Security Target for Nordic Semiconductor nRF5340

Document number:	001
Version:	1.0
Release Number:	01
Author	Nordic Semiconductor ASA
Date of Issue:	30/06/2023

Abstract

PSA Certified is the independent security evaluation scheme for Platform Security Architecture (PSA) based IoT systems. It establishes trust through a multi-level assurance program for chips containing a security component called a Root of Trust (PSA-RoT) that provides trusted functionality to the platform. The multi-level scheme has been designed to help device makers and businesses get the level of security they need for their use case.

PSA Certified Level 2 is a fixed time, test laboratory based, evaluation of the PSA-RoT. It is aimed at IoT devices that need to protect against basic software attacks. The Level 2 documents include: a SESIP Profile that describes the Target of Evaluation, its assets, the security objectives and security functions that will be evaluated and an Attack Methods (AM) document describing the attacks in scope.

Developers submit their PSA-RoT to an approved test laboratory, listed on **www.psacertified.org**, for Level 2 evaluation and receive an Evaluation Technical Report. If the PSA-RoT is assessed as passing and approved by the independent Certification Body, a digital certificate will be issued on the PSA Certified website.

1 Keywords

PSA Certified Level 2, SESIP, Certification, IoT, Platform Security Architecture, Questionnaire, PSA, Security

Non-Confidential Proprietary Notice

Your access to the information in this document is conditional upon your acceptance that you will not use or permit others to use the information for the purposes of determining whether implementations infringe any third-party patents.

THIS DOCUMENT IS PROVIDED "AS IS". ARM PROVIDES NO REPRESENTATIONS AND NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE DOCUMENT. For the avoidance of doubt, Arm makes no representation with respect to, and has undertaken no analysis to identify or understand the scope and content of, patents, copyrights, trade secrets, or other rights.

This document may include technical inaccuracies or typographical errors.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL ARM BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF ARM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This document consists solely of commercial items. You shall be responsible for ensuring that any use, duplication or disclosure of this document complies fully with any relevant export laws and regulations to assure that this document or any portion thereof is not exported, directly or indirectly, in violation of such export laws. Use of the word "partner" in reference to Arm's customers is not intended to create or refer to any partnership relationship with any other company. Arm may make changes to this document at any time and without notice.

If any of the provisions contained in these terms conflict with any of the provisions of any click through or signed written agreement covering this document with Arm, then the click through or signed written agreement prevails over and supersedes the conflicting provisions of these terms. This document may be translated into other languages for convenience, and you agree that if there is any conflict between the English version of this document and any translation, the terms of the English version of the Agreement shall prevail.

Arm Limited. Company 02557590 registered in England.
110 Fulbourn Road, Cambridge, England CB1 9NJ.

Contents

2 About this document

2.1 Release Information

The change history table lists the changes that have been made to this document.

Date	Version	Confidentiality	Change
17/02/2023	0.9	Non-confidential	Initial version
21/03/2023	0.91	Non-confidential	Added Abstract section to comply with “SESIP Profile for PSA Certified™ Level 2” V1.0 Rel 02.
11/04/2023	0.92	Non-confidential	Updated the PSIRT URL
30/06/2023	1.0	Non-confidential	Updated based on EM2 remarks

2.2 References

This document refers to the following documents.

2.2.1 Normative references

Ref	Doc No	Author(s)	Title
[PSA-L1]	JSADEN001	JSA	PSA Certified Level 1 Questionnaire
[PSA-EM-L2]	JSADEN003	JSA	PSA Certified: Evaluation Methodology for PSA L2
[PSA-EM-L3]	JSADEN010	JSA	PSA Certified: Evaluation Methodology for PSA L3
[PSA-AM]	JSADEN004	JSA	PSA Certified Attack Methods
[PSA-PP-L2]	JSADEN002	JSA	PSA Certified Level 2 Lightweight Protection Profile
[PSA-PP-L3]	JSADEN009	JSA	PSA Certified Level 3 Lightweight Protection Profile
[SESIP-PP-L3]	JSADEN011	JSA	SESIP Profile for PSA Certified™ Level 3
[PSA-L2-COMP]	JSADEN017	JSA	SESIP Profile for PSA Certified™ RoT Component Level 2
[PSA-L3-COMP]	JSADEN018	JSA	SESIP Profile for PSA Certified™ RoT Component Level 3
[SESIP]	GP_FST_070	GlobalPlatform	Security Evaluation Standard for IoT Platforms (SESIP) v1.1
[CEM]	CCMB-2017-04-004	Common Criteria	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, revision 5, April 2017.

2.2.2 Informative references

Ref	Doc No	Author(s)	Title
[GP-ROT]	GP_REQ_025	GlobalPlatform	Root of Trust Definitions and Requirements, Version 1.1, Public Release, June 2018
[PSA-SM]	ARM DEN 0079	Arm	Platform Security Model

2.3 Terms and Abbreviations

This document uses the following terms and abbreviations (see PSA-SM and PSA-L1).

Term	Meaning
Application	Used in this SESIP profile to refer to the components which are out of the scope of the evaluation.
Application Root of Trust Service(s)	Application specific security service(s) that are not defined by PSA. Such services execute in the Secure Processing Environment and are required to be in Secure Partitions.
Application Specific Software	Software that provides the functionality required of the specific device. This software runs in the Non-Secure Processing Environment, making use of the System Software, Application RoT Services and PSA-RoT Services.
Critical Security Parameter	Secret information, with integrity and confidentiality requirements, used to maintain device security, such as authentication data (passwords, PIN, certificates), secret cryptographic keys, etc.
Evaluation Laboratory	Laboratory or facility that performs the technical review of questionnaires submitted for Level 1 PSA certification. The list of evaluation laboratories participating to PSA Certified can be found on www.psacertified.org
Hardware Unique Key (HUK)	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.
Host Platform	The entity which when used in composition with a certified PSA Level 2 RoT Component [PSA-L2-COMP] or a certified PSA Level3 RoT Component [PSA-L3-COMP] form the scope of the certification covered in this profile.
Initial Attestation Key (IAK)	A PSA-RoT secret private key from an asymmetric key-pair used to sign attestation reports, thus ensuring that the report is bound to a unique PSA- RoT (and so device) instance.
Non-secure Processing Environment (NSPE)	The processing environment that hosts the non-secure System Software and Application Specific Software. PSA requires the NSPE to be isolated from the SPE. Isolation between partitions within the NSPE is not required by PSA though is encouraged where supported.
Partition	The logical boundary of a software entity with intended interaction only via defined interfaces, but not necessarily isolated from software in other partitions. Note that both the NSPE and SPE may host partitions.
Platform	Used in this SESIP Profile to refer to the components which are in the scope of the evaluation.
PSA	Platform Security Architecture

Term	Meaning
PSA Certification Body	The entity that receives applications for PSA security certification, issues certificates, maintains the security certification scheme, and ensures consistency across all the evaluation laboratories.
PSA Functional APIs	PSA defined Application Programming Interfaces on which security services can be built. APIs defined so far include Crypto, Secure Storage and Attestation.
PSA Functional API Certification	Functional certification confirms that the device implements the PSA Functional APIs correctly by passing the PSA Functional certification test suites.
PSA Root of Trust (PSA-RoT)	The PSA defined combination of the Immutable Platform Root of Trust and the Updateable Platform Root of Trust and is considered to be the most trusted security component on the device. See [PSA-SM].
Immutable Platform Root of Trust	The minimal set of hardware, firmware and data of the PSA-RoT, which is inherently trusted because it cannot be modified following manufacture. There is no software at a deeper level that can verify that it as authentic and unmodified.
Updateable Platform Root of Trust	The firmware, software and data of the PSA-RoT that can be securely updated following manufacture.
Platform Root of Trust Service(s)	PSA defined security services for use by PSA-RoT, Application RoT Service(s) and by the NSPE. Executes in the Secure Processing Environment and may use Trusted Subsystems. This includes the services offered by the PSA Functional APIs.
SESIP Profile	Document providing a common set of functionality for similar products
Secure Partition	A Partition in the Secure Processing Environment.
Secure Processing Environment Partition Management	Management of the execution of software in Secure Partitions. Typical implementations will provide scheduling and inter partition communication mechanisms. Implementations may also enforce isolation between the managed Secure Partitions.
Secure Processing Environment (SPE)	The processing environment that hosts the PSA-RoT, the PSA-RoT Services, and any Application RoT Service(s).
Secure Boot	The process of verifying and validating the integrity and authenticity of updateable firmware and software components as a pre-requisite to their execution. This must apply to all the firmware and software in the SPE. It should also apply to the first NSPE image loaded, which may extend the NSPE secure boot chain further.
Security Target (ST)	Document providing an implementation-dependent statement of security of a specific identified platform.
System Software	NSPE software that may comprise an Operating System or some run-time executive, together with any middleware, standard stacks and libraries, chip specific device drivers, etc., but not the application specific software.

Term	Meaning
TOE	Target of Evaluation. In this SESIP Profile it is a synonym for Platform.
Trusted subsystem	A security subsystem that the PSA-RoT relies on for protection of its assets, or that implement some of its services.

3 Introduction

The Security Target describes the Platform (in this chapter) and the exact security properties of the Platform that are evaluated against [SESIP GP] (in chapter "Security Functional Requirements") and that a potential consumer can rely upon the product upholding if they fulfill the objectives for the environment (in chapter "Security objectives for the operational environment").

3.1 SESIP Profile Reference

Reference	Value
PP Name	SESIP Profile for PSA Certified Level 2
PP Version	V1.0 REL 02
Assurance Claim	SESIP Assurance Level 2 (SESIP 2)
Optional and additional SFRs	Secure debugging, Secure storage (internal storage), Residual information purging

Table 1: SESIP Profile Reference

3.2 ST Reference

See title page.

3.3 Platform Reference

The platform is uniquely identified by its chip (hardware) reference and its PSA defined Root of Trust (software) reference as described below. The developer declares that only the evaluated and successfully certified products identify in this way.

Reference	**Value**	
Platform Name	nRF5340	
Platform Version	1	
Platform Identification	Chip name and version	nRF5340-xxxx-D00 xxxx indicates the package variant, and it is irrelevant for platform identification.
	PSA-RoT name and version	Fork of TF-M open-source version 1.6.0 and MCUboot 1.10.0-dev Public release tag for Nordic: nRF Connect SDK 2.2.x
Platform Type	Arm Cortex-M33 microcontroller, running Trusted Firmware-M and MCUboot as the Platform Root-of-trust	
Trusted Subsystem Identification	*N/A*	
Trusted Sub-system Certification	*N/A*	

Table 2: Platform Reference

3.4 Included Guidance Documents

The following documents are included with the platform:

Reference	Name	Version
[NCS]	nRF Connect SDK Documentation https://developer.nordicsemi.com/nRF_Connect_SDK/doc/2.2.0/nrf/index.html	*V2.2.0*
[MCUBOOT]	MCUboot documentation in the nRF connect SDK https://developer.nordicsemi.com/nRF_Connect_SDK/doc/2.2.0/mcuboot/wrapper.html	V1.9.99
[TFM]	Trusted Firmware-M documentation https://developer.nordicsemi.com/nRF_Connect_SDK/doc/2.2.0/tfm/index.html	V1.6.0
[PSASTORAGE]	PSA Secure Storage API https://arm-software.github.io/psa-api/storage/	V1.0.0
[PSACRYPTO]	PSA Crypto API https://arm-software.github.io/psa-api/crypto/	V1.0.0
[PSAATTESTATION]	PSA Attestation API https://arm-software.github.io/psa-api/attestation/	V1.0.2
[NRF5340]	nRF5340 Product Specification https://infocenter.nordicsemi.com/pdf/nRF5340_PS_v1.3.pdf	V1.3

Table 3: Guidance Documents

3.5 Platform Functional Overview and Description

3.5.1 TOE Type

nRF5340 is an ultra-low power wireless System on Chip (SoC) with two Arm® Cortex®-M33 processors and a multiprotocol 2.4 GHz transceiver. The two flexible processors, combined with advanced security features is suitable for professional lighting, advanced wearables, and other complex IoT applications.

3.5.2 Platform Type

The Platform is a microcontroller based on Arm Cortex-M33 with integrated flash and RAM, a multiprotocol 2.4 GHz transceiver, and with security features for cryptographic algorithms, key management and SPE/NSPE isolation.

3.5.3 Physical Scope

The hardware is a *System-on-Chip.*

The hardware is in the scope of the security evaluation as it provides security features, such as immutable storage, isolation features, cryptographic functionality and key management, which are essential for ensuring the security of the implementation.

ToE consist of an Arm Cortex-M33 CPU with security extensions, which allows the CPU to operate in a secure or non-secure mode. The secure mode implements the SPE, while the non-secure mode implements the NSPE. The

SoC also contains another Arm Cortex-M33 CPU as the network core. However, this CPU is outside the scope of the TOE and can be considered as an attacker.

ToE has a CryptoCell cryptographic chip, a Key Management unit (KMU) peripheral, System Protection Unit (SPU) peripheral which configures TrustZone non-secure, secure and non-secure callable memory regions, functionality for enabling/disabling debugger access to CPU registers and memory mapped addresses (APPROTECT). Residual information purging is supported with ERASEALL dependent on ERASEPROTECT. Details are available in [NRF5340].

3.5.4 Logical Scope

The scope for a SESIP Security evaluation, or Target of Evaluation (TOE), according to this profile is the combination of the trusted hardware and firmware components implementing a PSA-RoT with the Security Functional Requirements stated in this document, see Figure 3-1.

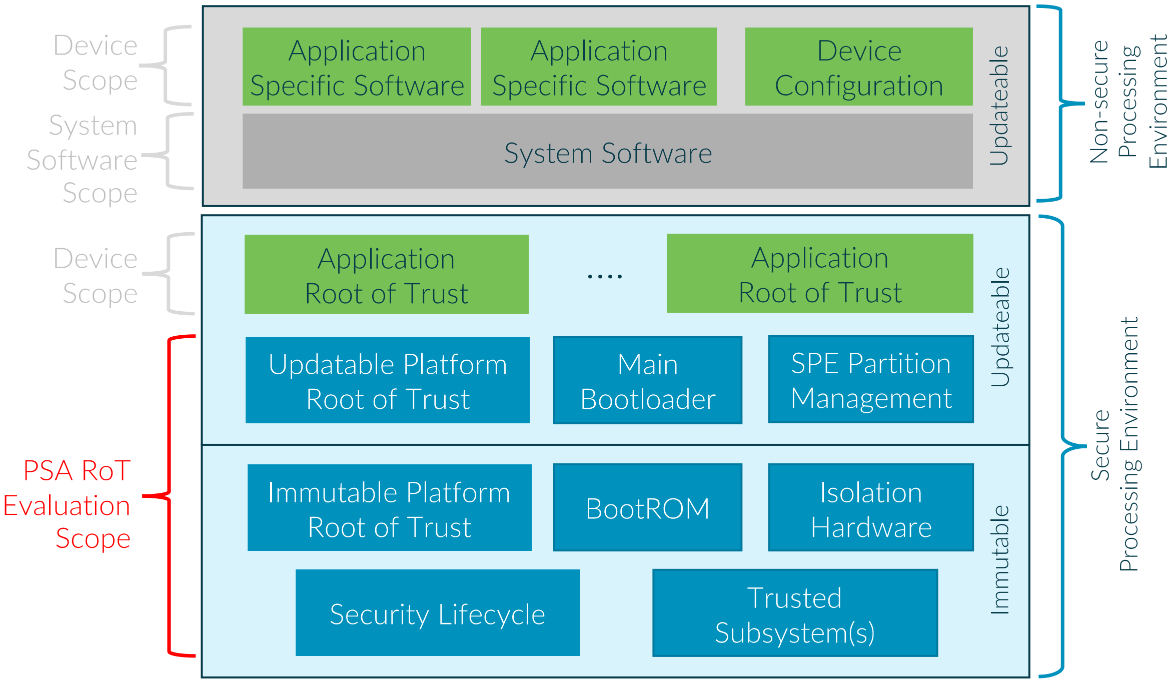

Figure 3-1: Scope of PSA Certified Level 2

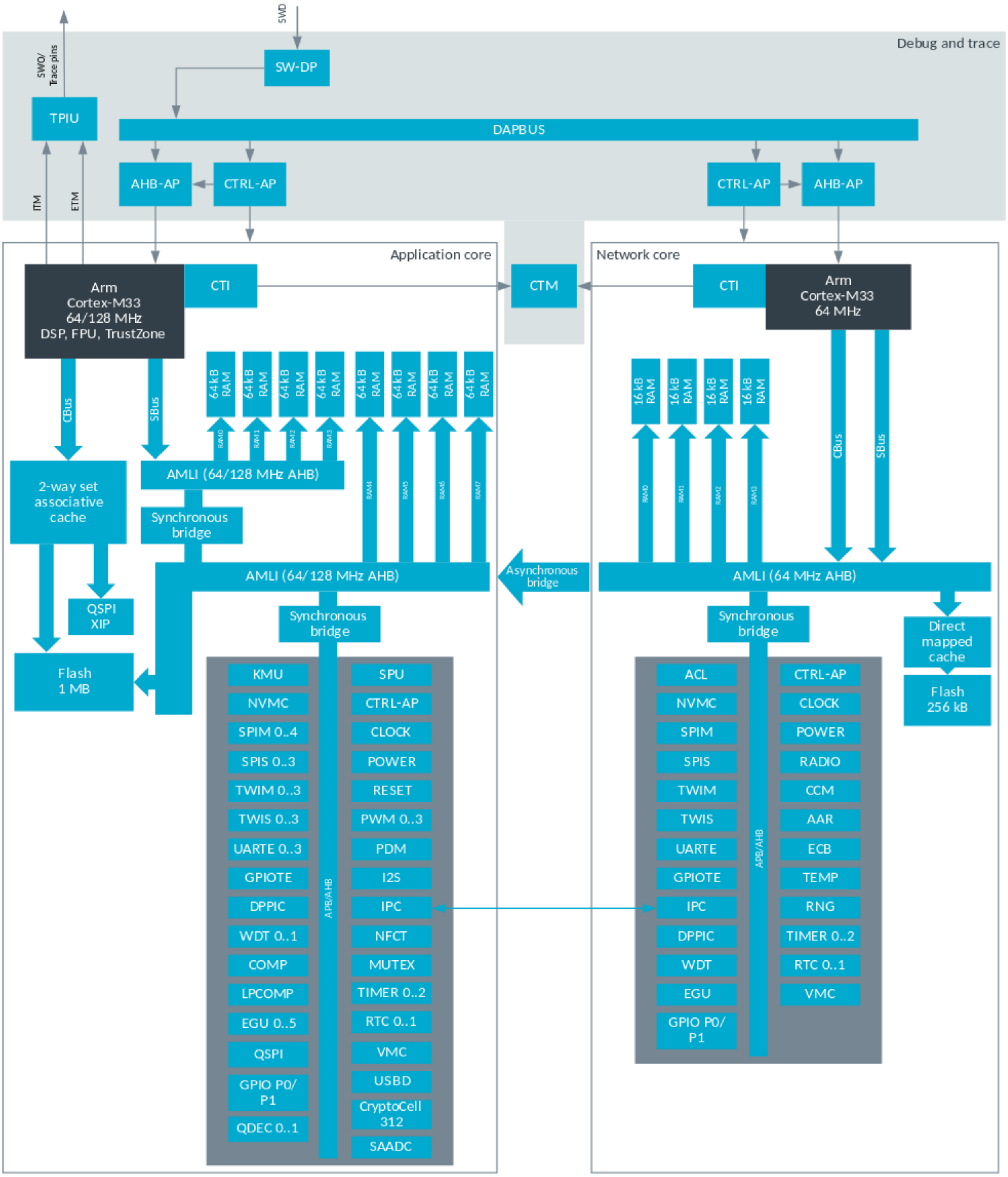

Figure 3-2: TOE architecture

The Chip security evaluation scope includes the following Secure Processing Environment PSA-RoT elements, as described in [PSA-SM]:

- Immutable Platform Root of Trust, for example, immutable bootloader, any root parameters, the NSPE/SPE isolation hardware, and any hardware-based security lifecycle management and enforcement.
- Updateable Platform Root of Trust, for example, a main bootloader, the code that implements the SPE Partition Management function, the code that implements the PSA defined services such as attestation, secure storage, and cryptography.

The platform scope hardware is a system-on-chip with security peripherals as outlined in 3.5.3 and detailed in [NRF5340].

The software scope is an immutable bootloader (NSIB) as part of the immutable Platform Root of Trust, the updateable platform root of trust running from the main bootloader based on MCUboot, and an updatable system firmware based on Trusted Firmware-M running in the SPE. The secure firmware provides cryptographic functionality, secure storage and attestation APIs that are in the logical scope of evaluation.

3.5.5 Usage and Major Security Features

This profile considers the following features for the purpose of PSA Level 2 security evaluation:

- A Secure Processing Environment (SPE) isolated by hardware mechanisms to protect critical services and related assets from the Non-Secure Processing Environment.
- A Secure Boot process to verify integrity and authenticity of executable code in a chain of trust starting from the immutable bootloader. Related certificates are protected in integrity by hardware mechanisms.
- Support for Secure Storage, to protect integrity and confidentiality sensitive assets for the SPE and related applications. These assets include at least the Hardware Unique Key (HUK), the PSA-RoT Public Key (ROTPK), the Initial Attestation Key (IAK), and the unique instance ID.
- A Security Lifecycle for the SPE, to protect the lifecycle state for the device and enforce the transition rules between states.
- Cryptographic functions services for SPE and NSPE applications.
- Support for an attestation method, for example Entity Attestation Token (according to IETF specification).
- Arm CryptoCell Hardware Accelerator CC312
- Support for CPU-inaccessible keys through the Key Management Unit (KMU) peripheral. Stored keys can only be accessed and used by the CryptoCell hardware accelerator
- Support for OTP memory in non-volatile memory in the UICR register interface
- Access protection through APPROTECT, SECUREAPPROTECT and ERASEPROTECT
- Nordic proprietary IDAU implementation called System Protection Unit (SPU) to configure RAM and peripherals as well as supporting locking until the next reset.

3.5.6 Required Hardware/Software/Firmware

No additional non-TOE hardware, software, or firmware is required.

4 Security Objectives for the operational environment

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

ID	Description	Reference
KEY_MANAGEMENT	Cryptographic keys and certificates outside of the Platform are subject to secure key management procedures.	[NCS] "Security", "Trusted Firmware-M Samples – *Provisioning image* and *PSA template*", "Other samples – Bootloader"
TRUSTED_USERS	Actors in charge of Platform management, for instance for signature of firmware update, are trusted.	[NCS] "Security", "Trusted Firmware-M Samples – *Provisioning image* and *PSA template*", "Other samples – Bootloader"
UNIQUE_ID	The integrity and uniqueness of the unique identification of the Platform must be provided by the Platform user during the personalization stage.	[NCS] "Security", "Trusted Firmware-M Samples – *Provisioning image* and *PSA template*"

Table 4: Security Objectives for the Operational Environment

5 Security Requirements and Implementation

5.1 Security Assurance Requirements

The claimed assurance requirements package is **SESIP2** as described in Section 6.1.

5.1.1 Flaw Reporting Procedure (ALC_FLR.2)

In accordance with the requirement for a flaw reporting procedure (ALC_FLR.2), including a process to report flaw and generate any needed update and distribute it, the developer has defined the following procedure:

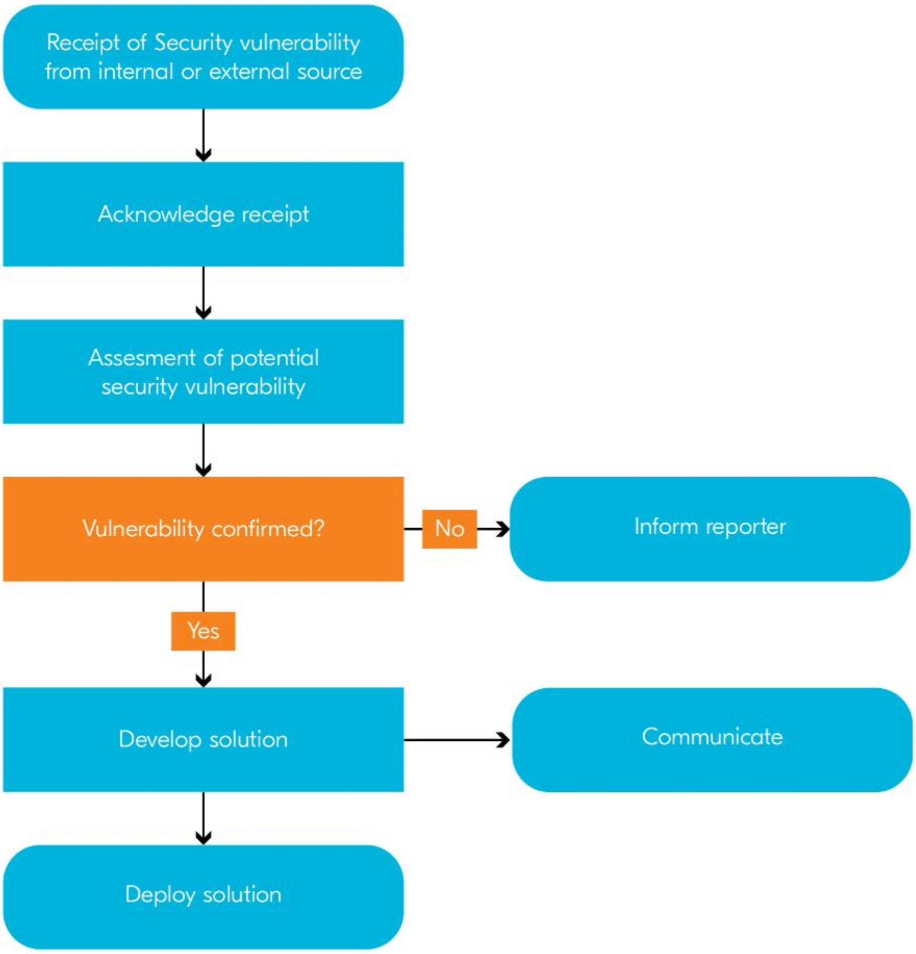
Receipt of Security vulnerability from internal or external source
Acknowledge receipt
Assesment of potential security vulnerability
Vulnerability confirmed?
No
Inform reporter
Yes
Develop solution
Communicate
Deploy solution

Figure 5-1: Flaw remediation process

More details about the vulnerability disclosure program is available here
https://www.nordicsemi.com/Support/Security/Vulnerability-Disclosure

5.2 Base PP Security Functional Requirements

As a base, the platform fulfils the following security functional requirements:

5.2.1 Verification of Platform Identity

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

Conformance rationale:

The hardware can be identified by inspecting the device marking. The marking shall read as follows:

```
N5340
ppAAD0
YYWWLL
```

pp indicates the packaging and it is irrelevant for identification purpose.

YYWWLL specified the Year code, Assembly week number, and Wafer lot code which are not relevant for TOE identification purpose.

The software can be identified by verifying the tag of the SDK. The tag shall be identical to “PSA-RoT name and version” stated in the Platform reference. The attestation token provided by the PSA Initial Attestation service also contains Implementation ID as well as the SW components in the platform firmware.

5.2.2 Verification of Platform Instance Identity

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

Conformance rationale:

The Instance ID is calculated from the Attestation public key. The asymmetric Attestation Key is created either by using HW enabled random number generator on-device or through key provisioning in a secure production line. The generated or provisioned attestation key is required to be unique per-device.

This unique information is provided to the application through the PSA Initial Attestation service.

5.2.3 Attestation of Platform Genuineness

The platform provides an attestation of the “Verification of Platform Identity” and “Verification of Platform Instance Identity”, in a way that ensures that the platform cannot be cloned or changed without detection.

Conformance rationale:

The system utilizes asymmetric key material (the Initial Attestation Key) to create signed attestations (ECDSA using secp256r1). The key is either generated on the device (and never shared outside of the device) or provisioned in a secure production line. The key is encrypted using a hardware unique key that is either generated on the device or provisioned in a secure production line. Decrypting the attestation key material requires access to the CryptoCell hardware registers, which is configured to be accessible only to privileged mode. The hardware unique encryption key is stored in a Key Management Unit (KMU) peripheral, which is a secure-only peripheral that only allows keys to be accessed by CryptoCell hardware peripheral. The decryption key material can't be directly accessed by the CPU.

The KMU peripheral supports a write-once mechanism, which means the key material can't be changed after the key has been written. The only way to change the key is to erase it using the NVMC functionality ERASEALL. This clears all code and key-material on the device.

As part of the functionality provided by the PSA Initial Attestation service, "Verification of Platform Identity" is fulfilled by the presence of *Implementation ID* as well as *SW components in the platform firmware* in the attestation token. "Verification of Platform Instance Identity" is fulfilled by the presence of *Instance ID* in the attestation token.

5.2.4 Secure Initialization of Platform

The platform ensures its authenticity and integrity during platform initialization. If the platform authenticity or integrity cannot be ensured, the platform will go to **a state where no other operation except optionally Secure Update of Platform can be performed**.

Conformance rationale:

The platform has an immutable bootloader called NSIB (Nordic Secure Immutable Bootloader) and an upgradable second stage bootloader. All images in the system are verified using a ROTPK (ECDSA using secp256r1) - including the second stage bootloader image(s), the secure image and the non-secure image, as well as a firmware image for the external network core.

The immutable bootloader is located at address zero and it is always executed on every reset in the system. It enables a write lock using the SPU hardware peripheral, ensuring that the bootloader is immutable. The role of the Immutable bootloader is to verify the next firmware image in the boot chain using a ROTPK. The next firmware image is selected using version information stored in the image metadata. NSIB chooses the image from two available slots. When the newest valid image is identified, the slot containing it will be write-protected and the immutable bootloader executes it. If no valid image is found in either slot, then the system will not boot. There is no recovery option in this case.

A version of MCUboot is provided for the second stage bootloader. The MCUboot image will verify a combination of the SPE and the NSPE images (except data storage in non-volatile memory) before booting into TF-M in the SPE image. If no valid firmware is found in the primary slot or in the secondary slot (used for Device Firmware Upgrade), then the system will not boot. Optionally a recovery mechanism using serial UART can be enabled to program a replacement image, relying on signature validation to ensure only valid images are booted.

The system supports multiple ROTPK used to verify FW images. The keys are write-protected but they can be revoked. The different ROTPKs are calculated from unique private keys and placed on the device as a list of available keys. The ROTPK keys can be revoked if a firmware upgrade is transmitted that has a signature generated from a private key with a higher index than the current key-pair in use. In this situation the keys of lower index are revoked and are no longer available for use. The hash and metadata of the ROTPK are stored in the OTP region of UICR [NRF5340] in a format that allows one-time revocation with no option to undo the operation.

The Trusted Firmware-M SPE image will then initialize the NSPE image containing the application and OS.

5.2.5 Attestation of Platform State

The platform provides an attestation of the state of the platform, such that it can be determined that the platform is in a known state.

Conformance rationale:

The platform attests its lifecycle state, boot seed and all platform SW components as a part of the attestation provided by the PSA Initial Attestation Service.

5.2.6 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.

Conformance rationale:

The system supports updating the second stage bootloader as well as a combination of the updateable root of trust and non-secure image.

The immutable Root of Trust is provided by the first stage bootloader, called NSIB. This is a bootloader that has no transport mechanism. It will decide between 2 selectable slots based on signature validation using a ROTPK of images that include version information. This utilizes hardware counters stored in the OTP region of UICR to ensure anti-rollback protection. Once the slot has been selected, it is write-protected and booted into. The other slot is then available to store a candidate version of the second stage bootloader during normal operation of the device. Selection of a valid new second stage image happens after a reset.

The second stage bootloader supports a banking scheme based on receiving and banking the new firmware in a secondary slot, and then activating it by copying it to the primary slot after a reset. The decision to activate a new firmware image is based on signature check using a ROTPK and version information to ensure anti-rollback protection. The candidate for new firmware is a combination of the updatable Root of Trust and the non-secure image, which is signed and versioned as a whole.

5.2.7 Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)

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 platform provides isolation between NSPE and SPE through the TrustZone support of the HW and using the TF-M firmware to enable isolated secure services running in the SPE.

5.2.8 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 second level of isolation is provided by Trusted Firmware-M by using the TrustZone security extensions as well as unprivileged/privileged memory separation between ARoTs and the PRoT. Additionally, the register interface for secure peripherals must be set as privileged, to prevent unprivileged DMA BUS access.

5.2.9 Cryptographic Operation

The platform provides the application with **Operations in Table 5** functionality with **algorithms in Table 5** as specified in **specifications in Table 5** for key lengths **described in Table 5** and modes **described in Table 5**.

Conformance rationale:

Algorithm	Operations	Specification	Key lengths	Modes
AES	Encryption/Decryption Authenticated encryption with additional data	NIST FIPS 197 (AES) NIST SP800-38A (ECB, CBC, CFB, OFB, CTR) NIST SP800-38C (CCM) NIST SP800-38D (GCM)	128, 192, 256	ECB, CTR, CBC CFB*, OFB* CCM GCM
ChaCha20-Poly1305	Authenticated encryption with additional data	RFC7539	256	
RSA	Encryption Decryption Signature generation Signature verification	PKCS#1	1024, 2048, 3072	PSS, OAEP
ECDSA	Signature generation Signature verification	NIST FIPS 186-4 SEC 2		secp192r1 secp224r1 secp256r1 secp512r1 secp192k1 secp224k1 secp256k1
ECDH	Key agreement	NIST SP 800-56A rev. 2		secp192r1 secp224r1 secp256r1 secp512r1 secp192k1 secp224k1 secp256k1
EdDSA	Signature generation Signature verification	Ed25519		Curve25519
x25519	Key agreement	x25519		Curve25519
SHA	Secure hashing Keyed hashing for HMAC	NIST FIPS 180-3		SHA-1* SHA-224 SHA-256 SHA-384* SHA-512*
HMAC	Message authentication	RFC2104		HMAC-SHA1* HMAC-SHA-224 HMAC-SHA-256 HMAC-SHA-384* HMAC-SHA-512*

HKDF	Key derivation	RFC5869 NIST SP800-56C Rev 2		?
AES-CMAC	Message authentication and key derivation	NIST SP800-38B NIST SP800-108r1	128, 192, 256	

Table 5: Cryptographic Operations

(*) Not recommended for use as cryptographic operations

The algorithms are executed on the CryptoCell HW.

5.2.10 Cryptographic Random Number Generation

The platform provides the application with a way based on the CryptoCell RNG peripheral to generate true random numbers to as specified in NIST-800-90B.

Conformance rationale:

This function is exposed through the PSA Crypto APIs implemented on the TF-M firmware. This provides a secure API to the NSPE to generate random numbers from a PRNG seeded by TRNG from CryptoCell 312, which is compliant with specification NIST-800-90A.

5.2.11 Cryptographic Key Generation

The platform provides the application with a way to generate cryptographic keys for use in **cryptographic operations in** Table 6 as specified in **specifications in** Table 6 for key lengths **described in** Table 6.

Conformance rationale:

ID	Algorithm	Specification	Key lengths
RSA	RSA OAEP, RSA PSS, RSA PKCS#1	PKCS#1 v1.5/2.1	1024, 2048, 3072
ECC	ECDH ECDSA	SEC 2 FIPS 186-4 Ed25519 x25519	According to curve type
Symmetric keys	AES, ChaCha-Poly	NIST FIPS 197 NIST SP800-38C NIST SP800-38D ChaCha/Poly1305	AES: 128, 192, 256 ChaCha-Poly: 256

Table 6: Cryptographic Key Generation

5.2.12 Cryptographic KeyStore

The platform provides the application with a way to store cryptographic keys and data at rest such that not even the application can compromise this data. This data can be used for the cryptographic operations listed in chapter 4.2.9 “Cryptographic Operation”.

Conformance rationale:

Key storage is provided by the PSA Internal Trusted Storage service. This provides confidentiality from unprivileged code in SPE as well as from NSPE.

The Hardware Unique Key(s)(HUK) is stored in the KMU and it can only be accessed and used by the Arm CryptoCell hardware accelerator.

The initial attestation key is stored in encrypted form inside the KMU and can be decrypted by a HUK stored in the KMU.

The hash of the root of trust public keys are stored in the secure only OTP peripheral.

5.3 Optional Security Functional Requirements

5.3.1 Secure Debugging

The platform only provides *non-secure Application Core* authenticated as specified in *Debug and trace section of [NRF5340]* with debug functionality. The platform ensures that all data stored by the application, with the exception of *none* is made unavailable.

Conformance rationale:

User can disable the debug access to the secure mode of the Application core by enabling Application core UICR.SECURE-APPROTECT.

5.3.2 Secure Encrypted Storage (internal storage)

The platform ensures that all data stored by the application, except for *none*, is encrypted as specified in [PSASTORAGE] with a platform instance unique key of key length 128 bits.

Conformance rationale:

Secure Encrypted Storage is provided by the PSA Protected Storage service [PSASTORAGE], which provides functionality to store generic data in non-volatile memory inside the SPE. This is used for generic data-at-rest storage and certificate storage.

The PSA PS uses a 128 bit key derived from a Hardware Unique Key (HUK) stored in the KMU peripheral to encrypt and authenticate the data using an AEAD algorithm executed by Arm CryptoCell hardware accelerator. This provides authenticity and integrity. The use of a HUK Key ensures that the encrypted storage is bound to a unique instance of the platform.

The secure service is exposed to the NSPE and any ARoT service and it provides authenticity and integrity for the stored data.

Additional confidentiality (at-rest and in-use) is provided for items stored by any ARoT service based on a partition identifier ensuring limited access. In this case only the specific ARoT services will have access to decrypt and use their data.

5.3.3 Secure Storage (internal storage)

The platform ensures that all data stored by the application is protected to ensure its authenticity and integrity as specified in [PSASTORAGE] with a platform instance unique key of key length of 128 bits.

Conformance rationale:

Secure Storage is provided by the PSA Internal Trusted Storage service [PSASTORAGE], which provides functionality to store generic data and key material in secure non-volatile memory inside the SPE.

PSA Internal Trusted Storage is exposed as a secure storage service through PSA Crypto. The PSA Crypto service provides mechanisms to import or generate new key material from NSPE or any ARoT service, but it provides confidentiality and access control by disallowing keys to be exported back to the NSPE or any ARoT service. In this case the keys can only be used for cryptographic algorithms, by a key reference.

Symmetric and private keys cannot be exported once it is imported. Public key material calculated from private keys can be exported using standardized APIs in the PSA Crypto service.

Access control for stored data is provided by using a partition identifier.

PSA Protected Storage implementation inside the SPE uses PSA Internal Trusted Storage for physical storage.

5.4 Additional Security Functional Requirements

5.4.1 Residual Information Purging

The platform ensures that *all non-volatile memory including UICR registers*, with the exception of *none*, is erased using the method specified in *7.21.8.4 ERASEALL of [NRF5340]* before the memory is used by the platform or application again and before an attacker can access it.

Conformance rationale:

Setting the ERASEALL register to 1 erase all non-volatile memory including UICR registers. This would prevent an attacker to access any remaining data.

6 Mapping and Sufficiency Rationales

6.1 Assurance

The assurance activities defined in [PSA-EM-L2] fulfil the SESIP2 activities. In particular, the required source code review, vulnerability analysis and testing to an equivalent of 25 person-days of the [PSA-EM-L2] is applicable.

Assurance Class	Assurance Family	Covered by
ASE: Security Target evaluation	ASE_INT.1 ST Introduction	Section “Introduction” and title page of the Security Target
	Rationale: ST reference, Platform Reference, and Platform Functional Overview and Description of this document fulfills ASE_INT.1.	
	ASE_OBJ.1 Security requirements for the operational environment	Section “Security Objectives for the Operational Environment” of the Security Target
	Rationale: Guidance is available to cover objectives for the operational environment.	
	ASE_REQ.3 Listed Security requirements	Section “Security Requirements and Implementation” of the Security Target
	Rationale: SFRs are only taken from [SESIP]. Both mandatory “Verification of Platform Identity” and “Secure Update of Platform” are included.	
	ASE_TSS.1 TOE Summary Specification	Section “Security Requirements and Implementation” of the Security Target
	Rationale: SFRs are listed individually. SFRs are grouped according to the PP.	
ADV: Development	ADV_FSP.4 Complete functional specification	Documentation in [NCS], [NRF5340], [TFM], [MCUBOOT]
	Rationale: TSFIs are industry standard and completely defined in the guidance documents.	
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	Documentation in [NCS], [NRF5340], [TFM], [MCUBOOT]
	Rationale: The guidance documents explained how to operate the TOE securely.	
	AGD_PRE.1 Preparative procedures	Documentation in [NCS], [NRF5340], [TFM], [MCUBOOT]
	Rationale: The guidance documents explained how to prepare the TOE securely.	

Assurance Class	Assurance Family	Covered by
ALC: Life-cycle support	ALC_FLR.2 Flaw reporting procedures	ALC_FLR section in the Security Target
	Rationale: The flaw reporting and remediation process is described in this document.	
ATE: Tests	ATE_IND.1 Independent testing: conformance	Testing carried out by the laboratory
	Rationale: The laboratory shall perform independent test.	
AVA: Vulnerability Assessment	AVA_VAN.2 Vulnerability analysis	Vulnerability and testing carried out by the laboratory
	Rationale: The laboratory shall perform vulnerability analysis and penetration test.	

Table 7: Assurance Mapping and Sufficiency Rationales

6.2 Functionality

PSA Security Function	Covered by SESIP SFR	Rationale
F.INITIALIZATION	Secure Initialization of Platform	Full coverage by NSIB (Nordic Secure Immutable Bootloader) as well as bootloader based on MCUBoot.
F.SOFTWARE_ ISOLATION	Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)	Full coverage by TrustZone from Cortex-M33 processor
	Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services)	Full coverage by using unprivileged/privileged memory separation between ARoTs and the PRoT
F.SECURE_ STORAGE	Secure Storage (internal storage)	TF-M Protected Storage (PS) service implements the secure storage and are accessible by PSA Protected Storage APIs.
	Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)	Stored data is isolated from the NSPE and Application Root of Trust Services by using a unique HUK for each platform.
F.FIRMWARE_ UPDATE	Secure Update of Platform	Full coverage by NSIB (Nordic Secure Immutable Bootloader) as well as bootloader based on MCUBoot.

PSA Security Function	Covered by SESIP SFR	Rationale
F.SECURE_STATE	Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)	Full coverage
	Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services)	Full coverage
	Partially covered by the SFR “Secure initialization of platform” and “Secure update of platform”.	Full coverage
F.CRYPTO	Cryptographic Operation	Full coverage by TF-M accessible through PSA Crypto API.
	Cryptographic KeyStore	Full coverage by TF-M accessible through PSA Crypto API.
	Cryptographic Random Number	Full coverage by TF-M accessible through PSA Crypto API.
	Cryptographic Key Generation	Full coverage by TF-M accessible through PSA Crypto API.
F.ATTESTATION	Verification of Platform Identity	The HW can be identified by the marking. The SW can be identified by the git tag. This information is also available in the attestation token.
	Verification of Platform Instance Identity	This information is available in the attestation token.
	Attestation of Platform Genuineness	“Verification of Platform Instance” and “Verification of Platform Instance Identity” are included in the attestation token.
	Attestation of Platform State	This information is available in the attestation token.
F.AUDIT	Audit Log Generation and Storage	Since the TOE is a resource constrained device, this optional requirement is not implemented.
F.DEBUG	Secure Debugging	Debug port can be locked with UICR.SECUREAPPROTECT.

Table 8 Functionality Mapping and Sufficiency Rationales