STM32C5xxxx SESIP security target

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 STM32C5 platform and the exact security properties of the platform that are evaluated against the GlobalPlatform® Security Evaluation Standard for IoT Platforms SESIP.

The protection profile reference and conformance claims for this security target are described below.

Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

Note: The Arm word and logo are trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All rights reserved.

arm

Table 1. Protection profile reference and conformance claims

Reference	Value
Protection profile name	SESIP Profile for PSA CertifiedTM Level 3 iSE/SE and RoT Component [PP]
Protection profile version	2.0 REL 01
Assurance claim	SESIP Assurance Level 3 - Refer to Section 3.1
SESIP Standard	Security Evaluation Standard for IoT Platforms (SESIP), version 1.2 (July 2023), GlobalPlatform, GP_FST_070 [GP-SESIP]
Optional and additional SFRs	Field return of platform, Secure encrypted storage

1.1 Security target reference

This document: *STM32C5xxxx SESIP security target (ST0063), revision 1.0, STMicroelectronics*.

1.2 Platform reference

Several platforms are certified as described in the tables below.

Table 2. Platform reference (256kB flash)

Reference	Value
Platform name	STM32C542xx from STM32C5 series advanced Arm®-based 32-bit MCUs
Platform version	*Revision Z*
Platform identification	0x44F
Platform type	General purpose microcontroller device for IoT, industrial, or consumer applications.

Table 3. Platform reference (512kB flash)

Reference	Value
Platform name	STM32C562xx from STM32C5 series advanced Arm®-based 32-bit MCUs
Platform version	*Revision Y*
Platform identification	0x44E
Platform type	General purpose microcontroller device for IoT, industrial, or consumer applications.

Table 4. Platform reference (1MB flash)

Reference	Value
Platform name	STM32C5A3xx from STM32C5 series advanced Arm®-based 32-bit MCUs
Platform version	*Revision Z*
Platform identification	0x45A
Platform type	General purpose microcontroller device for IoT, industrial, or consumer applications.

1.3 Included guidance documents

The following documents are included with the platform:

Table 5. Guidance documents

Category	Name	Reference
User manual	SG0062 user manual STM32C5xxxx security guidance for SESIP level 3 certification	[SG]
Product reference manual	RM0522 reference manual STM32C5xxxx series Arm®-based 32-bit MCUs	[RM]
Product errata sheet	STM32C5xxxx device errata sheet: • ES0677 for STM32C5A3xx, STM32C593xx, and STM32C591xx. • ES0661 for STM32C551xx, STM32C552xx, and STM32C562xx. • ES0676 for STM32C531xx, STM32C532xx, and STM32C542xx.	[ES]

1.4 Platform functional overview and description

1.4.1 Platform type

The platform is a general-purpose microcontroller member of the general purpose MCU series, ensuring simple and cost-reduced integration, energy efficiency, multiple choice of power modes and various serial link connectivities.

The platform consists of an Arm® Cortex®-M33 based microcontroller with internal flash memories, RAMs, and peripherals.

The platform provides the necessary hardware building blocks for the platform integrator to implement a secure boot with a protected Root of Trust.

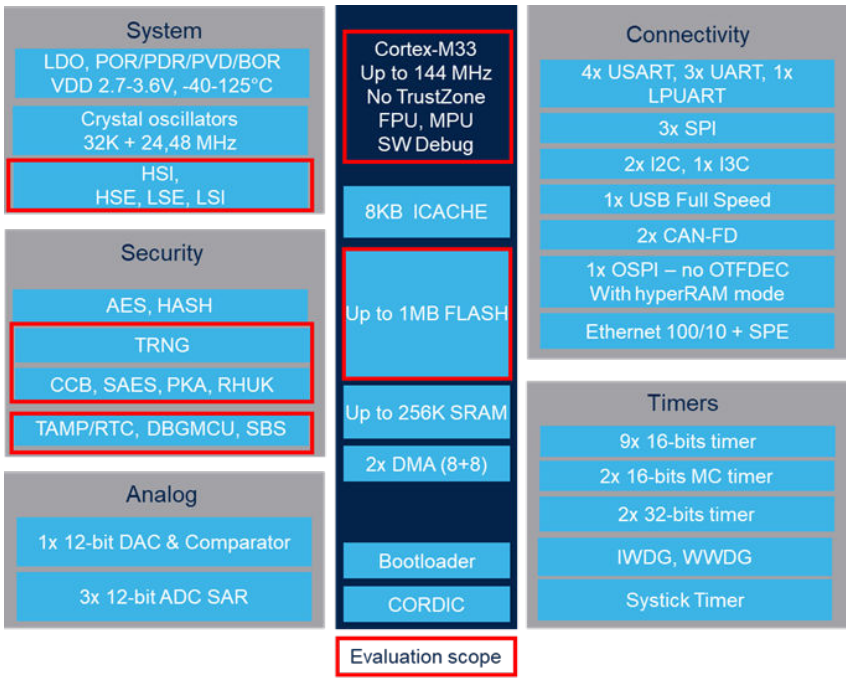
The platform is mainly envisioned to be the lower-level platform part for further composition of evaluation activities.

1.4.2 Physical scope

The physical scope of the platform is implemented in the STM32C5 series of MCU products described in the reference manual [RM]. The block diagram on Figure 1 provides an overview of the major features supported by this MCU.

The platform definition is identical across all devices in the series.

Figure 1. Platform physical scope



DT80711V1

The platform perimeter resides in the components and interfaces listed in Table 7 and fully described in the reference manual [RM], and in the errata sheet [ES].

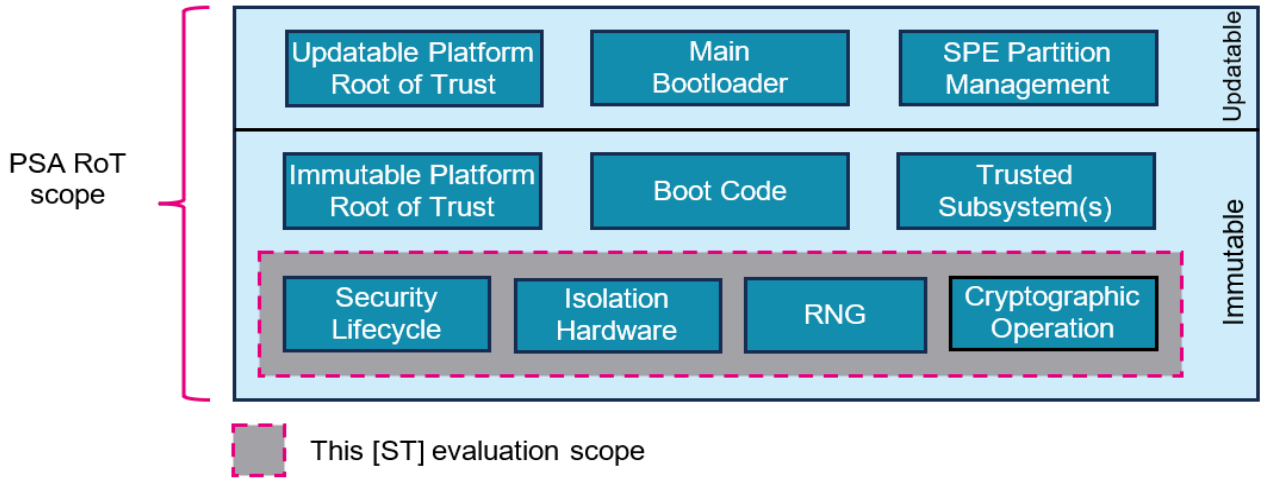
Table 6. Hardware components and interfaces of the TOE

Component/interface	Description	STM32C54xx	STM32C56xx	STM32C5Axx
System				
CPU	ARM Cortex-M33	Y	Y	Y
Debug ports	JTAG/SWD, DBGMCU	Y	Y	Y
Memories	FLASH	256 kB	512 kB	1 MB
Peripherals	TAMP, RCC, SBS	Y	Y	Y
Cryptography				
TRNG	-	Y	Y	Y
SAES	-	-	-	Y
PKA	-	-	-	Y
CCB	-	-	-	Y

1.4.3 Logical scope

The block diagram on Figure 2 based on [PSA-PP] *section 2.4.3* recaps the PSA Root Of Trust expectations that are specified in the PSA security model [PSA-SM] document.

Figure 2. **Platform logical scope**



DT80712V1

The logical scope of the platform includes:

- the security lifecycle resources,
- the isolation hardware resources,
- the cryptographic random number generation,
- the cryptographic operations.

The logical scope of the platform does not include:

- The immutable platform Root of Trust, being for example, the boot code, any root parameters, with management and enforcement of the isolation and security lifecycle hardware resources.
- The updateable platform Root of Trust, being for example, the main bootloader code, the code that implements the SPE partition management function, and the code that implements the PSA defined services such as attestation, secure storage, and cryptography.
- The trusted subsystems components that the PSA Root of Trust relies on for the protection of its assets or implements some of its services, for example, a subscriber identification module or a secure element.

1.4.4 Usage and major security features

The platform supports the following major security features:

- The RDP level manages the product state in the life cycle. In RDP level 0, the product is fully open for development, debugging, prototyping, and programming of both user flash and user nonvolatile options known as option bytes. In RDP level 2, the product is closed. The nonvolatile configuration cannot be changed, and the debug link is locked. RDP level 2 with boundary scan is identical to RDP level 2 with on top the possibility to perform boundary scan (test on IOs).
- The securable memory area HDP mechanism manages flash memory region protection. The main purpose of the securable memory area is to protect a specific part of flash memory against undesired access. After the system reset, the code in the securable memory area can be executed before the securable area becomes inaccessible until the next system reset. This allows the implementation of software security services such as isolation or secure initialization. The base securable memory area is defined by option byte at manufacturing time and is unmodifiable in RDP level 2. The code executed in the securable memory area can optionally extend the securable memory area, which is then locked for any later access.
- The RNG is a true random number generator that provides full entropy outputs to the application as 32-bit samples. It is composed of multiple analog noise sources and an internal conditioning component.

In addition, STM32C5A3xx devices support the following security features:

- The secure AES peripheral provides encryption, decryption, and authenticated encryption with associated data (AEAD) computation supporting ECB, CBC, CTR, GCM, GMAC, and CCM modes of operation.
- The PKA peripheral provides RSA and ECC cryptography (ECDSA/ECDH/ECIES)
- The coupling and chaining bridge (CCB) peripheral provides the protected mechanism that ensures asymmetric key store.
- The platform instance unique key of key length 128-bit and 256-bit, with a value that differs according to the execution context.

Security functional requirements are supported depending on the platform reference as described in the table below.

Table 7. SFRs

SFR	STM32C542xx	STM32C562xx	STM32C5A3xx
Base PP SFRs			
Verification of platform identity	Y	Y	Y
Secure update of platform	-	-	-
Physical attacker resistance	Y	Y	Y
Software attacker resistance: Isolation of platform parts (between PSA-RoT and Application RoT services)	Y	Y	Y
Cryptographic operation	-	-	Y
Cryptographic random number generation	Y	Y	Y
Cryptographic key store	-	-	Y
Additional SFRs			
Field return of platform	Y	Y	Y
Optional SFRs			
Secure encrypted storage	-	-	Y

Life cycle

The platform life cycle is based on the device RDP mechanism detailed in [RM] *section 3.7.1*.

According to the product life cycle expectation exposed in [GP-SESIP] *section 2.3 Connected Product Life Cycle*, the state mapping shall be as follow:

- In RDP level 0, the state of the device is “OPEN”. RDP level 0 shall be used in the “User delivery” state.
- In RDP level 2, the state of the device is “CLOSE”. RDP level 2 shall necessarily be used in the “Normal usage” state to ensure the activation of SFRs listed in *section 3*.
- Intermediate RDP level 2 with boundary scan is not included in the platform evaluation scope.

Use case

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

The environmental conditions under which the platform 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 executes code that is unknown to the product developer.

1.4.5 Required hardware/software/firmware

As defined in Section 1.4.3: Logical scope, the platform does not include any software component in the evaluation perimeter.

Required nonplatform hardware/software/firmware (ASE_INT.1.6C)

The platform aims to host a secure boot and an immutable platform Root of Trust in a subsequently composite platform as shown in Figure 2 of the platform logical scope.

Consequently, the platform requires a secure boot firmware to achieve at least the following operations on the platform itself:

- Verification of the nonvolatile parameters configured for the state of the live cycle.
- Activation of the HDP securable memory area when switching from the first stage immutable secure boot to the second stage updatable firmware. HDP activation makes the immutable Root of Trust inaccessible for later application code.

The required nonplatform secure boot firmware expectations are exhaustively described in [SG] *section 4.2.2*.

The secure boot firmware might support other security features, such as integrity, verification, or update of the next stage firmware. However, those additional features are not mandatory for the SFRs claimed by the platform.

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.

Table 8. Security objectives for the operational environment

ID	Description	Reference
UNIQUE_ID	The platform user must provide the integrity and uniqueness of the identification of the platform during the personalization stage.	[SG] *Section 4.2.4 Security measures* [SG] *Section 4.2.4 Security measures*
KEY_MANAGEMENT	Cryptographic keys and certificates outside of the platform are subject to secure key management procedures.	
TRUSTED_INTEGRATOR	The integrator builds/personalizes the platform and uses the security functionalities needed by the user application following the security guidance documentation. The integrator is trusted and does not attempt to thwart the security functionalities nor bypass them.	
LIFECYCLE	The integrator is expected to configure the nonvolatile product state according to the stage of product development and deployment.	

2.2 Inherited objectives for the operational environment

The platform does not include platform parts that have previously been 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 the GlobalPlatform® Technology Security Evaluation Standard for IoT Platforms [GP-SESIP].

3.1.1 Flaw reporting procedure (ALC_FLR.2)

Due to the TOE type, meaning “component of a system-on-chip hardware”, the SFR secure update of the platform is not applicable since the implemented hardware is not reprogrammable.

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 in https://www.st.com/content/st_com/en/about/security-and-privacy/psirt.html.

3.2 Base PP security functional requirements

The platform fulfills the following base security functional requirements:

3.2.1 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: Platform reference provides the following identifiers.

STM32C542xx

Table 9. STM32C542xx platform identifiers

Field	Address	Halfword value	Comments
Device identifier (DEV_ID)	0x4402 4000	0x44F	-
Revision identifier (REV_ID)	0x4402 4002	0x1001	Revision Z

The platform also provides the following identifier for the platform configuration.

Table 10. STM32C542xx product configuration

Field	Address	Bitfields	Comments
Product configuration	0x4402 2428	4, 7 reset	AES, HASH enable

STM32C562xx

Table 11. STM32C562xx platform identifiers

Field	Address	Halfword value	Comments
Device Identifier (DEV_ID)	0x4402 4000	0x44E	-
Revision Identifier (REV_ID)	0x4402 40020	0x1003	Revision Y

The platform also provides the following identifier for the platform configuration.

Table 12. **STM32C562xx product configuration**

Field	Address	Bitfields	Comments
Product configuration	0x4002 24280	4, 7 reset	AES, HASH enable

STM32C5A3xx

Table 13. **STM32C5A3xx platform identifiers**

Field	Address	Halfword value	Comments
Device Identifier (DEV_ID)	0x4402 4000	0x45A	-
Revision Identifier (REV_ID)	0x4402 4002	0x1001	Revision Z

The platform also provides the following identifier for the platform configuration.

Table 14. **STM32C5A3xx product configuration**

Field	Address	Bitfields	Comments
Product configuration	0x4002 2428	1, 4, 5, 6, 7 reset	SAES, AES, PKA, CCB, HASH enable

3.2.2 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 platform does not include any firmware component and the implemented hardware is not re-programmable.

3.2.3 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:

STM32C542xx and STM32C562xx

The platform provides the following hardware countermeasures against physical attacks:

- Redundancy checks to prevent RDP and HDP deconfiguration by physical tampering or perturbation.

STM32C5A3xx

The platform provides the following hardware countermeasures against physical attacks:

- Redundancy checks to prevent RDP and HDP deconfiguration by physical tampering or perturbation.
- Detection of transient perturbation attacks in crypto functions (SAES, PKA private operations).
- Prevention of leakage of information via side channels when using AES algorithm (in SAES) or private key cryptography (in PKA).

3.2.4 Software attacker resistance: Isolation of platform (between PSA-RoT and Application Root of Trust Services)

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 functional requirements.

Conformance rationale:

The HDP mechanism prevents any firmware code executed outside the region defined by HDP boundaries from performing any access inside the HDP region. This region can be freely used by the integrator to protect any data or code ensuring the secure initialization of a composite platform.

3.2.5 Cryptographic operation

The platform provides the *operations* in Table 15 functionality with the *algorithms* in Table 15 as specified in the *specifications* in Table 15 for *key lengths* and *modes* described in Table 15

Table 15. 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(2)	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	ECDH ECIES	ANSI X9.42 ANSI X9.63 FIPS PUB 186-4 SEC 1, SEC 2(3)		

1. *Running in side-channel attack resistant SAES peripheral.*
2. *Other PKA operations not written in this table (such as RSA CRT exponentiation or ECDSA signature verification) are not protected against side channel attacks.*
3. *Standards for Efficient Cryptography: SEC1, SEC2*

Conformance rationale:

STM32C5A3xx only

Refer to [RM]:

- *Section 28, Secure AES coprocessor* (SAES)
- *Section 30, Public Key Accelerator* (PKA)

3.2.6 Cryptographic random number generation

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

Conformance rationale:

The TOE includes an RNG peripheral compliant with NIST SP800-90B recommendations. The application must use this peripheral to generate true random numbers.

Refer to [RM] *Section 26 True random number generator (RNG)* for details.

3.2.7 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 15.

Conformance rationale

STM32C5A3xx only

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: 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 [RM] *section 28.4.14: SAES operation with wrapped keys.*

The platform provides hardware mechanisms to protect the confidentiality of RSA and ECC private keys. When the user encrypts those keys under control of the CCB peripheral using the DHUK or a user key wrapped by DHUK, they can only be decrypted in this specific device. The CPU code is never granted access to the values of these keys. The operational secrets are available only in the PKA RAM, isolated during the cryptographic operation and erased before giving back the PKA RAM for next programming. Refer to [RM] *section 25.4.4: CCB coupling and chaining operation*.

3.3 Additional security functional requirements

The platform fulfills the following additional security functional requirements defined in [GP-SESIP].

3.3.1 Field return of the platform

The platform can be returned to the vendor without user data.

Conformance rationale

In the certified configuration (RDP Level 2), the integrator allows the platform to regress to RDP Level 0, when the TOE secret OEMKEY is successfully provisioned, and OEMLOCK option bit is set. The detailed sequence “Regression to L0 open debug level” is described in [RM] *Section 6.5.8: RDP level transitions*. RDP regression to level 0 allows to go to the product's virgin state (flash and protected memories are first erased before reopening the JTAG interface with full debug capabilities).

Note:
1. *If the Integrator sets RDP to Level 2 without programming the OEMKEY the product is locked, and it is not possible to change the RDP level.*
2. *The user should not store any data in OTP as this data is not erased during RDP regression to level 0.*

3.4 Optional security functional requirements

3.4.1 Secure encrypted storage

The platform ensures that all data stored by the application, except for the data stored outside the region encrypted by SAES using DHUK, is encrypted as specified in with a Platform instance unique key of key length described in .

Table 16. Secure encrypted storage cryptographic operations

Operations	Algorithms	Specifications	Key lengths	Modes
Authenticated encryption or decryption	AES(1)	NIST SP800-38C NIST SP800-38D	128, 256 bits	GCM, CCM

1. *AES algorithm running in SAES peripheral (with side-channel resistance).*

Conformance rationale:

STM32C5A3xx only

As described in the conformance rationale of Section 3.2.7: Cryptographic KeyStore, any data encrypted with the DHUK can only be decrypted in this specific device, DHUK is never disclosed to any application code or debugger, and is only usable in side-channel protected SAES peripheral.

Refer to [RM] *Section 28.4.17: SAES key registers for details on selecting DHUK for any supported AES operation*.

4 Mapping and sufficiency rationales

4.1 SESIP3 sufficiency

Table 17. 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	Sections 3.2 to 3.4	All SFRs in this ST are taken from [GP-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	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.

Assurance class	Assurance families	Covered by	Rationale
ALC: Life-cycle support	ALC_FLR.2 Flaw reporting procedures	Section 3.1.1	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: Vulnerability Assessment	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

Table 18. **Reference documentation**

Reference	Definition
Evaluation documents	
[GP-SESIP]	Security Evaluation Standard for IoT Platforms (SESIP), version 1.2 (July 2023), GlobalPlatform, GP_FST_070
[PP]	SESIP Profile for PSA Certified iSE/SE and RoT Component, version 2.0 REL 01, JSADEN018
[PSA-PP]	SESIP Profile for PSA Certified Level 3, version 1.0 REL 02, JSADEN011
[SP 800-90B]	NIST Special Publication (SP) 800-90B (Draft), Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018
[PSA-SM]	Platform Security Model 1.1, (01/12/2021), JSADEN014
Developer documents	
[SG]	STM32C5 security guidance for SESIP level 3 certification, STMicroelectronics, Rev 1
[RM]	RM0522 Reference manual STM32C5 Series Arm®-based 32-bit MCUs, STMicroelectronics, Rev 1
[ES]	STM32C5 device errata sheet: • ES0677 for STM32C5A3xx STM32C593xx, and STM32C591xx. • ES0661 for STM32C551xx, STM32C552xx, and STM32C562xx. • ES0676 for STM32C531xx, STM32C532xx, and STM32C542xx.

6 Glossary

Table 19. **Glossary**

Term	Glossary
Application	Used in SESIP to refer to the components which are out of the scope of the evaluation.
Hardware Unique Key	Secret and unique to the device symmetric key that must not be accessible outside the PSA Root of Trust. It is a Critical Security Parameter.
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
PSA Root of Trust	PSA defined combination of the Immutable Platform Root of Trust and the Updateable Platform Root of Trust. It is the most trusted security component on the device. Refer to [PSA-PSM].

7 Abbreviations

Table 20. **Abbreviations**

Term	Definition
DHUK	Derived hardware unique key
HDP	Hide data protection
HUK	Hardware unique key
PRoT	Platform Root-of-Trust
PSA	Platform security architecture
RDP	Read data protection
RoT	Root-of-Trust
RNG	Random number generator
SFR	Security functional requirement
TOE	Target of evaluation
CCB	Coupling and chaining bridge

Revision history

Table 21. **Document revision history**

Date	Version	Changes
06-Mar-2026	1	Initial release.

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.