KW45 / K32W148 / MCX W71 Product Family

SESIP Security Target

Rev. 1.6 — 25 March 2024 **Evaluation document**

Document information

Information	Content
Keywords	SESIP, PSA, Security Target, KW45 / K32W148 / MCX W71
Abstract	Security target for evaluation of the KW45 / K32W148 / MCX W71 developed and provided by NXP Semiconductors, according to SESIP Assurance Level 2 (SESIP2) based on SESIP methodology, version 1.2, and PSA Certified Level 2, NIST 8425, RED

Revision History

Rev.	Date	Description
0.1	21 April 2023	Initial release
0.2	5 June 2023	Update after first review
0.3	13 June 2023	Add more details for Secure Boot and Secure Update SFRs
0.4	1 August 2023	Add compliance to EU Radio Equipment Directive (RED) Article 3
1.0	10 October 2023	First released version
1.1	16 November 2023	Miscellaneous editorial fixes
1.2	15 December 2023	Fix incorrect reference for hardware components and interfaces
1.3	10 January 2024	Add clarification for Secure Update of Platform SFR
1.4	19 February 2024	Revise conformance rationale for Decommission of Platform SFR Miscellaneous editorial fixes
1.5	1 March 2024	Add NIST 8425 conformance claim
1.6	25 March 2024	Add MCX W71 variant to the scope Rework RED and NIST 8425 mappings Miscellaneous editorial fixes

1 Introduction

This Security Target describes the KW45 / K32W148 / MCX W71 platform and the exact security properties of the platform that are evaluated against GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2, SESIP Assurance Level 2 (SESIP2) [7].

1.1 ST Reference

KW45 / K32W148 / MCX W71, SESIP Security Target, Revision 1.6, NXP Semiconductors, 25 March 2024.

1.2 SESIP Profile Reference and Conformance Claims

Table 1. SESIP Profile for Secure MCUs and MPUs Conformance Claims

Reference	Value
SP Name	GlobalPlatform Technology SESIP Profile for Secure MCUs and MPUs [8]
SP Version	Version 1.0
Assurance Claim	SESIP Assurance Level 2 (SESIP2)
Package Claim	Base SP, Package Security Services, Package Software Isolation

Table 2. SESIP Profile for PSA Certified Level 2 Conformance Claims

Reference	Value
SP Name	SESIP Profile for PSA Certified Level 2 [9]
SP Version	V1.0 REL 02
Assurance Claim	SESIP Assurance Level 2 (SESIP2)
Optional and Additional SFRs	See Section 4.3

1.3 Other Conformance Claims

1.3.1 RED Conformance Claim

KW45 / K32W148 / MCX W71 is compliant to the requirements from DIRECTIVE 2014/53/EU, Article 3 for radio equipments [28]. In particular, the following requirements are fulfilled by KW45 / K32W148 / MCX W71:

- Requirement 3.3 (d): radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;
- Requirement 3.3 (e): radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;
- Requirement 3.3 (f): radio equipment supports certain features ensuring protection from fraud;

1.3.2 NIST 8425 Conformance Claim

KW45 / K32W148 / MCX W71 fulfills the requirements from NIST 8425 [29] for IoT products. Please note that, the platform is not strictly in the scope of NIST 8425 because it is not an end product. Rather, the platform should be programmed with an OEM firmware and integrated with a host device to become an end product. Nevertheless, it is claimed that the platform meets all the requirements mandated by NIST 8425 and this shall directly contribute to the end product being fully compliant to NIST 8452.

1.4 Platform Reference

KW45 / K32W148 / MCX W71 consists of three product variants, namely:

- ***KW45***
- ***K32W148***
- ***MCX W71***

The three product variants are aimed at different markets. The MCX W71 variant is a derivative of the K32W148 variant and they are identical in terms of physical properties except their namings. For the two variants KW45 and K32W148, they only differ in terms of external markings and for some configurations, package types and number of pins. Please refer to [12] and [14] for further details. Other than that, the three product variants and their configurations have the identical physical and logical scopes as described in Section 1.6.3 and Section 1.6.4.

Table 3. Platform Reference

Reference	Value	
Platform Name and Version	See Table 5	
Platform Identification	Chip name and version	KW45 / K32W148 / MCX W71, 01b
Platform Type	Microcontroller platform for IoT applications	
Security Subsystem Identification	EdgeLock Enclave (ELE S200), version KW45 / K32W148 / MCX W71 A2	

1.5 Included Guidance Documents

The following documents are included with the platform:

Table 4. Guidance Documents

Document	Reference
Reference Manual	KW45 Reference Manual [11]
Reference Manual	K32W1480 Reference Manual [13]
Reference Manual	KW45 Security Reference Manual [15]
Reference Manual	K32W1480 Security Reference Manual [16]
Datasheet	KW45 Product Family Data Sheet [12]
Datasheet	K32W1480 Product Family Data Sheet [14]
Guidance and Manual	MCX W71 Guidance and User Manual [17]
SESIP Security Target	KW45 / K32W148 / MCX W71, SESIP Security Target, Revision 1.6, NXP Semiconductors, 25 March 2024.
Software Development Kit Guidance	MCUXpresso SDK builder for KW45B41Z-EVK (KW45B41Z83xxxA) and K32 W148-EVK (K32W1480xxxA) [24]
Tool User Guidance	Secure Provisioning SDK (SPSDK) [23]
Application Note	AN13931, Managing Lifecycles on KW45 and K32W148 [18]
Application Note	AN13860, Creating Firmware Update Image for KW45B41Z/K32W148 using Over the Air Programming Tool [19]
Application Note	AN13883, Updating KW45 Radio Firmware via ISP using SPSDK [20]
Application Note	AN13855, KW45B41Z/K32W148 - Integrating the OTAP Client Service into a Bluetooth LE Peripheral Device [21]

Table 4. Guidance Documents*...continued*

Document	Reference
Application Note	AN13838, Secure Boot for KW45 and K32W [22]
API Reference Manual	PSA Attestation API 1.0 [2]
API Reference Manual	PSA Cryptography API 1.1 [3]
API Reference Manual	PSA Storage API 1.0 [4]
API Reference Manual	Mbed TLS API [5]
TF-M User Manual	Trusted Firmware M [6]

1.6 Platform Overview and Description

The KW45 / K32W148 / MCX W71 product family is a low-power, highly secure, single-chip wireless MCU that integrates a high performance Bluetooth Low Energy version 5.3 radio and CAN FD for IoT, Automotive and Industrial applications.

The family integrates a state-of-the-art, scalable security architecture including Arm TrustZone-M, a resource domain controller, and an isolated EdgeLock™ Secure Enclave supporting hardware cryptographic accelerators, random number generators and key generation, storage and management and secure debug. Flash memory contents can optionally be stored as encrypted data and then decrypted on-the-fly enabling protection of sensitive data and algorithms.

1.6.1 Platform Security Features

KW45 / K32W148 / MCX W71 includes a security subsystem, EdgeLock Enclave (ELE S200), which together with its Crypto Library and firmware parts provides the following security features:

- AES 128/192/256 with ECB, CBC, CTR, GCM and CCM modes.
- ECDSA and ECDH (ECC Diffie-Hellman Key Exchange) with NIST P-192, P-224, P-256, P-384 and P-521 curves.
- EdDSA and MontDH with Curve25519.
- SHA2-256/384/512 cryptographic hash function.
- HMAC-SHA2-256 and AES-CMAC algorithms.
- Key derivation function
- Cryptographic random number generators including TRNG and DRBG.
- Key storage services.
- A messaging unit to communicate with the host.

On top of ELE S200, KW45 / K32W148 / MCX W71 provides the following security features at SoC level:

- Secure boot to ensure authenticity, integrity and confidentiality of the device bootloader, firmware, and other software during the boot process and that the intended secure life-cycle state is reached. A firmware image can be signed by either ECDSA P-256 or ECDSA P-384 algorithm.
- Secure debug to protect access to debugging features by using certificate-based authentication with ECDSA P-256 or P-384 algorithm.
- Secure firmware update using SB3.1 file format guaranteeing authenticity and integrity (via ECDSA P-256 or P-384 algorithm) and confidentiality (via AES-CBC algorithm).
- Secure isolation to partition the platform into multiple functional/security domains. Trusted Resource Domain Controller (TRDC) and Arm Trust-Zone.
- Secure attestation to provide proof to a remote party on the platform's genuine identity, its software and firmware versions, as well as its integrity and life cycle state.
- Secure storage to provide on-the-fly flash memory encryption with PRINCE cipher and device-unique keys.

For more product features beyond security, refer to Chapter 2 of [11] and [13].

1.6.2 Platform Type

The platform consists of a micro-processor with internal hardware isolation with Arm TrustZone technology, secure memory, and a secure subsystem.

1.6.3 Platform Physical Scope

The physical scope is the KW45 / K32W148 / MCX W71 microcontroller silicon chip as shown in Figure 1.

The hardware components and interfaces are listed in Chapter 2 of [13] and [11].

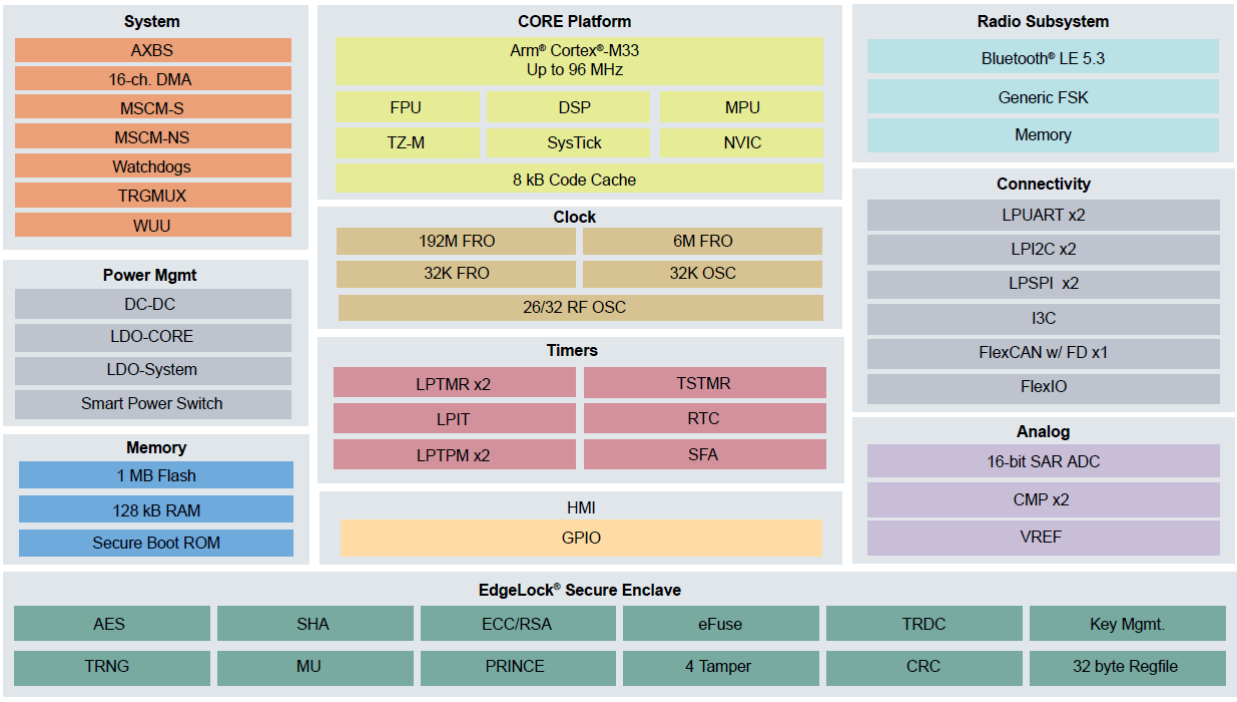

Figure 1. KW45 / K32W148 / MCX W71 Block Diagram

1.6.4 Platform Logical Scope

The logical scope includes:

- The IC itself with the Arm CM33 core and the embedded security enclave EdgeLock Enclave and its own firmware residing in the internal ROM of the EdgeLock Enclave.
- The ROM firmware which resides in the platform's ROM and the ROM firmware patch. The ROM firmware includes the bootloader and other pieces of code to enforce security features including life-cyle state, secure boot, secure update, etc. The ROM firmware also includes a security library which provides APIs to access cryptographic functions of the EdgeLock Enclave. These APIs are further wrapped by the mbedTLS crypto library APIs which are directly accessible by the users.
- The TF-M integration software package for implementing TF-M functionalities.

All the platform deliverables are listed in Table 5 below. Any additional firmware, OS or application software stored on the platform is not in scope of this evaluation.

Table 5. Platform Deliverables

Type	Name	Release	Form of delivery
IC Hardware	KW45 / K32W148 / MCX W71	01b	Silicon Chip
ROM Firmware	KW45 / K32W148 / MCX W71 ROM	1.1	Onchip ROM Firmware
ROM Firmware Patch	KW45 / K32W148 / MCX W71 ROM Patch	1.2.1	Onchip Firmware
Security Enclave	EdgeLock Enclave (ELE S200)	KW45 / K32W148 / MCX W71 A2	Onchip Hardware Subsystem
Security Enclave Software	EdgeLock Enclave Crypto Library	1.2.1	Onchip ROM Firmware
TF-M Integration	KW45 / K32W148 / MCX W71 TF-M Integration	1.5	Software Package (part of SDK)
Security API Enablement	EdgeLock Enclave Drivers and Mbed TLS Integration	2.28.0	Software Package (part of SDK)

For the guidance documents that shall be considered by the users, please refer to Section 1.5

1.6.5 Required Non-Platform Hardware/Software/Firmware

No additional non-platform hardware, software or firmware is required for the correct functioning of the security claims described in this document.

1.6.6 Life Cycle

The life cycle (LC) is managed by the platform, see [18] for further information. The LC states are as Table 6:

Table 6. Life Cycle States

LC State	Description
NXP Internal (Blank, NXP-Fab, NXP-Provisioned, NXP-Returned)	This is initial silicon state which is used for NXP manufacturing, testing, trust provisioning and field return analysis.
OEM-Open	OEM-Open is the state in which NXP delivers the chip to the OEM. This state is for OEM firmware development stage and initial configuration.
OEM-Secured_World_Closed	OEM-Secure_World_Closed is the life-cycle state in which the OEM has decided to lock the Trust Zone's secure world, i.e., test and debug ports are closed. This allows the development of non-secure software to continue while preventing secure world from being accessed. To access the secure area, the debug authentication must be performed.
OEM-Closed	OEM-Closed is the life-cycle state in which the OEM has decided to lock both secure and non-secure worlds or lock the part further coming from the OEM-Secure_World_Closed.
OEM-Locked	OEM-Locked is the life-cycle state in which the OEM has decided to lock the device. This means that this device may continue to be updated in the field, but all debug/test ports can be disabled permanently. This is configurable by OEM.
OEM-Returned	OEM-Returned is the life-cycle state in which the end product must be returned to the OEM for failure analysis testing. Once in OEM-Returned state, Bootloader makes sure that OEM assets and flash memory are erased before loading and then executing diagnostic firmware.

The Boot ROM is responsible for checking the life-cycle state. Based on the life-cycle state, the ROM determines what boot flow is used, including whether the control is passed to the application code or not. The

ROM also handles the opening of test and debug ports based on the life-cycle state. If the platform is in any invalid life-cycle state, then the ROM locks the platform as described above. The transitions among LC states are given in Figure 2.

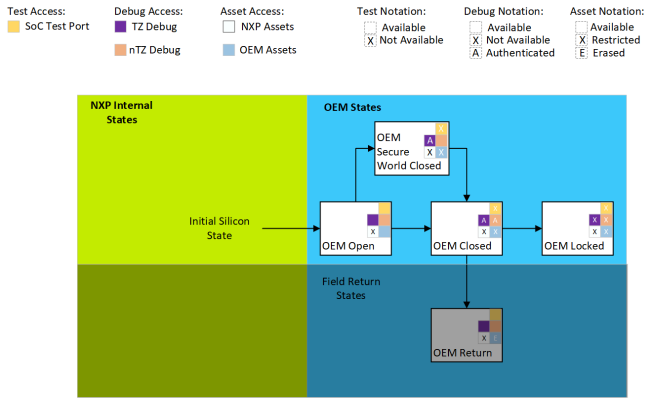

Figure 2. KW45 / K32W148 / MCX W71 Life Cycle Transitions

1.6.7 Use Case

[trusted user]

The platform is expected to be used by trusted users only.

[trusted code]

Only trusted code is expected to run the platform. The platform enforces this by secure boot feature. On the field, the platform firmware can be updated. However, the update process must be done in a secure manner which protects the confidentiality and integrity of the firmware.

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) shall fulfill the following objectives:

Table 7. Platform Objectives for the Operational Environment

Title	Description	Reference
Platform Verification	The operating system or application code are expected to verify the correct version of all platform components it depends on, as described in Section 3.2.1.1 of this document.	Section 3.2.1.1
Secure Boot	The operating system or application code are expected to make use of the Secure Boot feature as described in [22].	[22]
Secure Debug	The integrating environment is expected to configure the debug functionality as described in [18]	[18]
Key Management	Cryptographic keys and certificates outside of the Platform are subject to secure key management procedures.	This document
Trusted Users	Actors in charge of platform management, for instance for signature of firmware update, are trusted.	This document
SW Integration	The operating system or application code are expected to ensure the correct version of the crypto library and SDK drivers are integrated and configured.	This document
Secure Update and Key Revoke	The operating system or application code are expected to update an image with proper remedy solution and version increased and/or revoke key in case of security incidence occurrence of the image and/or the key.	[19]
Lifecycle Management	The operating system or application code are expected to provide lifecycle states and secure mechanism of lifecycle state transition according to the use case, and the operational environment is expected to configure the platform accordingly for lifecycle state transitions. In general, the operating system or application code are expected to configure the platform to OEM-Closed or OEM-Locked state.	[18]

3 Security Requirements and Implementation

3.1 Security Assurance Requirements

The claimed assurance requirements package is: **SESIP Assurance Level 2 (SESIP2)** as defined in Chapter 4 of GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2 [7].

3.1.1 Flaw Reporting Procedures (ALC_FLR.2)

In accordance with the requirement for flaw reporting procedures (ALC_FLR.2), the developer has defined the following procedure:

NXP has defined a Product Security Incident Response Process (PSIRP), implemented by a dedicated team (PSIRT). This process provides a publicly available interface (https://nxp.com/psirt), and includes four major steps:

- **Reporting**. The process begins when the PSIRT becomes aware of a potential security vulnerability in an NXP product. The reporter receives an acknowledgment and updates throughout the handling process.
- **Evaluation**. The PSIRT confirms the potential vulnerability, assesses the risk, determines the impact and assigns a processing priority. If the vulnerability is confirmed, the priority determines how the issue is handled throughout the remaining steps in the process.
- **Solution**. Working with PSIRT, the product team develops a solution that mitigates the reported security vulnerability. Solutions will take different forms based on the vulnerability. Because of the nature of NXP products – mostly silicon products where the firmware is in ROM -, very often the solution can only be provided in a next version of the chips and the short-term solution will consist of recommending security measures to be applied in systems using the NXP product.
- **Communication**. As said above, because of the nature of the NXP products, the solution to systems using the affected products often needs to be found in additional countermeasures in those systems. The communication on the vulnerability and solutions will in most cases be done directly towards the affected customers. For previously unknown or unreported issues, NXP will acknowledge the reporter of the issues (unless the reporter requests otherwise).

The platform's Secure Boot feature is able to verify the authenticity of customer code, i.e., the OEM firmware, during the boot sequence. In addition, the platform also provide Secure Update feature to allows the update of the OEM firmware to a newer version. Once updated, it is not possible to revert back to any older version of the firmware. The update mechanism can also be used to update the TF-M software package provided by the platform since the TF-M package is an integrated part of the OEM firmware. See Section 3.2.2.1 for further information.

Other software components of the platform including the ROM firmware are not updatable as it resides in read - only memory of the platform.

3.2 Security Functional Requirements

In the following Security Functional Requirements, the term **platform** covers the **KW45 / K32W148 / MCX W71 physical and logical scope**, and the term **application** refer to any additional firmware, OS or application software which is out of evaluation scope. It represents a part of the final connected device.

KW45 / K32W148 / MCX W71 fulfils the following security functional requirements:

3.2.1 Identification and Attestation of Platforms and Applications

3.2.1.1 Verification of Platform Identity

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

Conformance rationale:

The identification for different parts of the platform can be done by using `GetProperty` command in ISP (In-System Programming) mode as specified in Chapter 15.2.6.2 of [11] and [13]. The returned values shall be the same as the values indicated Section 1.6.4. More specifically,

- IC hardware version: ISP command `GetProperty`, tag 16 to retrieve the `SystemDeviceID` property.
- ROM version: ROM version is 1.1 and it is coupled with the IC hardware version 01b. Therefore, it is sufficient to identify the correct IC hardware version to identify the correct ROM version.
- Secure Enclave and the corresponding Secure Enclave software are at version KW45 / K32W148 / MCX W71 A2 and 1.2.1, respectively. They are both coupled with IC hardware version 01b. Therefore, it is also sufficient to identify the correct IC hardware version to verify the correct Secure Enclave and Secure Enclave software.
- ROM patch version: ISP command `GetProperty`, tag 24 to retrieve the `CurrentVersion` property.

The TF-M integration and Mbed TLS integration are delivered as software packages in the SDK for the platform. They can be identified by referring to `SW-Content-Register.txt` that comes with the SDK.

3.2.1.2 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:

The platform stores a 128-bit IETF RFC4122 compliant non-sequential Universally Unique Identifier (UUID). It can be read out by using ISP command `GetProperty` to retrieve `UniqueDeviceId` property.

3.2.1.3 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:

Trust provisioning is a process used for creation of initial Device Identity keys. Its major objective is to provide a cryptographic proof of the device’s origin and to offer a set of tools to OEM for secure provisioning of their own assets. In a nutshell, a device-unique private-public key pair is created on every device, the public portion of which is collected and signed by NXP. That signed public key is installed back onto every device in a form of device-unique certificate, which serves the actual proof of the platform’s origin. See more in [25]

KW45 / K32W148 / MCX W71 with TF-M Port also supports the PSA attestation API to produce an initial attestation token in IETF EAT format containing measurements of the firmware, which provides an attestation service which reports on the device identity, firmware measurements and run-time state of the device. The attestation can be verified by remote entities. The tokens are signed using attestation keys stored in the internal flash. See more in [1] and [2].

3.2.1.4 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:

See Section 3.2.1.3.

3.2.1.5 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 *infinite loop or ISP mode for Secure Update (configurable)*.

Conformance rationale:

Secure boot prevents unauthorized code from being executed on a given product. It achieves this level of security by always leaving the device's ROM in an executing mode when coming out of a reset. This allows the ROM to examine the first user executable image resident in internal flash memory to determine the authenticity of that code. If the code is authentic, then control is transferred to it. This establishes a chain of trusted code from the ROM to the user boot code. This chain can be further extended, through the verification of digital signatures associated with additional code layers.

The platform's ROM boot loader which is always executed after reset provides the secure boot operation. The firmware to be loaded is signed with ECDSA P-256 or P-384 algorithm and the signature is attached to the end of the firmware image. The entire firmware image includes some meta-data and most importantly a certificate block that contains public keys and corresponding certificates. These certificates are validated before it can be used to verify the ECDSA signature on the signed image. Please see [22] for more details.

If the ROM boot loader fails to validate the firmware image, the platform can enter an infinite sleep mode and the failure is reported. This is configurable as specified in Chapter 15.2 of [11] and [13].

3.2.2 Product Lifecycle: Factory Reset / Install / Update / Decommission

3.2.2.1 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:

Secure Update is the process used to securely update the OEM firmware to a newer version. The OEM firmware includes the TF-M package provided by the platform and thus this secure update process provides a mechanism to update the platform. The firmware image is encrypted using AES-128 or AES-256 and signed using ECDSA P-256 or P-384 algorithm, following the SB3.1 firmware image format. Secure Update is required to guarantee the authenticity and confidentiality of the new image. In addition, it also ensures that the new image is up-to-date, preventing the rollback to an older image.

The platform's ROM boot loader KW45 / K32W148 / MCX W71 provides secure firmware update operation. The Secure Update can be enabled when the platform is booted into ISP (In-System Programming) mode and the ReceiveSBFile command is available. This is not the case for certain life-cycle states including OEM-Returned or NXP-Returned states. in these states, Secure Update is not possible. The platform uses SB3.1 firmware image format and meets the security requirements for Secure Update as follows:

- Integrity and Authenticity: a firmware image to be updated is signed by using ECDSA P-256 or P-384 algorithm so that its integrity and authenticity can be verified before the new firmware can be decrypted and programmed to the platform's flash memory. The OEM's trusted root key is securely programmed into a fuse named CUST_PROD_OEMFW_AUTH_PUK in advance so that it can be used for ECDSA signature verification. Please note that, the key can be revoked via another fuse CUST_PROD_OEMFW_AUTH_PUK_REVOKE to prevent compromised OEM's root key can be used to program malicious firmware into the platform.
- Confidentiality: the new firmware image is encrypted with AES-128 or AES-256 in CBC mode. The encryption key is also securely programmed into a fuse named CUST_PROD_OEMFW_ENC_SK in advance so that it can be used to decrypt the new firmware image.

- Anti roll-back: the platform provides several monotonic counters, e.g., CM33_S_VER_CNT for OEM firmware version counter, in the fuse SOC_VER_CNT to prevent old firmware version from being programmed into the platform's flash memory.

Please refer to Chapter 15.2 of [11] and [13] for further details.

3.2.2.2 Field Return of Platform

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

Conformance rationale:

KW45 / K32W148 / MCX W71 provides secure Field Return feature as part of its life-cycle management.

In the OEM's Field Return state (OEM-Returned), all OEM assets are erased before entering the state. For NXP's Field Return state (NXP-Returned), NXP assets are further removed before running further tests. In addition, in the field return states, on every boot, the platform's bootloader in ROM verifies if the flash and OEM/NXP assets are blank. If not, it proceeds to erased all the flash and make sure OEM/NXP assets are flushed before enabling debugging ports for running diagnostic tests. See more in [18] and Chapter 15.2.1 of [11] and [13].

3.2.2.3 Decommission of Platform

The platform can be decommissioned.

Conformance rationale:

The End-of-Life security life-cycle state can be used by customers or NXP to remove a chip permanently from regular use and erase all sensitive data stored on the chip, see Chapter 5.6 of [15] and [16]. When a part is decommissioned, it is switched to OEM-Locked life-cycle state then disables read access to all fuses such that the secure enclave no longer boots. Debug and test ports are closed and the bootloader is irreversibly configured in a way that it enters an infinite loop waiting for the secure enclave to initialize and renders the part non-functional by any party. See also [18] and Chapter 15.2.1 of [11] and [13].

3.2.3 Extra Attacker Resistance

3.2.3.1 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 any other claimed security functional requirements.

Conformance rationale:

There are multiple isolation features presented in the platform.

Arm TrustZone enables secure Isolation during run-time by providing four distinct levels of privilege: secure-privileged, secure-user, non-secure-privileged and non-secure-user. The Memory Block Checker (MBC) implements access controls for on-chip internal memories and slave peripherals based on a fixed-sized block format. The Memory Region Checker (MRC) implements the access controls for external off-chip memories and peripherals based on the pre-programmed region descriptor registers. TRDC along with MBC and MRC blocks can be programmed with only the highest level of privilege, which is secure-privileged. Additionally, PSA Level 2 Isolation is supported by TF-M integration which makes use of TrustZone and Memory Protection Unit (MPU) on the platform's Arm v8-M core.

The platform's ELE S200 module is a security subsystem supporting a wide range of cryptographic algorithms and providing strong key isolation from the rest of the system. When embedded in an SoC, ELE S200 serves as the main building block of the SoC's immutable Root of Trust. It is used as part of the trust anchor during secure boot, secure debug access, life-cycle management, and trust provisioning. ELE S200 has its own controller

and exclusive system resources with enforced access control, hence it is isolated from the rest of platform. See more in Chapter 36.1 of [11] and [13].

The memory encryption with PRINCE cipher also ensures Secure Isolation between multiple IP vendors. The cipher's Initial Vector (IV) is derived by secure-privileged and a different value is used for every independent memory region, ensuring the isolation between each other. See more in See more in Chapter 7 of [11] and [13].

3.2.3.2 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 any other claimed security functional requirements.

Conformance rationale:

The isolation between PSA-RoT and Application Root of Trust Services is included in Section 3.2.3.1.

3.2.4 Cryptographic Functionality

3.2.4.1 Cryptographic Operation

The platform provides the application with *operations in Table 8* functionality with *algorithms in Table 8* as specified in *specifications in Table 8* for key lengths *described in Table 8* and modes *described in Table 8*.

Table 8. Cryptographic Operations

Operation	Algorithm	Specification	Key Lengths (bits)	Modes
Encryption and decryption	AES	NIST FIPS 197	128, 192, 256	ECB, CBC, CTR
Authenticated Encryption, Authenticated Decryption	AES	NIST SP.800-38d	128, 192, 256	CCM, GCM
Hashing	SHA2	NIST FIPS 180-4	224, 256, 384, 512	-
MAC generation and verification	HMAC	RFC2104	Up to 512	SHA-256
MAC generation and verification	CMAC	RFC4493	128, 192, 256	AES CMAC
KDF	HKDF	ANSI X9.63	128 to 256	-
Key Exchange	ECDH	NIST FIPS 800-56A	192 to 521	NIST P-192, P-224, P-256, P-384 and P-521 curves
Signature generation and verification	ECDSA	ANSI X9.62	192 to 521	NIST P-192, P-224, P-256, P-384 and P-521 curves
Signature generation and verification	EdDSA	IETF RFC 8032	256	Curve25519
Key Exchange	MontDH	IETF RFC 7748	256	Curve25519

Conformance rationale:

The crypto accelerators are located in ELE S200. Crypto Library for ELE S200 has been developed leveraging these accelerators to provide several cryptographic algorithms including AES, ECDSA, etc. See more in

Chapter 36.1 of [11] and [13]. All supported cryptographic algorithms are implemented so that they are resistant against remote attacks.

The cryptographic operations are available to users via Mbed TLS integration, see [5]. Supported algorithms are further enabled in the TF-M port via PSA Crypto API, see [3].

3.2.4.2 Cryptographic Key Generation

The platform provides the application with a way to generate cryptographic keys for use in *algorithms in Table 9* as specified in *specifications in Table 9* for key lengths *described in Table 9*

Table 9. Cryptographic Key Generation

ID	Algorithm	Specification	Key Lengths
ECC	ECC	ANSI X9.62	192, 224, 256, 384 and 512 bits
Symmetric	Symmetric	None	128, 192 and 256 bits

Conformance rationale:

The ECC key generation function is provided by Crypto Library for ELE S200. User can access this function via Mbed TLS integration, see [5] as well as in the TF-M port via PSA Crypto API, see [3].

The AES key generation is provided by DRBG as defined in Section 3.2.4.4.

3.2.4.3 Cryptographic KeyStore

The platform provides the application with a way to store *cryptographic keys* such that not even the application can compromise the *authenticity, integrity, confidentiality* of this data. This data can be used for the cryptographic operations *encryption, decryption, signature generation, MAC generation and verification, key derivation, shared secret generation*.

Conformance rationale:

The platform provides a dedicated flash area for cryptographic key storage. Access to this dedicated flash area is managed by hardware only. On top of the flash memory encryption, the stored keys are wrapped with AES-CCM AHEAD cipher algorithm with per-device key, random IV and security attributes for owner and key usage policy. An encrypted key blob including the key itself and its security attributes can be loaded into the ELE S200 cryptographic module which can be unwrapped and used for cryptographic operations if permitted by the associated security attributes. Please note that, ELE S200 only keeps the loaded keys in its volatile memory. In addition, it is isolated from the rest of the platform via Arm TrustZone and Trusted Resource Domain Controller (TRDC). See Section 3.2.3.1.

3.2.4.4 Cryptographic Random Number Generation

The platform provides the application with a way based on *methods in Table 10* to generate random numbers to as specified in *specifications in Table 10*.

Table 10. Cryptographic Random Number Generation

Methods	Specifications
Physical Noise (TRNG)	NXP's RNG4 entropy source [10]
DRBG	NIST SP800-90A CTR-DRBG with AES-128 or AES-256 [27]

Conformance rationale:

The platform's ELE S200 provides a physical true random number generator (TRNG) and a DRBG module as defined in NIST SP800-90A [27]. The TRNG is compliant to [10]. Furthermore, the TRNG is capable of passing AIS 31 statistical tests T0-T8.

Access to random number generators are enabled via Mbed TLS integration, see [5] as well as in the TF-M port via PSA Crypto API, see [3].

3.2.5 Compliance Functionality

3.2.5.1 Secure Encrypted Storage

The platform ensures that all data stored by the application, except for *data not stored in the configured address area*, is encrypted as specified in *PRINCE [26]* with a platform instance unique key of key length *128 bits*.

Conformance rationale:

This device offers support for real-time encryption and decryption for on-chip flash using the PRINCE encryption algorithm. See more in Chapter 7 of [11] and [13].

3.2.5.2 Secure Debugging

The platform only provides *Arm's Serial Wire Debug (SWD) interface* authenticated as specified in *[11] and [13].* with debug functionality.

The platform ensures that all data stored by the application, with the exception of *subdomain(s) debug access enabled* , is made unavailable.

Conformance rationale:

The availability of debug functionality depends on the life-cycle state of the platform. This is enforced by life-cyle management of the platform as specified in [18]. For example, in NXP-Fab and NXP-Provisioned states, access to debug functionality is always possible. On the other hands, the same access is completely disabled in OEM-Closed state.

In the other life-cyle states, e.g., OEM-Open and OEM-Closed states, that access to debug functionality is enabled but shall be authorized. The platform enforces a debug authentication protocol as a mechanism to authenticate the debugger (an external entity) which owns its credentials approved by the product manufacturer before granting debug access to the platform. The authentication protocol is a challenge-responsed protocol based on ECDSA algorithm. See more in [18] and Chapter 15.2 of [11] and [13].

.

3.2.5.3 Residual Information Purging

The platform ensures that *key store area*, with the exception of *none*, is erased using the method specified in *overwriting with random numbers* before the memory is (re)used by the platform or application again and before an attacker can access it.

Conformance rationale:

As the key store area are in the platform's internal flash, the platform implements residual information purging by providing APIs to program and erase flash memory. This is also enforced by the platform's bootloader in ROM for field return states (OEM-Returned and NXP-Returned). See Section 3.2.2.2.

3.2.5.4 Reliable Index

The platform implements a strictly increasing function.

Conformance rationale:

The platform implements monotonic counters including ones that support the anti roll-back mechanism is employed as described in Section 3.2.2.1. Please refer to monotonic counters described in Table 75 in [15] and [16] for further details.

4 Mapping and Sufficiency Rationales

4.1 SESIP2 Sufficiency

Table 11. SESIP2 Sufficiency

Assurance Class	Assurance Family	Covered By	Rationale
ASE: Security target evaluation	ASE_INT.1 ST Introduction	Section 1	The ST reference is in ST Reference, the TOE reference in Section 1.4, the TOE overview and description in Section 1.6.
	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	Security Requirements and Implementation	All SFRs in this ST are taken from [7]. SFR "Identification of Platform Type" is included. SFR "Secure Update of Platform" is mentioned but refers to ALC_FLR.2.
	ASE_TSS.1 TOE Summary Specification	Security Requirements and Implementation	All SFRs are listed per definition, and for each SFR the implementation and verification are defined in the SFR.
ADV: Development	ADV_FSP.4 Complete functional specifications	Section 1.5	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	Section 1.5	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
	AGD_PRE.1 Preparative procedures	Section 1.5	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
ALC: Life-cycle support	ALC_FLR.2 Flaw reporting procedures	Section 3.1.1	The flaw reporting and remediation procedure is described.
ATE: Test	ATE_IND.1 Independent testing: conformance	Material provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis	N.A. A vulnerability analysis is performed by the evaluator to ascertain the presence of potential vulnerabilities.	The 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 evaluator assuming an attack potential of Basic.

4.2 Conformance Mapping for SESIP Profile for Secure MCUs and MPUs

This section provides rationales of conformance claimed in Section 1.2

Table 12. SESIP Profile for Secure MCUs and MPUs Sufficiency

Package Claimed	Security Functional Requirements	Covered By
Base	Verification of Platform Identity	Section 3.2.1.1

Table 12. SESIP Profile for Secure MCUs and MPUs Sufficiency*...continued*

Package Claimed	Security Functional Requirements	Covered By
	Secure Initialization of Platform	Section 3.2.1.5
	Secure Updated of Platform	Section 3.2.2.1
	Residual Information Purging	Section 3.2.5.3
	Secure Debugging	Section 3.2.5.2
Security Services	Cryptographic Operation	Section 3.2.4.1
	Cryptographic Key Generation	Section 3.2.4.2
	Cryptographic KeyStore	Section 3.2.4.3
	Cryptographic Random Number Generation	Section 3.2.4.4
Software Isolation	Software Attacker Resistance: Isolation of Platform	Section 3.2.3.1, Section 3.2.3.2
Additional Security Functional Requirements (Optional)	Verification of Platform Instance Identity Attestation of Platform Genuineness Attestation of Platform State Decommission of Platform Field Return of Platform Secure Encrypted Storage Reliable Index	Section 3.2.1.2 Section 3.2.1.3 Section 3.2.1.4 Section 3.2.2.3 Section 3.2.2.2 Section 3.2.5.1 Section 3.2.5.4

4.3 Conformance Mapping for SESIP Profile for PSA Certified Level 2

This section provides rationales of conformance claimed in Section 1.2

Table 13. SESIP Profile for PSA Certified Level 2 Sufficiency

Package Claimed	Security Functional Requirements	Covered By
Base	Verification of Platform Identity	Section 3.2.1.1
	Verification of Platform Instance Identity	Section 3.2.1.2
	Attestation of Platform Genuineness	Section 3.2.1.3
	Secure Initialization of Platform	Section 3.2.1.5
	Attestation of Platform State	Section 3.2.1.4
	Secure Updated of Platform	Section 3.2.2.1
	Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)	Section 3.2.3.1
	Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services)	Section 3.2.3.2
	Cryptographic Operation	Section 3.2.4.1
	Cryptographic Key Generation	Section 3.2.4.2
	Cryptographic KeyStore	Section 3.2.4.3
	Cryptographic Random Number Generation	Section 3.2.4.4
Optional SFR	Secure Debugging	Section 3.2.5.2
	Secure Encrypted Storage (internal storage)	Section 3.2.5.1

4.4 Conformance Rationales for DIRECTIVE 2014/53/EU (RED)

This section provides conformance rational for RED conformance claim described in Section 1.3.1.

Table 14. Conformance Rationales for RED

RED Requirement ID	Description	RED Article d: network assets e: privacy assets f: financial assets	Fulfilled By
ACM-1	Applicability of access control mechanisms	d/e/f	Section 3.2.4.1 Section 3.2.4.2 Section 3.2.4.3 Section 3.2.4.4 AVA_VAN
ACM-2	Appropriate access control mechanisms	d/e/f	Same as above
ACM-3	Default access control for children in toys	e	Same as above
ACM-4	Default access control to children's privacy assets for toys and childcare equipment	e	Same as above
ACM-5	Parental/Guardian access controls for children in toys	e	Same as above
ACM-6	Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys	e	Same as above
AUM-1	Applicability of authentication mechanisms	d/e/f	Same as above
AUM-2	Appropriate authentication mechanisms	d/e/f	Same as above
AUM-3	Authenticator validation	d/e/f	Same as above
AUM-4	Changing authenticators	d/e/f	Same as above
AUM-5	Password strength	d/e/f	Same as above
AUM-6	Brute force protection	d/e/f	Same as above
SUM-1	Applicability of update mechanisms	d/e/f	Section 3.2.2.1 Section 3.1.1
SUM-2	Secure updates	d/e/f	Same as above
SUM-3	Automated updates	d/e/f	Same as above
SSM-1	Applicability of secure storage mechanisms	d/e/f	Section 3.2.5.1
SSM-2	Appropriate integrity protection for secure storage mechanisms	d/e/f	Same as above
SSM-3	Appropriate confidentiality protection for secure storage mechanisms	d/e/f	Same as above

Table 14. Conformance Rationales for RED*...continued*

RED Requirement ID	Description	RED Article d: network assets e: privacy assets f: financial assets	Fulfilled By
SCM-1	Applicability of secure communication mechanisms	d/e/f	Section 3.2.4.1 Section 3.2.4.2 Section 3.2.4.3 Section 3.2.4.4
SCM-2	Appropriate integrity and authenticity protection for secure communication mechanisms	d/e/f	Same as above
SCM-3	Appropriate confidentiality protection for secure communication mechanisms	d/e/f	Same as above
SCM-4	Appropriate replay protection for secure communication mechanisms	d/e/f	Same as above
LGM-1	Applicability of logging mechanisms	e/f	Section 3.2.4.1 Section 3.2.4.2 Section 3.2.4.3 Section 3.2.4.4 Section 3.2.5.1
LGM-2	Logging mechanisms – Persistent storage	e/f	Same as above
LGM-3	Logging mechanisms – Minimum number of Events	e/f	Same as above
LGM-4	Logging mechanisms – Time related information	e/f	Same as above
DLM-1	Applicability of deletion mechanisms	e	Section 3.2.2.2 Section 3.2.2.3 Section 3.2.5.3
RLM-1	Applicability of resilience mechanisms	d	Section 3.2.1.5 Section 3.2.4.1 Section 3.2.4.2 Section 3.2.4.3 Section 3.2.4.4
NMM-1	Applicability of and appropriate network monitoring mechanisms	d	Section 3.2.4.1 Section 3.2.4.2 Section 3.2.4.3 Section 3.2.4.4
TCM-1	Applicability of and appropriate traffic control mechanisms	d	Section 3.2.4.1 Section 3.2.4.2 Section 3.2.4.3 Section 3.2.4.4
UNM-1	Applicability of user notification mechanisms	e	Not applicable

Table 14. Conformance Rationales for RED*...continued*

RED Requirement ID	Description	RED Article d: network assets e: privacy assets f: financial assets	Fulfilled By
UNM-2	Content of user notification	e	Not applicable
CCK-1	Appropriate Confidential cryptographic keys (CCKs)	d/e/f	Section 3.2.1.5 Section 3.2.2.1 Section 3.2.4.1 Section 3.2.4.2 Section 3.2.4.3 Section 3.2.4.4 Section 3.2.5.1 Section 3.2.5.2 Section 3.2.1.3 Section 3.2.1.4
CCK-2	Confidential cryptographic key generation mechanisms	d/e/f	Same as above
CCK-3	Preventing static default values for preinstalled CCKs	d/e/f	Same as above
GEC-1	Up-to-date software and hardware with no publicly known exploitable vulnerabilities	d/e/f	AVA_VAN AGD_PRE and AGD_OPE
GEC-2	Limit exposure of services via related network interfaces	d/e/f	Same as above
GEC-3	Configuration of optional services and the related exposed network interfaces	d/e/f	Same as above
GEC-4	Documentation of exposed network interfaces and exposed services via network interfaces	d/e/f	Same as above
GEC-5	No unnecessary external interfaces	d/e/f	Same as above
GEC-6	Input validation	d/e/f	Same as above
GEC-7	Documentation of external sensing capabilities	e	Same as above
GEC-8	Equipment Integrity	f	Same as above
CRY-1	Best practice Cryptography	d/e/f	Section 3.2.1.5 Section 3.2.2.1 Section 3.2.4.1 Section 3.2.4.2 Section 3.2.4.3 Section 3.2.4.4 Section 3.2.5.1 Section 3.2.5.2

4.5 Fulfillment Rationales for NIST 8425

This section provides fulfillment rationales for NIST 8425 claim described in Section 1.3.2

Table 15. Fulfillment Rationales for NIST 8425

NIST 8425 Element	Rationale	Fulfilled By
AI1	The platform provides methods for its users to identify different parts that make up the platform, including hardware and firmware versions. In addition, the platform implements functionality supporting the attestation of the platform identity and its authenticity to an external party.	Section 3.2.1.1 Section 3.2.1.2 Section 3.2.1.3
AI2	Same as above.	Section 3.2.1.1 Section 3.2.1.2 Section 3.2.1.3
DP1	The platform enforces protection of data stored in the platform by various means including cryptography, access control, firewall, secure boot, etc.	Section 3.2.1.1 Section 3.2.1.2 Section 3.2.1.5 Section 3.2.2.1 Section 3.2.3.1 Section 3.2.3.2 Section 3.2.4.3 Section 3.2.5.1 Section 3.2.5.2
DP2	The platform provides means to manage its life-cycle states.	Section 3.2.2.2 Section 3.2.2.3 Section 3.2.5.3
DP3	The platform implements various cryptographic functionalities to support securing data transmission.	Section 3.2.4.1 Section 3.2.4.2 Section 3.2.4.3 Section 3.2.4.4
IAC1a	The platforms implements mechanisms to lock down un-used interfaces including ones for debugging and testing before deployment.	Section 3.2.5.2
IAC1b	The platforms implements access control mechanisms and cryptographic functionalities to support the access control measures.	Section 3.2.4.1 Section 3.2.4.2 Section 3.2.4.3 Section 3.2.4.4 Section 3.2.5.2
IAC1c	The platform implements hardware-based mechanisms to divide and isolate the platform's resources into different security domains and isolate them from each other.	Section 3.2.3.1 Section 3.2.3.2
SU1	The platform implements a mechanism to allow the platform's software to be updated. The updated image shall be encrypted and signed to guarantee its confidentiality, integrity and authenticity. Once completed, the updated	Section 3.2.1.3 Section 3.2.1.4 Section 3.2.2.1 Section 3.2.3.1 Section 3.2.3.2

Table 15. Fulfillment Rationales for NIST 8425*...continued*

NIST 8425 Element	Rationale	Fulfilled By
	platform can be verified by an external party via the attestation process mentioned above.	
SU2	The platform implements a mechanism to allow the software on the platform to be securely updated on the field.	Section 3.2.2.1
CSA1	The platform collects and stores some information which can be later used for security purposes including the attestation process described above.	Section 3.2.1.3 Section 3.2.1.4 Section 3.2.3.1 Section 3.2.3.2
D1ai	The required information shall be archived in different documents (e.g., this document, guidance document, evaluation, report, etc.) as mandated by SESIP evaluation standard for which this Security Target is fully compliant to.	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2 [7]
D1aii	Same as above.	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2[7]
D1aiii	Same as above.	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2[7]
D1aiv	Same as above.	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2[7]
D1av	Same as above.	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2[7]
D1avi	Same as above.	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2[7]
D1avii	Same as above.	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2[7]
D1aviii	Same as above.	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2[7]
D1b	Same as above.	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2[7]
D1c	Same as above.	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2[7]
D1d	Same as above.	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2[7]
D1e	Same as above.	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2[7]
D1fi	Same as above.	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2[7]
D1fii	Same as above.	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2[7]
D1fiii	Same as above.	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2[7]
D1gi	Same as above.	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2[7]

Table 15. Fulfillment Rationales for NIST 8425*...continued*

NIST 8425 Element	Rationale	Fulfilled By
D1gii	Same as above.	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2[7]
D1giii	Same as above.	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2[7]
D1giv	Same as above.	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2[7]
D1gv	Same as above.	GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2[7]
IQR1a	NXP implements a process to archive, track and manage vulnerabilities found its products including the platform described in this Security Target.	Section 3.1.1
IQR1b	Same as above.	Section 3.1.1
InD1a	Same as above.	Section 3.1.1
InD1b	Same as above.	Section 3.1.1
InD1c	Same as above.	Section 3.1.1
InD1d	Same as above.	Section 3.1.1
InD1e	Same as above.	Section 3.1.1
InD2	Same as above.	Section 3.1.1
PEA1ai	The platform provides guidance documents to inform and educate its users on all aspects of managing the platform.	Section 1.5
PEA1aii	Same as above.	Section 1.5
PEA1aiii	Same as above.	Section 1.5
PEA1aiv	Same as above.	Section 1.5
PEA1b	Same as above.	Section 1.5
PEA1c	Same as above.	Section 1.5
PEA1d	Same as above.	Section 1.5
PEA1e	Same as above.	Section 1.5

5 Bibliography

5.1 Evaluation Documents

[1] Arm Platform Security Architecture Firmware Framework 1.0, Arm Limited, DEN 0063. Issue number 0, Jun 2019
[2] PSA Attestation API 1.0, Arm Limited, IHI 0085, Issue Number 0, Jun 2019.
[3] PSA Cryptography API 1.1, Arm Limited, IHI 0086, Issue Number 0, Feb 2022
[4] PSA Storage API 1.0, Arm Limited, IHI 0087, Issue Number 0, Jun 2019.
[5] Mbed TLS API, Arm Limited, https://mbed-tls.readthedocs.io/.
[6] Trusted Firmware M, Arm Limited, https://tf-m-user-guide.trustedfirmware.org/releases/1.5.0.html, Release 1.5.0.
[7] GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2, GP_FST_070.
[8] GlobalPlatform Technology SESIP Profile for Secure MCUs and MPUs, Version 1.0, GPT_SPE_150.
[9] SESIP Profile for PSA Certified Level 2, V1.0 REL 02, PSA JSA, 24th November 2022.

5.2 Developer Documents

[10] Design of the Entropy Source in the NXP RNG4 Random Number Generator, v1.24,NXP Semiconductors, 16 October 2023.
[11] KW45 Reference Manual, Rev. 7, NXP Semiconductors, November 2022.
[12] KW45 Product Family Data Sheet, Rev. 9, NXP Semiconductors, December 2022.
[13] K32W1480 Reference Manual, Rev. 4, NXP Semiconductors, September 2022.
[14] K32W1480 Product Family Data Sheet, Rev. 3, NXP Semiconductors, December 2022.
[15] KW45 Security Reference Manual, Rev. 5, NXP Semiconductors, March 2024.
[16] K32W1480 Security Reference Manual, Rev. 5, NXP Semiconductors, March 2024.
[17] MCX W71 Guidance and User Manual, Rev. 1, NXP Semiconductors, April 2024.
[18] AN13931, Managing Lifecycles on KW45 and K32W148, Rev. 0, NXP Semiconductors, 25 April 2023.
[19] AN13860, Creating Firmware Update Image for KW45B41Z/K32W148 using Over the Air Programming Tool, Rev. 1, NXP Semiconductors, 21 March 2023.
[20] AN13883, Updating KW45 Radio Firmware via ISP using SPSDK, Rev. 0, NXP Semiconductors, 10 March 2023.
[21] AN13855, KW45B41Z/K32W148 - Integrating the OTAP Client Service into a Bluetooth LE Peripheral Device, Rev. 0, NXP Semiconductors, 1 March 2023.
[22] AN13838, Secure Boot for KW45 and K32W, Rev. 0, NXP Semiconductors, 25 January 2023.
[23] Secure Provisioning SDK (SPSDK), Rev. 2.1.0, NXP Semiconductors, https://spsdk.readthedocs.io/en/2.1.0/.
[24] MCUXpresso SDK builder for KW45B41Z-EVK (KW45B41Z83xxxA) and K32W148-EVK (K32W1480xxxA), NXP Semiconductors, http://mcuxpresso.nxp.com.
[25] AN6259, Common Trust Provisioning Conceptional Overview, Rev 1.1, NXP Semiconductors, March 2021.

5.3 Standards

[26] J. Borghoff, et al, PRINCE - A Low-latency Block Cipher for Pervasive Computing Applications, Cryptology ePrint Archive, Report 2012/529.
[27] NIST SP 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, National Institute of Standards and Technology, January 2012.

[28] DIRECTIVE 2014/53/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014L0053-20180911.
[29] NIST IR 8425, Profile of the IoT Core Baseline for Consumer IoT Products, https://doi.org/10.6028/NIST.IR.8425.

6 Legal information

6.1 Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

6.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

Suitability for use in automotive applications — This NXP product has been qualified for use in automotive applications. If this product is used by customer in the development of, or for incorporation into, products or services (a) used in safety critical applications or (b) in which failure could lead to death, personal injury, or severe physical or environmental damage (such products and services hereinafter referred to as "Critical Applications"), then customer makes the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, safety, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. As such, customer assumes all risk related to use of any products in Critical Applications and NXP and its suppliers shall not be liable for any such use by customer. Accordingly, customer will indemnify and hold NXP harmless from any claims, liabilities, damages and associated costs and expenses (including attorneys' fees) that NXP may incur related to customer's incorporation of any product in a Critical Application.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

6.3 Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

Tables

Tab. 1. SESIP Profile for Secure MCUs and MPUs Conformance Claims 3
Tab. 2. SESIP Profile for PSA Certified Level 2 Conformance Claims 3
Tab. 3. Platform Reference 4
Tab. 4. Guidance Documents 4
Tab. 5. Platform Deliverables 7
Tab. 6. Life Cycle States 7
Tab. 7. Platform Objectives for the Operational Environment 9
Tab. 8. Cryptographic Operations 14
Tab. 9. Cryptographic Key Generation 15
Tab. 10. Cryptographic Random Number Generation 15
Tab. 11. SESIP2 Sufficiency 18
Tab. 12. SESIP Profile for Secure MCUs and MPUs Sufficiency 18
Tab. 13. SESIP Profile for PSA Certified Level 2 Sufficiency 19
Tab. 14. Conformance Rationales for RED 20
Tab. 15. Fulfillment Rationales for NIST 8425 23

Figures

Fig. 1. KW45 / K32W148 / MCX W71 Block Diagram 6
Fig. 2. KW45 / K32W148 / MCX W71 Life Cycle Transitions 8

Contents

1 Introduction 3
1.1 ST Reference 3
1.2 SESIP Profile Reference and Conformance Claims 3
1.3 Other Conformance Claims 3
1.3.1 RED Conformance Claim 3
1.3.2 NIST 8425 Conformance Claim 3
1.4 Platform Reference 4
1.5 Included Guidance Documents 4
1.6 Platform Overview and Description 5
1.6.1 Platform Security Features 5
1.6.2 Platform Type 6
1.6.3 Platform Physical Scope 6
1.6.4 Platform Logical Scope 6
1.6.5 Required Non-Platform Hardware/Software/Firmware 7
1.6.6 Life Cycle 7
1.6.7 Use Case 8
2 Security Objectives for the Operational Environment 9
2.1 Platform Objectives for the Operational Environment 9
3 Security Requirements and Implementation 10
3.1 Security Assurance Requirements 10
3.1.1 Flaw Reporting Procedures (ALC_FLR.2) 10
3.2 Security Functional Requirements 10
3.2.1 Identification and Attestation of Platforms and Applications 11
3.2.1.1 Verification of Platform Identity 11
3.2.1.2 Verification of Platform Instance Identity 11
3.2.1.3 Attestation of Platform Genuineness 11
3.2.1.4 Attestation of Platform State 11
3.2.1.5 Secure Initialization of Platform 12
3.2.2 Product Lifecycle: Factory Reset / Install / Update / Decommission 12
3.2.2.1 Secure Update of Platform 12
3.2.2.2 Field Return of Platform 13
3.2.2.3 Decommission of Platform 13
3.2.3 Extra Attacker Resistance 13
3.2.3.1 Software Attacker Resistance: Isolation of Platform (between SPE and NSPE) 13
3.2.3.2 Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services 14
3.2.4 Cryptographic Functionality 14
3.2.4.1 Cryptographic Operation 14
3.2.4.2 Cryptographic Key Generation 15
3.2.4.3 Cryptographic KeyStore 15
3.2.4.4 Cryptographic Random Number Generation 15
3.2.5 Compliance Functionality 16
3.2.5.1 Secure Encrypted Storage 16
3.2.5.2 Secure Debugging 16
3.2.5.3 Residual Information Purging 16
3.2.5.4 Reliable Index 16
4 Mapping and Sufficiency Rationales 18
4.1 SESIP2 Sufficiency 18
4.2 Conformance Mapping for SESIP Profile for Secure MCUs and MPUs 18
4.3 Conformance Mapping for SESIP Profile for PSA Certified Level 2 19
4.4 Conformance Rationales for DIRECTIVE 2014/53/EU (RED) 20
4.5 Fulfillment Rationales for NIST 8425 23
5 Bibliography 26
5.1 Evaluation Documents 26
5.2 Developer Documents 26
5.3 Standards 26
6 Legal information 28

For more information, please visit: http://www.nxp.com

Date of release: 25 March 2024