Technical Note

STM32MP25x Product Family SESIP Security Target

Document information

This security target document is based on GlobalPlatform® Security Evaluation Standard for IoT Platforms (SESIP), version 1.2 (July 2023), GP_FST_070.

1 Introduction

This Security Target describes the STM32MP25x platform and the exact security properties of the platform that are evaluated against GlobalPlatform® Security Evaluation Standard for IoT Platforms [SESIP].

The Protection Profile reference and conformance claims for this security target are described below.

Table 1. SESIP profile for Secure MCUs and MPUs conformance claims

Reference	Value
SP name	SESIP Profile for Secure MCUs and MPUs [SP1]
SP version	1.0
Package claim	Base SP, Security Services, Software Isolation, Hardware Protections
Assurance claim	Refer to Section 3.1

Table 2. SESIP profile for PSA certified RoT component conformance claims

Reference	Value
SP name	SESIP Profile for PSA Certified RoT Component Level 3 [SP2]
SP version	1.0
Optional and additional SFRs	Base profile
Assurance claim	Refer to Section 3.1

1.1 Security Target Reference

This document: TN1533 STM32MP25x Product Family SESIP Security Target, Revision 1, STMicroelectronics.

1.2 Platform Reference

Table 3. Platform reference

Reference	Value
Platform name	STM32MP25 Series Arm® -based 32/64-bit MPUs
Platform version	Revision 2.1
Platform identification	STM32MP25xC, STM32MP25xF
Platform type	General purpose microprocessor device for IoT, industrial, or consumer applications.

1.3 Included Guidance Documents

The following documents are included with the platform:

Table 4. Guidance documents

Category	Name	Reference
User Manual	UM3370 STM32MP25x security guidance for SESIP level 3 certification	[SG]
Product reference manual	RM0457 reference manual STM32MP25xx advanced Arm®-based 32/64-bit MPUs	[RM]
Errata sheet	ES0598 STM32MP251x/3x/5x/7x device errata	[ES]

1.4 Platform Functional Overview and Description

1.4.1 Platform type

The platform in the STM32MP25 series is a second-generation of microprocessors enabling secure, advanced edge AI in the Industry 4.0. STM32MP25x devices include enhanced security features such as TrustZone^{TM} on Cortex$^{®}$-A35 and Cortex$^{®}$-M33, STM32 Compartment ID for runtime protection, OTP, crypto accelerators and ROM-based immutable root of trust. Refer to [RM] Section 5 for more details.

The platform consists of an Arm$^{®}$ Cortex$^{®}$-A35 processor executing in isolation embedded ROM code thanks to TrustZone^{TM} and STM32 Compartment ID technologies. It also includes embedded SRAM, non-volatile fuses, cryptographic accelerators, and a true random number generator.

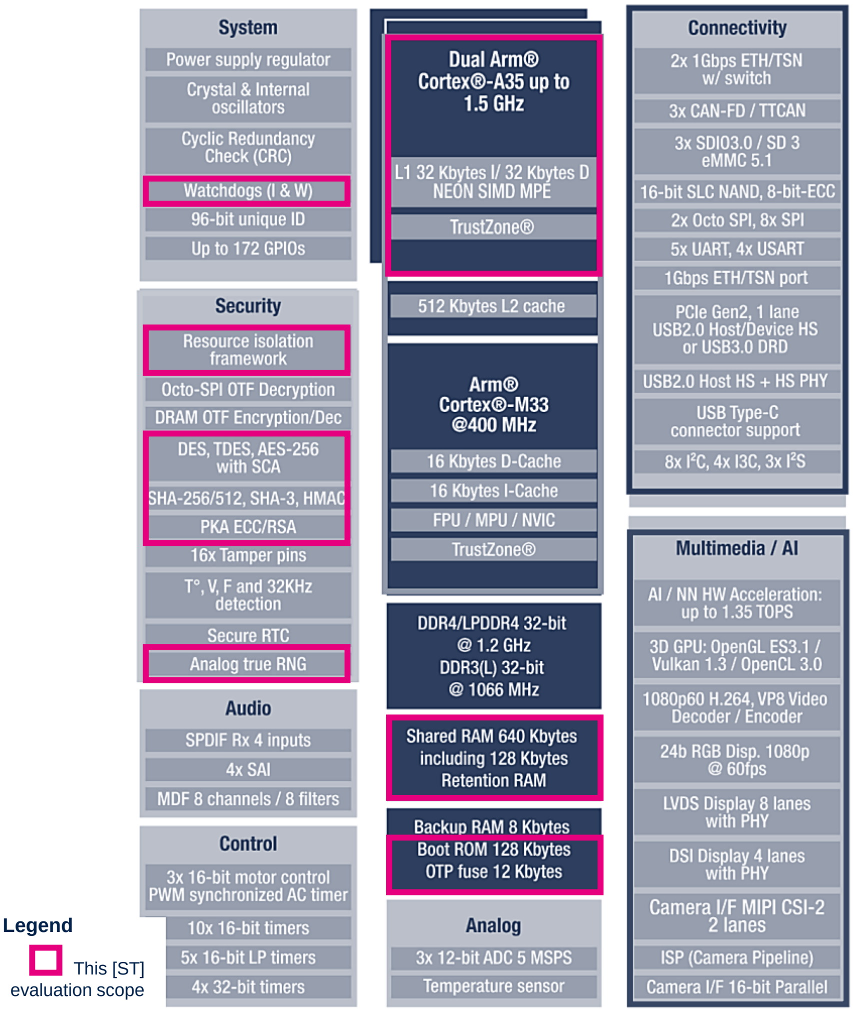
The platform provides the necessary hardware and immutable code building blocks for the platform integrator to implement a connected platform as defined in the SESIP Profile for Secure MCUs and MPUs [SP1]. It can also be a basis for further composition of evaluation activities.

Note: Arm and TrustZone are registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

1.4.2 Platform physical scope

The physical scope of the platform is implemented in the STM32MP25 series of MPU products identified in Section 1.2. The block diagram in Figure 1 provides an overview of the major features supported by this MPU. The features in the scope of the platform are highlighted in red.

Figure 1. STM32MP25x block diagram


System
Power supply regulator
Crystal & Internal oscillators
Cyclic Redundancy Check (CRC)
Watchdogs (I & W)
96-bit unique ID
Up to 172 GPIOs
Security
Resource isolation framework
Octo-SPI OTF Decryption
DRAM OTF Encryption/Dec
DES, TDES, AES-256 with SCA
SHA-256/512, SHA-3, HMAC
PKA ECC/RSA
16x Tamper pins
T°, V, F and 32KHz detection
Secure RTC
Analog true RNG
Audio
SPDIF Rx 4 inputs
4x SAI
MDF 8 channels / 8 filters
Control
3x 16-bit motor control PWM synchronized AC timer
10x 16-bit timers
5x 16-bit LP timers
4x 32-bit timers
Dual Arm® Cortex®-A35 up to 1.5 GHz
L1 32 Kbytes I/ 32 Kbytes D NEON SIMD MPE
TrustZone®
512 Kbytes L2 cache
Arm® Cortex®-M33 @400 MHz
16 Kbytes D-Cache
16 Kbytes I-Cache
FPU / MPU / NVIC
TrustZone®
DDR4/LPDDR4 32-bit @ 1.2 GHz DDR3(L) 32-bit @ 1066 MHz
Shared RAM 640 Kbytes including 128 Kbytes Retention RAM
Backup RAM 8 Kbytes
Boot ROM 128 Kbytes
OTP fuse 12 Kbytes
Analog
3x 12-bit ADC 5 MSPS
Temperature sensor
Connectivity
2x 1Gbps ETH/TSN w/ switch
3x CAN-FD / TTCAN
3x SDIO3.0 / SD 3 eMMC 5.1
16-bit SLC NAND, 8-bit-ECC
2x Octo SPI, 8x SPI
5x UART, 4x USART
1Gbps ETH/TSN port
PCIe Gen2, 1 lane USB2.0 Host/Device HS or USB3.0 DRD
USB2.0 Host HS + HS PHY
USB Type-C connector support
8x I²C, 4x I3C, 3x I²S
Multimedia / AI
AI / NN HW Acceleration: up to 1.35 TOPS
3D GPU: OpenGL ES3.1 / Vulkan 1.3 / OpenCL 3.0
1080p60 H.264, VP8 Video Decoder / Encoder
24b RGB Disp. 1080p @ 60fps
LVDS Display 8 lanes with PHY
DSI Display 4 lanes with PHY
Camera I/F MIPI CSI-2 2 lanes
ISP (Camera Pipeline)
Camera I/F 16-bit Parallel
Legend
This [ST] evaluation scope

The hardware components and interfaces that constitute the platform is defined in Table 5. They are described in the [RM] reference manual and [ES] errata sheet.

Table 5. Hardware components and interfaces of the TOE

Component/Interface	Description	Identification
CPU	Cortex-A35 subsystem (includes MMU and caches)	Hardware revision [1]
Communication ports	-	
Memories	ROM, SYSRAM, RETRAM	
Infrastructure	RCC, PWR, BSEC, RIFSC, RISAB1/2/5, IWDG1/2, TAMP, SYSCFG, STGEN, FMC, GPIO	
Cryptography	SAES, PKA, CRYP1, HASH, RNG	

[1] Refer to Platform version in Table 3 of Section 1.2

1.4.3 Platform logical scope

The software components and interfaces that constitutes the platform are shown on Figure 2, and listed in Table 6. Any additional firmware, OS or application software stored on the platform is not in scope of this evaluation. As shown the STM32MP25 Series of MPU products embeds three Arm® Cortex® cores (A35, M33 and M0+), with two cores supporting TrustZone™ technology (C-A35, C-M33).

Figure 2. Platform logical scope

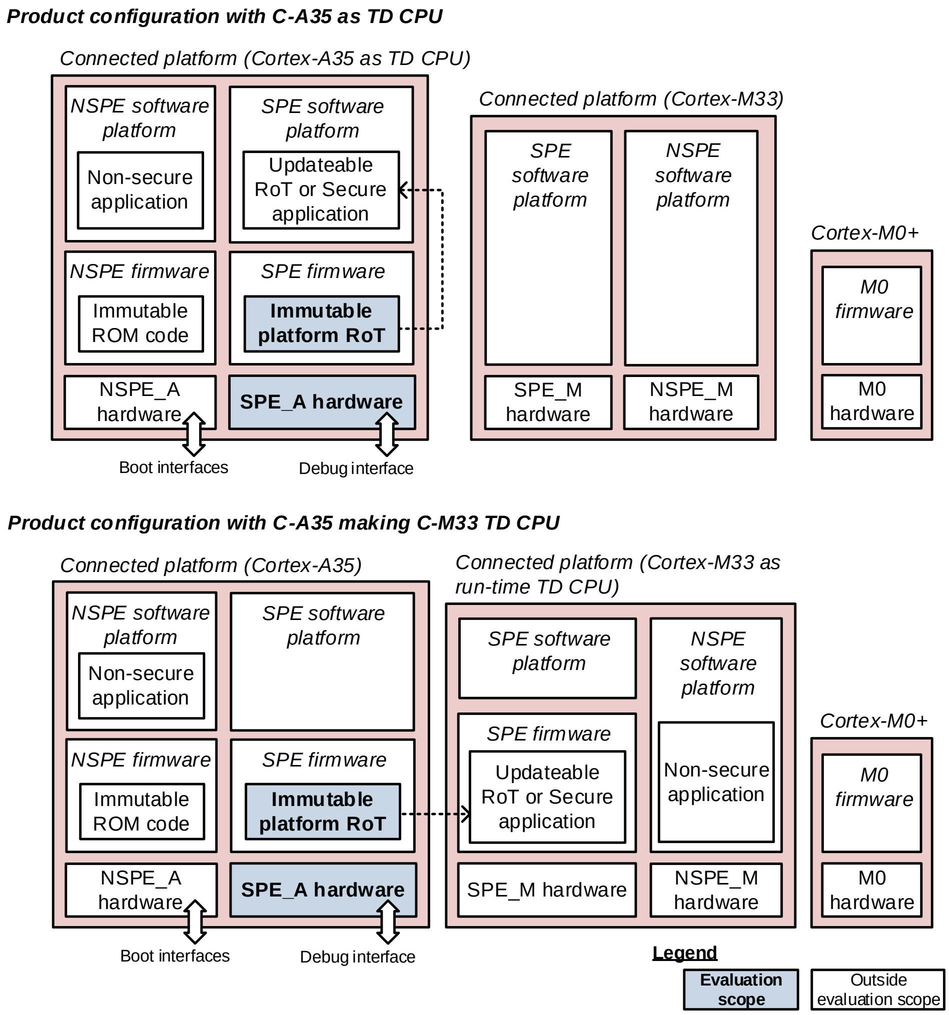


Table 6. Software components and interfaces of the TOE

Component/Interface	Description	Identification/Version
Boot ROM (secure)	Embedded ROM code reserved to Cortex-A35 running in SPE mode.	Same as the silicon (1)
APIs	*Not supported*	*Not applicable*

(1) Refer to Platform version in Table 3 of Section 1.2

The logical scope of the platform includes:

- the security lifecycle resource summarized in Section 1.4.4,
- the cryptographic operations with random number generation,
- and the immutable platform Root of Trust with boot code (running in the C-A35 SPE), any root parameters, with management, enforcement or monitoring of the isolation hardware resources related to the immutable RoT functionality.

Note: As shown on Figure 2 the immutable platform RoT is used in two configurations; the C-A35 is TD CPU, or the C-A35 makes C-M33 TD CPU as part of the boot process. Refer to Section 3.3.2 for details.

The logical scope of the platform does not include:

- The updateable Platform Root of Trust, being for example, the main bootloader code and its related root parameters, the code that implements the SPE partition management function, and the code that implements the secure firmware update of the product.
- The trusted subsystem components on which the final IoT product relies to build the connected platform described in the SESIP profile [SP1].

1.4.4 Platform security features and usage

The platform, defined in Sections 1.4.2 and 1.4.3, supports the following major security features:

- Following any device reset the platform executes its embedded secure ROM code, ensuring the second stage of the microprocessor trusted boot chain. Multiple mode of operations is supported (see Section 3.3.2).
- Residual information purging for life cycle handling.

Optional packages in [SP1] have been selected to accommodate the context of use of the platform:

- Cryptographic operations, based on hardware cryptographic accelerators (Secure AES, PKA).
- True random number generator (RNG) that provides full entropy outputs to the application.
- Hardware protection to handle hostile environments.
- Isolation mechanisms controlling access between certified and non-certified parts of the software building the product.

Regarding security features please note the following:

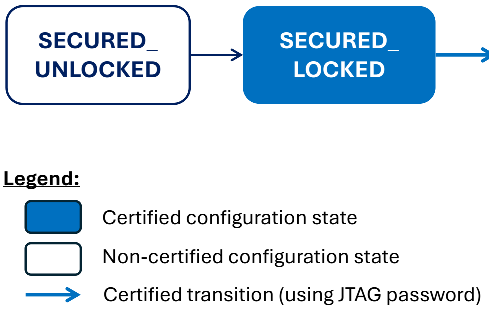
- Secure debugging of the platform is implemented but not accessible to the users. Debugging of the non-TOE application can be activated using an authenticated boot image in certified configuration (no debug by default).
- Secure update of platform is not applicable since the platform does not support the patching of the embedded ROM.
- The C-M33 executing in SPE is not part of the platform (see Section 1.4.3).

Platform usage is detailed in the guidance documentation [SG].

Life Cycle

The product life cycle shown in Figure 3, is used in the SFRs when references to a life cycle are required. The product on-the-field should imperatively be configured in “*Secured_locked*”, in accordance with [SG] Section 3.2.3.

Figure 3. Reference product life cycle


SECURED_ UNLOCKED
SECURED_ LOCKED
RMA
Legend:
Certified configuration state
Non-certified configuration state
Certified transition (using JTAG password)

STMicroelectronics delivers “*Secured_unlocked*” STM32MP25x devices without RoT keys or RMA password provisioned. The provisioning of those is described in the [SG] Section 3.2.2.

The integrity and confidentiality of the platform during the life of the STM32MP25x devices is ensured because the ROM part of the TOE and the TOE secrets are hidden from the integrator code or debugger.

The transition to “*RMA*” state is initiated via the JTAG interface by the integrator using its own 128-bit password. After integrator-defined X consecutive wrong password attempts (X<5), the RMA sequence always fails.

As mentioned in *Nonvolatile storage of secrets in OTP* of the [SG] Section 4.2.1, the integrator must store its security-sensitive information (secrets AES keys, private ECC or RSA keys) in OTP words 256 to 367, so that no secret information leaks when the device goes to “*RMA*” state.

Use Case

The platform is intended to be used by an integrator wishing to implement a secure boot with the necessary Root of Trust services.

The environmental conditions under which the platform in certified configuration can be securely used are defined below:

- [**Any user**] the product may be physically accessed by an unknown or untrusted user, in an environment where access to the product cannot be sufficiently controlled or even in a more hostile environment.
- [**Any code**] it cannot be excluded that the product will execute code that is unknown to the product developer.

1.4.5 Required Hardware/Software/Firmware

As defined in Section 1.4.3 the platform includes a single software component in the evaluation perimeter (C-A35 immutable ROM code, executing in SPE).

Required non-platform hardware/software/firmware (ASE_INT.1.6C)

The platform aims to host an *updatable platform Root of Trust* or a *secure application* in a subsequent composed platform as shown in Figure 2.

Consequently, the platform requires a trusted firmware to achieve at least the following operation on the platform itself:

- Configuration of RIF
- Keeping the *jump address to Dstandby wakeup* unchanged (see Section 3.3.2 for details)

The required non-platform trusted firmware expectations are exhaustively described in [SG] Section 4.2.2.

2 Security Objectives for the Operational Environment

2.1 Platform Objectives for the Operational Environment

For the platform to fulfil its security requirements, the operational environment (technical or procedural) must fulfil the following objectives.

- The operating system or application code is expected to verify the correct version of all platform components that it depends on, as described in the Section 1.2.
- The operating system or application code is expected to make use of the secure boot feature as described in the Section 3.3.2.

2.2 Inherited Objectives for the Operational Environment

This is inapplicable as the platform is not composite.

3 Security Requirements and Implementation

3.1 Security Assurance Requirements

The claimed assurance requirements package is **SESIP Assurance Level 3 (SESIP3)**, as defined in Chapter 4 of GlobalPlatform® Technology Security Evaluation Standard for IoT Platforms [SESIP].

3.2 Flaw Reporting Procedure (ALC_FLR.2)

The SFR Secure update of platform is not applicable since the platform does not support the patching of the immutable ROM firmware. Outside the platform the integrator can implement their own secure update mechanism in their code, leveraging the boot image revocation method (see [SG] Section 4.2.1 for details).

In accordance with the requirement for a flaw reporting procedure (ALC_FLR.2), including a process to generate any needed update and distribute it, the developer has defined the procedure described in [PSIRT].

3.3 Base SP Security Functional Requirements

The platform fulfills the following security functional requirements:

3.3.1 Verification of Platform Identity

The platform provides a unique identification of the platform, including all its parts and their versions.

Conformance rationale:

The platform referred to in Section 1.2 provides the identifiers listed on Table 7.

Table 7. **Platform identifiers**

Field	Address	Value (halfword)	Comments
Device identifier (DEV_ID)	0x5423 6400 (SYSCFG_IDC on AHB4)	0x0505	STM32MP25x
Major revision identifier (MAJOR_REV_ID)		0x2000	Major revision 2

The platform stores the minor revision information as Revision Identification (REV_ID) in OTP word 102 (value= 0x11). One method to read it is described in *Secure acceptance* of [SG] Section 3.1.

3.3.2 Secure Initialization of Platform

The platform ensures its authenticity and integrity during the platform initialization. If the platform's authenticity or integrity cannot be ensured, the platform will go to locked state.

Conformance rationale:

Following any device reset the platform executes its embedded secure ROM code, ensuring the second stage of the microprocessor trusted boot chain. As described on Figure 4 and Table 8, the secure initialization of platform has multiple modes of operation.

Table 8. **Secure initialization options**

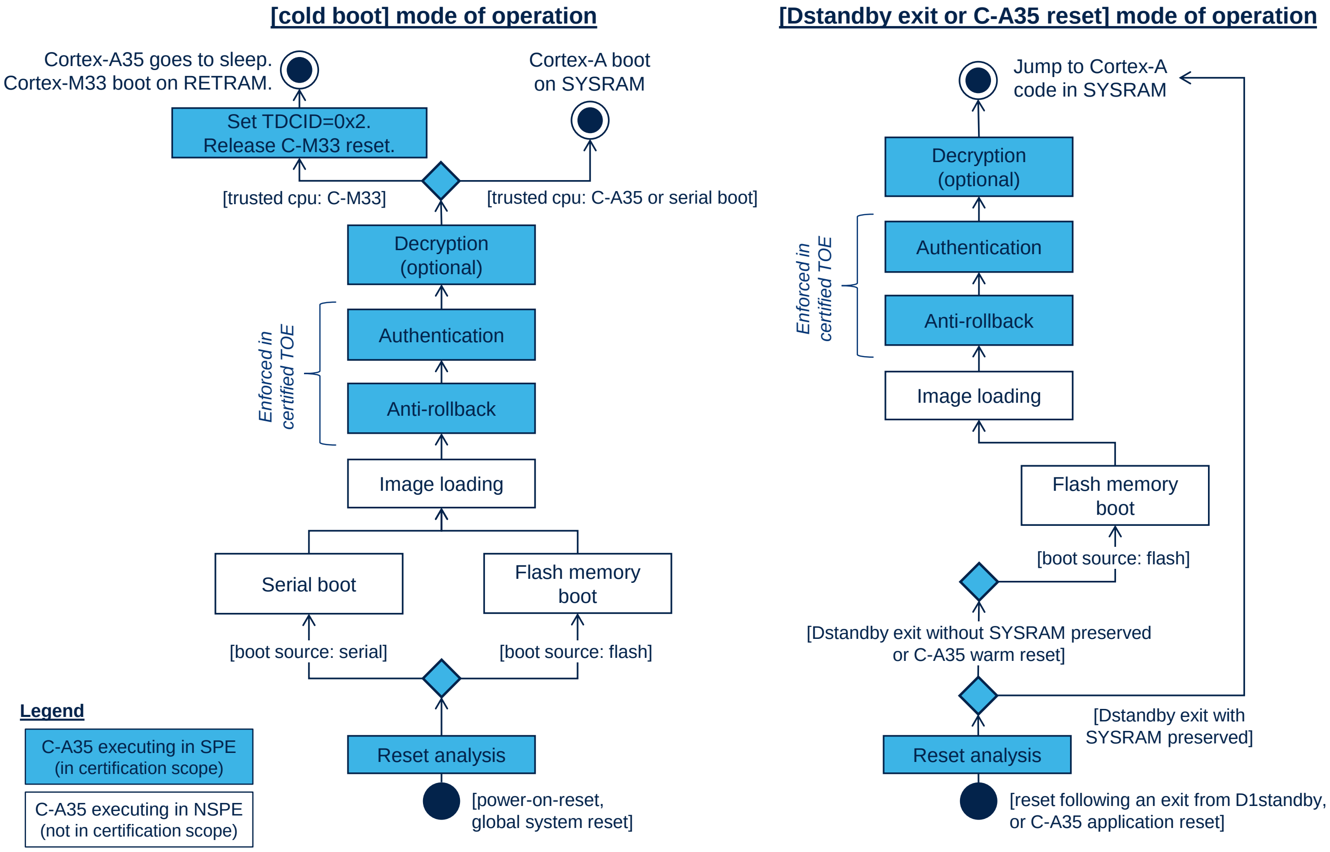
Device reset	SYSRAM preserved	Jump to…	C-A35 executing alone?	Comment
Power on reset Global system reset	No	Cold boot image (C-A35)	Yes	C-A35 is TD CPU. C-A35 cold boot image coming from flash or serial interface.
		flash boot image (C-M33)		C-A35 launches C-M33 as TD CPU. C-M33 boot image only coming from flash interface.
C-A35 reset	No	flash boot image (C-A35)	Yes	-
DStandby exit	No		No (1)	-
	Yes	Dstandby wakeup image		-

(1) Isolation methods are described in Section 3.5.1.

The platform authenticity and integrity are enforced thanks to the following principles:

- *For jumps to <any> boot image*: Platform transfers control to a secure bootloader code verified in integrity and authenticity using elliptic curve digital signature. Indeed, the bootloader code SHA-256 digest is always signed using an active 256-bit ECDSA private key, based on NIST prime256v1 or brainpoolP256t1 curves. The platform can choose one among eight ECDSA public keys when verifying the bootloader code signature. The selected key is provided clear-text in the boot image, with its SHA-256 digest protected in the platform on-chip fuses.
- *For jump to Dstandby wakeup image*: When the trusted application transfers control to the exit firmware, this firmware could not be modified by any code or any user while in low power (SYSRAM in read-only, retention mode).

Figure 4. Platform secure initialization modes of operation



As shown on Figure 4 the NSPE code that manages the image loading (in ROM) is not part of the platform (see Section 1.4.3). The transition after “image loading” is the TOE interface “*Boot image interface”* described in [SG] Section 4.2.2.

Anytime during the platform ROM execution any fuse perturbation prevents boot chain execution, forcing an application reset. This way, when the platform’s authenticity or integrity cannot be ensured, it leads to a locked state where the application secrets stored in on-chip fuses are locked from any code, and debugger/ test modes are disabled for any user until an application reset is done. Refer to Section 6.3 of BSEC peripheral in [RM].

3.3.3 ~~Secure Update of Platform~~

~~The platform can be updated to a newer version in the field such that the integrity, authenticity and confidentiality of the platform is maintained.~~

Non-conformance rationale:

The absence of this functionality is justified in Section 3.2 “Flaw Reporting Procedure (ALC_FLR.2)”.

3.3.4 Residual Information Purging

The platform ensures that all SRAM used by the platform, with the exception of the SRAM not used by the platform, is erased using the method specified in this section before the memory is used by the platform or application again and before an attacker can access it.

Conformance rationale:

- Following a reset the platform erases SRAM contents before using the memory instances listed in Table 5.
- After usage the platform erases all SRAM area and registers that contain secrets, using random values.
- Before jumping to the authenticated application, the platform clears all its allocated embedded SRAM by writing zeroes on each allocated SRAM address. The platform also sticky-reload-locks its secrets stored in BSEC.

3.3.5 ~~Secure Debugging~~

~~The platform only provides <list of endpoints> authenticated as specified in <specification> with debug functionality.~~

~~The platform ensures that all data stored by the application, with the exception of <list of exceptions>, is made unavailable.~~

Non-conformance rationale:

This SFR is removed because the secure Cortex-A35 debug feature while the platform executes is not available to the users. It is implemented but not accessible.

For the other debug features of the product, the platform is certified with all debug features disabled out of cold boot reset (see Section 1.4.4 Life cycle). This debug protection can be frozen anytime until next reset by setting the DENREG bit in BSEC peripheral. The platform systematically sets this bit when *debug_lock* fuses are burnt in OTP word 18 (see Secure debug in [SG] Section 4.2.1).

If the user activates any debug capability on the device following a cold boot defined in Section 3.3.2 the debugging of platform ROM code remains not accessible.

3.4 Package “Security Services” Security Functional Requirements

The platform fulfills the following security functional requirements:

3.4.1 Cryptographic Operation

The platform provides the *operations* in Table 9 functionality with the *algorithms* in Table 9 as specified in *specifications* in Table 9 for *key lengths* and *modes* described in Table 9.

Table 9. Platform cryptographic operations

Operations	Algorithms	Specifications	Key lengths	Modes
Encryption, decryption	AES[1]	FIPS PUB 197 NIST SP800-38A	128, 256 bits	ECB, CBC, CTR
Authenticated encryption or decryption		NIST SP800-38C NIST SP800-38D		GCM, CCM
Cipher-based message authentication code		NIST SP800-38D		GMAC
Protected modular exponentiation (signature, decryption, key agreement...)	RSA[2]	IETF RFC 8017 NIST SP800-56B FIPS PUB 186-4	Up to 4096 bits	RSA 2048, 3072, 4096
Signature	ECDSA	ANSI X9.62 IETF RFC 7027 FIPS PUB 186-4 SEC 1, SEC 2[3]	Up to 640 bits	Nist: P256, P384, P521 Brainpool: bp256r1, bp384r1, bp512r1 SEC 2[3]: secp256k1, secp256r1, secp384r1, secp521r1
ECC scalar multiplication (public key generation, key agreement, shared secret generation...)	ECDH ECIES	ANSI X9.42 ANSI X9.63 FIPS PUB 186-4 SEC 1, SEC 2[3]		

[1] AES algorithm with key sizes of 128 and 256 bits (and not DES/TDES) can run accelerated with side-channel attack resistance in SAES peripheral.

[2] Other operations not written in this table (like RSA CRT exponentiation or ECDSA signature verification) are not protected against side channel attacks.

[3] Standards for Efficient Cryptography: SEC1, SEC2

Conformance rationale:

When the platform is not executing, the application can use the SAES and PKA peripherals to access cryptographic operations resources. For more details refer to [RM]:

- Section 58 Secure AES coprocessor (SAES)
- Section 61 Public Key Accelerator (PKA)

The STM32MP25x device also provides useful cryptographic operations without special side-channel attack resistance, listed in Table 10. Do not manipulate SESIP assurance level 3 sensitive information when using those cryptographic operations.

For more details refer to [RM] Section 60 Hash processor (HASH).

Table 10. Cryptographic operations available outside the platform

Operations	Algorithm	Specification	Key lengths	Modes
Cryptographic hash	SHA-2	FIPS PUB 180-4	N/A	SHA-256, SHA-384, SHA-512
	SHA-3	FIPS PUB 202	N/A	SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256

3.4.2 Cryptographic KeyStore

The platform provides a way to store cryptographic keys such that not even the application can compromise the confidentiality of this data. This data can be used for the cryptographic operations listed in Table 9, algorithm AES.

Conformance rationale:

The platform provides hardware mechanisms to protect the confidentiality of AES 128 or 256-bit keys. When the user encrypts those keys in the SAES peripheral using the derived hardware unique key (DHUK), they can only be decrypted in this specific device, and the decrypted keys are only available in the SAES write-only key registers. Note that if the application tries to overwrite part of the key, the whole key is erased.

The DHUK is never disclosed to any application code or debugger and is only usable in side-channel protected SAES peripheral. Refer to *SAES operation with wrapped keys* in [RM] Section 58 for details.

3.4.3 Cryptographic Random Number Generation

The platform provides the application with a way based on analog live entropy source to generate random numbers as specified in NIST [SP 800-90B].

Conformance rationale:

The platform includes an RNG peripheral compliant with NIST SP800-90B recommendations. When the platform is not executing, the application must use this peripheral to generate true random numbers.

Refer to [RM] Section 57 for details.

3.5 Package “Software Isolation” Security Functional Requirements

The platform fulfills the following security functional requirements:

3.5.1 Software Attacker Resistance: Isolation of Platform

The platform provides isolation between the application and itself, such that an attacker able to run code as an application on the platform cannot compromise the other security functional requirements.

Conformance rationale:

The platform uses following isolation techniques, so that the application cannot compromise the secure initialization of platform defined in Section 3.3.2.

- Before setting D1 domain in DStandby mode application must set the RIF configuration as defined in *Resource isolation* of [SG] Section 4.2.1, otherwise the platform ROM code goes in locked state. A trusted firmware can be in charge of it.
  - This mandatory RIF configuration ensures that no active master is accessing the same resource as the platform ROM code. It also make sure the platform has exclusive access to its peripherals.
- The platform ROM code and some non-volatile assets in BSEC peripheral are hidden from any application code following a cold boot. Refer to [RM] Section 6.3.9 for details.
- The platform ROM code running in SPE manages the RIF configuration to protect itself against ROM code running in NSPE, as shown on Figure 4.
- As defined in *Jump to DStandby wakeup image* of [SG] Section 4.2.1 the platform checks that the backup register 11 is secure and contains a valid jump address. This address must be a pointer to the retention code in SYSRAM area.
  - The required non-platform trusted firmware defined in Section 1.4.5 must not modify the value the C-A35 secure firmware has written in backup register 11.
- In all modes of operation, the platform ROM code manages its RNG peripheral configuration.
- As stated in [RM] Section 9.3 only C-A35 can program the firewalls protecting its SYSRAM.

Above platform protections apply whether the application selects the secure Cortex-A35 or secure Cortex-M33 as TD CPU (see Figure 2 for details).

For more details on RIF refer to [RM] Section 5.2.

3.6 Package “Hardware Protections” Security Functional Requirements

The platform fulfills the following security functional requirements:

3.6.1 Physical Attacker Resistance

The platform detects or prevents attacks by an attacker with physical access before the attacker compromises any of the other functional requirements.

Conformance rationale:

The platform provides the following hardware countermeasures against physical attacks:

- ROM code execution hardening using redundancy checks and time jittering.
- Detection of transient perturbation attacks in crypto functions (SAES, PKA private operations).
- Detection of unauthorized modification of sensitive data stored in fuses.
- Prevention of leakage of information through electro-magnetic emissions and power consumption when using AES algorithm (in SAES) or private key cryptography (in PKA).

Although not activated by default the integrator can activate the tamper-detection and response hardware present in the platform. Doing so does not impact the SFR secure initialization of platform described in Section 3.3.2.

Refer to the security guidance [SG] Section 4.2.1 for details on anti-tamper optional features available in the platform.

4 Mapping and Sufficiency Rationales

4.1 SESIP3 Sufficiency

Table 11 SESIP3 Sufficiency

Assurance Class	Assurance Families	Covered by	Rationale
ASE: Security Target evaluation	ASE_INT.1 ST Introduction	Section 1	The ST reference is in the Title, the TOE reference in the "Platform Reference", the TOE overview and description in "Platform Functional Overview and Description".
	ASE_OBJ.1 Security requirements for the operational environment	Section 2	The objectives for the operational environment in "Security Objectives for the Operational Environment" refer to the guidance documents.
	ASE_REQ.3 Listed Security requirements	Section 3.3 to Section 3.6	All SFRs in this ST are taken from [SESIP]. "Verification of Platform Identity" is included. "Secure Update of Platform" is not included with justification in ALC_FLR.2.
	ASE_TSS.1 TOE Summary Specification	Section 3	All SFRs are listed per definition, and for each SFR the implementation and verification are defined in "Security Functional Requirements".
ADV: Development	ADV_FSP.4 Complete functional specification	Section 1.3, and material provided to the evaluator	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ADV_IMP.3 Complete mapping of the implementation representation of the TSF to the SFRs	Material provided to the evaluator	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	Section 1.3	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
	AGD_PRE.1 Preparative procedures	Section 1.3	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE	Section 1.3	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ALC_CMS.1 TOE CM Coverage	Section 4.2, and material provided to the evaluator	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ALC_FLR.2 Flaw reporting procedures	Section 3.2	The flaw reporting and remediation procedure is described.
ATE: Tests	ATE_IND.1 Independent testing: conformance	Material provided to the evaluator	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
AVA_VAN.3	AVA_VAN.3 Focused Vulnerability analysis	N.A. A vulnerability analysis is performed by the platform evaluator to ascertain the presence of potential vulnerabilities.	The platform evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE. Penetration testing is performed by the platform evaluator assuming an attack potential of Enhanced-Basic.

4.2 PSA Security Functions Mapping

This table refers to *SESIP Profile for PSA Certified RoT Component Level 3* [SP2]. This section provides rationales of conformance claimed in Section 1.

Table 7. **PSA Security Functions Mapping**

PSA Security Function	Covered by SESIP SFR	Reference
F.INITIALIZATION	Secure Initialization	Section 3.3.2
F.SOFTWARE_ISOLATION	Software Attacker Resistance: Isolation of Platform	Section 3.5.1
F.FIRMWARE_UPDATE	Secure Update of Platform	Section 3.3.3
F.SECURE_STATE	Software Attacker Resistance: Isolation of Platform	Section 3.5.1
	Secure Initialization	Section 3.3.2
	Secure Update of Platform	Section 3.3.3
F.CRYPTO	Cryptographic Operation	Section 3.4.1
	Cryptographic KeyStore	Section 3.4.2
	Cryptographic Random Number	Section 3.4.3
F.ATTESTATION	Verification of Platform Identity	Section 3.3.1
F.DEBUG	Secure Debugging	Section 3.3.5
F.PHYSICAL	Physical Attacker Resistance	Section 3.6.1

5 Documentation references

Table 12. References

Reference	Definition
Evaluation Documents	
[SESIP]	Security Evaluation Standard for IoT Platforms (SESIP), version 1.2 (July 2023), GlobalPlatform, GP_FST_070
[SP1]	SESIP Profile for Secure MCUs and MPUs, version 1.0 (Oct 2021), GlobalPlatform, GPT_SPE_150
[SP2]	SESIP Profile for PSA Certified RoT Component Level 3, version 1.0 REL 02, JSADEN018
[SP 800-90B]	NIST Special Publication (SP) 800-90B (Draft), Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018
Developers Documents	
[SG]	UM3370 STM32MP25x security guidance for SESIP level 3 Certification, STMicroelectronics, rev 1
[RM]	RM0457 Reference Manual STM32MP25xx advanced Arm®-based 32/64-bit MPUs, STMicroelectronics, rev 5
[ES]	ES0598 STM32MP251x/3x/5x/7x device errata, STMicroelectronics, rev 2
[PSIRT]	DM00882158, PSIRT ST PRODUCT SECURITY INCIDENT RESPONSE TEAM (PSIRT) MANAGEMENT, Rev 1.0

Glossary

Table 13. Glossary

Term	Definition
Application	Used in SESIP to refer to the components which are out of the scope of the evaluation.
Non-secure Processing Environment (NSPE)	The Arm Cortex processing environment that hosts the non-secure system software and application specific software.
Platform	Used in SESIP to refer to the components which are in the scope of the evaluation. It is a synonym for Connected platform.
Product	Used by SESIP as a synonym for Connected product
Secure Processing Environment (SPE)	The Arm Cortex processing environment that usually hosts the RoT, and any application RoT Service(s).

Abbreviations

Table 14. Abbreviations

Term	Definition
C-A35	Arm® Cortex® A35
C-M33	Arm® Cortex® M33
DHUK	Derived Hardware Unique Key
NSPE	Non-Secure Processing Environment
RIF	Resource Isolation Framework
RoT	Root of Trust
SP	SESIP Profile
SPE	Secure Processing Environment

Revision history

Table 15. Document revision history

Date	Revision	Changes
11-Dec-2024	1	Initial release.

Contents

1 Introduction 2
1.1 Security Target Reference 2
1.2 Platform Reference 2
1.3 Included Guidance Documents 2
1.4 Platform Functional Overview and Description 3
1.4.1 Platform type 3
1.4.2 Platform physical scope 3
1.4.3 Platform logical scope 4
1.4.4 Platform security features and usage 5
1.4.5 Required Hardware/Software/Firmware 6
2 Security Objectives for the Operational Environment 7
2.1 Platform Objectives for the Operational Environment 7
2.2 Inherited Objectives for the Operational Environment 7
3 Security Requirements and Implementation 8
3.1 Security Assurance Requirements 8
3.2 Flaw Reporting Procedure (ALC_FLR.2) 8
3.3 Base SP Security Functional Requirements 8
3.3.1 Verification of Platform Identity 8
3.3.2 Secure Initialization of Platform 8

3.3.3 ~~Secure Update of Platform~~ 9
3.3.4 Residual Information Purging 10
3.3.5 ~~Secure Debugging~~....10
3.4 Package “Security Services” Security Functional Requirements 10
3.4.1 Cryptographic Operation 10
3.4.2 Cryptographic KeyStore 11
3.4.3 Cryptographic Random Number Generation....11
3.5 Package “Software Isolation” Security Functional Requirements....12
3.5.1 Software Attacker Resistance: Isolation of Platform 12
3.6 Package “Hardware Protections” Security Functional Requirements....12
3.6.1 Physical Attacker Resistance 12
4 Mapping and Sufficiency Rationales 13
4.1 SESIP3 Sufficiency 13
4.2 PSA Security Functions Mapping 14
5 Documentation references 15

List of tables

Table 1. SESIP profile for Secure MCUs and MPUs conformance claims......2
Table 2. SESIP profile for PSA certified RoT component conformance claims......2
Table 3. Platform reference 2
Table 4. Guidance documents 2
Table 5. Hardware components and interfaces of the TOE 4
Table 6. Software components and interfaces of the TOE......5
Table 7. Platform identifiers 8
Table 8. Secure initialization options 8
Table 9. Platform cryptographic operations 10
Table 10. Cryptographic operations available outside the platform 11
Table 11 SESIP3 Sufficiency 13
Table 12. References......15
Table 13. Glossary......16
Table 14. Abbreviations 17
Table 15. Document revision history......18

List of figures

Figure 1. STM32MP25x block diagram....3
Figure 2. Platform logical scope....4
Figure 3. Reference product life cycle....6
Figure 4. Platform secure initialization modes of operation....9

IMPORTANT NOTICE – PLEASE READ CAREFULLY

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgement.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of Purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, please refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.