Security target for STM32MP13xx

Document information

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

1 Introduction

This security target describes the STM32MP13xx platform and the exact security properties of the platform that are evaluated against the GlobalPlatform™ Security Evaluation Standard for IoT Platforms [SESIP].

This security target is inspired by the GlobalPlatform™ protection profile referenced in [SP], but it is not compliant to it.

This security target covers critical security functional requirements for the development of PCI PTS POI-compliant devices based on the STM32MP13xx platform, according to [SR] and [DTS]. The expectation is the platform to be labeled as “PCI ready” by the security evaluation laboratory.

Table 1. Protection profile reference and conformance claims

Reference	Value
Protection profile name	None
Protection profile version	None
Assurance claim	Refer to Section 3.1

1.1 Security target reference

This document: *STM32MP13xx security target* (ST0049) revision 3 (03-Oct-2025), STMicroelectronics.

1.2 Platform reference

The table below contains the platform reference values.

Table 2. Platform reference

Reference	Value
Platform name	STM32MP13xx advanced Arm®-based 32-bit MPUs
Platform version	1.2
Platform identification	STM32MP13xC, STM32MP13xF (DieID: 0x1003)
Platform type	General-purpose microprocessor device for IoT, industrial, or consumer applications.

1.3 Included guidance documents

The platform includes the following documents. All documents are available from http://www.st.com

Table 3. Guidance documents

Category	Name	Reference
Product user manual	*UM2885 user manual STM32MP13xx security guidance*	[SG]
Product reference manual	*RM0475 Reference manual STM32MP13xx advanced Arm®-based 32-bit MCUs*	[RM]
Product errata sheet	*ES0539 STM32MP131x/3x/5x device errata sheet*	[ES]
Datasheet	*DS13483 datasheet STM32MP135C STM32MP135F* *DS13875 Datasheet STM32MP133C STM32MP133F* *DS13877 Datasheet STM32MP131C STM32MP131F*	[DS]

1.4 Platform functional overview and description

1.4.1 Platform type

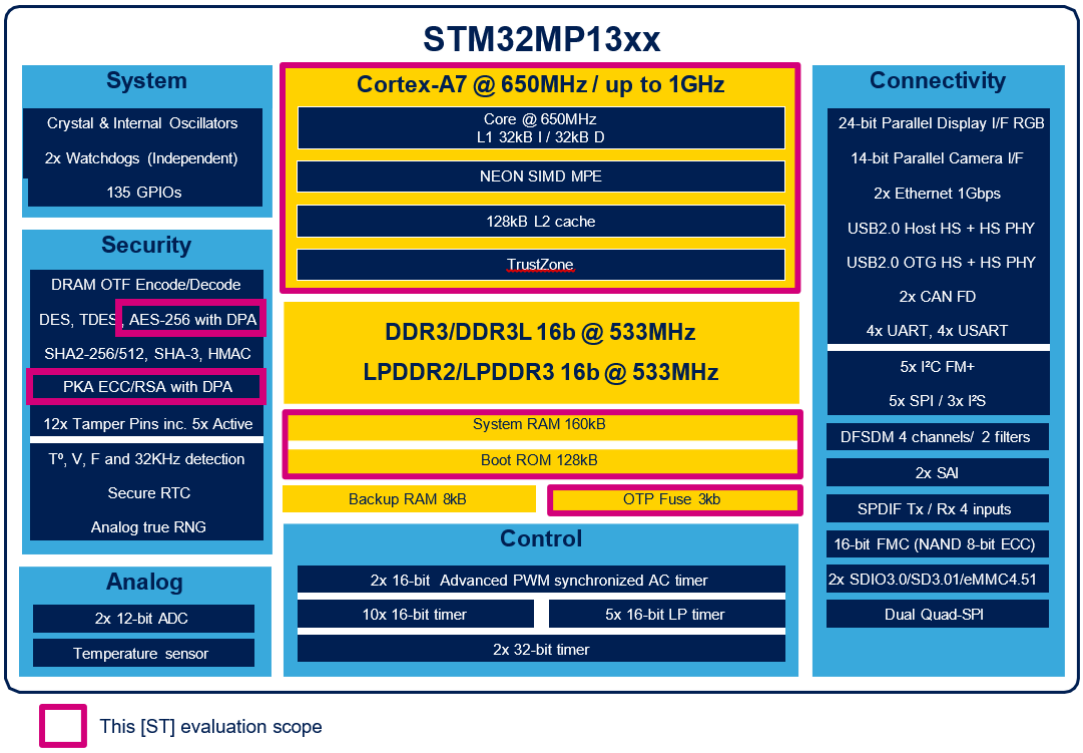
The STM32MP13xx microprocessor is the SESIP certified member of the STM32MP13 family of general-purpose microprocessor solution (MPU). It provides a new optimal balance between performance, power, and security.

The platform consists of an Arm® Cortex®-A7 based microprocessor with an immutable ROM firmware, and with key security hardware features likeTrustZone®, secure embedded SRAM, antifuses, and crypto accelerators.

1.4.2 Physical scope

The physical scope of the platform is implemented in the STM32MP13 lines of MPU products described in Section 1.2. The block diagram on 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. STM32MP13xx block diagram



The hardware components and interfaces that constitute the platform are defined below. They are described in the [RM] and the [ES]. Devices form factors are documented in [DS].

- The STM32MP13xx microprocessor device defined in Table 2.
- The boot ROM embedded in it.
- The hardware interfaces of the TOE listed in section 4.2.2 of [SG]

1.4.3 Logical scope

The software components and interfaces that constitute the platform are listed in Table 4. Any additional firmware, OS, or application software stored on the platform is not in the scope of this evaluation.

Table 4. Software components and interfaces of the TOE

Component/interface	Description	Identification/Version
Boot ROM	Device embedded ROM code (same version as the silicon)	1.2

The logical scope of the platform includes:

- The security life cycle resources, summarized in Section 1.4.5: Life cycle.
- The cryptographic operations.
- The immutable platform Root of Trust with boot code (running in SPE), any root parameters, with management, enforcement or monitoring of the isolation hardware resources related to the immutable RoT functionality.

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, 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 [SP].

1.4.4 Security features and usage

The platform, defined in Section 1.4.2 and Section 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.
- Residual information purging for life cycle handling.

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

- Cryptographic operations, based on hardware cryptographic accelerators (Secure AES, PKA).
- Hardware protection to handle hostile environments.
- Isolation mechanisms controlling access between certified and non-certified parts of the software building the product.

Regarding the security features, note that:

- 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.

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

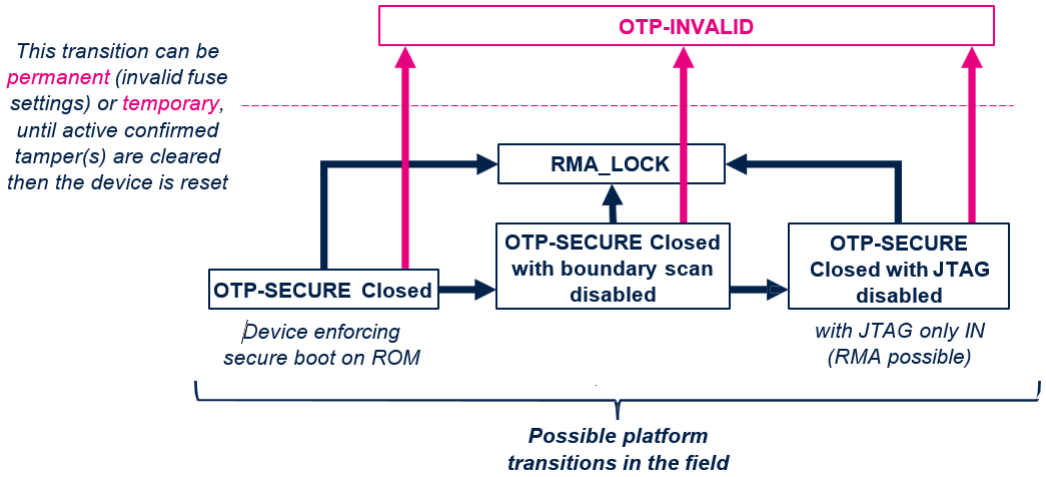
1.4.5 Life cycle

Following the purchase of a device through www.st.com or STMicroelectronics certified resellers, the integrator must follow the secure acceptance, installation, and preparation methods described in sections 3.1 and 3.2 of the [SG].

Transitions to the life cycle states of the platform are irrevocably triggered by burning fuse bits in BSEC. Those transitions are summarized in Figure 2.

In OTP-SECURE Closed states, the TOE is certified with all debug features disabled out of reset. This debug protection can be frozen anytime until the next reset by setting the DENREG bit in the BSEC peripheral.

Figure 2. **Platform life cycle overview**



The transition to RMA_LOCK state is initiated by the integrator using its own 32-bit password. After three consecutive wrong password attempts, the RMA sequence always fails.

The integrator must store its security-sensitive information (secrets keys, certificate, RMA key) in OTP words 32 to 95. It is mandatory in order not to leak secret information when the device transits to RMA_LOCK state.

1.4.6 Use case

The TOE is intended to be used by trusted integrators as a SESIP Level 3 compliant Root-of-Trust platform. The integrator would add on top of it the required components to make a connected product. Such components include a Root of Trust software layer, an operating system, some connectivity, as well as additional hardware components as required by the final product.

2 Security objectives for the operational environment

2.1 Platform objectives for the operational environment

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

- TOE_SECRETS: protection of root of trust related sensitive material, as described in section 4.2.4 of [SG].
- TOE_PREPARATION: after verifying TOE genuineness (section 3.1 of [SG]) the integrator personalizes the TOE following the TOE documentation in section 4.2.4 of [SG].
- TRUSTED_INTEGRATOR: the integrator uses the security functionalities of the TOE in certified configuration following the TOE documentation in section 4.2.4 of [SG]. The integrator is trusted and does not attempt to thwart the TOE security functionalities nor attempt to bypass them.

2.2 Inherited objectives for the operational environment

The platform does not include platform parts previously evaluated under any SESIP certification scheme.

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. Customer can implement their own secure update mechanism in their code.

In accordance with the requirement for a flaw reporting procedure (ALC_FLR.2), including a process to generate and distribute any needed update, the developer has defined the procedure in https://www.st.com/content/st_com/en/about/security-and-privacy/psirt.html

3.3 Security functional requirements

The platform fulfills the following security functional requirements:

3.3.1 Verification of the 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 following unique identifications:

- Integrated circuit hardware revision (RevID) and DieID, readable using the debugger or via USB
- Device part number readable in RPN register at address 0x5C00 5204. Expected values are:
  - 0x6C8 (STM32MP131C) or 0xEC8 (STM32MP131F)
  - 0x0C0 (STM32MP133C) or 0x8C0 (STM32MP133F)
  - 0x000 (STM32MP135C) or 0x800 (STM32MP135F)

Verification methods and expected values are summarized in section 3.1 of [SG].

3.3.2 Secure initialization of the platform

The platform ensures its authenticity and integrity during the platform initialization. If the platform authenticity or integrity cannot be ensured, the platform goes to a list of controlled states detailed in “Errors” description of “Flash memory interfaces” and “Serial boot interfaces” in section 4.2.2 of [SG].

Informational

This SFR contributes to meet the PCI PTS POI requirement B1 as it provides proof of integrity and authenticity of the platform. It is useful for the test cases TB1.1, TB1.10 and TB1.11 (refer to [DTS]).

Conformance rationale

Hardware initialization steps

Following the chain of trust principles, embedded ROM code in the device always manages system reset events, split into two categories:

- An application reset, for instance the VDD power-on, reset button press, an HSE clock failure, an IWDG1/2 reset, a VDD brownout reset, or the setting of MPSYSRST bit in the RCC.
- A wake-up from low-power mode (VDDCORE power-on reset)

According to the execution condition, and fuse values, the ROM code can:

1. Decide to proceed with the boot chain, attempting to execute genuine First Stage Boot Loader (FSBL) code from the embedded SRAM.
2. Discover that a confirmed tamper event is blocking access to fuses and has erased secrets in the device. In this case the ROM code transforms this confirmed tamper as a potential tamper, to execute the OEM FSBL following a system reset.

3. Detect fuse perturbations that prevent boot chain execution (for example, invalid OTP security state). In this scenario the only possible outcome is an application reset.
4. Branch to the LPLV-Stop2 exit firmware located in the embedded SRAM.

Regarding platform integrity, it is enforced by hardware in all of the above cases:

- In case 1: ROM code uses immutable fuses provisioned by OEM to verify the integrity of FSBL before executing it from embedded SRAM, robust against hardware fault injections (see next subsection).
- In case 2 and 3: Only the trusted ROM code executes, leading to a system reset. When the fuse errors are uncoverable case 3 leads to a state where the chip cannot be exploited as it will never execute any external code, keeping secrets locked from debugger and test modes.
- In case 4: Standby exit firmware has been verified in authenticity/integrity before going to Standby mode.

Software initialization steps

ROM code is in charge of loading, checking, optionally decrypting and launching the First Stage Boot Loader (FSBL) that is stored in an external flash memory.

When the chip boots, the processing starts by the ROM execution, which analyzes chip state in accordance with life cycle (TOE life cycle is shortly described in Section 1.4.2).

As TOE is in OTP-SECURE closed state, the ROM applies secure boot mechanisms. It verifies the integrity and authenticity of the FSBL by verifying an elliptic curve digital signature. The algorithm used is a 256-bit ECDSA (NIST prime256v1 or brainpoolP256t1) signature of an SHA256 message digest of the FSBL code.

The public key used to sign the FSBL is verified against eight possible root keys, which fingerprint is stored in the device's manufacturer-programmable on-chip fuses.

The ROM verifies that the version of the FSBL is higher or equal than the current version installed, preventing roll-back and downgrading attacks.

The ROM decrypts the FSBL and verifies the plain text integrity when the decryption is required.

In case of failure, the ROM first looks for a recovery boot FSBL (the flash memory may contain several copies of FSBL), before waiting on a serial downloader (on UART or USB) for an authenticated and optionally encrypted FSBL.

For more details, refer to section 4.2.1 of [SG].

3.3.3 ~~Secure update of the 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 explained in Section 3.2

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 ROM code erases SRAM contents before using the memory.

The boot ROM erases all SRAM area and registers, which has contained secrets with random values after usage.

The boot ROM also erases all its SRAM data before jumping to the authenticated application.

3.3.5 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.

Informational

This SFR contributes to meet the PCI requirements A1, A3, A4, A5, A6, A7, A8, and indirectly to A10 and A13 (Refer to [DTS]).

Conformance rationale

The platform provides the following countermeasures against physical attacks:

- ROM code execution is hardening using redundancy checks and time jittering
- Tamper-detection and response hardware (that is, automatic erase/blocking if confirmed tamper), defining in the device a protected area for the following sensitive functions:
  - Nonvolatile fuse storage
  - Volatile secret key storage in backup domain registers
  - Embedded SRAM3 storage
  - Crypto functions in hardware engines (SAES, CRYP, HASH, PKA)
- Detection of transient perturbation attacks in crypto functions (SAES, PKA private operations)
- External clock glitch filtering and clock loss detection:
  - For LSE clock, in all system modes, including VBAT mode
  - For HSE clock (input of the PLL feeding the Cortex® A7) loss can be detected in Run mode and in Stop modes when the HSE oscillator is enabled. PLL filters glitches.
- Detection of temperature, power supply, and clock frequency out of operational range, following an erase response triggered before the security properties cannot be ensured any longer.
  - V_{DDCORE} and V_{DDCPU} monitoring is deactivated in Stop, Standby, and V_{BAT} modes
  - V_{DD} supply, used by IWDG1 and its clock source, is monitored in all modes excluding Standby or V_{BAT} mode
  - Backup domain supply monitoring is available in all system modes, including V_{BAT} mode
- 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)
- Detection of physical penetration attempts using passive or active tamper pins (for example, using meshes)
- Side channel analysis countermeasures, protecting AES computations (in SAES) and private key cryptography (in PKA).

3.3.6 ~~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 <exceptions>, is made unavailable.~~

Non-conformance rationale

This feature is not available to the users. It is implemented but not accessible.

Indeed, the TOE is certified with all debug features disabled out of reset. This debug protection can be frozen anytime until the next reset by setting the DENREG bit in the BSEC peripheral. ROM code in the TOE is not setting this bit.

As described in section 1.4.5, the JTAG, or SWD interface remains enabled (under reset only) to inject the RMA password that can switch the device to the RMA_LOCK state. In this state, OTP secrets stored in words 32 to 95 are hidden, hence the platform is no more functional.

Although not part of the TOE-certified configuration, it is possible to select any JTAG or SWD connection as a source of internal tamper, as described in “anti-tamper” part of section 4.2.1 of [SG].

3.4 Additional security functional requirements

The platform fulfills the following security functional requirements:

3.4.1 Cryptographic operation

The platform provides the cryptographic operations such as encryption, decryption, hashing, authentication, signature functionality with a list of algorithms specified in Table 5 for key lengths and modes defined in Table 5.

Informational

This SFR contributes to meet the PCI requirements B9, B10, B11, B24, and B26 (Refer to [DTS]). Cryptographic algorithms and key sizes are listed in appendix E of [DTS].

Conformance rationale

The platform provides to applications the cryptographic algorithms, modes of operation and minimum/maximum key size described in Table 5. Side channel resistance is described in notes.

For more details on side channel resistant cryptographic algorithms, refer to “Hardware-accelerated cryptography” part of section 4.2.1 in [SG]. For more information on hashing algorithms, refer to section 34 in [RM].

Some of those algorithms are used by the boot ROM.

Table 5. TOE cryptographic operations

Operations	Algorithm	Specification	Key lengths	Modes
Encryption, decryption	AES(1)	FIPS PUB 197 NIST SP800-38A	128, 192, 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 1024, 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 SEC 1 SEC 2(3)		
Cryptographic hash	SHA-2(4)	FIPS PUB 180-4(5)	N/A	SHA-224, SHA-256, SHA-384, SHA-512
	SHA-3(4)	FIPS PUB 202	N/A	SHA3-224, SHA3-256, SHA3-384, SHA3-512. SHAKE128, SHAKE256

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, https://www.secg.org*
4. *These algorithms must not be used when manipulating sensitive information.*
5. *The algorithms in scope are defined respectively in section 6.3, 6.2, 6.5 and 6.4.*

3.4.2 Cryptographic KeyStore

The platform provides a way to store secret keys such that not even the application can compromise the confidentiality of this data. This data can be used for the cryptographic operations encryption, decryption, authenticated encryption/ decryption.

Informational

This SFR contributes to meet the PCI requirements B9 and B18 (Refer to [DTS]).

Conformance rationale

The platform provides hardware mechanisms to protect the integrity and confidentiality of AES 128 or 256-bit keys in the KeyStore, thanks to encryption using a key derived from the device hardware unique key (HUK). Resulting decrypted keys are automatically stored in write-only key registers, without disclosing any clear-key data to the application. Additionally, if an application tries to overwrite part of the key, the whole key is erased. The key derived from the HUK is never disclosed to the MPU and is only accessible by the SCA-protected AES hardware crypto engine (SAES peripheral). The key derived from the HUK is different if it is used by a secure code or a nonsecure code.

Application-defined 256-bit BHK, stored in tamper-protected backup registers, can be XORed with DHUK when encrypting KeyStore items. This way, the KeyStore cannot be decrypted until BHK is reinstalled by secure boot code.

DHUK and BHK are only usable in side-channel attacks resistant SAES peripheral.

For more details, refer to “Cryptographic key storage” parts of Section 4.2.1 in [SG].

4 Mapping and sufficiency rationales

4.1 SESIP3 sufficiency

Table 6. 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 3.4	All SFRs in this ST are taken from [SESIP]. Verification of the platform identity is included. ~~"Secure update of the platform"~~ is not included (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 Base PP security functional requirements.
ADV: Development	ADV_FSP.4 Complete functional specification	Section 1.3, and material provided to the evaluator	The platform evaluator determines 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 determines 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 determines whether the provided evidence is suitable to meet the requirement.
	AGD_PRE.1 Preparative procedures	Section 1.3	The platform evaluator determines 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 determines whether the provided evidence is suitable to meet the requirement.
	ALC_CMS.1 TOE CM coverage	Section 5, and material provided to the evaluator	The platform evaluator determines 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 determines 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.

5 Reference documentation

The table below contains the evaluation and developer documents, as well as the standards used as reference documentation for this security target.

Table 7. Reference documentation

Reference	Definition
Evaluation documents	
[SESIP]	*Security Evaluation Standard for IoT Platforms (SESIP)*, version 1.2 (July 2023), GlobalPlatform, GP_FST_070
[SR]	*PIN Transaction Security (PTS), Point of Interaction (POI), Modular Security Requirements, version 6.0 (June 2020), PCI Security Standards Council LLC*
[DTS]	*PIN Transaction Security (PTS), Point of Interaction (POI), Modular Derived Test Requirements, version 6.0 (June 2020), PCI Security Standards Council LLC*
Developer documents	
[SG]	*UM2885 STM32MP13xx security guidance*, STMicroelectronics, revision 3
[RM]	*RM0475 Reference manual STM32MP13xx advanced Arm®-based 32-bit MPUs*, STMicroelectronics, revision 4
[ES]	*ES0539 STM32MP131x/3x/5x device errata*, STMicroelectronics, revision 6
[DS]	*DS13483 Datasheet STM32MP135C STM32MP135F*, STMicroelectronics, revision 7 *DS13875 Datasheet STM32MP133C STM32MP133F*, STMicroelectronics, revision 7 *DS13877 Datasheet STM32MP131C STM32MP131F*, STMicroelectronics, revision 7
Standards	
[SP]	*SESIP Profile for Secure MCUs and MPUs, version 1.0 (Oct 2021), GlobalPlatform, GPT_SPE_150*

6 Glossary

Table 8. **Glossary**

Term	Definition
Boot hardware key	256-bit AES encryption or decryption key stored in backup registers, erased in case of tamper, and not readable or writable after boot by the application (dedicated key bus to SAES).
Hardware unique key	The device embeds two hardware unique keys: DHUK and RHUK.

7 Abbreviations

Table 9. **Abbreviations**

Term	Definition
BHK	Boot hardware key
DHUK	Derived HUK
HUK	Hardware unique key
PCI	Payment card industry
PKA	Public key accelerator
POI	Point of interaction
POS	Point of sales
PTS	Pin transaction security
RHUK	Root HUK
RoT	Root of trust
SPE	Secure processing environment

Revision history

Table 10. **Document revision history**

Date	Version	Changes
09-Sep-2025	1	Initial release.
22-Sep-2025	2	Updated Section 3.2: Flaw reporting procedure (ALC_FLR.2) and Section 5: Reference documentation
03-Oct-2025	3	Updated Section 1.1: Security target reference

Contents

List of tables

List of figures

IMPORTANT NOTICE – 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.

In the event of any conflict between the provisions of this document and the provisions of any contractual arrangement in force between the purchasers and ST, the provisions of such contractual arrangement shall prevail.

The 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 acknowledgment.

The 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 the 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.

If the purchasers identify an ST product that meets their functional and performance requirements but that is not designated for the purchasers' market segment, the purchasers shall contact ST for more information.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, 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.