STM32C0 SESIP security target for PSA certified™ RoT component level 3

Document information

This security target document is based on the GlobalPlatform™ Security Evaluation Standard for IoT Platforms (SESIP), version 1.2 (June 2021), GP_FST_070.

STM32C0 series are based on Arm®-based 32-bit MCU.

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

1 Introduction

This security target describes the STM32C0 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.

Table 1. Protection profile reference and conformance claims

Reference	Value
Protection profile name	SESIP Profile for PSA Certified RoT Component Level 3 [PP]
Protection profile version	1.0 REL 02
Base PP SFR	Verification of the platform identity, Secure update of the platform, Physical attacker resistance
SFRs for PSA-RoT Component	Software attacker resistance: Isolation of the platform
Assurance claim	Refer to Section 3.1: Security assurance requirements

1.1 Security target reference

This document: *STM32C0 SESIP security target for PSA certified™ RoT component level 3* (TN1590) revision 1.0, STMicroelectronics.

1.2 Platform reference

The table below contains the platform reference values.

Table 2. Platform reference

Reference	Value		
Platform name	STM32C0x031/011 from STM32C0 series advanced Arm®-based 32-bit MCUs		
Platform version	**Configuration standard:**		
	Commercial name:	*Revision:*	
	STM32C011	Z	
	STM32C031	Z	
	STM32C051	A	
	STM32C071	Z	
	STM32C09x	A	
Platform identification	*Commercial name:*	*Die identifier:*	*On chip flash size:*
	STM32C011	0x443	32 KBytes
	STM32C031	0x453	32 Kbytes
	STM32C051	0x44C	64 Kbytes
	STM32C071	0x493	128 KBytes
	STM32C09x	0x44D	256 KBytes
Platform type	General purpose microcontroller device for IoT, industrial, or consumer applications.		

1.3 Included guidance documents

The platform includes the following documents:

Table 3. Guidance documents

Category	Name	Reference
Product user manual	*User manual STM32C0 security guidance for SESIP level 3 certification*	[SG]
Product reference manual	*RM0490 Reference manual STM32C0 Series Arm®-based 32-bit MCUs*	[RM]
Product errata sheet	STM32C0 devices errata sheet: • STM32C011 (ES0569) • STM32C031 (ES0568) • STM32C051 (ES0624) • STM32C071 (ES0618) • STM32C091-92 (ES0625)	[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 connectivity.

The platform consists of an Arm® Cortex®-M0+ based microcontroller with internal flash memories, RAM 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.

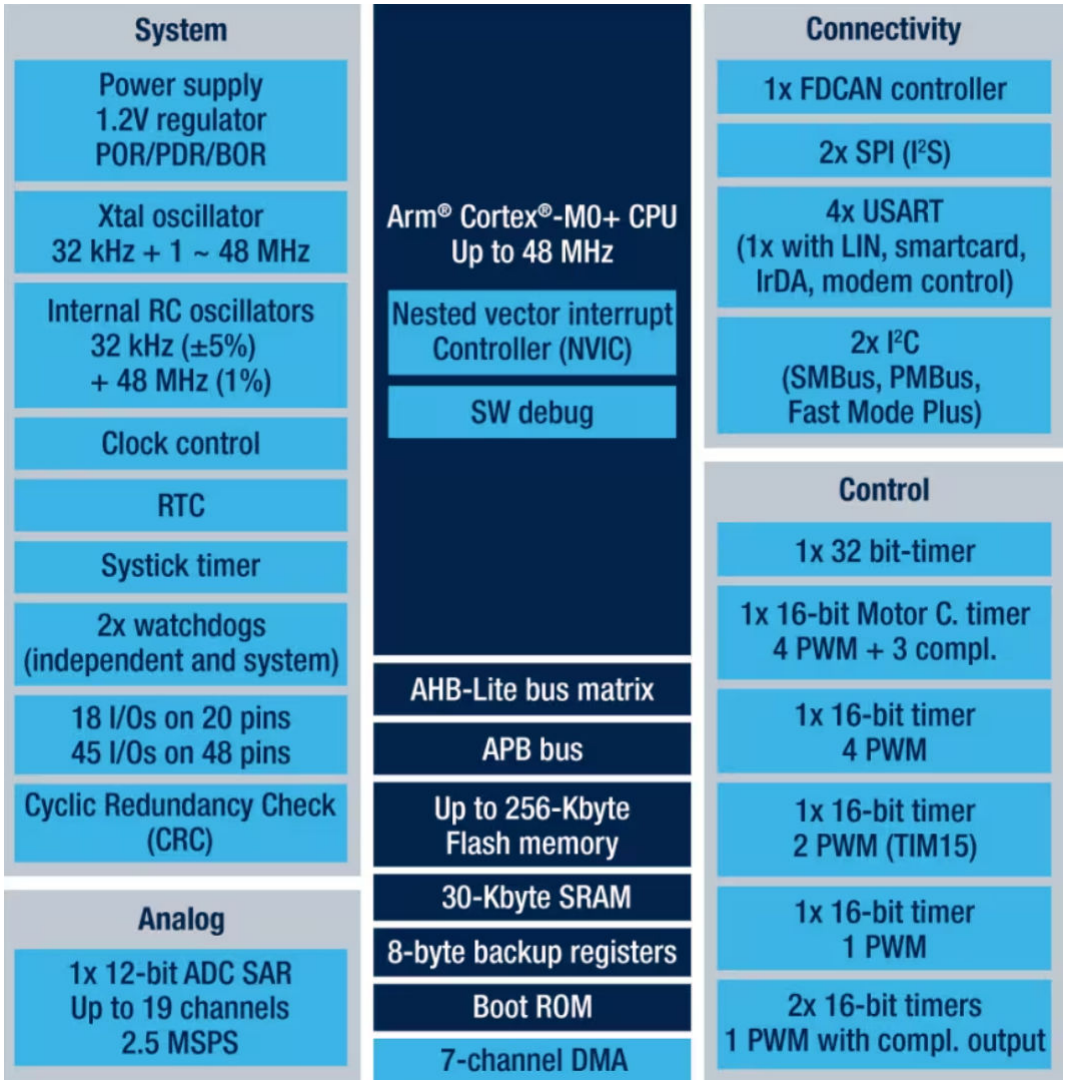
The platform is mainly envisioned to be the lower-level platform part for further composition of evaluation activities.

1.4.2 Physical scope

The physical scope of the platform is implemented in the STM32C0 series of MCU products described in [RM]. The block diagram on Figure 1 provides an overview of the major features supported by these MCU.

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

Figure 1. **Platform physical scope**



The platform perimeter resides in the components and interfaces listed in Table 4. They are described in the [RM] and the [ES].

Table 4. **Hardware components and interfaces of the TOE**

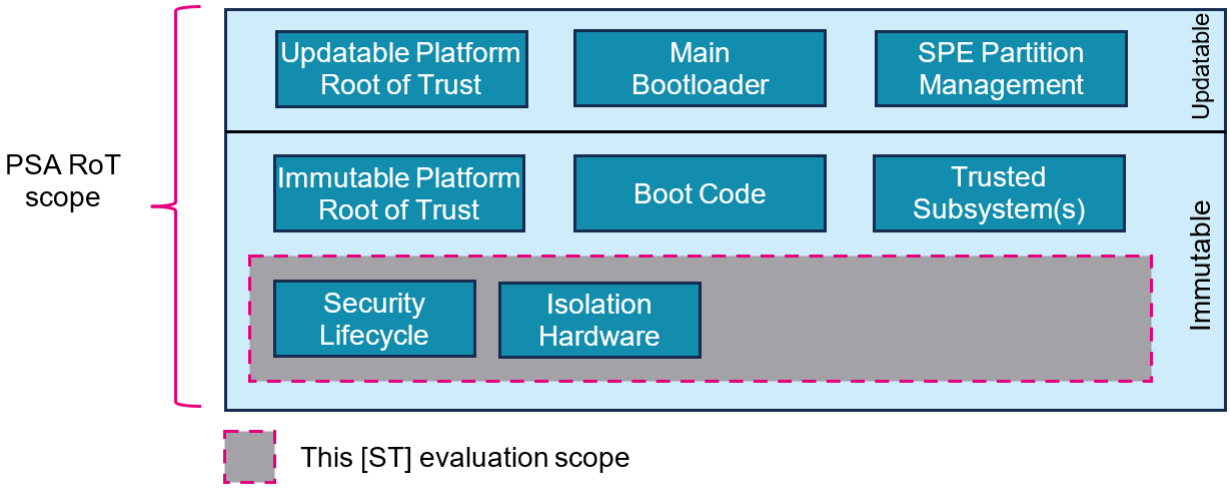
Component/Interface	Description	Identification
CPU	Not applicable	Hardware revision (1)
Debug ports	JTAG/SWD, DBGMCU	
Memories	Flash	
Cryptography	None	

1. *Refer to Platform version in Table 2.*

1.4.3 Logical scope

The block diagram on Figure 2 extracted from [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**



The logical scope of the platform includes:

- The security lifecycle resources.
- The isolation hardware resources.

The logical scope of the platform does not include:

- The immutable platform Root of Trust, for example, includes the boot code, any root parameters, with management and enforcement of the isolation and security lifecycle hardware resources.
- The updateable platform Root of Trust, for example, includes 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 are components that the PSA Root of Trust relies on for the protection of its assets or implement some of its services, for example, a subscriber identification module or a secure element.

The platform has a single configuration as shown in Table 5:

Table 5. **Platform configuration**

Parts	STM32C0x1 (1)
Life cycle	Yes
Isolation hardware	Yes
RNG	No
Cryptographic operation	No

1. *Standard configuration*

1.4.4 Usage and major security features

The platform supports the following major security features:

- RDP: 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 1, the product is still open for debugging with limited debug and execution capabilities. In RDP level 2, the product is closed, the nonvolatile configuration cannot be changed and the debug link is locked. The unique boot entry address is necessarily in user flash.

- HDP (HiDe Protect): The securable memory area mechanism manages the 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 only be executed until the securable area becomes inaccessible, and it remains inaccessible until the next system reset. This allows the implementation of software security services such as trusted storage or a secure boot stage.
  - The base securable memory area is defined by option byte at manufacturing time and is unmodifiable in an RDP level not equal to zero.
  - The code executed in the securable memory area can optionally extend the securable memory area, which is then locked against any later access.

Note: The securable memory area is described as HDP area in the remaining of this document and any associated documents.

Life cycle

The platform life cycle is based on the device RDP mechanism detailed in [RM] section 4.10.1.

According to the product life cycle expectation exposed in [SESIP] section 2.3 Connected Product Life Cycle, the state mapping must be as follows:

- In RDP level 0, the state of the device is “OPEN”. The RDP level 0 must be used in the “User delivery” state to ensure the manufacturer provisioning operation.
- In RDP level 2, the state of the device is “CLOSE”. The RDP level 2 must be used in the “Normal usage” state to ensure the activation of the SFRs listed in [SESIP] section 3.

Note: Intermediate RDP level 1 is not included in the evaluation perimeter.

Configurations

In any version, the platform implements the core minimum security features, meeting the security requirements defined in Section 3.3: Base PP security functional requirements and Section 3.4: SFRs for PSA RoT component. The MCU ensures the execution of platform trusted code, particularly the functions related to secure boot, updatability, and code isolation. It also ensures a secure lifecycle.

Use case

The platform is intended for use by an integrator wishing to implement its proprietary secure boot and Root of Trust.

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 the 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

Note: As defined in Section 1.4.3: Logical scope, the platform does not include any software component in the evaluation perimeter. Required non-platform 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 non-volatile 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. The HDP activation makes the immutable Root of Trust inaccessible for later application code.

The required non-platform secure boot firmware expectations are described in [SG], section 4.2.5 Modes of operation (AGD_OPE.1.5C).

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 6. Security objectives for the operational environment

ID	Description	Reference
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.	[SG], section 4.2.4 Security Measures.
LIFECYCLE	The integrator is expected to configure the non-volatile 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 *GlobalPlatform™ Technology Security Evaluation Standard for IoT Platforms* [SESIP].

3.2 Flaw reporting procedure (ALC_FLR.2)

Since the implemented hardware is not reprogrammable, and due to the TOE type (meaning “component of a system on chip hardware”), the SFR secure update of the platform is not applicable.

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

3.3 Base PP security functional requirements

The platform fulfills the following security functional requirements:

3.3.1 Verification of the platform identity

The platform provides unique platform identification, including all the platform parts and versions.

Conformance rationale

The platform referred to in Section 1.2: Platform reference provides the following identifiers:

Table 7. Platform identifiers

Field	Address	Commercial product	Halfword value	Comments
Device identifier (DEV_ID)	0x40015800	STM32C011	0x443	-
		STM32C031	0x453	-
		STM32C051	0x44C	-
		STM32C071	0x493	-
		STM32C091 STM32C092	0x44D	-
Revision identifier (REV_ID)	0x40015802	STM32C011	0x1001	Revision Z
		STM32C031	0x1001	Revision Z
		STM32C051	0x1000	Revision A
		STM32C071	0x1001	Revision Z
		STM32C091 STM32C092	0x1000	Revision A

3.3.2 Secure update of the platform

Non-conformance rationale:

The platform does not include any firmware component.

The implemented hardware is not re-programmable.

3.3.3 Physical attacker resistance

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

Conformance rationale

The platform provides the following hardware countermeasures against physical attacks:
RDP and HDP specific coding that provides higher Hamming distance to prevent physical fault injection attacks.

3.4 SFRs for PSA RoT component

The platform fulfills the following security functional requirements:

3.4.1 Software attacker resistance: Isolation of the 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 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 reside any data or code ensuring the secure initialization of a composite Platform.
The RoT code is executed in the HDP protected region, after platform boot. The HDP protection is activated after RoT execution, when jumping to the application execution. When HDP is activated, no access read/write is allowed to the regions protected by the HDP boundary.

4 Mapping and sufficiency rationales

4.1 SESIP3 sufficiency

Table 8. SESIP3 sufficiency

Assurance class	Assurance families	Covered by	Rationale
ASE: Security Target evaluation	ASE_INT.1 ST Introduction	Section 1: Section 1	The ST reference is available in the title. The TOE reference is available in Platform reference. The TOE overview and description are available in Platform functional overview and description.
	ASE_OBJ.1 Security requirements for the operational environment	Section 2	The objectives for the operational environment in Section 2 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 with justification in ALC_FLR.2.
	ASE_TSS.1 TOE Summary specification	Section 3	All SFRs are listed per definition. 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 used as reference documentation for the security target.

Table 9. Reference documentation

Reference	Definition
Evaluation documents	
[SESIP]	*Security Evaluation Standard for IoT Platforms (SESIP)*, version 1.1 (June 2021), GlobalPlatform, GP_FST_070
[PP]	*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
[PSA-SM]	*Platform Security Model 1.1*, (01/12/2021), JSADEN014
Developer documents	
[SG]	*UM3520 STM32C0 security guidance for SESIP level 3 certification*, STMicroelectronics, Rev 1
[RM]	*RM0490 Reference manual STM32C0x1 Series Arm®-based 32-bit MCUs*, STMicroelectronics, Rev 5.0
[ES]	*ES0568 STM32C031 device errata*, STMicroelectronics, Rev 4.0
	ES0569 STM32C011 device errata, STMicroelectronics, Rev 4.0
	ES0624 STM32C051 device errata, STMicroelectronics, Rev 1.0
	ES0618 STM32C071 device errata, STMicroelectronics, Rev 1.0
	ES0625 STM32C091-92 device errata, STMicroelectronics, Rev 1.0
[PSIRT]	*DM00882158, PSIRT ST PRODUCT SECURITY INCIDENT RESPONSE TEAM (PSIRT) MANAGEMENT*, Rev 1.0

6 Glossary

Table 10. **Glossary**

Term	Definition
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-SM].

7 Abbreviations

Table 11. **Abbreviations**

Term	Definition
RoT	Root of trust
HDP	HiDe protection (also known as securable memory)
HUK	Hardware unique key
PRoT	Platform Root of Trust
PSA	Platform security architecture
RDP	Read data protection
RNG	Random number generator
SFR	Security functional requirement
TOE	Target of evaluation

Revision history

Table 12. **Document revision history**

Date	Version	Changes
17-Jun-2025	1	Initial release.

Contents

List of tables

List of figures