Security Target for

W77Q[64/128]J[V/L] Secure Flash Memory

Version 1.0,

dated 2024-04-16.

Winbond Electronics Corporation

Version Control

Version	Date	Description
0.7	*2023-10-18*	*First release*
0.8	*2023-11-23*	*Updated release*
0.9	*2024-01-15*	*Evaluation Candidate*
1.0	*2024-04-16*	*Official version*

Table of Contents

1 Introduction

The Security Target describes:

- The Platform (in this Section),
- The objectives for the operational environment (in Section 2), that are required for Platform to fulfill its security requirements.
- The exact security properties of the Platform (in Section 3), as evaluated against [GP-SESIP] and [17927].
- The Security Target claims conformance to "SESIP profile for Secure External Memories" as defined in [GP-SPE] and "SESIP Profile for PSA Certified™ RoT Component Level 2" as defined in [PSA-Com-L2].
- Claimed assurance level is SESIP2.

1.1 ST Reference

See the Title page

1.2 Platform Reference

Platform Name	*SpiFlash® TrustME™ Secure Flash Memory*
Platform Version	B
Platform Identification	W77Q[64/128]J[V/L]
Platform Type	Secure External Memory

1.3 Included Guidance Documents

Reference	**Name**	**Version**
[Datasheet]	*W77Q128JV/W77Q64JV Secure Serial NOR Flash Memory Datasheet*	*Version A8*
[Datasheet2]	*W77Q128JL/W77Q64JL Secure Serial NOR Flash Memory Datasheet*	*Version A1*
[FSP]	*W77Q Secure Serial NOR Flash Memory, Functional Specifications, Winbond*	*Version A*
[OPE]	*W77Q128JV/W77Q64JV/W77Q128JL/ W77Q64JL Secure Flash Operational User Guidance*	*Version A3*
[PRE]	*W77Q128JV/W77Q64JV/W77Q128JL/W77Q64JL Secure Flash Preparative User Guide*	*Version A3*
[SA]	*W77Q128/W77Q64 Secure Serial NOR Flash Memory Security Manual*	*Version E1*

1.4 Platform Functional Overview and Description

Platform Type

The Platform is a secure external memory chip.

Platform Description

The Platform is an external memory Flash IC dedicated to be embedded into systems that need protection of their memory contents. In particular, the Platform is dedicated to the secure storage of the code and data for IoT applications.

Level of Compliance

The platform selects the level of compliance "**Augmented Memory**" defined in [GP-SPE].

REQUIREMENT	FULFILLMENT	COMMENT
Communicated data confidentiality protection	Yes	Data encryption for read and write commands issued for protected data
Authenticity and integrity protection	Yes	Replay-protected signature on write commands issued for protected data
Access control: authenticated User	Yes	User Authentication for allowing read access to protected data, e.g., by establishing a secure channel with mutual authentication
SESIP2	Yes	Platform evaluated per SESIP2

Usage and Major Security Features

- ***Secure separation*** between *Test mode* and *User mode*. More precisely, Test mode entry is cryptographically protected – an unauthorized switch from User mode to Test mode erases all protected user data and all TSF data;
- Protection against **leakage and physical** attacks;
- ***Confidentiality, authenticity*** and ***integrity*** of Secret User Data;
- ***Authenticity*** and ***integrity*** of Authenticated User Data;
- ***Integrity protection*** of the flash content by error detection codes (CRC-32) and SHA2-256b (64b) - for authenticity protection;
- Memory **Rollback** protection, **Reliable Index** and **Clone Replace Protection;**
- ***Secure Communication Channel*** with the host device and a remote operator. Encrypted, authenticated, replay protected;
- ***Memory Access Control*** of the flash content by implementing an access control

policy with different levels of authorization, typically:

- Integrity Protection
- Write Protection
- Rollback Protection
- Plain Access Read
- Plain Access Write/Erase
- Plain Access for Authenticated User

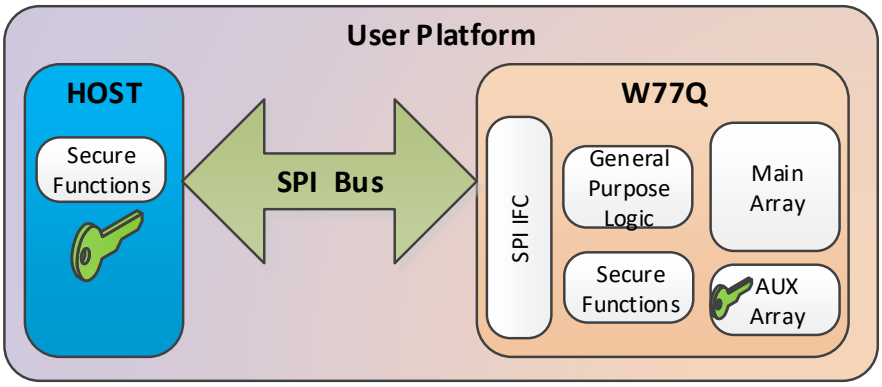
- Protection of the **secure boot of the Host and secure update** process by Rollback protected, atomic, authenticity protection;
- Secure Key-Provisioning Mechanism.

Required Hardware/Software/Firmware

The Platform is a secure component to be embedded with the Host to perform the task of data and code storage in a secure manner.

Platform Logical Scope

The platform logical scope is depicted in the following diagram.



The Platform includes the W77Q[64/128]J[V/L] device only. In particular, the Platform does not comprise the following:

- The Host that will embed the Platform and will be needed to run the Platform in order to stimulate the TSF
- SPI Bus for the communication between the Host device and the Platform

The contents of the memory array, namely, the Host code and data, are not delivered with the Platform. Still, they are within the boundaries of the Platform, insomuch that it provides

associated security services, namely the Host Boot code integrity protection and secure code update process.

Platform Physical Characteristics

- Performance:
  - Up to 133 MHz Standard/Quad SPI clocks (STR mode)
  - Up to 66 MHz Standard/Quad SPI clocks (DTR mode)
  - Up to 66 MB/s continuous data transfer rate (plain text)
  - Up to 6 MB/s encrypted and authenticated data transfer rate
- Endurance:
  - More than 100,000 erase/program cycles
  - More than 20-year data retention
- Operating conditions:
  - Single 2.7-3.6V power supply (V version) or single 2.5-3.6V power supply (L version)
  - -40°C to +85°C or 105°C operating range

Platform Physical Scope

The Platform consists of:

- HW IC Part number (see Section 1.2) delivered in known good die and assembled forms, via Courier.
- The associated IC documentation (see section 1.3) delivered in PDF, via e-mail.

The table below lists possible forms of the delivery. The difference between these forms is only in packaging. The silicon is the same in all cases.

NO	TYPE	IDENTIFIER	PART NUMBER	DELIVERY METHOD
FORM OF DELIVERY : KNOWN GOOD DIE FORM				
1	HW	IC Part number	W77Q64J[V/L]W	Via Courier
2	HW	IC Part number	W77Q128J[V/L]W	Via Courier
FORM OF DELIVERY : KNOWN GOOD DIE REDISTRIBUTION LAYER (RDL) FORM				
1	HW	IC Part number	W77Q64J[V/L]R	Via Courier
2	HW	IC Part number	W77Q128J[V/L]R	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN SOP16 300MIL (THICKNESS 2.64 MM)				
1	HW	IC Part number	W77Q64J[V/L]SF	Via Courier
2	HW	IC Part number	W77Q128J[V/L]F	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN SOP8 208 MIL (THICKNESS 2.16MM)				
1	HW	IC Part number	W77Q64J[V/L]SS	Via Courier
2	HW	IC Part number	W77Q128J[V/L]S	Via Courier

NO	TYPE	IDENTIFIER	PART NUMBER	DELIVERY METHOD
FORM OF DELIVERY : ASSEMBLED DEVICE IN VSOP8 208 MIL (THICKNESS 1.0MM)				
1	HW	IC Part number	W77Q64J[V/L]ST	Via Courier
2	HW	IC Part number	W77Q128J[V/L]T	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN WSON8 6X5 (THICKNESS 0.8 MM)				
1	HW	IC Part number	W77Q64J[V/L]ZP	Via Courier
2	HW	IC Part number	W77Q128J[V/L]P	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN TFBGA24 8X6 (5X5-1 BALL ARRAY)				
1	HW	IC Part number	W77Q64J[V/L]TB	Via Courier
2	HW	IC Part number	W77Q128J[V/L]B	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN TFBGA24 8X6 (6X4 BALL ARRAY)				
1	HW	IC Part number	W77Q64J[V/L]TC	Via Courier
2	HW	IC Part number	W77Q128J[V/L]C	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN 12-BALL WLCSP (THICKNESS 0.54 MM)				
1	HW	IC Part number	W77Q64J[V/L]BY	Via Courier
2	HW	IC Part number	W77Q128J[V/L]Y	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN 12-BALL WLCSP (THICKNESS 0.5 MM)				
1	HW	IC Part number	W77Q64J[V/L]BJ	Via Courier
2	HW	IC Part number	W77Q128J[V/L]J	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN 12-BALL WLCSP (THICKNESS 0.5 MM)				
1	HW	IC Part number	W77Q64J[V/L]BK	Via Courier
2	HW	IC Part number	W77Q128J[V/L]K	Via Courier

FORM OF DELIVERY: ASSOCIATED IC DEDICATED DOCUMENTATION				
1	PDF	Operational User Guidance [8]	Version A3	Mail
2	PDF	Preparative Procedure [9]	Version A3	Mail
3	PDF	Security Manual [10]	Version E1	Mail
4	PDF	Datasheet [7]	Version A8	Mail
5	PDF	Datasheet2 [8]	Version A1	Mail

2 Security Objectives for the Operational Environment

For the Platform to fulfill its security requirements, the operational environment (technical or procedural) shall aim for the Security Objectives described in this section.

2.1 Compliance to the Protection Profile

According to the Protection Profile [GP-SPE], the operational environment must fulfil the following objectives:

- The application shall verify the correct version of all platform components it depends on
  Reference: This objective must be fulfilled as described in [PRE] Section 3.2.
- The application shall support the invocation of an update mechanism, if such mechanism exists in the platform.
  Reference: This objective is further expounded in Section 2.7
- The application shall implement the secure channel defined in "Secure Communication Enforcement" by implementing the protocol mentioned, including detection of failed authenticity and integrity check.
  Reference: This objective is further expounded in Section 2.4
- The application shall store data to be protected for authenticity, integrity, or confidentiality in the area that is indeed protected for authenticity/integrity/confidentiality.
  Reference: This objective must be fulfilled as described in [OPE] Section 2.4.
- The application shall where relevant implement a freshness/anti-rollback protection using a "Reliable Index" provided by the platform
  Reference: This objective is not relevant here, since the freshness and anti-rollback protection is done by the Platform, not by an application. Reference to [OPE] section 2.2.1.

According to the Protection Profile [PSA-Com-L2], the operational environment must fulfill the following objectives for the operational environment:

- KEY_MANAGEMENT: Cryptographic keys and certificates outside of the platform are subject to secure key management procedures.
  Reference: This objective is described in Section 3.4.2 and 3.4.3 in [PRE].
- TRUSTED_USERS: Actors in charge of platform management, for instance for signature of firmware update, are trusted.
  Reference: This objective is described in Section 1.1 in [PRE] and Section 1.1 in [OPE].
- UNIQUE_ID: The integrity and uniqueness of the unique identification of the platform must be provided by the platform user during the personalization stage.
  Reference: This objective is described in Section 3.4.4 in [PRE] and Section 2.3 in [OPE].

2.2 Generation of device's Individual Identifier

Before a Platform instantiation is used, it shall be allotted with its own unique ID.

The device is provided by Winbond with a pre-programmed ID, namely the 64-bit Winbond ID (WID), that is unique per device. In addition, the device can be programmed with a customer-specific ID, as described in [OPE] Section 2.3

2.3 Protection of the Platform Keys

Security procedures shall be used by the Platform User to maintain the confidentiality and the integrity of the Platform keys, as described in [PRE] Section 3.4. Namely:

- The keys shall be generated with the required amount of entropy.
- The provisioning of the Device Master Key shall be done in a secure environment where the communication with the Platform is protected from eavesdropping.

Note: Provisioning of all other keys is protected by the Platform based on the confidentiality of the Device Master Key.

- Keys stored in the authorized Host and shared with the Platform shall be protected by the Host.
- Keys stored at the authorized remote operator and shared with the Platform shall be protected by the operator.

2.4 Secure Communication with the Platform

The authorized user shall support the trusted communication channel with the Platform protecting the confidentiality, integrity, and freshness of the transmitted data, as described in [OPE] Section 2.2.

Notes:

- In order to protect the data, its storage location shall be configured as the Secure Storage, as described in [OPE] Section 2.4.1. This prevents any access to it except through the Secure Communication channel
- Data freshness means that the stored and transmitted data is always the one resulting in the last change carried out by the authorized user on the Platform.

2.5 Secret User Data Encryption

The Host shall encrypt secret User Data stored on the platform according to the chosen encryption standard with a platform-unique key of the desired length, as described in [OPE] Section 2.4.

2.6 Boot protected by Platform

The Host shall boot from code stored on the Platform in a dedicated *authenticated and integrity-protected* memory section, as described in [OPE] Section 2.5.

2.7 Genuine Software Update

The Host update of the code stored on the Platform shall be carried out by an authorized remote operator using the protective mechanisms of the Platform, as described in [OPE] Section 2.6.

Note: The secure Software Update shall be delivered in encrypted and genuine protected form by the authorized issuer together with its security attributes.

3 Security Requirements and Implementation

The claimed assurance and functional requirements package is **SESIP2** as defined in [GP-SESIP] and [17927].

PP conformance claim: [GP-SPE] and [PSA-Com-L2].
Note that SFRs in [GP-SPE] were modified as necessary to conform to [GP-SESIP] and [17927].

3.1 Security Assurance Requirements

3.1.1 Complete functional specification (ADV_FSP.4)

In accordance with the requirement for a complete functional specification (ADV_FSP.4) the developer has provided the document [FSP], where the entire TSF is represented (full set of SFRs) and the SFRs are traced to the TSFIs. Moreover, related to each TSFI, the following information is given:

- Identification and description of all parameters
- Description of purpose and method of use
- Description of actions
- Description of error messages that may result from an invocation of the TSFI

3.1.2 Operational user guidance (AGD_OPE.1)

In accordance with the requirement for an operational user guidance (AGD_OPE.1), the developer provided the operational user guidance [OPE] for the Platform. This guidance includes the following information:

- The user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
- How to use the available interfaces provided by the Platform in a secure manner.
- Available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
- Security-relevant events.
- Modes of operation of the Platform (TEST mode and USER mode).
- Security rules to be followed in order to fulfil the security objectives for the operational environment.

3.1.3 Preparative procedures (AGD_PRE.1)

In accordance with the requirement for preparative procedures (AGD_PRE.1), the developer provided the Preparative User Guides [PRE] for the Platform. This guide includes the following information:

- Necessary steps for secure acceptance of the delivered Platform in accordance with the developer's delivery procedures.

- Necessary steps for secure installation of the Platform and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment.

3.1.4 Flaw Reporting Procedure (ALC_FLR.2)

Due to the Platform type (Memory Flash IC), and due to the fact that the Platform is a platform part with no software (no OS and no application), the SFR “Secure update of platform” is not applicable, since updates to the Platform are not possible, only replacement of the Memory Flash IC.

In accordance with the requirement for a flaw reporting procedure (ALC_FLR.2), the developer has defined procedures described in [FLR] covering the following points:

- Reporting
- Evaluation.
- Solution.
- Communication.

Whenever a third party detects an issue, it is expected that the third party will contact the composite product vendor and this will further notify Winbond through the URL: https://www.winbond.com/hq/support/technical-support/?__locale=en.

3.1.5 Independent testing: conformance (ATE_IND.1)

In accordance with the requirement for Independent testing conformance (ATE_IND.1), the developer provides the Platform, the experimental set-up and the related documentation [ATE] for testing.

3.1.6 Vulnerability Analysis (AVA_VAN.2)

In accordance with the requirement for a Vulnerability Analysis (AVA_VAN.2), the developer provides the Platform and the necessary experimental set-up for testing.

3.2 Security Functional Requirements

The platform fulfills the security functional requirements as described in this Section.

Requirements mandated by [62443-4-2] and [NIST-8259A] are identified in the description of each SFR as **refinements in bold**. Also, the TSS descriptions describe which portions of how the SFRs are met and how the IEC62443-4-2/ NIST-8259A requirements are satisfied are *identified in italics*.

3.2.1 Verification of Platform Identity

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

Conformance rationale:

- The platform package top marking contains a label indicating the identity and correct version of the platform.
- There is also a die marking on the die indicating the correct die version.
- Refer to secure acceptance procedure described in [PRE] Section 2 for more details.

Implementation is assessed by functional testing and 3rd party lab evaluation.

3.2.2 Verification of Platform Instance Identity

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

Conformance rationale:

- Each device (i.e., a specific instantiation of the platform) is provided to the customer with a pre-programmed globally unique 64-bit Winbond ID (WID).
- In addition, the device can be programmed with a customer-specific 128 bit ID (SUID) via SET_SUID command, as specified in [SA] Section 5.3.4.
- The IDs can be read off the device by GET_WID and GET_SUID commands respectively, as specified in [SA] Section 5.2.1 and 5.2.2, *thus satisfying DI, DI2.*

Implementation is assessed by functional testing and 3rd party lab evaluation.

3.2.3 Attestation of Platform Genuineness

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

Conformance rationale:

- The WID is configured during production phase, in a secure environment. The environment protects against WID manipulation and cloning.
- The SUID is configured by the User via secure sessions described in [PRE], Section 3.4.4.
- To attest the Platform and the Platform Instance Identity, the user has to read from the Platform a signed copy of WID or SUID as described in [OPE], Section 2.3

Implementation is assessed by functional testing and 3rd party lab evaluation. The production environment is evaluated and certified against ISO/IEC 27001 standard.

~~3.2.4 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.~~

3.2.5 Secure Update of Application

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

Conformance rationale:

The Platform stores the code and data for the Host device and provides the Secure Code Update mechanism with rollback protection, as specified in [SA] Section 3.6.2.

Implementation is assessed by functional testing and 3rd party lab evaluation.

3.2.6 Secure Communication Enforcement

The platform ensures that the communication with the Secure Storage of **the platform** can only be done over the secure communication channel(s) supported by the platform using **the protocols described in the SFR "Secure Communication Support" for data requested to be protected for confidentiality, integrity, or authenticity**.

Conformance rationale:

After a memory section is configured as the Secure Storage, as described in [OPE] Section 2.4.1, the User is needs to open a session in order to communicate with the Platform. By opening the session, secure communication channel is established that protects the confidentiality, integrity, or authenticity of the transmitted data. See more in [OPE] Section 2.2.2 and [SA] Section 4.2.

The memory is split into eight sections and the limits of each section as well as its security attributes are defined in the TOE Metadata (Global Memory Configuration, Global Mapping Table, and Section Configuration Registers).

The protected User Data is defined as one of the following (or a combination of both):

- **Secret User Data** – Data (including executable codes) stored in the section of the Flash array that are defined as protected in terms of data confidentiality.
- **Authenticated User Data** – Data (including executable codes) stored in the section of the Flash array that are defined as protected in terms of data integrity and authentication.

Any plain data access is prevented to the section that contain the protected User Data.

Implementation is assessed by functional testing and 3rd party lab evaluation.

3.2.7 Secure Communication Support

The platform provides the application with one or more secure communication channel(s).

The secure communication channel authenticates **the application and platform** and protects against **disclosure, modification, replay, and impersonation** of messages between the endpoints, using **the secure SPI bus commands (I/F commands) and the following security measures:**

- A fresh session key is used for each session in a way that provides mutual authentication at both ends of the communication channel.
- In order to avoid key repetition, the TOE implements non-repetitive counters, namely a non-volatile Session Counter and a Transaction Counter, see Section 3.2.13
- The transmitted data (in both directions) and the command address are encrypted and signed.
    - The encryption key is generated for each transaction from the Session Key and the Transaction Counter to prevent replay attacks.
    - The signature is a calculated as a MAC tag with a combination of the Session Key and the Transaction Counter to prevent replay attacks.

Conformance rationale:

Most commonly, the following subjects interact with the TOE:

- The *Host that* embeds the TOE and communicates with it through the SPI Bus.
- An authorized *Remote Operator*, that communicates with the TOE with the Host passing the commands through.

There are two Section Master Keys are associated with each memory Section, that allow two logical communication channels for each Section with different access rights. Although the communication between the TOE and the Remote Operator is done through the same SPI bus, the logical channel separation (i.e., the different keys for different channels) guarantee the security of the communication even if the Host is compromised.

The confidentiality and the integrity of the communication is protected with the Session Key derived from the corresponding Master Key for each type of the logical communication channel, as described in [SA] Section 4.7.

Implementation is assessed by functional testing and 3rd party lab evaluation.

3.2.8 Physical Attacker Resistance

The platform detects or prevents attacks by an attacker with physical access before the attacker compromises any of the other functional requirements.

Conformance rationale:

To protect against physical manipulation, the Platform includes the following security mechanisms:

- The bus connecting the Flash array and the Platform internal HW logic is hidden by layers of HW logic.
- The checksum fields (CRC32) protect the stored keys, configuration information and the registers. When violation is detected, access is blocked, key usage is prevented, and status indication is raised.

Session Key is "salted" with Transaction Counter (TC) to (see [SA] Section 3.2.2) protect the TOE against the inherent or intentional leak of the keys used in TOE operations.

Implementation is assessed by functional testing and 3rd party lab evaluation.

3.2.9 Cryptographic Keystore

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

Conformance rationale:

The following keys and TOE Metadata fields are protected by the Platform:

- *Device Master Key* – used for secure key provisioning and memory configuration, protected in terms of integrity and confidentiality
- *Per-Section Keys* – used to access the section's data and its security functions, protected in terms of integrity and confidentiality*:*
    - *restricted Section Master Keys (read-only Section access)*
    - *non-restricted Section Master Keys (full Section access)*

  The *Per-Section Keys* are provisioned via a secure channel protected by the *Device Master Key* and cannot be modified without knowing this key.
- *TOE Metadata* protected in terms of integrity (namely, they cannot be changed without knowing the corresponding Master Key):
    - Winbond Device ID

  - Secure Unique Device ID
  - Global Memory Configuration
  - Global Mapping Table
  - Section Configuration Registers
- *Monotonic Counter* – used for replay protection, protected in terms of integrity (namely, it changes only in one direction – always incremented)
- The Keystore memory is not addressable by Read, Write and Erase commands. It can be updated only through the cryptographically protected Key Provisioning, as described in [PRE] Section 3.4.1.

Implementation is assessed by functional testing and 3rd party lab evaluation.

3.2.10 Secure Trusted Storage

The platform ensures that all user data stored, except for **non-Authenticated User data**, is protected to ensure its integrity, authenticity, and binding to the Platform instance.

Conformance rationale:

The Authenticated User Data is defined in the conformance rationale subsection of Secure Communication Enforcement. Any command modifying the content of a Section with Authenticated User Data shall be properly signed by a key derived from the Master Key, which is bound to the platform WID, of this Section.

Implementation is assessed by functional testing and 3rd party lab evaluation.

3.2.11 Secure Confidential Storage

The platform ensures that all data stored by the application, except for **non-Secret User data**, is protected to ensure its confidentiality, integrity, authenticity, and binding to the platform instance.

Conformance rationale:

The Secret User Data is defined in the conformance rationale subsection of Secure Communication Enforcement. The secret data may be accessed only by a Secure Read command that reads it encrypted by a key derived from the Master Key, which is bound to the platform WID, of this section.

Implementation is assessed by functional testing and 3rd party lab evaluation.

3.2.12 Residual Information Purging

The platform ensures that **user data, configurations and keys**, with the exception of **None**, is erased using the method specified in **the NIST Special Publication 800-88 [NIST-800-88]** before the memory is used by the platform or application again and before an attacker can access it.

Conformance rationale:

According to [NIST-800-88], Appendix A, Table A-8: "Flash Memory-Based Storage Device Sanitization", the guidance to clear the contents of Embedded Flash Memory on Boards and Devices is: "If supported by the device, reset the state to original factory settings."

- Upon entering the Test Mode, the platform uses the formatting procedure that resets the state of the memory array to the original factory settings, as described in [FSP], Section 3.5.2.3.
- This formatting is skipped only if user sets the Fault Analysis Mode entry flag in a cryptographically protected user register, as described in [FSP], Section 3.5.2.3. This flag should be set only after user has removed any sensitive information stored on the device.

Implementation is assessed by functional testing and 3rd party lab evaluation.

3.2.13 Reliable Index

The platform implements a strictly increasing function.
Conformance rationale:

- The platform implements a 64-bit Monotonic Counter mechanism described in [SA] Section 3.2.1. The counter is used in key derivation and signature calculation in a way that protects the secure communication from replay attacks.
- In addition, the Platform ensures that the version tag for the new stored data version in secure update is increasing. This ensures rollback protection for secure code updates.

Implementation is assessed by functional testing and 3rd party lab evaluation.

3.2.14 Secure Initialization of Platform

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

Conformance rationale:

The security initialization process verifies the integrity and the authenticity of the TSF data (described in Section 3.2.9, Cryptographic Keystore) that describes the memory partition, per-section memory access policies, and the keys. This approach mitigates the threat of physical manipulation of the TOE.

When an error is detected during the initialization process before the working State is reached, the TOE becomes locked. The user must enter Test Mode to resume regular initialization.

In addition, the Platform initialization contributes to the secure initialization of the system insomuch that it verifies the integrity and authenticity of the Authenticated User data, in particular the Boot code, prior to providing access to it, as described in [SA], Section 3.6.3

Implementation is assessed by functional testing and 3rd party lab evaluation.

4 Mapping and sufficiency rationales

4.1 SESIP2 sufficiency

Assurance Class	Assurance Families	Covered by	Rational
ASE: Security Target evaluation	*ASE_INT.1 ST Introduction*	Section "Introduction" and title page	The ST reference is in the Title, the Platform reference in the "Platform Reference", the Platform overview and description in "Platform Functional Overview and Description".
	ASE_OBJ.1 Security requirements for the operational environment	Section "Security Objectives for the Operational Environment"	The objectives for the operational environment are described in the "Security Objectives for the Operational Environment" Section. Thereby the references to the guidance documents where these objectives are addressed are provided
	ASE_REQ.3 Listed Security requirements	Section "Security Functional Requirements" and "Security Process Package"	The relevant SFRs/SPPs are taken from [GP-SESIP], [17927], [PSA-Com-L2] and [GP-SPE]. "~~Secure update of platform~~" not included (justification in ALC_FLR.2)
	ASE_TSS.1 Platform Summary Specification	Section "Security Requirements and Implementation"	All SFRs are listed per definition, and for each SFR the implementation and verification are defined in "Security Functional Requirements" Section.
ADV: Development	*ADV_FSP.4 Complete functional specification*	[FSP]	The [FSP] document precisely specifies all the platform's interfaces with a sufficient level of details, including direct error messages
AGD: Guidance documents	*AGD_OPE.1 Operational user guidance*	[OPE]	The [OPE] document provides a description of secure operation of the Platform and security rules to fulfil with security objectives for the operational environment.

	AGD_PRE.1 Preparative procedures	[PRE]	The [PRE] document provides a description of secure acceptance procedures and installation.
ALC: Life-cycle support	*ALC_FLR.2 Flaw reporting procedures*	[FLR]	The [FLR] document provides the flaw reporting and remediation procedure Since updates to the Platform are not possible, the SFR "Secure update of platform" is removed.
ATE: Tests	*ATE_IND.1 Independent testing: conformance*	[ATE]	The [ATE] document provides evidence of testing. The Platform, the experimental set-up and the test plan has been delivered for the laboratory independent testing.
AVA: Vulnerability assessment	*AVA_VAN.2 Vulnerability analysis*	N.A.	All delivered documentation, Platform and experimental set-up are the input for the vulnerability analysis to be performed by the laboratory.

4.2 IEC62443-4-2 Mapping

The IEC62443-4-2 Sufficiency Mapping has been organized in the following way:

• W77Q64/128 as a subcomponent, fulfils subset of IEC62443-4-2 requirements;

• W77Q64/128 provides services which support the overall component fulfilling IEC62443-4-2 requirements.

4.2.1 Sufficiency of Subset of IEC62443-4-2 Requirements

W77Q, as a subcomponent of a targeted IACS component, fulfills subset of the IEC62443-4-2 requirements, which provides support for the component.

Note that W77Q is not targeted as a standalone device and therefore not targeted to comply with the whole set of IEC62443-4-2. The applicable requirements and the mapping of SFR is provided to Table 1.

IEC62443-4-2 requires component developed and supported following the secure product development process described in IEC 62443-4-1.

Requirement	**Description**	**SL-C**				**Covered by**	**Refinement**
		1	**2**	**3**	**4**		
CCSC 4	Software development process: IEC62443-4-1 Compliance	x	x	x	x	Security Assurance Requirements (general)	

Requirement	Description	SL-C				Covered by	Refinement
		1	2	3	4		
CR 1.1	Human user identification and authentication	x	x	x	x	Cryptographic Keystore	*TOE Metadata* protected in terms of integrity (namely, they cannot be changed without knowing the corresponding Master Key): • Winbond Device ID • Secure Unique Device ID • Global Memory Configuration • Global Mapping Table • Section Configuration Registers
CR 1.1 (1)	Unique identification and authentication		x	x	x	Cryptographic Keystore	*TOE Metadata* protected in terms of integrity (namely, they cannot be changed without knowing the corresponding Master Key): • Winbond Device ID • Secure Unique Device ID • Global Memory Configuration • Global Mapping Table • Section Configuration Registers
CR 1.1 (2)	Multifactor authentication for all interfaces			x	x	Cryptographic Keystore	
CR 1.2	Software process and		x	x	x	Verification of Platform	

Requirement	Description	SL-C				Covered by	Refinement
		1	2	3	4		
	device identification					Identity & Attestation of Platform Genuineness	
CR 1.2 (1)	Unique identification and authentication			x	x	Verification of Platform Instance Identity & Attestation of Platform Genuineness	
CR 1.3	Account management	x	x	x	x	Cryptographic Keystore	*TOE Metadata* protected in terms of integrity (namely, they cannot be changed without knowing the corresponding Master Key): • Winbond Device ID • Secure Unique Device ID • Global Memory Configuration • Global Mapping Table • Section Configuration Registers
CR 1.4	Identifier management	x	x	x	x	Cryptographic Keystore	*TOE Metadata* protected in terms of integrity (namely, they cannot be changed without knowing the corresponding Master Key): • Winbond Device ID • Secure Unique Device ID

Requirement	Description	SL-C				Covered by	Refinement
		1	2	3	4		
							• Global Memory Configuration • Global Mapping Table Section Configuration Registers
CR 1.5	Authenticator management	x	x	x	x	Cryptographic Keystore	The *Per-Section Keys* are provisioned via a secure channel protected by the *Device Master Key* and cannot be modified without knowing this key.
CR 1.5 (1)	Hardware security for authenticators			x	x	Cryptographic Keystore Physical Attacker Resistance	
NDR 1.6	Wireless access management	x	x	x	x	Verification of Platform Identity & Attestation of Platform Genuineness	
NDR 1.6 (1)	Unique identification and authentication		x	x	x	Verification of Platform Instance Identity & Attestation of Platform Genuineness	
CR 1.9	Strength of public key-based authentication		x	x	x	Secure Communication Enforcement	
CR 1.9 (1)	Hardware security for public key based authentication		x	x	x	Secure Communication Enforcement	
CR 1.10	Authenticator feedback	x	x	x	x	Secure Communication Enforcement	Any plain data access is prevented to the section that contain the protected User Data
CR 1.11	Unsuccessful login attempts	x	x	x	x	Secure Communication Enforcement	**Authenticated User Data** – Data (including executable codes) stored in the section of the Flash array that are defined as protected in terms of data

Requirement	Description	SL-C				Covered by	Refinement
		1	2	3	4		
							integrity and authentication
CR 1.14	Strength of symmetric key based authentication		x	x	x	Secure Communication Enforcement	*Use of session keys derived from the master key*
CR 1.14 (1)	Hardware security for symmetric key based authentication			x	x	Physical Attack Resistance & Secure Communication Enforcement	
CR 2.1	Authorization enforcement	x	x	x	x	Secure Communication Enforcement	
CR 2.1 (1)	Authorization enforcement for all users		x	x	x	Secure Communication Enforcement	
CR 2.6	Remote session termination		x	x	x	Secure Communication Support	*Fresh session keys usage*
CR 2.7	Concurrent session control			x	x	Secure Communication Support	*There is only the host device and the remote operator communicating the TOE through the Host Device. The amount of concurrent sessions is limited by the two master Keys associated to each memory section.*
CR 3.1	Communication integrity	x	x	x	x	Secure Communication Enforcement	
CR 3.1 (1)	Communication authentication		x	x	x	Secure Communication Enforcement	
CR 3.5	Input validation	x	x	x	x	Secure Communication Enforcement	
CR 3.7	Error handling	x	x	x	X	Secure Communication Enforcement	Any plain data access is prevented to the section that contain the protected User Data
CR 3.8	Session integrity		x	x	x	Secure Communication Enforcement	**Authenticated User Data** – Data (including executable codes) stored in the section of the Flash array that are defined as protected in terms of data integrity and authentication. Any plain data access is

Requirement	Description	SL-C				Covered by	Refinement
		1	2	3	4		
							prevented to the section that contain the protected User Data
EDR/NDR 3.10	Support for Updates	x	x	x	x	Secure Update of Application	
EDR/NDR 3.10 (1)	Update authenticity and integrity		x	x	x	Secure Update of Application	
EDR/NDR 3.11	Physical tamper resistance and detection		x	x	x	Physical Attacker Resistance	
EDR/NDR 3.12	Provisioning product supplier roots of trust		x	x	x	Cryptographic KeyStore	The *Per-Section Keys* are provisioned via a secure channel protected by the *Device Master Key* and cannot be modified without knowing this key
EDR/NDR 3.13	Provisioning asset owner roots of trust		x	x	x	Cryptographic KeyStore	The *Per-Section Keys* are provisioned via a secure channel protected by the *Device Master Key* and cannot be modified without knowing this key
EDR/NDR 3.14	Integrity of the boot process	x	x	x	x	Secure Initialization of Platform	The security policy initialization process verifies the integrity and the authenticity of the TSF data that describes the memory partition, per-section memory access policies, and the keys. This approach mitigates the threat of physical manipulation of the TOE.
EDR/NDR 3.14 (1)	Authenticity of the boot process		x	x	x	Secure Initialization of Platform	The security policy initialization process verifies the integrity and the authenticity of the TSF data that describes the memory partition, per-section memory access policies, and the keys. This approach mitigates the threat of

Requirement	Description	SL-C				Covered by	Refinement
		1	2	3	4		
							physical manipulation of the TOE.
CR 4.1	Information confidentiality	x	x	x	x	Secure Communication Enforcement	
CR 4.2	Information persistence		x	x	x	Residual Information Purging	
CR 4.2 (2)	Erase verification			x	x	Residual Information Purging	When first entering TM, the entire Flash is erased, including user data, configurations and keys, and device management data (Monotonic Counter, Winbond Unique ID, etc.). Test mode entry is disabled before the device is shipped. When re-entering TM (after it was previously disabled), the device is Formatted before switching to TM. This formatting is skipped if user sets the Fault Analysis Mode entry flag in a cryptographically protected user register. This flag should be set only after user has removed any sensitive information stored on the device.
CR 4.3	Use of cryptography	x	x	x	x	Security Communication Support	*Use of session keys derived from the master key*

Table 1 IEC62443-4-2 requirements Sufficiency

4.2.2 Features for Final Product towards IEC62443-4-2 Compliance

W77Q is designed to be used as a part of system, or in IEC62443-4-2 terms, as a subcomponent of an IEC62443-4-2 component. The features described in the SESIP SFRs can be safely utilized as part of the IEC62443-4-2 compliance of the final product.

Note it is up to the integrator on whether a feature is used for IEC62443-4-2 compliance and correct utilization of the feature, and this session is for guidance and informative purpose, but not in the scope of the SESIP evaluation. The integrator is responsible on how to design and architecture a component to fulfill IEC62443 requirements leveraging W77Q integrated to fit the purpose and security requirements.

4.3 NIST-8259A Mapping

Device cybersecurity capabilities [NIST-8259A], are cybersecurity features or functions that computing devices provide through their own technical means.

The IoT device cybersecurity capability core baseline is a set of device capabilities generally needed to support commonly used cybersecurity controls that protect devices as well as device data, systems, and ecosystems.

W77Q64/128 is designed to be used as a part of system, as a subcomponent. It fulfils subset of [NIST-8259A].

W77Q64/128 , as a storage/memory component fulfilled the relevant focal document element, based on OLIR Program [8259A-SESIP]:

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
Device Identification (DI)	**The IoT device can be uniquely identified logically and physically.**	Semantic	Intersects with	[3.1.1]	Verification of Platform Identity	N	The Platform provides the secure acceptance procedure described in [PRE] Section 2	
DI-1	**A unique logical identifier**	Semantic	Equal	[3.1.2]	Verification of Platform Instance Identity	Y	Each device (i.e., a specific instantiation of the platform) is provided to the customer with a pre-	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
							programmed globally unique 64-bit Winbond ID (WID)	
DI-2	**A unique physical identifier at an external or internal location on the device authorized entities can access**	Semantic	Intersects with	[3.1.1]	Verification of Platform Identity	N	The Platform provides the secure acceptance procedure described in [PRE] Section 2	
DI-2	**A unique physical identifier at an external or internal location on the device authorized entities can access**	Semantic	Intersects with	[3.1.2]	Verification of Platform Instance Identity	N	Each device (i.e., a specific instantiation of the platform) is provided to the customer with a pre-programmed globally unique 64-bit Winbond ID (WID),	
Device Configuration (DC)	**The configuration of the IoT device's software can be changed, and such changes can be performed by authorized entities only.**	Semantic	Superset of	[3.2.4]	Secure Update of Application	N	The Platform stores the code and data for the Host device and provides the Secure Code Update mechanism with rollback protection,	SESIP requirements for a security feature includes all related protections includin

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
							as specified in [SA] Section 3.6.2	g configuration capabilities
DC-1	**The ability to change the device's software configuration settings**	Semantic	Intersects with	[3.2.4]	Secure Update of Application	N	The Platform stores the code and data for the Host device and provides the Secure Code Update mechanism with rollback protection, as specified in [SA] Section 3.6.2	SESIP requirements for a security feature includes all related protections including configuration capabilities
DC-2	**The ability to restrict configuration changes to authorized entities only**	Semantic	Intersects with	[3.2.4]	Secure Update of Application	N	The Platform stores the code and data for the Host device and provides the Secure Code Update mechanism with rollback protection, as specified in [SA] Section 3.6.2	SESIP requirements for a security feature includes all related protections including configuration capabilities
DC-3	**The ability for authorized entities to restore the**	Semantic	Intersects with	[3.2.3]	Attestation of Platform	N	The platform provides an attestation	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
	device to a secure configuration defined by an authorized entity				Genuineness		of the "Verification of Platform Identity" **and "Verification of Platform Instance Identity"**, in a way that ensures that the platform cannot be cloned or changed without detection.	
Data Protection (DP)	**The IoT device can protect the data it stores and transmits from unauthorized access and modification.**	Semantic	Equal	[3.3.1]	Secure Communication Support	Y	The confidentiality and the integrity of the communication is protected as described above with the Session Key derived from the corresponding Master Key for each type of the logical communication channel	
Data Protection (DP)	**The IoT device can protect the data it stores and transmits**	Semantic	Equal	[3.3.2]	Secure Communication Enforcement	Y	**Secret User Data** – Data (including executable	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
	from unauthorized access and modification.						codes) stored in the section of the Flash array that are defined as protected in terms of data confidentiality	
Data Protection (DP)	**The IoT device can protect the data it stores and transmits from unauthorized access and modification.**	Semantic	Equal	[3.6.1]	Secure Storage	Y	The Authenticated User Data is defined in the Conformance rationale subsection of Secure Communication Enforcement. Any command modifying the content of a Section with Authenticated User Data shall be properly signed by a key derived from the Master Key of this section.	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
DP-1	**The ability to use demonstrably secure cryptographic modules for standardized cryptographic algorithms (e.g., encryption with authentication, cryptographic hashes, digital signature validation) to prevent the confidentiality and integrity of the device's stored and transmitted data from being compromised**	Semantic	Superset of	[3.5.3]	Cryptographic KeyStore	N	The Keystore memory is not addressable by Read, Write and Erase commands. It can be accessed only through the Key Provisioning, protected as described in [PRE] Section 3.4.1.	
DP-2	**The ability for authorized entities to render all data on the device inaccessible by all entities, whether previously authorized or not (e.g., through a wipe of internal**	Semantic	Equal	[3.3.2]	Secure Communication Enforcement	Y	**Secret User Data** – Data (including executable codes) stored in the section of the Flash array that are defined as protected in terms of data confidentiality	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
	storage, destruction of cryptographic keys for encrypted data)							
DP-3	**Configuration settings for use with the Device Configuration capability including, but not limited to, the ability for authorized entities to configure the cryptography use itself, such as choosing a key length**	Semantic	Intersects with	[3.5.3]	Cryptographic KeyStore	N	The Keystore memory is not addressable by Read, Write and Erase commands. It can be accessed only through the Key Provisioning, protected as described in [PRE] Section 3.4.1.	SESIP requirements for a security feature includes all related protections including configuration capabilities
Logical Access to Interfaces (LA)	**The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to authorized entities only.**	Semantic	Intersects with	[3.3.2]	Secure Communication Enforcement	N	**Secret User Data** – Data (including executable codes) stored in the section of the Flash array that are defined as protected in terms of data confidentiality	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
LA-1	**The ability to logically or physically disable any local and network interfaces that are not necessary for the core functionality of the device**	Semantic	Intersects with	[3.3.1]	Secure Communication Support	N	The confidentiality and the integrity of the communication is protected as described above with the Session Key derived from the corresponding Master Key for each type of the logical communication channel	
LA-1	**The ability to logically or physically disable any local and network interfaces that are not necessary for the core functionality of the device**	Semantic	Intersects with	[3.3.2]	Secure Communication Enforcement	N	**Authenticated User Data** – Data (including executable codes) stored in the section of the Flash array that are defined as protected in terms of data integrity and authentication	
LA-2	**The ability to logically restrict access to each network**	Semantic	Intersects with	[3.3.1]	Secure Communication Support	N	The confidentiality and the integrity of	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
	interface to only authorized entities (e.g., device authentication, user authentication)						the communication is protected as described above with the Session Key derived from the corresponding Master Key for each type of the logical communication channel	
LA-2	**The ability to logically restrict access to each network interface to only authorized entities (e.g., device authentication, user authentication)**	Semantic	Intersects with	[3.3.2]	Secure Communication Enforcement	N	**Authenticated User Data** – Data (including executable codes) stored in the section of the Flash array that are defined as protected in terms of data integrity and authentication	
LA-3	**Configuration settings for use with the Device Configuration capability including, but not limited to, the ability to**	Semantic	Intersects with	[3.3.1]	Secure Communication Support	N	The confidentiality and the integrity of the communication is protected as	SESIP requirements for a security feature includes all related

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
	enable, disable, and adjust thresholds for any ability the device might have to lock or disable an account or to delay additional authentication attempts after too many failed authentication attempts						described above with the Session Key derived from the corresponding Master Key for each type of the logical communication channel	protections including configuration capabilities
Software Update (SU)	**The IoT device's software can be updated by authorized entities only using a secure and configurable mechanism**	Semantic	Intersects with	[3.2.4]	Secure Update of Application	N	The Platform stores the code and data for the Host device and provides the Secure Code Update mechanism with rollback protection, as specified in [SA] Section 3.6.2	
SU-1	**The ability to update the device's software through remote (e.g., network download) and/or local means (e.g.,**	Semantic	Intersects with	[3.2.4]	Secure Update of Application	N	The Platform stores the code and data for the Host device and provides the Secure Code Update mechanism with rollback	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
	removable media)						protection, as specified in [SA] Section 3.6.2	
SU-2	**The ability to verify and authenticate any update before installing it**	Semantic	Intersects with	[3.2.4]	Secure Update of Application	N	The Platform stores the code and data for the Host device and provides the Secure Code Update mechanism with rollback protection, as specified in [SA] Section 3.6.2	
SU-3	**The ability for authorized entities to roll back updated software to a previous version**	Semantic	Intersects with	[3.2.4]	Secure Update of Application	N	The Platform stores the code and data for the Host device and provides the Secure Code Update mechanism with rollback protection, as specified in [SA] Section 3.6.2	
SU-4	**The ability to restrict updating actions to authorized entities only**	Semantic	Intersects with	[3.2.4]	Secure Update of Application	N	The Platform stores the code and data for the Host device and provides the Secure	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
							Code Update mechanism with rollback protection, as specified in [SA] Section 3.6.2	
SU-5	**The ability to enable or disable updating**	Semantic	Intersects with	[3.2.4]	Secure Update of Application	N	The Platform stores the code and data for the Host device and provides the Secure Code Update mechanism with rollback protection, as specified in [SA] Section 3.6.2	
SU-6	**Configuration settings for use with the Device Configuration capability including, but not limited to: a. The ability to configure any remote update mechanisms to be either automatically or manually initiated for update downloads and**	Semantic	Intersects with	[3.2.4]	Secure Update of Application	N	The Platform stores the code and data for the Host device and provides the Secure Code Update mechanism with rollback protection, as specified in [SA] Section 3.6.2	SESIP requirements for a security feature includes all related protections including configuration capabilities

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
	installations b. The ability to enable or disable notification when an update is available and specify who or what is to be notified							
Cybersecurity State Awareness (CSA)	**The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only**				N/A for W77Q			Not covered by W77Q

4.4 NISTIR 8425 Mapping

NISTIR 8425 - consumer profile of the IoT (Internet of Things) core baseline. Pinpoints the cybersecurity capabilities needed for consumer IoT products. The profile serves as a guide for small businesses when considering the purchase of IoT products. Provides a framework for cybersecurity outcomes that should be applied across the entire product spectrum. Developed as a response to Executive Order 14028, which directed NIST to establish criteria for cybersecurity labeling for consumer IoT products.

W77Q64/128 is designed to be used as a part of system, as a subcomponent. It fulfils subset of [NISTIR 8425].
W77Q64/128, as a storage/memory component fulfilled the relevant focal document element [NISTIR 8425-SESIP]:

Focal Document Element	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
AI1	Semantic	Superset of	[3.1.3]	Attestation of Platform Genuineness	y	fulfilled as describe in sec 3.2.3
AI1	Semantic	Superset of	[3.1.1]	Verification of Platform Identity	y	fulfilled as describe in sec 3.2.1
AI1	Semantic	Superset of	[3.1.2]	Verification of Platform Instance Identity	y	fulfilled as describe in sec 3.2.1
AI2	Semantic	Superset of	[3.1.3]	Attestation of Platform Genuineness	y	fulfilled as describe in sec 3.2.3
AI2	Semantic	Superset of	[3.1.1]	Verification of Platform Identity	y	fulfilled as describe in sec 3.2.1
AI2	Semantic	Superset of	[3.1.2]	Verification of Platform Instance Identity	y	fulfilled as describe in sec 3.2.1
PC1	Semantic	Intersects with	[3.2.4]	Secure Update of Application	y	fulfilled as describe in sec 3.2.5
PC1	Semantic	Intersects with	[3.7.2]	Authenticated Access Control	y	As describe in sec 1.4 Platform Functional Overview and Description, W77Q implementing an access control policy with different levels of authorization.
PC3	Semantic	Equal			N	Not covered by W77Q
DP1	Semantic	Superset of	[3.5.3]	Cryptographic Keystore	y	fulfilled as describe in sec 3.2.9
DP1	Semantic	Superset of	[3.4.2]	Physical Attacker Resistance	y	fulfilled as describe in sec 3.2.8
DP1	Semantic	Superset of	[3.6.2]	Secure Confidential Storage	y	fulfilled as describe in sec 3.2.11
DP1	Semantic	Superset of	[3.1.4]	Secure Initialization of Platform	y	fulfilled as describe in sec 3.2.14
DP1	Semantic	Superset of	[3.6.1]	Secure Trusted Storage	y	fulfilled as describe in sec 3.2.10

Focal Document Element	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
DP1	Semantic	Superset of	[D.3]	Security Objectives for the Operational Environment	y	Guidance are provided to secure data protection, the AGD delivery
DP1	Semantic	Superset of	[3.1.1]	Verification of Platform Identity	y	fulfilled as describe in sec 3.2.1
DP1	Semantic	Superset of	[3.1.2]	Verification of Platform Instance Identity	y	fulfilled as describe in sec 3.2.1
DP2	Semantic	Equal	[3.6.2]	Secure Confidential Storage	y	fulfilled as describe in sec 3.2.11
DP3	Semantic	Superset of	[3.5.3]	Cryptographic Keystore	y	fulfilled as describe in sec 3.2.9
DP3	Semantic	Superset of	[3.3.2]	Secure Communication Enforcement	y	fulfilled as describe in sec 3.2.6
DP3	Semantic	Superset of	[3.3.1]	Secure Communication Support	y	fulfilled as describe in sec 3.2.7
IAC1a	Semantic	Intersects with	[3.3.2]	Secure Communication Enforcement	y	fulfilled as describe in sec 3.2.6
IAC1a	Semantic	Intersects with	[3.3.1]	Secure Communication Support	y	fulfilled as describe in sec 3.2.7
IAC1b	Semantic	Intersects with	[3.7.2]	Authenticated Access Control	y	As describe in sec 1.4 Platform Functional Overview and Description, W77Q implementing an access control policy with different levels of authorization.
IAC1b	Semantic	Intersects with	[3.5.3]	Cryptographic Keystore	y	fulfilled as describe in sec 3.2.9
IAC1b	Semantic	Intersects with	[3.7.1]	Privileged Access Control	y	As describe in sec 1.4 Platform Functional Overview and Description, W77Q implementing an

Focal Document Element	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
						access control policy with different levels of authorization.
IAC1b	Semantic	Intersects with	[3.3.2]	Secure Communication Enforcement	y	fulfilled as describe in sec 3.2.6
IAC1b	Semantic	Intersects with	[3.3.1]	Secure Communication Support	y	fulfilled as describe in sec 3.2.7
IAC1c	Semantic	Equal	[3.7.2]	Authenticated Access Control	y	As describe in sec 1.4 Platform Functional Overview and Description, W77Q implementing an access control policy with different levels of authorization. Also, secure communication prevents the access and modification to the configuration. Root modifies everything and each user its section.
IAC1c	Semantic	Equal	[3.7.1]	Privileged Access Control	y	As describe in sec 1.4 Platform Functional Overview and Description, W77Q implementing an access control policy with different levels of authorization. Also, secure communication prevents the access and modification to the configuration. Root modifies everything and each user its section.
IAC2a	Semantic	Equal			N	Not covered by W77Q

Focal Document Element	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
IAC2a	Semantic	Intersects with	[4.x.x]	Development Requirements Tests Requirements Vulnerability Assessment Requirements	y	AVA, ADV and ATE activities verify that the interfaces provided at Platform level are restricted to only the necessary functions and privileges, and that there is no unnecessary privilege, interface and/or code remaining.
IAC2b	Semantic	Equal	[3.7.2]	Authenticated Access Control	y	As describe in sec 1.4 Platform Functional Overview and Description, W77Q implementing an access control policy with different levels of authorization. Also, secure communication prevents the access and modification to the configuration. Root modifies everything and each user its section.
IAC2b	Semantic	Equal	[3.3.2]	Secure Communication Enforcement	y	fulfilled as describe in sec 3.2.6
IAC2b	Semantic	Equal	[3.3.1]	Secure Communication Support	y	fulfilled as describe in sec 3.2.6
IAC2c	Semantic	Superset of	[3.7.2]	Authenticated Access Control	y	As describe in sec 1.4 Platform Functional Overview and Description, W77Q implementing an access control policy with different levels of authorization. Also, secure communication prevents the access and modification to the configuration. Root modifies everything and each user its section.

Focal Document Element	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
IAC2c	Semantic	Superset of	[3.1.4]	Secure Initialization of Platform	y	fulfilled as describe in sec 3.2.14
SU1	Semantic	Intersects with	[3.1.3]	Attestation of Platform Genuineness	y	fulfilled as describe in sec 3.2.3
SU1	Semantic	Intersects with	[3.4.1]	Limited Physical Attacker Resistance	y	fulfilled as describe in sec 3.2.8
SU1	Semantic	Intersects with	[3.4.2]	Physical Attacker Resistance	y	fulfilled as describe in sec 3.2.8
SU1	Semantic	Intersects with	[3.2.4]	Secure Update of Application	y	fulfilled as describe in sec 3.2.5
SU2	Semantic	Intersects with	[4.x.x]	Development Requirements	y	
SU2	Semantic	Intersects with	[4.x.x]	Guidance Documents Requirements	y	
SU2	Semantic	Intersects with	[4.x.x]	Life-cycle Support Requirements-ALC_FLR.2 Flaw reporting procedures	y	
CSA1	Semantic	Intersects with	[3.1.3]	Attestation of Platform Genuineness	y	fulfilled as describe in sec 3.2.3
CSA1	Semantic	Intersects with	[4.x.x]	Guidance Documents Requirements	y	
CSA1	Semantic	Intersects with	[3.4.1]	Limited Physical Attacker Resistance	y	fulfilled as describe in sec 3.2.8

Focal Document Element	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
CSA1	Semantic	Intersects with	[3.4.2]	Physical Attacker Resistance	y	fulfilled as describe in sec 3.2.8
D1ai	Semantic	Intersects with	[4.x.x]	Security Target Requirements Development Requirements Guidance Documents Requirements Tests Requirements Life-cycle Support Requirements Vulnerability Assessment Requirements	y	
D1aii	Semantic	Intersects with	[4.x.x]	Security Target Requirements Development Requirements Guidance Documents Requirements Tests Requirements Life-cycle Support Requirements Vulnerability Assessment Requirements	y	
D1aiii	Semantic	Intersects with	[4.x.x]	Security Target Requirements Development Requirements Guidance Documents Requirements Tests Requirements Life-cycle Support Requirements Vulnerability Assessment Requirements	y	

Focal Document Element	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
D1aiv	Semantic	Intersects with	[4.x.x]	Security Target Requirements Development Requirements Guidance Documents Requirements Tests Requirements Life-cycle Support Requirements Vulnerability Assessment Requirements	y	
D1av	Semantic	Intersects with	[4.x.x]	Security Target Requirements Development Requirements Guidance Documents Requirements Tests Requirements Life-cycle Support Requirements Vulnerability Assessment Requirements	y	
D1avi	Semantic	Intersects with	[4.x.x]	Security Target Requirements Development Requirements Guidance Documents Requirements Tests Requirements Life-cycle Support Requirements Vulnerability Assessment Requirements	y	

Focal Document Element	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
D1avii	Semantic	Intersects with	[4.x.x]	Security Target Requirements Development Requirements Guidance Documents Requirements Tests Requirements Life-cycle Support Requirements Vulnerability Assessment Requirements	y	
D1aviii	Semantic	Intersects with	[4.x.x]	Security Target Requirements Development Requirements Guidance Documents Requirements Tests Requirements Life-cycle Support Requirements Vulnerability Assessment Requirements	y	
D1b	Semantic	Intersects with	[4.x.x]	Security Target Requirements Development Requirements Guidance Documents Requirements Tests Requirements Life-cycle Support Requirements Vulnerability Assessment Requirements	y	

Focal Document Element	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
D1c	Semantic	Intersects with	[4.x.x]	Security Target Requirements Development Requirements Guidance Documents Requirements Tests Requirements Life-cycle Support Requirements Vulnerability Assessment Requirements	y	
D1d	Semantic	Intersects with	[4.x.x]	Security Target Requirements Development Requirements Guidance Documents Requirements Tests Requirements Life-cycle Support Requirements Vulnerability Assessment Requirements	y	

Focal Document Element	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
D1e	Semantic	Intersects with	[4.x.x]	Security Target Requirements Development Requirements Guidance Documents Requirements Tests Requirements Life-cycle Support Requirements Vulnerability Assessment Requirements	y	
D1fi	Semantic	Intersects with	[4.x.x]	Security Target Requirements Development Requirements Guidance Documents Requirements Tests Requirements Life-cycle Support Requirements Vulnerability Assessment Requirements	y	
D1fii	Semantic	Intersects with	[4.x.x]	Security Target Requirements Development Requirements Guidance Documents Requirements Tests Requirements Life-cycle Support Requirements Vulnerability Assessment Requirements	y	

Focal Document Element	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
D1fiii	Semantic	Intersects with	[4.x.x]	Security Target Requirements Development Requirements Guidance Documents Requirements Tests Requirements Life-cycle Support Requirements Vulnerability Assessment Requirements	y	
D1gi	Semantic	Intersects with	[4.x.x]	Security Target Requirements Development Requirements Guidance Documents Requirements Tests Requirements Life-cycle Support Requirements Vulnerability Assessment Requirements	y	
D1gii	Semantic	Intersects with	[4.x.x]	Security Target Requirements Development Requirements Guidance Documents Requirements Tests Requirements Life-cycle Support Requirements Vulnerability Assessment Requirements	y	

Focal Document Element	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
D1giii	Semantic	Intersects with	[4.x.x]	Security Target Requirements Development Requirements Guidance Documents Requirements Tests Requirements Life-cycle Support Requirements Vulnerability Assessment Requirements	y	
D1giv	Semantic	Intersects with	[4.x.x]	Security Target Requirements Development Requirements Guidance Documents Requirements Tests Requirements Life-cycle Support Requirements Vulnerability Assessment Requirements	y	
D1gv	Semantic	Intersects with	[4.x.x]	Security Target Requirements Development Requirements Guidance Documents Requirements Tests Requirements Life-cycle Support Requirements Vulnerability Assessment Requirements	y	
IQR1a	Semantic	Superset of	[4.1.5]	Life-cycle Support Requirements-ALC_FLR.2 Flaw reporting procedures	y	

Focal Document Element	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
IQR1b	Semantic	Superset of	[4.1.5]	Life-cycle Support Requirements-ALC_FLR.2 Flaw reporting procedures	y	
InD1a	Semantic	Superset of	[4.1.5]	Life-cycle Support Requirements-ALC_FLR.2 Flaw reporting procedures	y	
InD1b	Semantic	Superset of	[4.1.5]	Life-cycle Support Requirements-ALC_FLR.2 Flaw reporting procedures	y	
InD1c	Semantic	Superset of	[4.1.5]	Life-cycle Support Requirements-ALC_FLR.2 Flaw reporting procedures	y	
InD1d	Semantic	Superset of	[4.1.5]	Life-cycle Support Requirements-ALC_FLR.2 Flaw reporting procedures	y	
InD1e	Semantic	Superset of	[4.1.5]	Life-cycle Support Requirements-ALC_FLR.2 Flaw reporting procedures	y	

Focal Document Element	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
InD2	Semantic	Superset of	[4.1.5]	Life-cycle Support Requirements- ALC_FLR.2 Flaw reporting procedures	y	
PEA1ai	Semantic	Superset of	[4.1.4]	Guidance Documents Requirements	y	
PEA1aii	Semantic	Superset of	[4.1.4]	Guidance Documents Requirements	y	
PEA1aiii	Semantic	Superset of	[4.1.4]	Guidance Documents Requirements	y	
PEA1aiv	Semantic	Superset of	[4.1.4]	Guidance Documents Requirements	y	
PEA1b	Semantic	Superset of	[4.1.4]	Guidance Documents Requirements	y	
PEA1c	Semantic	Superset of	[4.1.4]	Guidance Documents Requirements	y	
PEA1d	Semantic	Superset of	[4.1.4]	Guidance Documents Requirements	y	

Focal Document Element	Rationale	Relationship	Reference Document Element	Reference Document Element Description	Fulfilled By (Y/N)	Comments (optional)
PEA1e	Semantic	Superset of	[4.1.4]	Guidance Documents Requirements	y	

5 References

[GP-SESIP] GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), Version 1.2, July 2023, GP_FST_070

[GP-SPE] SESIP profile for Secure External Memories, version 1.0, September 2021, GPT_SPE_148.

[PSA-Com-L2] SESIP Profile for PSA Certified™ RoT Component Level 2, version 1.0 BETA, 1 August 2022, JSADEN017.

[17927] prEN 17927:2023, Security Evaluation Standard for IoT Platforms (SESIP). An effective methodology for applying cybersecurity assessment and re-use for connected products, 01-Feb-2023, CEN/CENELEC

[Datasheet] W77Q128JV/W77Q64JV Secure Serial NOR Flash Memory, Ver A8, Winbond Technology Ltd

[Datasheet2] W77Q128JL/W77Q64JL Secure Serial NOR Flash Memory, Ver A1, Winbond Technology Ltd

[OPE] W77Q128JV/W77Q64JV/W77Q128JL/W77Q64JL Operational User Guidance, Ver A3, Winbond Technology Ltd

[PRE] W77Q128JV/W77Q64JV/W77Q128JL/W77Q64JL Preparative Procedure, Ver A3, Winbond Technology Ltd

[SA] W77Q128/W77Q64 Secure Serial NOR Flash Memory Security Manual, Ver E1, Winbond Technology Ltd

[FSP] W77Q Secure Flash Memory Functional Specification, Ver TBD, Winbond Technology Ltd

[FLR] W77Q Secure Flash Memory: Flaw Remediation, Ver C, Winbond Technology Ltd

[ATE] ATE Tests Mapping Table , Ver A + W77Q Secure Flash Memory ATE Document, Ver A, Winbond Technology Ltd

[62443-1-1] IEC TS 62443-1-1, Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models, edition 1.0, 2009, the International Electrotechnical Commission (IEC).

[62443-4-1] IEC TS 62443-4-1, Industrial communication networks - Network and system security - Part 4-1: Secure product development lifecycle requirements, edition 1.0, 2018, the International Electrotechnical Commission (IEC).

[62443-4-2] IEC TS 62443-4-2, Industrial communication networks - Network and system security - Part 4-2: Technical security requirements for IACS components, edition 1.0, 2019, the International Electrotechnical Commission (IEC).

[NIST-8259A] NISTIR 8259A - IoT Device Cybersecurity Capability Core Baseline, May 2020

[8259A-SESIP] OLIR Program: NIST-8259A-to-SESIP-v1.2 (1.0.0) Informative Reference Details, 08/17/2021

[NIST-800-88] NIST Special Publication 800-88 Revision 1, Guideline for Media Sanitization, December 2014

[NISTIR 8425] Profile of the IoT Core Baseline for Consumer IoT Products, September 2022

[NISTIR 8425-SESIP] TBD