bump NVCOUNTER in OTP — previous image can never be re-accepted.
- Distribute free-of-charge throughout the declared CRA support period.

CRA MAPPING

Directly satisfies Annex I § 1(k) "security updates without delay, free of charge" and § 2(2-b, 2-e) update distribution requirements.

Production security posture

Leaving SWD open ships a backdoor. STM32H5 provides graded debug access and physical anti-tamper.

DA

Debug Authentication

ECDSA-P256 challenge/response binds the debug adapter to an OEM-signed permission token. Tokens grant graded access: full, partial (e.g. NS-only), or none. Regression token returns device to factory in one step.

LIFE-CYCLE

Closed / Closed-Locked

Silicon transitions through Open → Closed → Closed-Locked states. Each transition is one-way and tightens debug, update, and provisioning capabilities. Closed-Locked cannot be reverted.

TAMP

Tamper detection

Four active I/Os (cryptographically paired pulse) plus internal monitors (temperature, voltage, clock). Detection erases backup registers and secret keys on the fly, optionally triggers reset and logs the event.

LOGGING

Event logging

TAMP, illegal-access (TZIC), boot-failure, update-failure, and ECC-error events are captured and retained across reset. Feeds upstream monitoring and CRA § 1(h) "record and monitor relevant internal activity".

Product cybersecurity requirements — STM32H5 coverage

Each § 1 requirement against the specific STM32H5 feature that addresses it.

| CRA Annex I requirement | How STM32H5 helps satisfy it |
|--|---|
| § 1(a) Secure-by-design, by-default configuration | STiRoT + OEMiRoT anchor every boot; Closed-Locked life-cycle prevents regression. |
| § 1(b) Protection from unauthorised access | RDP Level 1/2, Debug Authentication, HDP, OBK key isolation. |
| § 1(c) Confidentiality & integrity of stored data | MCE (AES-GCM internal), OTFDEC (AES-CTR external), OBK, WRP, PCROP. |
| § 1(d) Confidentiality & integrity of transmitted data | AES / SAES for symmetric, PKA (RSA, ECDSA, ECDH) for TLS handshakes, TRNG. |
| § 1(e) Process only minimum personal data necessary | Enabler: TrustZone isolates data-processing domains; app design determines scope. |
| § 1(f) Protection of availability · DoS resilience | Dual-bank A/B flash, watchdogs, Clock Security System, automatic bank-swap on boot failure. |
| § 1(g) Minimise impact on other devices / networks | GTZC peripheral attribution isolates network interfaces from application code. |
| § 1(h) Limit attack surfaces, external interfaces | TrustZone (SAU, IDAU, NSC), GTZC (TZSC, TZIC, MPCBB, MPCWM), Debug Auth tokens. |
| § 1(i) Reduce impact of an incident | HDP hides secrets post-boot; TAMP erases backup registers; RDP regression wipes flash. |
| § 1(j) Security-related information logged and monitored | TAMP events, TZIC illegal-access log, ECC errors retained across reset. |
| § 1(k) Security updates without delay, free of charge | Built-in Secure Boot + Secure FW Update; dual-bank; anti-rollback via NVCOUNTER OTP. |

Vulnerability handling requirements — STM32H5 coverage

Most § 2 items are process, not silicon — but some silicon support is essential.

| CRA Annex I requirement | How STM32H5 helps satisfy it |
|---|---|
| § 2(1) Identify and document components (SBOM) | ST publishes an SBOM for STM32Cube HAL, Cryptolib, and the TF-M secure partitions used by STiRoT/OEMiRoT. |
| § 2(2-a) Address vulnerabilities without delay | Built-in signed update mechanism (see page 9) makes fixes deployable end-to-end. |
| § 2(2-b) Apply effective security testing | Pre-verified: STM32H5 targets PSA Certified Level 3 and SESIP Level 3 third-party evaluation. |
| § 2(2-c) Security updates free of charge | STM32CubeProgrammer, STM32CubeIDE, and OEMiRoT loader stack shipped at no cost by ST. |
| § 2(2-d) Public disclosure of fixed vulnerabilities | ST PSIRT publishes security advisories with CVE references and affected part numbers. |
| § 2(2-e) Coordinated vulnerability disclosure policy | ST operates a CVD policy aligned with ISO/IEC 29147 — contact: psirt@st.com. |
| § 2(3) Secure distribution of updates | Firmware images encrypted (AES) and signed (ECDSA/RSA); verified by OEMiRoT before swap. |
| § 2(6-b) Mechanisms for automatic application of security updates | STiRoT/OEMiRoT + dual-bank boot enables silent, atomic, failsafe updates. |
| § 2(6-c) Machine-readable advisory format (CSAF) | ST publishes advisories in CSAF 2.0-compatible format via its security advisories portal. |

12 · THE REST OF THE STACK

What STM32H5 does not give you for free

Silicon is an enabler. These items remain the manufacturer's responsibility under the CRA.

APP-LEVEL

Application code

No MCU can compensate for a buffer overflow in your firmware. Secure coding, SAST/DAST, fuzzing, and peer review stay on the critical path. TrustZone reduces the blast radius, not the bug count.

SBOM

Your SBOM

ST's SBOM covers their stack. You must produce a machine-readable SBOM (SPDX or CycloneDX) for YOUR firmware — every third-party library, every version. Keep it updated on every release.

PSIRT

Your PSIRT

Coordinated vulnerability disclosure, 24h / 72h / 14d reporting to ENISA, CVE coordination, CSAF advisories, credit to reporters — this is your process, not ST's.

KEYS

Key management

OEMiRoT public key, update signing key, attestation keys. Generate, store, rotate, and revoke them. A key leak compromises every unit shipped — plan the HSM and ceremony before first silicon.

SUPPORT

Declared support period

The CRA requires a declared support period proportional to expected use (minimum five years in many cases). Commit to shipping updates. Plan engineering capacity. Budget accordingly.

CONFORMITY

Conformity assessment

Technical file, Declaration of Conformity, CE marking — product-level work. For Annex III Important or Annex IV Critical products, add Notified Body liaison.

13 · HOW BLACKIOT HELPS

From STM32H5 silicon to a CRA-compliant product

BlackIoT's engineering services bridge the gap between what the MCU enables and what the regulation demands.

ON THE SILICON

- STM32H5 reference-design based on our WildBay / Vallarta carriers.
- TrustZone partitioning and GTZC attribution designed into schematic + firmware.
- OEMiRoT provisioning flow with HSM-backed key ceremony.
- Dual-bank secure update over the declared support period.
- PSA Certified Level 3-ready firmware skeleton delivered in source.

AROUND THE SILICON

- Machine-readable SBOM (SPDX / CycloneDX), generated and maintained per release.
- PSIRT workflow + coordinated disclosure policy + 24h / 72h / 14d ENISA reporting.
- CSAF 2.0 security advisory pipeline integrated with your release process.
- Technical file, EU Declaration of Conformity, CE marking support.
- IPC Class 3 PCB design when reliability or aerospace-grade build is required.

CONTACT

info@blackiot.swiss · www.blackiot.swiss · Vacallo, Switzerland · CHE-192.005.916



Primary sources

This brief is synthesised from the following documents. Refer to them for any design decision.

| | |
|----------------------------------|---|
| RM0481 | STM32H5 Reference Manual — Security chapter (GTZC, TrustZone, MCE, OTFDEC). |
| AN5938 | STM32H5 Security overview Application Note. |
| AN5156 | Introduction to STM32 microcontrollers security. |
| UM2262 | Getting started with STM32CubeProgrammer. |
| X-CUBE-SBSFU | Secure Boot and Secure Firmware Update solution (applicable where STiRoT not used). |
| PSA Certified | psacertified.org — Level 3 certificate for STM32H5 family. |
| ST PSIRT | www.st.com/psirt — security advisories and coordinated disclosure contact. |
| Regulation (EU) 2024/2847 | eur-lex.europa.eu/eli/reg/2024/2847/oj — authoritative CRA text. |
| ENISA | enisa.europa.eu — CRA guidance, reporting platform, CSAF 2.0 format. |

This document is a technical brief — not legal advice. For interpretation of the Regulation, consult the EUR-Lex text and qualified counsel.