life.augmented

TN1481

Technical note

STM32U0 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 1.1 (June 2021), GP_FST_070.

1 Introduction

This Security Target describes the STM32U0 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
Package claim	Platform Identity, Isolation of Platform, Physical Attacker, Cryptographic Random Number Generation
Assurance claim	Refer to Section 3.1.

1.1 Security Target Reference

This document: *STM32U0 SESIP Security Target for PSA Certified™ RoT Component Level 3* (TN1481) revision 1, STMicroelectronics.

1.2 Platform Reference

Table 2. Platform reference

Reference	Value		
Platform name	STM32U0 ultra-low-power Arm® Cortex®-M0+ 32-bit MCU		
Platform version	Revision 1		
Platform identification	Commercial name:	Die Identifier:	On-chip flash:
	STM32U073/083xx	489	256 Kbytes
	STM32U031xx	459	128 Kbytes
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 3. Guidance documents

Document	Name	Reference
User manual	User manual *STM32U0 security guidance for SESIP level 3 certification*	[SG]
Product reference manual	Reference manual *STM32U0 series advanced Arm®-based 32-bit MCUs*	[RM]

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

1.4 Platform functional overview and description

1.4.1 Platform type

The Platform is a general-purpose microcontroller member of the ultra-low-power and entry-level MCU series. It ensures simple and cost-reduction integration, energy efficiency, multiple choice of power modes, and serial link connectivity.

The Platform consists of an Arm® Cortex®-M0+ based microcontroller with internal flash memories, RAMs, and peripherals.

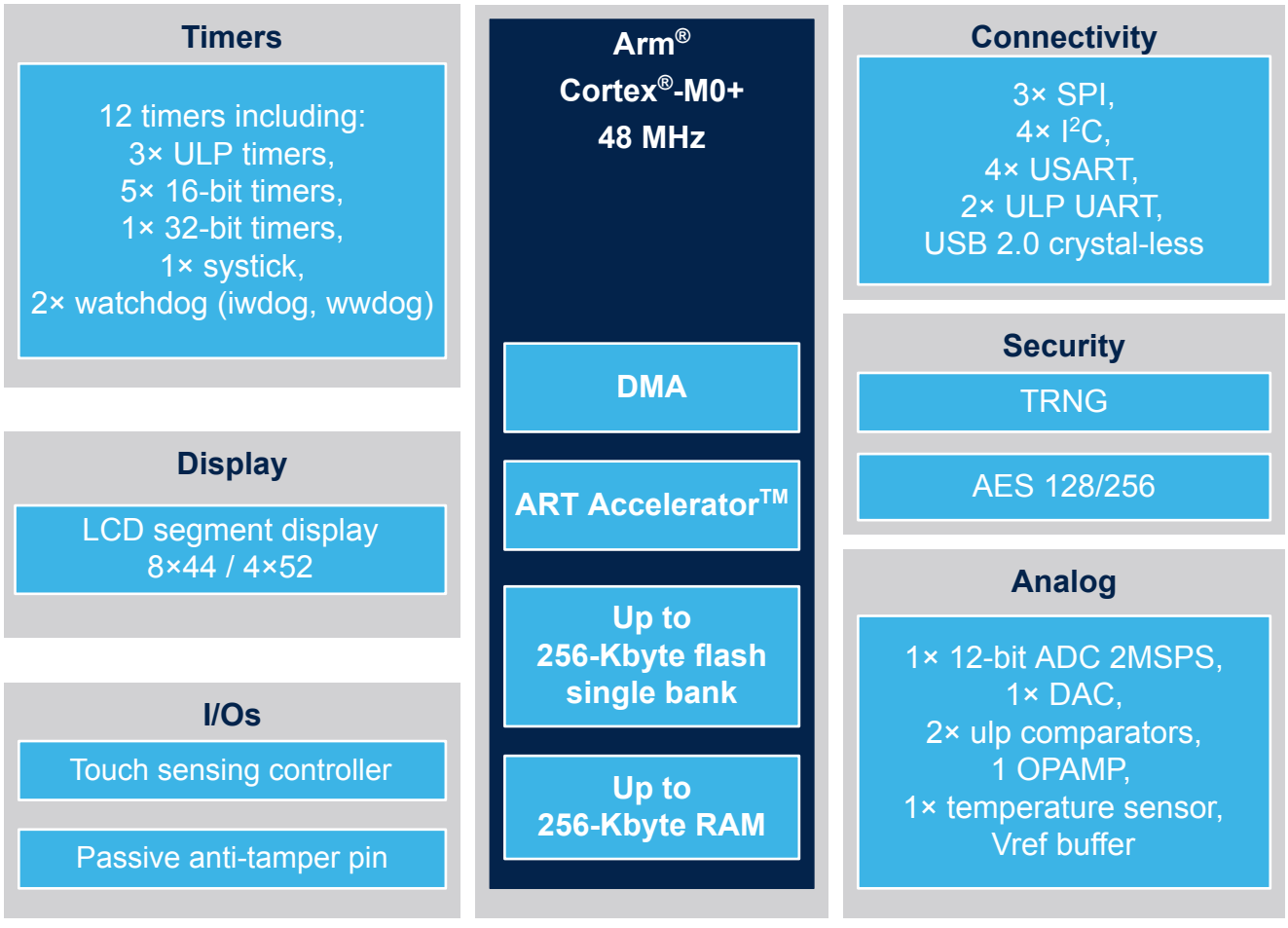
The Platform provides the necessary hardware building blocks for the TOE integrator to implement a secure boot with a protected Root of Trust.

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

1.4.2 Physical scope

The physical scope of the Platform is implemented in the STM32U0 series of MCU products described in the [RM] reference manual. The block diagram below provides an overview of the major features supported by this MCU.

Figure 1. Platform physical scope



The Platform perimeter resides in the memory protection features of the flash interface [RM] Section 3.5 and in the random number generator [RM] Section 21.

1.4.3 Logical scope

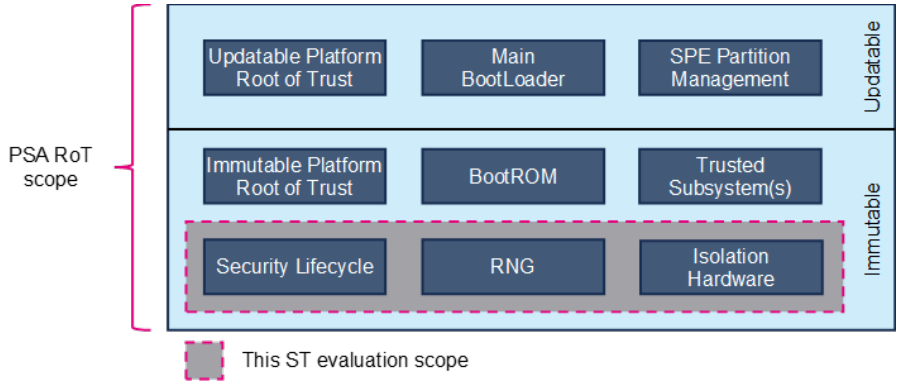
The STM32U0 hardware features in the scope of the security evaluation are a subset of a system-on-chip product that achieves all mandatory operations:

- To protect the memory region where a secure boot code should be executed,
- To provide physically generated random number seeding the Platform and enabling boot cryptographic algorithm,
- To lock down the product configuration when deployed in the field.

Guidance documentation for the STM32U0 hardware security features is listed in Section 1.3.

The logical scope of the security evaluation conforms to the Platform Root of Trust description explained in [PSA-SM] Section 2:

Figure 2. Platform logical scope



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 1, the product is still open for debugging but without access to user flash or nonvolatile configuration change. 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.
- The securable memory area HDP 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 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 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.

Life cycle

The Platform life cycle is based on the device RDP mechanism detailed in [RM] Section 3.5.1.

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 RDP0, the state of the device is “OPEN”. RDP0 must be used in the **“User delivery”** state to ensure manufacturer provisioning operation.
- In RDP1, the state of the device is “OPEN” with limitations as described in [RM] Table 15. RDP1 might optionally be used for provisioning verification purposes.

- In RDP2, the state of the device is “CLOSE”. RDP2 must mandatorily be used in the **“Normal usage”** state to ensure the activation of SFRs listed in Section 3.

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 TOE 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

The TOE 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 composed Platform as shown in Figure 2 of the logical scope Platform.

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 security 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 untrusted 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.

UNIQUE_ID:

The Platform user must provide the integrity and uniqueness of the identification of the Platform during the personalization stage, as described in Section 4.2.4 “Security Measures” of [SG].

KEY_MANAGEMENT:

Cryptographic keys and certificates outside of the Platform are subject to secure key management procedures, as described in Section 4.2.4 “Security Measures” of [SG].

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 or bypass them, as described in Section 4.2.4 “Security Measures” of [SG].

LIFECYCLE:

The integrator is expected to configure the nonvolatile product state according to the stage of product development and deployment, as described in Section 4.2.4 “Security Measures” of [SG].

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 [SESIP].

3.2 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 give generate any needed update and distribute it, the developer has defined the procedure described in *https://www.st.com/content/st_com/en/security/report-vulnerabilities.html*.

3.3 Base PP 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 for each of the evaluated dice, including all its parts and their versions.

Conformance rationale:

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

Table 4. Document revision history

Field	Address	Halfword value	Comments
Device Identifier (DEV_ID)	0x4001 5800	0x489	STM32U073/083xx
Device Identifier (DEV_ID)	0x4001 5800	0x459	STM32U031xx
Revision Identifier (REV_ID)	0x4001 5802	0x1000	V1.0

3.3.2 Secure Update of Platform

Nonconformance rationale:

The Platform does not include any firmware components and the implemented hardware is not reprogrammable.

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 functional requirements.

Conformance rationale:

The Platform provides hardware countermeasures based on redundancy checks to prevent RDP and HDP deconfiguration by 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 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.

3.4.2 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 21 True random number generator (RNG) for details.

4 Mapping and Sufficiency Rationales

4.1 SESIP3 Sufficiency

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	For the objectives of 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 [1]. “Verification of Platform Identity” is included. “Secure Update of 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 “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	NA 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 a potential attack of enhanced-basic.

5 Reference documents

Table 5. Reference documents

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 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018
[PSA-SM]	Platform Security Model 1.1, January 12, 2021, JSADEN014
Developer documents	
[SG]	User manual *STM32U0 security guidance for SESIP level 3 certification* (UM3271) revision 1
[RM]	Reference manual *STM32U0 series advanced Arm®-based 32-bit MCUs* (RM0503) revision 1

6 Glossary

Table 6. **Glossary**

Term	Definition
Application	Used in SESIP to refer to the components that are out of the scope of the evaluation.
Platform	Used in SESIP to refer to the components that are in the scope of the evaluation. It is a synonym for a connected platform.
Product	Used by SESIP as a synonym for connected product

7 Abbreviations

Table 7. **Abbreviations**

Term	Definition
RoT	Root of Trust
HDP	Hide data protection
RDP	Read data protection
RNG	Random number generator
SFR	Security Functional Requirement
TOE	Target of evaluation

Revision history

Table 8. **Document revision history**

Date	Revision	Changes
06-Mar-2024	1	Initial release.

Contents

List of tables

List of figures