Security Target for SAM L11-KPH with Kinibi-M v1.0

Version *1.2*, dated 2021-12-21

Microchip Technologies
Trustonic

Based on [SESIP] methodology, version “Public Release v1.1”

1 Version history

Version	Date	Description	Author
1.0	05 November 2021	First release	Brightsight B.V.
1.1	18 November 2021	Fixes after EM1	Brightsight B.V.
1.2	21 December 2021	Configuration clarifications	Brightsight B.V.

2 Introduction

The Security Target describes the Platform (in this chapter) and the exact security properties of the Platform that are evaluated against [SESIP] (in chapter “Security requirements and implementation”) 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”).

2.1 ST reference

See title page.

2.2 Platform reference

	Value	**Verification method described in**
Commercial name	*SAM L11-KPH with Kinibi-M v1.0*	*Product Identification System [DS]* *Section 16.11 [DS]*
HW reference	*ATSAML11D14A-MUT KPH*	
HW version	*DSU.DID=0x20830100*	
TEE reference	*Kinibi-M /SAM L11-KPH*	*Section 3.1 [KDEV-DG]*
TEE version	*1.0*	
Platform Type	*Microcontroller Unit (MCU) with a Trusted Execution Environment (TEE)*	

Table 1 Platform identification

2.3 Included guidance documents

The documents listed in section 6.1 are included with the platform.

2.4 Platform functional overview and description

With the increasing growth of Internet of Things (IoT) end points and, consequently, the increased frequency of security breaches, designers are looking for MCUs that can help reduce power consumption while adding robust security. The SAM L11 family of MCUs takes an innovative approach to solving these challenges by integrating a wide variety of peripherals, including security features, into the industry's lowest-power MCUs in their class. This allows you to develop secured applications without the battery constraints of less power-efficient MCUs. These MCUs run at 32 MHz with memory configuration of up to 64 KB Flash and 16 KB SRAM. They come in two variant options, SAM L11 and SAM L11-KPH, and boast ultra-low power consumption as well as an enhanced Peripheral Touch Controller and advanced analog features. Both variants come in 24- and 32-pin package options and are targeted for use in IoT and security, low-power, capacitive touch and general-purpose embedded control applications.

The SAM L11 and SAM L11-KPH add integrated hardware security with respect to other families. The SAM L11-KPH adds a factory-provisioned root of trust key to provide the MCU with a secure identity that can be used for developing secure IoT applications. Therefore,

SAM L11-KPH is SAM L11 hardware personalized and preloaded with Kinibi-M and Trustonic Key.

The Platform consists of an MCU with a TEE. The Platform is intended to be used by an integrator that deploys it into an IoT solution together with its own user application, providing assurance that the IoT application is securely booted and operates securely, safeguarding the Secure World.

The main security features of the Platform are:

- *Secure boot by means of Boot ROM*
    - *Integrity checks at all boot stages*
    - *Security Management*
    - *Interface for the Host Debugger*
- *Isolation at different levels*
    - *Software: Isolated Secure Modules*
    - *Data: Secure File System*
    - *Hardware: Trustzone to separate Secure and Non Secure regions.*
    - *Peripherals Ownership using the Peripheral Access Controller (PAC)*
- *Hardware security mechanisms*
    - Data Scrambling in Data Flash and TrustRAM.
    - TrustRAM with Active shield protection to resist microprobing attacks
    - Tamper Detection on IO pins and TrustRAM shield
    - Secure Data Flash on the 2kB EEPROM portion of the flash
    - Secure pin multiplexing
- Parameters checks
    - Non-secure to Secure
    - Secure to Secure
- Cryptographic Operation by means of the Crypto accelerator and available through CRYA APIs
    - AES encryption and decryption
    - SHA-256
    - GCM using AES engine
- True Random Number Generator (TRNG)
- Key Storage

The Platform scope is depicted in Figure 1 . The blue parts surrounded by the red dotted line are within the evaluation scope and the gray parts are outside of the evaluated scope. The out of scope part comprises the custom security modules in the SPE and any components in the NSPE.

The physical scope includes a silicon chip SAM L11-KPH and the accompanying TEE (Kinibi-M) developed by Trustonic and its accompanying key adapted for SAM L11-KPH. Therefore, SAM L11-KPH is SAM L11 hardware personalized and preloaded with Kinibi-M and Trustonic Key. Trustonic's Kinibi-M is distributed as an SDK through its website. Once the user provides basic info, a downloadable package is provided which contains developer SDK, production SDK and the cloud enrolment demo. The website also provides basic info about the different SDK contents and has an FAQ section that answers all relevant questions.

The logical scope includes the modules displayed in Figure 1, more specifically:

- *Updatable Platform Root of Trust using the EC25519 Signature validator of the Updater module in the TEE (Kinibi-M) executed in Secure RAM and utilizes the AES crypto block as well.*
- *Main Bootloader, which is executed right after the Boot ROM to initiate the TEE*
- *SPE Partition Management using Trustzone that provides MPU based isolation and secure cross-module communications enforced by the TEE kernel*
- *Immutable Platform Root of Trust*
- *BootROM using the SAM L11-KPH hardware Boot ROM*
- *Isolation Hardware using ARM's Trustzone*
- *Security Lifecycle Management enabled by TEE*
- *Trusted Subsystems(s) using TEE*

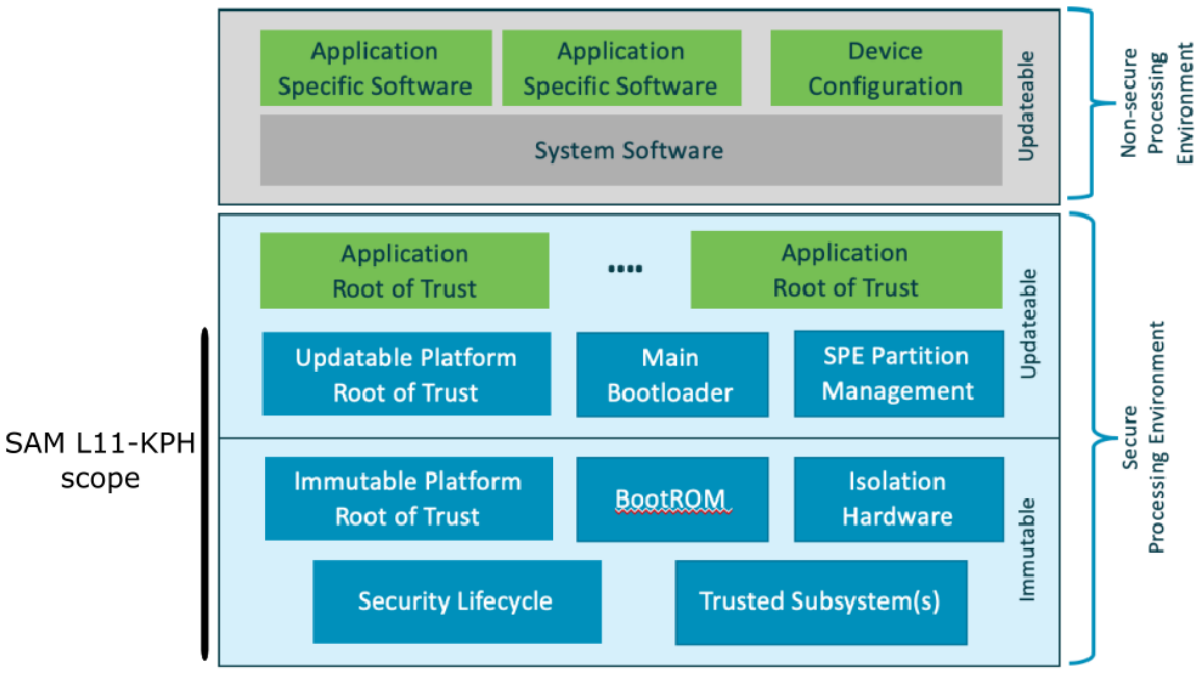


Figure 1 Platform scope PSA view

Also Figure 2 presents the platform scope marked with the dotted line with the design components that implement the security functionality:

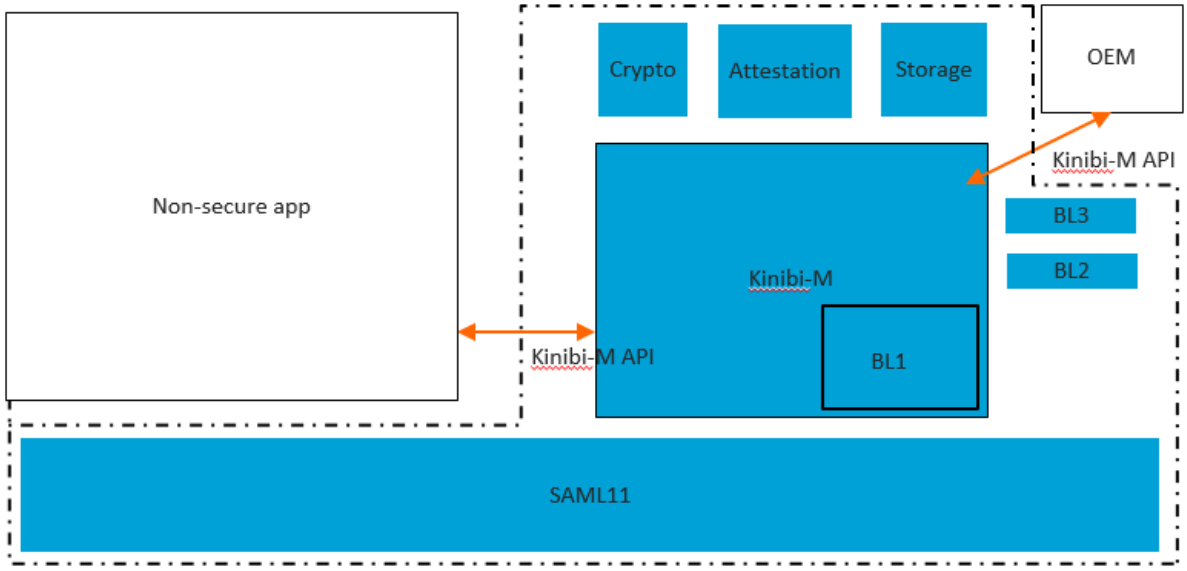


Figure 2 Design view of the platform scope

Kinibi-M / SAM L11-KPH lifecycle:

- Preparation phase in SIP factory: Kinibi-M image (composed of Kinibi-M bootloader, kernel and system modules) is written to device Secure Flash memory. Additionally, a device unique key and a device receipt are injected by Trustonic KPH in device Secure Data Flash. Device receipt is signed into the Trustonic PKI and can later be used by modules to attest this device.
- Development phase by OEMs: New modules can be developed using Kinibi-M SDK and then added to the device modules list. To ensure a secure update of these modules, a public key is also injected in factory in Kinibi-M KeyStore. This public key will be used later to verify modules update signature.
- End-usage phase: Device is shipped to end customers with Kinibi-M and its modules in Secure Flash, and a Non-Secure operating system. The Non-Secure OS can call Secure modules through a single API.

Kinibi-M / SAM L11-KPH platform scope:

Kinibi-M components	
BL1	1st bootloader started by the MCU BootRom. Starts BL2 if platform in update mode. (Updatable Bootloader)
BL2	Updater bootloader. Started by BL1, starts BL3. (Updatable Bootloader)
BL3	Updater module. Started by BL2. Process Trusted OS and Trusted Modules update commands. (Updatable Bootloader)

Kernel and System Modules	Handles Secure Partition Management; Internal Trusted Storage, Binding, Cryptographic Service and Initial Attestation Service as defined in PSA Security Model. (Updatable Platform Root Of Trust / SPE)

3 Security Objectives for the operational environment

3.1 Platform Objectives for the Operational Environment

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

- The operating system or application code in the NSPE are expected to verify the correct version of all platform components it depends on, as described in 16.11 [DS] and [KPSA] detailed steps can be found in [AGD_SESIP].
- The operating system or application code are expected to lock the debug functionality as described in 2.2 [SRG] detailed steps can be found in [AGD_SESIP].

Other objectives for the environment shall be considered according to [PSA L2 Profile]:

- Cryptographic keys and certificates outside of the TOE are subject to secure key management procedures, as described in [AGD_SESIP]
- Actors in charge of TOE management, for instance for signature of firmware update, are trusted, as described in 1.1 [KREF-MAN] and [AGD_SESIP].
- The integrity and uniqueness of the unique identification of the platform is provided by the SAM-L11-KPH hardware serial number in [DS] section 10.3 Serial Number.

4 Security requirements and implementation

4.1 Security Assurance Requirements

The claimed assurance requirements package is: **SESIP2** as defined in [SESIP] section 4.2.

4.1.1 Flaw Reporting Procedure (ALC_FLR.2)

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

Microchip has created a website that can be used for vulnerability reporting.
Microchip Vulnerability Reporting Website

Never say never when it comes to security. While implementing good security practices contributes significantly to the protection of information, credentials, intellectual property or assets, there is no perfect solution to make a system or product impossible to attack. Since the security of our products is of critical importance to us and our customers, we take any reports of potential security vulnerabilities seriously.

The Microchip Product Security Incident Response Team (PSIRT) is responsible for receiving and responding to reports of potential security vulnerabilities in our products, as well as in any related hardware, software, firmware, and tools. Once a report is received, the PSIRT will take the necessary steps to review the issue and determine what actions might be required to address any potential impacts to our products.

Once a vulnerability is reported, the PSIRT team uses a process called CVDP (Coordinated Vulnerability Disclosure Process) to connect security experts and stakeholders to provide a quick/efficient response.

Even though Kinibi-M is offered by Trustonic, it is still considered as a firmware/software that works on SAM L11-KPH.

Any vulnerability found on Kinibi-M will first be reported to Microchip and we have an internal contractual agreement to first triage the concern and then work with Trustonic directly if the issue is identified to be bug in Kinibi-M code.

The website is provided to report vulnerability. If there are security concerns identified, then a document will be created along with a public communication option that will provide a work around or a solution to the issue.

Regarding ALC_FLR.2, Kinibi-M SAM L11 provides an update mechanism. Through the UART channel, TEE OS image and Trusted Services can be updated through a dedicated update module. Update module integrity is enforced through a SHA256 hash embedded in the TEE OS bootchain. Any update for TEE OS image or any Trusted Modules is validated through a ED25519 signature.

The update mechanism DOES NOT verify prior to installation that the version of the update is higher (more recent) than the current version installed.

4.2 Security Functional Requirements

The platform fulfills the following security functional requirements:

4.2.1 PSA Level 2 Security Functional Requirements

4.2.1.1 Verification of Platform Identity

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

Conformance rationale:

HW reference value accessible by reading a reqister named DID. This register and its bitfields are described in the datasheet, see details in section 16.11 [DS].

0x18	DID	7:0	DEVSEL[7:0]		
		15:8	DIE[3:0]		REVISION[3:0]
		23:16	FAMILY[0]	SERIES[5:0]	
		31:24	PROCESSOR[3:0]		FAMILY[4:1]

HW reference value to read is the following: DSU.DID=0x20830100

The TEE OS provides a unique version identifier which can be retrieved dynamically through a system command. See [KPSA].

4.2.1.2 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:

SUID can be retrieved dynamically through a system command. See section 3.4.1.1 TEE_CMD_GET_SUID [KDEV-API].

4.2.1.3 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 cannot be cloned or changed without detection.

Conformance rationale:

During manufacturing, SAM L11-KPH devices are provisioned with a unique key generated by a Factory KPH based on the device SUID. A provisioning receipt is also stored on the device to attest its genuineness later on the field. This receipt is signed using a Factory KPH private key. Kinibi-M provides an API to generate attested messages. These messages are signed

using the device key. The receipt is attached to the signature for validation. See section 2.3.6 KM_ATTEST [KREF-MAN].

4.2.1.4 Secure Initialization of Platform

The platform ensures its authenticity and integrity during the platform initialization. If the platform authenticity or integrity cannot be ensured, the platform will go to:

- ***Bootloader mode***
- ***Halt mode***

Conformance rationale:

A Secure Boot with SHA-256-based authentication on a configurable portion on the Flash (BS memory area) is available with verification mechanisms allowing to reset and restart the authentication process in case of a failure. See section 14 [DS] for details.

Kinibi-M OS and its services are started through a Secure Initialization process. Each code section integrity is verified through SHA256 hashes. TEE OS and services code sections cannot be modified except during an update process (see below).

If the Kinibi-M OS integrity check fails in BL1, platform enters bootloader mode and waits for a proper BL2 image to continue.

If a Trusted Module integrity check fails in Kinibi-M kernel, the platform halts (print HALT on serial and goes into infinite loop).

Host debugger is detailed in the following sections of the datasheet: [DS Section 14]:
- 14.2 Block Diagram
- 14.4.5 Boot ROM Interactive Mode

~~4.2.1.5 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.~~

4.2.1.6 Cryptographic Operation

The platform provides the application with **cryptographic operations specified in Table 2** functionality with **algorithms specified in Table 2** as specified in **specifications and standards in Table 2** for key lengths **specified in Table 2** and modes **specified in Table 2**.

Algorithms	Cryptographic operations	Specification / Standard	Key size(s)	Mode(s)
AES	Authenticated Encryption & Decryption GF(2128) multiplication for AES-GCM hash	FIPS 197 NIST 800-38D	128 bits	GCM combining CTR with and authentication hash function
SHA	Secure hash	FIPS PUB180-4	256 bits	SHA-256

Table 2 Cryptographic operation iterations

Conformance rationale:

All applications that need access to crypto operations (including Kinibi-M) will call the CRYA Api's described in section 13.3 of the datasheet.

Kinibi-M SAM L11 provides Crypto API for Trusted Modules so as to use crypto mechanism listed in the table above.

4.2.1.7 Cryptographic Random Number Generation

The platform provides the application with a way based on ***the timing jitter in the signals produced by two oscillators*** to generate random numbers to as specified in ***NIST Special Publication 800-22 and Random Test Suites***.

Conformance rationale:

Random Number Generartion is done by the TRNG block. (Section 39 of [DS])

Kinibi-M SAM L11 provides Crypto API for Trusted Modules so as to platform Random Number Generator.

4.2.1.8 Secure Storage (internal storage)

The platform ensures that all data stored by the application, except for ***that outside the secure portion of the Data Flash or TRAM***, is protected to ensure its authenticity and integrity as specified in ***Figure 3*** with a platform instance unique key of ***30-bit key length defined by the user***.

Conformance rationale:

Kinibi-M SAM L11 provides a Secure Filesystem API for Trusted Modules to store their data and keys protected. Secure Flash is used for this purpose and can only be accessed by the Secure Filesystem module. Kinibi-M Secure Filesystem module ensures data isolation per module and enforces their authenticity and integrity.

SAM-L11 secure flash and TRAM controller scrambles data read/write operation.

Trusted Data Storage in Data flashVM (1 Data ROW) features:

- *Optimized for secure key storage*
- *Scrambled and masked access with user-defined keys*
- *Silent Access allows reduced side-channel signature*
- *Rapid Tamper Erase if tamper attempt detected*

TrustRam : 256-byte of secure RAM intended for volatile secret data storage.

- *Address scrambling to the RAM*
- *Data scrambling to/from the RAM*
- *Silent data access for side-channel protection*
- *Data remanence prevention (Data "burn-in" effects during long storage)*
- *Active shielding with physical tamper detection on RAM*

- *Automatic Full erase of scramble key and RAM content on external/internal tamper detection*

See section 30.6 [DS] for details.

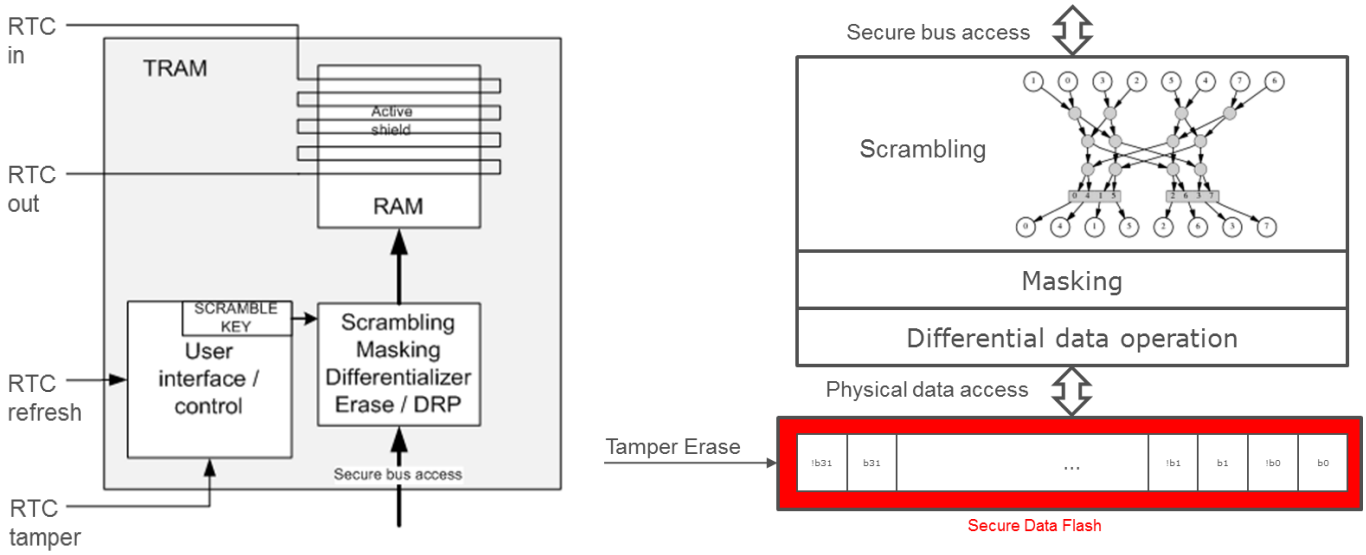


Figure 3 Data Scrambling mechanism

4.2.2 Extra attacker resistance Security Functional Requirements

The extra attacker resistance SFRs are presented in a separate section to aid the ST reader detect the targeted attacker resistance and how the secure functionality presented in section 4.2.1 are protected.

4.2.2.1 Limited Physical Attacker Resistance

The platform detects or prevents attacks by an attacker with physical access before the attacker compromises ***the following SFRs:***

- ***Secure Storage (internal storage)***

Conformance rationale:

The TOE has very limited protection against physical attacks. Scope of protection is on some memory blocks (Trust RAM and Data Flash) that can be programmed to erase on external tamper. Upon tamper, a non-maskable interrupt is generated that erases flash and locks content.

Therefore, the only relevant SFR that the platform can protect is Secure Storage. Refer to SAM L11 Data sheet [DS] sections 10.1.2 and 31.6.2.6 for further details.

4.2.2.2 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:

Arm TrustZone for Cortex-M technology is a core extension, which enables the system and the software to be partitioned into Secure and Non-Secure domains.

Secure software can access both Secure and Non-Secure memories and resources, while Non-Secure software can only access Non-Secure memories and resources.

Kinibi-M benefits from SAM L11-KPH Trustzone by isolating the Kinibi-M core and its secure modules from the NSPE, as seen in Figure 4.

Refer to section 13.2 [DS] for details.

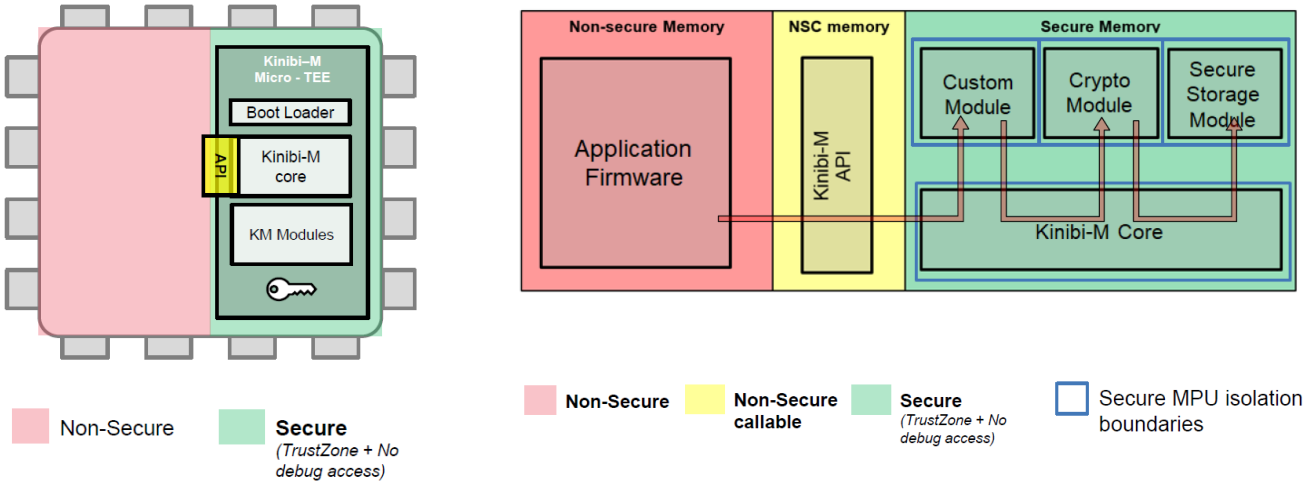


Figure 4 Isolation scenarios of Kinibi-M using Trustzone

4.2.2.3 Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application RoT 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.

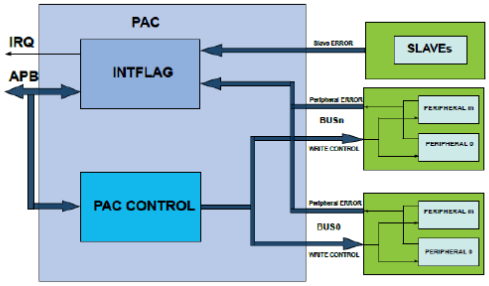
Conformance rationale:

Kinibi-M enforces the isolation between the TEE OS and third party modules through runtime memory isolation (enforced by MPU) and a restricted set of system calls. This isolation is also enforced at the data storage level by the Secure Filesystem module.

SAM L11-KPH also has a peripheral access controller which allows for hybrid programming of certain peripherals. (Secure, Non-Secure or Security-Aware). Whenever there is an illegal access of peripherals an interrupt is generated.

PAC - Peripheral Access Controller

- Manages peripheral write access protection and security attribution.
  - Security attribution is configured in flash UROW then loaded and locked by the BootROM prior to flash code execution .



Name: NONSECA
Offset: 0x54
Reset: 0x000000
Property: –

Bit	31	30	29	28	27	26	25	24
Access								
Reset								

Bit	23	22	21	20	19	18	17	16
Access								
Reset								

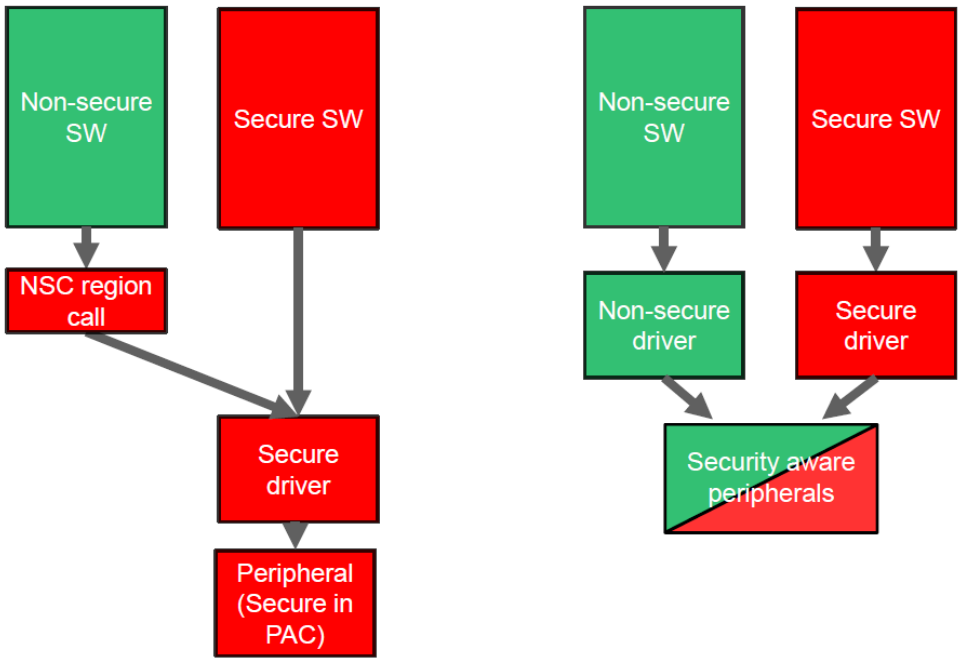
Bit	15	14	13	12	11	10	9	8
			AC	PORT	FREQM	EIC	RTC	WDT
Access			R	R	R	R	R	R
Reset			0	0	0	0	0	0

Bit	7	6	5	4	3	2	1	0
	GCLK	SUPC	OSC32KCTRL	OSCCTRL	RSTC	MCLK	PM	PAC
Access	R	R	R	R	R	R	R	R
Reset	0	0	0	0	0	0	0	0

- PAC Generates an interrupt in case of a peripheral access violation.

Mix-Secure peripherals (1/2)

- L11 integrates two types of integrated peripherals



- Security aware peripherals have specific secure feature , that can only be accessed by secure bus access.

- List of L11 Security aware peripherals:
  - **PORT**
    - Individual I/Os can be reserved for secure mode
  - **EIC**
    - Individual ExtInts can be reserved for secure mode
    - ExtInt[3:0] have individual irqs, and are well suited for secure use
  - **EVSYS**
    - Individual channels can be reserved for secure mode
    - Channel[3:0] have individual irqs, and are well suited for secure use
  - **NVMCTRL**
  - **DSU**

4.2.2.4 Software Attacker Resistance: Isolation of Application Parts (between each of the Application Root of Trust Services

The platform provides isolation between parts of the application, such that an attacker able to run code as one of the **Secure Partitions in the Application Root of Trust** cannot compromise the integrity and confidentiality of the other application parts.

Conformance rationale:

Kinibi-M enforces the isolation between the third party modules through runtime memory isolation (enforced by MPU) and a restricted set of system calls. This isolation is also enforced at the data storage level by the Secure Filesystem module.

SAM L11-KPH also has a peripheral access controller which allows for hybrid programming of certain peripherals. (Secure, Non-Secure or Security-Aware). Whenever there is an illegal access of peripherals an interrupt is generated.

5 Mapping and sufficiency rationales

5.1 SESIP2 sufficiency

Assurance Class	Assurance Families	Covered by	Rationale
ASE: Security Target evaluation	ASE_INT.1 ST Introduction	Section "Introduction" and "Title"	The ST reference is in the Title, the Platform reference in the "Platform reference", the Platform overview and description in "Platform functional overview and description".
	ASE_OBJ.1 Security requirements for the operational environment	Section "Security Objectives for the operational environment"	The objectives for the operational environment in "Security Objectives for the operational environment" refers to the guidance documents.
	ASE_REQ.3 Listed Security requirements	Section "Security requirements and implementation"	All SFRs in this ST are taken from [SESIP]. "Verification of Platform Identity" is included. "~~Secure Update of Platform~~" is not included due to the platform not having anti-rollback.
	ASE_TSS.1 Platform Summary Specification	Section "Security requirements and implementation"	All SFRs are listed per definition, and for each SFR the implementation and verification is defined in "Security requirements and implementation".
ADV: Development	ADV_FSP.4 Complete functional specification	Functional specification conformed of the Functional	The evaluator will validate suitability of the provided evidence.

		specification and guidance documents listed in 6.1.	
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	D*ocuments listed in section "Included guidance documents"*	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
	AGD_PRE.1 Preparative procedures	Documents *listed in section "Included guidance documents"*	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
ALC: Life-cycle support	ALC_FLR.2 Flaw reporting procedures	Section "Flaw Reporting Procedure (ALC_FLR.2)"	The flaw reporting and remediation procedure is described.
ATE: Tests	ATE_IND.1 Independent testing: conformance	N/A	The evaluator will perform independent testing.
AVA_VAN.2	AVA_VAN.2 Vulnerability analysis	N/A	The evaluator will perform penetration testing.

5.2 PSA completeness

This section intends to demonstrate which of the secure functions specified in chapter 5 of [PSA L2 PP] are covered by the platform described in this document. Those SFRs in scope of this platform are marked in **bold text**.

Note that the mapping of PSA functions to SESIP has been discussed in section 5.2 of [PSA L2 Profile]. Those optional requirements not met by the platform are marked in gray text.

PSA Secure functions	SESIP SFR	Rationale
F.INITIALIZATION	**Secure Initialization of Platform**	Full coverage, see 4.2.1.4
F.SOFTWARE_ISOLATION	**Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)**	Full coverage, see 4.2.2.2
	Software Attacker	Full coverage,

	Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services)	see 4.2.2.3
	Software Attacker Resistance: Isolation of Application Parts (between each of the Application Root of Trust services)	Full coverage, see 4.2.2.4
F.SECURE_STORAGE	Secure Encrypted Storage (internal storage)	not provided by the TOE
	Secure Storage (internal storage)	Full coverage, see 4.2.1.8
	Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)	Full coverage, see 4.2.2.2
	Secure External Storage	not provided by the TOE
F.FIRMWARE_UPDATE	Secure Update of Platform	Partial coverage: *Kinibi-M SAM L11 provides an update mechanism. Through the UART channel, TEE OS image and Trusted Services can be updated through a dedicated update module. Update module integrity is enforced through a SHA256 hash embedded in the TEE OS bootchain. Any update for TEE OS image or any Trusted Modules is validated through a ED25519 signature.* *The update mechanism DOES NOT verify prior to installation that the version of the update is higher (more recent) than the current version installed.*
F.SECURE_STATE	**Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)**	Full coverage, see 4.2.2.2
	Software Attacker	Full coverage, see 4.2.2.3

	Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services)	
	Partially covered by the SFR "Secure initialization of platform".	Full coverage, see 4.2.1.4 and 4.2.1.5
F.CRYPTO	**Cryptographic Operation**	Full coverage through CRYA API, see 4.2.1.6
	Cryptographic Keystore	not provided by the TOE
	Cryptographic Random Number Generation	The evaluation of the random number generator follows a recognized methodology.
	Cryptographic Key Generation	not provided by the TOE
F.ATTESTATION	**Verification of Platform Identity**	Unique identification of platform, see 4.2.1.1
	Verification of Platform instance Identity	Unique identification of the platform instance
	Attestation of Platform Genuineness	"Verification of Platform Instance" and "Verification of Platform Instance Identity" are included in the attestation token.
	Attestation of Platform State	not provided by the TOE
F.AUDIT	Audit Log Generation and Storage	not provided by the TOE
F.DEBUG	Secure Debugging	not provided by the TOE

6 References

6.1 Evidence required by the SARs including guidance

[DS]	Datasheet - Ultra Low-Power, 32-bit Cortex-M23 MCUs with TrustZone, Crypto, and Enhanced PTC Datasheet, rev. F, 06/2020
[AN2699]	UART Bootloader for SAM L10/SAM L11, rev. B 2019
[SRG]	SAM L11 Security Reference Guide, rev. B, April 2019
[FSP]	FSP mapping, v.1.1
[KDEV-GS]	Getting Started with Trustonic Kinibi-M SDK, v 1.1 December 6th 2018
	[KDEV-DG] Kinibi-M Developer's Guide, v1.1, February 13 2019
[KDEV-API]	Kinibi-M API Documentation, v1.0, August 30th 2018
[KPRO-GS]	Getting Started with Trustonic Kinibi-M Production SDK, v1.0 February 20 2019
[KPSA]	Kinibi-M PSA User Guidance, v1.0, June 8th 2020
[AGD_SESIP]	Security Guidance v1.1
[KREF-MAN]	Kinibi-M reference manual

6.2 SESIP documentation

[PSA L2 PP]	PSA Certified™ Lightweight Protection Profile, Document reference JSADEN0002, Version 1.1, 18/02/2020
[PSA L2 Profile]	SESIP Profile for PSA Certified Level 2, Document reference JSADEN012, Version 1.0 (BET02): ARM PSA L1 (Chip), version 1.0, 10/02/2021
[SESIP]	GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.1, June 2021

6.3 Terms and definitions

DAL	Debug Access Level
IoT	Internet of Things
MCU	MicroController Unit
NVM	Non-Volatile Memory
NSPE	Non-Secure Processing Environment
PAC	Peripheral Access Controller
RAM	Random Access Memory
ROM	Read Only Memory
SESIP	Security Evaluation Standard for IoT Platforms
SPE	Secure Processing Environment
TEE	Trusted Execution Environment
TRAM	Trusted RAM