MWCT20D2A / MWCT20D2

SESIP Security Target

Rev. 2.1 — 11 June 2025 **Evaluation document**

Document information

Information	Content
Keywords	SESIP Security Target, MWCT20D2A and MWCT20D2
Abstract	Security target for evaluation of the MWCT20D2A / MWCT20D2 developed and provided by NXP Semiconductors, according to SESIP Assurance Level 2 (SESIP2) based on SESIP methodology, version 1.2

Revision History

Rev.	Date	Description
0.1	21 April 2023	First draft
0.2	5 June 2023	Second draft
0.3	18 August 2023	Third draft
0.4	26 September 2023	Fourth draft
1.0	25 October 2023	1st official release
1.1	13 November 2023	Updated platform configurations Added interfaces available for ISP commands
1.2	04 December 2023	Updated Secure Boot and Secure Debugging SFRs Updated Cryptographic Random Number Generation SFR Added Field Return and Decommission SFRs Reworked claim for Trust Provisioning Fixed miscellaneous typos
1.3	15 December 2023	Removed HMAC from the scope of evaluation
1.4	10 January 2024	Updated references
1.5	05 March 2024	Correct ISP command to read out ROM version
1.6	09 April 2024	ECDSA signature generation and ECC key generation are compliant to ANSI X9.62 instead of FIPS-186-4 Remove MWCT20D2AVLHM variant from the scope Update reference to SRM
1.7	10 June 2024	Updated references to PP and guidance documents Add errata sheet for B1.0 Correct description of life cycle states including OEM_Closed and Bricked states Remove OEM_Closed_No_Return life cycle state Miscellaneous typo fixes
1.8	02 December 2024	Add B1.1 to the scope of evaluation and remove B1.0 from the scope
1.9	29 April 2024	Updated references to guidance documents for B1.1
2.0	03 June 2025	Updated the platform name
2.1	11 June 2025	Updated with a statement on B1.1 and versions of hardware and firmware components

1 Introduction

This Security Target describes the MWCT20D2A / MWCT20D2 (or MWCT20D2x for short) 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) [1].

1.1 ST Reference

MWCT20D2A / MWCT20D2, SESIP Security Target, Revision 2.1, NXP Semiconductors, 11 June 2025.

1.2 SESIP Profile Reference and Conformance Claims

Table 1. SESIP Profile Reference and Conformance Claims

Reference	Value
SP Name	SESIP Profile for WPC Qi Secure Storage Subsystem
SP Version	Version 1.0 [2] [1]
Assurance Claim	SESIP Assurance Level 2 (SESIP2)

[1] This Protection Profile was approved based on SESIP v1.1 while the platform is evaluated against SESIP v1.2. Therefore, the SFRs claimed in this Security Target are updated to be compliant with SESIP v1.2 where applicable, i.e., the updated SFRs are not weakened.

1.3 Platform Reference

Table 2. Platform Reference

Reference	Value
Platform Name	MWCT20D2A / MWCT20D2 or MWCT20D2x for short
Platform Version	B1.1 (See Table 4 for identification information of each component of the platform)
Platform Identification	MWCT20D2A and MWCT20D2
Platform Type	Digital Signal Controller (DSC) for Qi Wireless Charging also known as Secure Storage Subsystem (SSS)

1.4 Guidance Documents

The following documents are included with the platform:

Table 3. Guidance Documents

Document	Reference
Product Reference Manual	MWCT2xx2A Reference Manual [4]
Product Data Sheet	MWCT2xx2A Data Sheet [5]
User Manual	Secure Provisioning SDK (SPSDK) [3]
Security Reference Manual	MWCT20D2 Wireless Charging Controller Security Reference Manual [7]
SESIP Security Target	MWCT20D2A / MWCT20D2, SESIP Security Target, Revision 2.1, NXP Semiconductors, 11 June 2025.

1.5 Platform Overview and Description

MWCT20D2x is digital signal controller (DSC) product series possesses an efficient 32-bit 56800EX Digital Signal Processor (DSP) core, flash memory, etc. The product series devices are well suited to a wide range of applications for industrial control, motion control, home appliances, general-purpose inverters, smart sensors, fire and security systems, switched-mode power supply, power management, wireless charging, UPS, Solar inverter, and medical monitoring applications. The product series offers a broad range of memory, peripherals and performance options. Devices in this series share common peripherals and pin-out, allowing developers to migrate easily within a chip series or among other chip series to take advantage of more memory or feature integration. MWCT20D2x offers compliance to WPC requirements for support of the Qi authentication protocol version 1.3 [8]. The platform consists of two variants including MWCT20D2A and MWCT20D2 which are physically identical but for different markets with the MWCT20D2A variant being compliant to AEC-Q100 and therefore for automotive market.

For a complete description of features provided by MWCT20D2x, please refer to [4].

1.5.1 Platform Security Features

The platform MWCT20D2x provides the following security features:

- The platform implements a secure boot process such that the signature of the present firmware is verified before it can be executed. See Section 3.2.1.4.
- Platform attestation based on Qi Specification - Authentication Protocol [8] is supported. See Section 3.2.1.3.
- The platform supports for the following cryptographic functions: ECDSA using NIST P256 curve for digital signature and SHA256 cryptographic hash function. See Section 3.2.3.1. This is provided via a cryptographic module called Digital Signature Security Subystem (DSASS) and its associated DSASS library.
- The platform supports ECC key generation also using NIST P256 curve. See Section 3.2.3.2. This is also provided via DSASS hardware and its associated DSASS library.
- The platform provides a dedicated and protected memory region for cryptographic key store. See Section 3.2.3.3.
- The platform provides a physical true random number generator (TRNG) and a Hash-based deterministic random bit generator (DRBG). The TRNG is only used to seed the Hash-based DRBG. See Section 3.2.3.4. The TRNG is provided via DSASS hardware while the Hash-based DRBG is provided via DSASS library.
- The platform supports platform customer/OEM firmware update with anti-downgrading. The updated firmware shall be encrypted and signed before being programmed into the platform. See Section 3.2.2.1.
- The platform implements secure debugging via JTAG. The access to debugging functionality is under life cycle management. See Section 3.2.4.1.

1.5.2 Platform Physical Scope

The logical scope is the or MWCT20D2x for short micro-controller silicon chip including the on-chip ROM. The hardware components and interfaces are listed in Section 2.4 of [4] and Figure 1 shows the superset block diagram of the MWCT20D2x family.

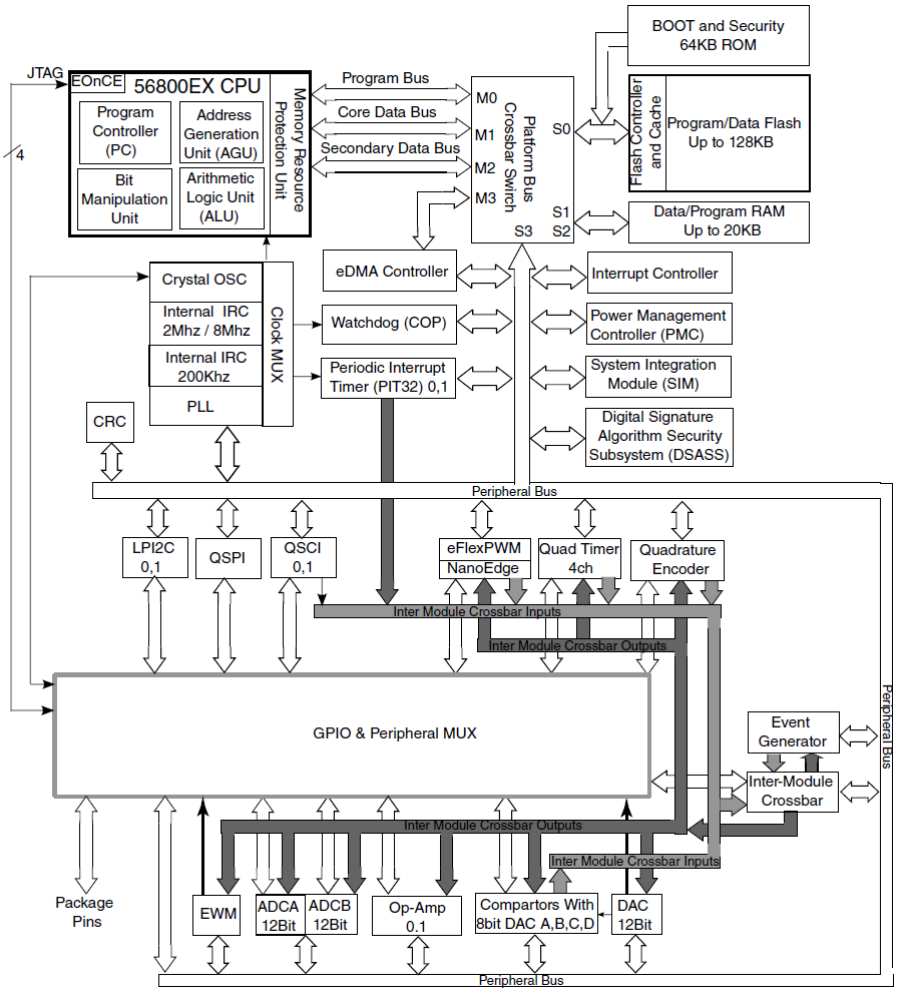

Figure 1. MWCT20D2A / MWCT20D2 Block Diagram

1.5.3 Platform Logical Scope

The platform consists of its hardware and firmware parts as shown in Figure 2. The versions of all components of the platform are as listed in Table 4. The combination of the specific hardware and firmware parts identified in Table 4 results in version B1.1 of the platform.

Any additional firmware, OS or application software stored on the platform (e.g., OEM firmware) is not in scope of this evaluation.

Table 4. Platform Deliverables

Type	Name	Release	Form of delivery
IC Hardware	MWCT20D2x	0xAB32A61D	Silicon Chip and On Chip ROM
ROM Firmware	MWCT20D2x ROM Firmware[1]	2.0.0	Software package
ROM Firmware	DSASS Library	2.0.0	Software package

[1] The ROM implements APIs that user's code can call. In addition, it is also accessible by users via so-called In System Programming (ISP) commands. The ISP commands can be sent to the platform via UART or I2C interfaces.

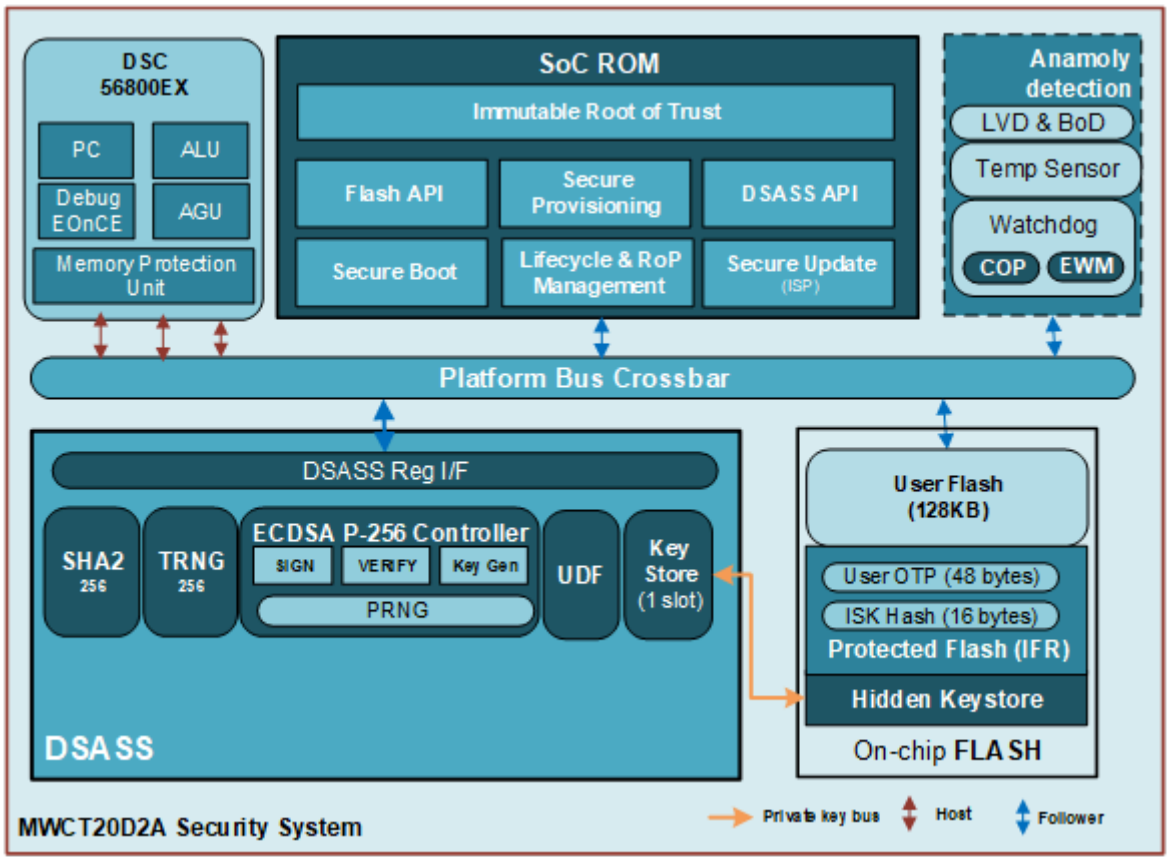

Figure 2. MWCT20D2A / MWCT20D2 Evaluation Scope

1.5.4 Required Non-Platform Hardware/Software/Firmware

MWCT20D2A / MWCT20D2 has on-chip flash, which is used to store the customer/OEM firmware image.

1.5.5 Life Cycle

The life cycle (LC) is managed by the platform, see Chapter 4 of [7] for further information. The LC states are described in Table 5:

Table 5. Life Cycle States

LC State	Description
NXP Internal	This is life cycle state used by NXP exclusively, i.e., trust provisioning.
OEM_Open	The platform is delivered to OEM for software installation and initial configuration. In this state, the accesses to ISP and debugging feature are enabled but access to testing is password protected. This is also the state for field return.
OEM_Closed	The platform is operational in the field. The access to ISP and debugging feature are configurable by the OEM and secure boot is enforced. From this state, the platform can be switched to OEM_Open state for field return (flash erase with new firmware securely loaded and/or OEM's credential required).
Bricked	The platform is not accessible anymore including all accesses to ISP, debugging and testing features. The Bricked state can be moved into from any other life cycle state.

NXP ensures secure provisioning of the NXP credentials and the initial life cycle configuration. NXP's customer (also referred as OEM) will receive the device in OEM_Open state, and shall perform software installation and

configuration and OEM credential provision in OEM_Open and then configure the device to OEM_Closed state in their technical and/or procedural secure environment. The OEM_Closed is the normal device usage state. From any state, the platform's life cycle can be moved to the Bricked state in which no access to the platform is possible any more.

2 Security Objectives for the Operational Environment

2.1 Platform Objectives for the Operational Environment

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

Table 6. 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, and it shall match the corresponding information from the guidance document.	Chapter 6 of [7]
Unique Identification during Personalization	The integrity and uniqueness of the unique identification of the platform must be provided by the platform user during the personalization stage.	Trust Provisioning Package
Secure Boot	The operating system or application code are expected to make use of the Secure Boot Mode as described in Chapter 2 of [7].	Chapter 2 of [7]
Secure Debug	The integrating environment is expected to configure the debug functionality as described in Chapter 7 of [7].	Chapter 7 of [7]
Key Management	Cryptographic keys and certificates outside of the Platform are subject to secure key management procedures.	Chapter 3 of [7]
Trusted Users	Actors in charge of platform management, for instance for signature of firmware update, are trusted.	Chapter 3 of [7]
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.	Chapter 6 of [7] and [6]
Secure Update	The operating system or application code are expected to enable secure communication for security update, and in case of update, the update image is expected to be properly signed and distributed in secure manner as well. The operating system or application code are expected to use the anti-roll back feature.	Chapter 2 of [7]
Life-cycle Management	The operating system or application code are expected to configure the LC state according the stage of product development and deployment.	Chapter 4 of [7]

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 [1].

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 hardware and firmware located in the on-chip ROM of or MWCT20D2x for short cannot be updated due to their immutable nature. The platform's Secure Boot feature further supports to verify the authenticity of customer code, providing an appropriate mechanism for supporting the update of customer code. See Section 3.2.1.4 and Section 3.2.2.1 for further information. The update mechanism beyond of the scope of this Security Target of has to be provided by the customer, and such mechanism as well as the customer code is not in scope of this evaluation.

3.2 Security Functional Requirements

In the following Security Functional Requirements, the term **platform** covers the **MWCT20D2A / MWCT20D2 physical and logical scope**, and the term **application or OEM firmware** refer to any additional firmware, OS or application software which is out of evaluation scope. It represents a part of the final connected device.

MWCT20D2A / MWCT20D2 fulfils the following security functional requirements:

3.2.1 Identification and Attestation of Platforms and Applications

3.2.1.1 Verification of Platform Identity

Requirement

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

Refinement

Assets and protections related to this SFRs are:

Table 7. Refinement Operations

Asset	Protection required
SSS module Platform Identity	Integrity

Conformance rationale

The platform identity consists of the identification of its hardware and firmware components as described in Section 1.5.3. The hardware/firmware identification and version protected in integrity can be obtained as follow:

- Hardware version can be read via GetProperty command to read SystemDeviceID property under ISP (In-System Programming) mode. The read-out value is the same of JTAG ID for the platform. See Chapter 5.5, 9.2.3 and 9.2.4 in [4].
- ROM Firmware version is readable by using GetProperty command to read TargetVersion property under ISP mode. See Chapter 5.5 in [4].
- DSASS library version can be read out by calling DSASS_GetVersion() function. See [7]

3.2.1.2 Verification of Platform Instance Identity

Requirement

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

Refinement

Assets and protections related to this SFRs are:

Table 8. Refinement Operations

Asset	Protection required
SSS module Platform Identity	Integrity

Conformance rationale

A 9-byte unique device identifier (UID) compliant to WPC Qi specification [8] is provisioned to identify the SSS module platform identity. It can be read from by executing ISP_WPC_GET_ID command in ISP (In-System Programming) mode. See [7].

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:

The platform implements an ECC-based authentication protocol for an external party (e.g., a Power Receiver) to verity the identity of the platform (i.e., acting on behalf of the Power Transmitter) that is compliant to Qi Specification - Authentication Protocol [8]. All cryptographic algorithms required by the standard including ECDSA on NIST P-256 curve, SHA-256 and random number generators are applicable and provided by the platform (see Section 3.2.3.1 and Section 3.2.3.4). The keys and certificates used in the authentication protocol are trust provisioned into the platform during the trust provisioning process (see Section 3.3).

3.2.1.4 Secure Initialization of Platform

Requirement

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 *ISP mode*.

Refinement

Assets and protections related to this SFRs are:

Table 9. Refinement Operations

Asset	Protection required
SSS module firmware	Integrity and authentication

Conformance rationale

The platform's bootloader which resides in the platform ROM, is always executed after reset and depending the current life cycle state of the platform (e.g., OEM_Closed life-cycle state), secure boot is enforced. When secure boot is enforced, the bootloader verifies the customer's public key signed by NXP by using the public key that is provisioned into the platform during manufacturing already. Once the customer's public key is verified, the bootloader verifies the signature on the present OEM firmware to confirm its authenticity and integrity. The digital signature ECDSA on NIST P-256 curve is used for signature generation and verification. If the firmware signature is successfully verified, the bootloader jumps to the OEM firmware to start its execution. If the verification fails, the platform enters ISP mode to provide the possibility for recovery via Secure Update mechanism described below. The complete secure initialization process is described in [7].

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

3.2.2.1 Secure Update of Platform

Requirement

The platform can be updated to a newer version in the field such that the integrity, authenticity and confidentiality of the platform is maintained.

Refinement

Assets and protections related to this SFRs are:

Table 10. Refinement Operations

Asset	Protection required
SSS module Firmware and Software	Integrity and Authenticity
SSS module Firmware and Software	Monotonic

Conformance rationale

Secure Update is the process used to securely update the OEM firmware image in the field. The firmware image is encrypted using XTEA-128 block cipher and signed using ECDSA P-256, following the SB3.1 firmware image format. This is so that the Secure Update process is able to guarantee the integrity and authenticity of the new image. In addition, it also ensures that the new image is up-to-date, preventing any attempt to rollback to an older image.

The platform's ROM boot loader provides the secure firmware update operation. The Secure Update process can be enabled when the platform is booted into ISP (In-System Programming) mode and the ReceiveSBFile command is available. This is possible for all life cycle states except Bricked. The anti-rollback mechanism is also enforced by the platform's ROM boot loader during the Secure Update process by verifying the version of the new image against the version of the current firmware. The keys used to verifying and decrypting the new image are trust provisioned into the platform as described in Section 3.3.

More details can be found in [7].

3.2.2.2 Field Return of Platform

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

Conformance rationale:

Field Analysis Mechanism is available as described in Chapter 4 of [7]. The life cycle state for field return analysis is OEM_Open which is the same life cycle state used for OEM software development. In order to enter OEM_Open state, the flash is erased with a new diagnosis firmware being securely loaded. In addition, OEM's credential is required depending on the specific configurations of OEM_Closed life cycle state.

3.2.2.3 Decommission of Platform

The platform can be decommissioned.

Conformance rationale

The End-of-Life security life cycle state, or Bricked state, can be used to remove a chip permanently from regular use, see Chapter 4 of [7].

In Bricked state, all debug and test ports are disabled and locked. In addition, no access to ISP commands in possible. The policy is enforced by the ROM bootloader.

3.2.3 Cryptographic Functionality

3.2.3.1 Cryptographic Operation

Requirement

The platform provides the application with *operations in Table 11* functionality with *algorithms in Table 11* as specified in *specifications in Table 11* for key lengths *described in Table 11* and modes *described in Table 11*.

Table 11. Cryptographic Operations

Operation	Algorithm	Specification	Key Lengths / Message Lengths	Modes
Hashing	SHA-256	NIST FIPS 180-4 [9]	256 bits	NA
Signature generation	ECDSA	ANSI X9.62 [13]	256 bits	NIST P256 curve
Signature verification	ECDSA	NIST FIPS 186-4 [10] and ANSI X9.62 [13]	256 bits	NIST P256 curve

Conformance rationale:

Cryptographic operations SHA-256 and ECDSA are provided by the platform's cryptographic module DSASS and the associated DSASS library. See [7].

3.2.3.2 Cryptographic Key Generation

Requirement

The platform provides the application with a way to generate cryptographic keys for use in *algorithms in Table 12* as specified in *specifications in Table 12* for key lengths *described in Table 12*

Table 12. Cryptographic Key Generation

ID	Algorithm	Specification	Key Lengths
ECC key generation	ECDSA	ANSI X9.62 [13]	256 bits

Conformance rationale

Cryptographic key generation for ECC is provided by the platform's cryptographic module DSASS and the associated DSASS library. See [7].

3.2.3.3 Cryptographic KeyStore

Requirement

The platform provides a way to store *Qi private key ECDSA-P256* such that not even the application can compromise the *authenticity, integrity, confidentiality* of this data. This data can be used for the cryptographic operations *Qi authentication support of the Power Transmitter by the Power Receiver*.

Table 13. Cryptographic KeyStore

Assets	Security Property	List of Operations
Qi private key ECDSA-P256	Authenticity, integrity and confidentiality	Qi authentication support of the Power Transmitter by the Power Receiver

Conformance rationale

The platform provides a dedicated memory region called special Indexed Flash Region (IFR) to store secret keys provisioned into the platform. Once provisioned, This special IFR is hidden in a sense that it is only accessible by hardware engine and no software is able to access this memory region. In addition, the content stored in this memory region is scrambled with obfuscation data taken from the platform's cryptographic module DSASS. The Qi private key is loaded in to the DSASS keystore for cryptographic operations (e.g., attestation) by hardware only if the image in flash is authenticated by the secure bootloader in ROM. The bootloader verifies that the image is signed by a key whose corresponding public key is signed by NXP. The NXP public key is provisioned into the platform during manufacturing already.

See [7] for further details.

3.2.3.4 Cryptographic Random Number Generation

The platform provides a way based on an entropy source as described below to generate random numbers to as specified in NIST SP800-90A in the following list: *Hash-DRBG (SHA-256)*.

Entropy source details: source that accumulates entropy from *a True Random Number Generator (SA-TRNG)* with a minimum of *256 bits* of entropy. The entropy source SA-TRNG adheres to NIST 800-90B.

Conformance rationale:

The platform provides a physical true random number generator (TRNG) as part of the DSASS cryptographic module. The TRNG is compliant to NIST SP800-90B as specified in [12].

In addition, the platform also provides a Hash-based DRBG module as defined in NIST SP800-90A [11] via the DSASS library which makes use of SHA-256 engine in the DSASS cryptographic module. The DRBG is seeded with the TRNG mentioned above.

The two random number generators are available for users via API functions described in [7].

3.2.4 Compliance Functionality

3.2.4.1 Secure Debugging

Requirement

The platform only provides *JTAG interface* authenticated as specified in *Chapter 6 of [7]* with debug functionality.

The platform ensures that all data stored by the application, with the exception of *none* is made unavailable.

Refinement

All assets defined in other Security Functional Requirements and accessible through the Secure Debugging mechanism shall be protected against unauthorized access.

Conformance rationale

JTAG debugging functionality can be only accessed by if it is allowed by the platform's life cycle state (see [7]) and in addition, a valid credential is required. When the platform is in the field, e.g., the life cycle state is OEM_Closed_No_Return, or Bricked, debugging feature is completely disabled and no access to debugging functionality is possible.

See [7] for further details.

3.2.5 Limited Physical Attacker Resistance

The platform detects or prevents attacks by an attacker with physical access before the attacker compromises the requirements claimed as part of the SFR Cryptographic Operation.

Conformance rationale:

Countermeasures are implemented to within the platform's cryptographic module DSASS to protect against fault-injection attacks and side-channel analysis for the ECDSA signature generation and verification operations described in Section 3.2.3.1.

3.3 Trust Provisioning Package

Requirement

The Trust Provisioning system ensures the secure management in a trusted environment of Qi Authentication keys and its loading into the platform for the following use cases: Authentication compliant with Qi Authentication.

Both the trusted environment and the platform protect access, confidentiality, integrity of provisioned data.

Conformance rationale

The trust provisioning process is handled by NXP within its ISO27001 facilities. The platform shall be in a life cycle state exclusively used for NXP during the trust provisioning process. A special firmware is downloaded into the platform and is in charge of generating an ECC key pair. The secret portion of the provisioned key pair is further protected by the platform itself as described in Section 3.2.3.3. The trust provisioning data including the platform's UUID and its device-unique public key generated above are uploaded into NXP's trust provisioning back-end server which is also located within NXP's secure premise. The back-end server shall perform uniqueness test of trust provisioning data as required by [2].

For more information, please refer to Chapter 3.2 of [7].

4 Mapping and Sufficiency Rationales

4.1 SESIP2 Sufficiency

Table 14. 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 Section 1.1, the TOE reference in Section 1.3, the TOE overview and description in Section 1.5.
	ASE_OBJ.1 Security requirements for the operational environment	Section 2	The objectives for the operational environment in Section 2 refer to the guidance documents.
	ASE_REQ.3 Listed security requirements	Section 3	All SFRs in this ST are taken from [1]. 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	Section 3	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 1.4	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	Section 1.4	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
	AGD_PRE.1 Preparative procedures	Section 1.4	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.

5 Bibliography

5.1 Evaluation Documents

[1] GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2, GP_FST_070.

[2] GlobalPlatform Technology SESIP Profile for WPC Qi Secure Storage Subsystem, Version 1.0, Version 1.0, GPT_SPE_153, May 2024.

5.2 Developer Documents

[3] Secure Provisioning SDK (SPSDK), Rev. 2.0.1, NXP Semiconductors, https://spsdk.readthedocs.io/en/2.0.1/.

[4] MWCT2xx2A Reference Manual, Rev. 3, NXP Semiconductors, April 2025.

[5] MWCT2xx2A Data Sheet, Rev. 2.2, NXP Semiconductors, April 2025.

[6] Getting Started with MCUXpresso SDK for MC56F81000-EVK ,Rev. 3, NXP Semiconductors, 25 December 2023.

[7] MWCT20D2 Wireless Charging Controller Security Reference Manual, Rev. 3, NXP Semiconductors, 24 April 2025.

5.3 Standards

[8] Qi Specification, rev 1.3, Wireless Power Consortium.

[9] FIPS PUB 180-4: Secure Hash Standard (SHS), Federal Information Processing Standards Publication, Information Technology Laboratory, National Institute of Standards and Technology, August 2015.

[10] FIPS PUB 186-4: Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, US Department of Commerce/National Institute of Standards and Technology, July 2013.

[11] NIST SP 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, National Institute of Standards and Technology, January 2012.

[12] NIST SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation, National Institute of Standards and Technology, January 2018.

[13] ANSI X9.62-2005: Public Key Cryptography for the Financial Services Industry: the Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standards Institute (ANSI), 2005.

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

Figures

Contents

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

Date of release: 11 June 2025