TrustME © W77Q64/W77Q128 Sub-Chip Cryptographic Module FIPS 140-3

Non-Proprietary Security Policy

Table of Contents

List of Tables

List of Figures

1. General

1.1. Overview

This document is the non-proprietary FIPS 140-3 Security Policy for the module TrustMe © W77Q64/W77Q128 Sub-Chip (Version 1.0) flash device by Winbond which will also be referred to as “the cryptographic module” , “SHA block” or “the module” throughout this document. This Security Policy specifies the security rules under which the module should operate to meet FIPS 140-3 Level 1 requirements.

This cryptographic module is a hardware cryptographic module implemented as a sub-chip running on the single-chip standalone W77Q64/W77Q128 flash device.

The cryptographic service provided by the module is the message digest calculation based on the SHA2-256 cryptographic algorithm.

The FIPS 140-3 security levels for the module are as follows:

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	1
2	Cryptographic Module Specification	1
3	Cryptographic Module Interfaces	1
4	Roles, Services, and Authentication	1
5	Software/Firmware Security	N/A
6	Operational Environment	1
7	Physical Security	1
8	Non-Invasive Security	N/A
9	Sensitive Security Parameter Management	N/A
10	Self-Tests	1
11	Life-Cycle Assurance	1
12	Mitigation of Other Attacks	N/A

Table 1 – Security Levels

2. Cryptographic Module Specification

The module type is hardware and has a single-chip embodiment (as stated in **FIPS 140-3 IG 2.3.B**) which provides the W77Q64/W77Q128 device with SHA2-256 message digest functionality. The module is validated at overall security level is 1. Please refer to Table 1 for security levels of individual sections.

Model	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features
W77Q64/ W77Q128 Sub-Chip	Part number: W77Q64/W77Q128 Version: 1.0	N/A	Hardware sub-chip cryptographic module responsible for providing SHA2-256 message digest capabilities

Table 2 - Cryptographic Module Tested Configuration

2.1. Module Description and Cryptographic Boundary

The physical perimeter encompasses the entire W77Q64/W77Q128 flash device (monolithic die). The cryptographic boundary is defined as only the SHA2-256 sub-chip that is the only part of the device with cryptographic operation capabilities to provide the SHA2-256 cryptographic algorithm. The SHA2-256 sub-chip also has all the logic related to the self-test implementation, zeroization, error handling, etc.

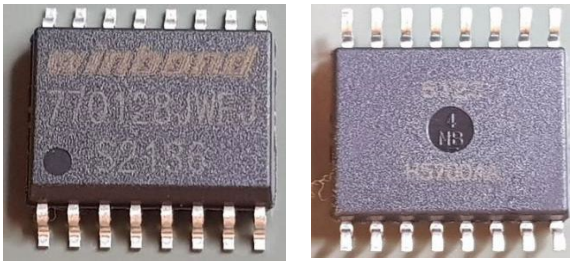

Figure 1 - W77Q64/W77Q128 flash devices

The following list shows the main components of the W77Q64/W77Q128 device:

- **SRAM** – Input and output buffer serving as a user interface to the Secure Functions
- **Flash Array** – Non-Volatile Flash memory cells
- **Matrix** – Data transfer connectivity matrix
- **CTRL** – Control Logic to control command flows and data transfer
- **SHA** – The SHA2-256 block is the only one with cryptographic operation capabilities to provide the SHA2-256 function, self-tests, zeroization, error handling, etc.
- **Keys** – Session control parameters
- **OSC** – Internal Clock oscillator
- **SPI IFC** – SPI front-end

The SHA module is used by internal operations (No direct user interface is available to the SHA function) of the W77Q64/W77Q128 device and is controlled by the CTRL module through the **Control input interface.** The CTRL block also controls data transfer over the Matrix.

The connectivity matrix handles the transfer of data to the SHA block through the **Data input interface** and message digest calculation through the **Data Output Interface** to send them to the CTRL block.

Moreover, the SHA function is also used by the keys block. In this case, the CRTL module loads the SHA function with the required parameters from the Keys block through the **Data Input Interface** and launches the SHA calculation. Then the SHA block outputs the message digest to the keys block through the **Data Output Interface**.

The SHA block notifies the W77Q64/W77Q128 device when it is performing self-tests, operating, or if an error occurs through the **Status Output Interface** connected to the CTRL block.

Considering that the module is not connected to any other cryptographic modules, **Control Output Interface** is not required. Therefore, the only block related to the cryptographic operation of the device is the SHA block that corresponds to the cryptographic boundary as detailed below:

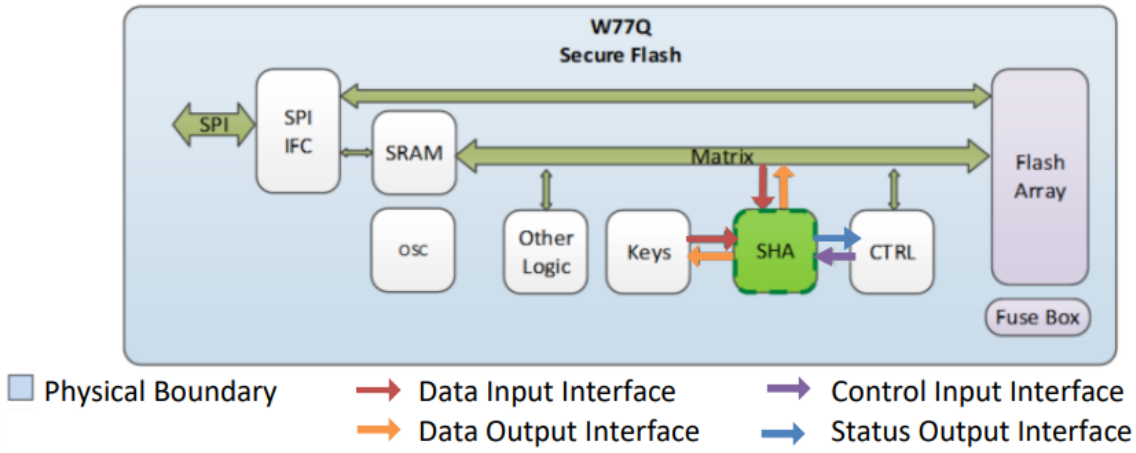

Figure 2 - Block diagram of the physical perimeter of the Module

2.2. Modes of Operation and Security Functions

The module only operates in Approved mode providing a SHA2-256 message digest as an approved cryptographic functionality. Approved mode of operation is entered upon powering on the module and successful completion of pre-operational self-test.

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key size(s)/Key Strength(s)	Use/Function
A2317	SHA2-256 [FIPS 180-4]	SHA2-256	Message Length: 0-768	Message digest generation

Table 3 - Approved Algorithms

The module only supports Approved algorithms so below tables are not included:

- Non-Approved Algorithms Allowed in the Approved Mode of Operation
- Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed
- Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

There is no specific security design, rules of operation or initialization requirements applicable to this module.

3. Cryptographic Module Interfaces

The table below summarizes the associations between the logical interfaces required by FIPS 140-3 and the physical ports of the module:

Physical port	Logical interface	Data that passes over port/interface
Matrix-In-Data	Data input interface	Data input (32b)
Matrix-In-Addr		Address of the input data word to write to (4b). It selects which 32b data-in word is accessed (out of 64B)
Keys-Data-In		Direct Data-input (128b) from KEYS function
Matrix-Out-Addr	Data output interface	Address of the output data to read from (3b). It selects which 32b data-out word is accessed (out of 32B)
Matrix-Out-Data		Data output (32b) from the SHA result
Keys-Data-Out		Direct Data-output (128b) to KEYS function (from Hash result)
Reset	Control input interface	Reset/Initialize the SHA module and internal states
SHA-Start		Start execution of SHA Iteration
SHA-VER	Status output interface	Indicates the module version
CMVP-DONE		If set, indicates the self-tests execution is complete
CMVP-PASS		If set, indicates the self-tests are passed with success
CMVP-FAIL		If set, indicates the self-tests have failed
SHA-BUSY		If set, indicates that the SHA operation is being performed. Otherwise, the calculation is complete, and module is idle
Power Interface	Power interface	The entire device has a single power supply that provides the sub-chip cryptographic module with the expected power 1.8V relative to GND and a maximal current of 20mA

Table 4 - Ports and Interfaces

When the module is performing self-tests, or is in error state, all data output from data output interfaces (except status output interface) are inhibited. The module does not implement control output interface. In addition, the Module does not support the maintenance role, therefore it does not require to implement a maintenance interface.

4. Roles, Services, and Authentication

4.1. Roles and Authentication

The module does not implement any authentication mechanism. The module supports implicit User and Crypto Officer roles based on the services detailed in the table below. The module does not provide a maintenance role, bypass capability or concurrent operators.

Role	Service	Input	Output
CO	Module Initialization	N/A	N/A
User	Message Digest	Plaintext data	Message digest of data
User	Zeroization	Residual data from the hashing process	N/A
User	Self-test	CMVP_BIST command or reset	CMVP_PASS = 0/1 signal
User	Show-status	Request SSR_STATE	Current state (LOCK, RESET, WORK)
User	Show module versioning information	GET_VERSION command	Module version

Table 5 - Roles, Service Commands, Input and Output

The states returned by SSR_STATE are described below:
LOCK = Self-test error state.
RESET = Data output inhibition state during self-test.
WORK = Self-test passed, ready to execute message digest.

4.2. Services

The table below lists the services that can be invoked by Crypto Officer and User. The module does not support bypass capability, self-initiated cryptographic capability or firmware loading.

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Module Initialization	Secure initialization of the module	N/A	N/A	CO	N/A	CMVP_DONE
Message Digest	SHA2-256 hash calculation	SHA2-256 [FIPS 180-4] A2317	N/A	User	N/A	SHA_BUSY = 1 while executing, SHA_BUSY = 0 after completion
Zeroization	Used to zeroize residual data from the hashing process	N/A	N/A	User	N/A	N/A
Self-test	Run pre-operational self-test on demand	SHA2-256 [FIPS 180-4] A2317	N/A	User	N/A	CMVP_PASS = 0 or 1 after completion
Show-status	Show the current state of the module	N/A	N/A	User	N/A	Current state from SSR_STATE (LOCK, RESET, WORK)
Show module versioning information	Show version of the module	N/A	N/A	User	N/A	Version in hex format (0x1) parsed from version of single-chip

Table 6 - Approved Services

The module does not implement any non-approved services.
According to the FIPS 140-3 standard and the **FIPS 140-3 IG 2.4.C**, the module must indicate when an approved cryptographic algorithm is being used either executing an approved security function or during the self-tests. Please refer to Table 6 for indicator of services provided by the module.

- According to **FIPS 140-3 IG 2.4.C**, the execution of self-test service does not require the approved services indicator because it is invoked by resetting/rebooting the module, however in this case the

indicator is provided.

- The show version service consists of a physical signal that is constantly output from the module.
- The show status service to obtain the current status of the module is not an independent service itself, since the status of the module can be mapped to the value of the Busy bit **(SHA_BUSY)** and the **CMVP_DONE** and **CMVP_PASS** signals detailed in Table 4: Module ports and interfaces.

5. Software/Firmware Security

This section is not applicable because it is a hardware sub-chip cryptographic module defined into the W77Q64/W77Q128 secure flash memory.

6. Operational Environment

The module is a hardware sub-chip cryptographic module, and its operational environment can be classified as non-modifiable operational environment. There are no security rules, settings or restrictions to the configuration of the operational environment.

7. Physical Security

The module is a Security Level 1 sub-chip module and has a single-chip embodiment. The module is composed of production-grade components with a hard, opaque enclosure that is the physical boundary defined by the entire W77Q64/W77Q128 secure flash memory.

8. Non-Invasive Security

This section is not applicable to the module.

9. Sensitive Security Parameter Management

The only cryptographic operation supported by the module is the message digest calculation based on SHA2-256 cryptographic algorithm. Hence, SSPs are not employed, and this section is not applicable for the module.

9.1. Random Bit Generators

The module does not implement RBG because it does not perform SSP generation nor SSP establishment.

9.2. Sensitive Security Parameter Generation

The module does not implement any method to perform SSPs generation.

9.3. Sensitive Security Parameter Establishment

The module does not implement SSPs establishment methods.

9.4. Sensitive Security Parameter Entry and Output

The module does not implement SSPs entry and output methods.

9.5. Sensitive Security Parameter Storage

The module does not store any SSPs inside its boundary.

9.6. Sensitive Security Parameter Zeroization

The module does not employ any SSPs that can be zeroized. The module uses FLUSH command to remove any information residues related to the message digest calculation.

10.Self-Tests

This section specifies the pre-operational and conditional self-tests performed by the module to ensure its correct functionality. The module has one error state, called the error state. If an error occurs during a self-test, the module enters the error state and indicates it to the user via the status output interface by the **CMVP_PASS = 0** signal. In addition, while the module is in error state, all data output interfaces except the status output interfaces are inhibited.

- Pre-Operational Self-Tests:

Once the module is powered on, the pre-operational self-tests are triggered automatically prior to the module being ready to provide any data related to cryptographic operation through the data output interface.
The module does not implement bypass test or critical function tests.

- Software Integrity Test

The FIPS 140-3 standard requires to perform the software/firmware integrity test during the pre-operational self-tests once the module is powered on, however, considering that the module is a purely hardware module and that it does not contain any software or firmware, then the module executes the following known answer test associated to the SHA2-256 cryptographic algorithm complying with the requirement of testing at a minimum once cryptographic algorithm as required in section “Pre-operational software/firmware integrity test” of the FIPS 140-3 standard:

  - KAT for message digest calculation based on SHA2-256

- Conditional Self-Test

The module does not support any conditional self-tests. The only self-test supported is the pre-operational SHA2-256 KAT.

- Periodic Self-Test

The module allows the user to execute the self-tests periodically by either sending the **CMVP_BIST command** to the module or by resetting the module.

11.Life-Cycle Assurance

11.1. Configuration Management

The configuration management list is composed of the Configuration Items version control, change control, flaw remediation tracking and module design revision which are managed by Winbond in a private Gitlab repository with write access restricted to the authorized Winbond personnel.

11.2. Configuration Items Identification Method

The internal versioning of the module is performed automatically, and the assigned version and revision are used internally to control the code development.
The W77Q64/W77Q128 device hardware version is shown in its internal HW_VER register that can be retrieved from the device by the SHOW VERSION service using the **GET_VERSION** command through its SPI interface:

31-24	Reserved	HC	00h	Reserved
23-20	FLASH_VER	HC	1h	**Flash Version**
19-16	Reserved	HC	0h	Reserved
15-12	SEC_VER	HC	2h	**Security Protocol Version:** <2> W77Q – Protocol Ver.2
11-8	SEC_REV	HC	4h	**Security Protocol Minor Revision:** **<4>** W77Q64/W77Q128
7-4	HASH_VER	HC	1h	**Sub-System Cryptographic Module Version:** <1> SHA 256 module
3-0	Reserved	HC	0h	Reserved

Figure 3 - Module Version details

As per Figure 3 above and considering that the single-chip device uses Little Endian representation, the hardware version of the single-chip device is “0x00102410” in hexadecimal. The module version is composed of the four bits (HASH_VER) with the value “1” in hexadecimal or “0001” in bits.
The module version is specified by using four bits in hexadecimal format:

- SHA module version (**HASH_VER)**: 0001 (1h).

The module identifier is specified by using the eight bits in hexadecimal format:

- Bits 15-12 (**SEC_VER**) and 11-8 (**SEC_REV**): 00020004 (2h and 4h)

The module identifier specified above correlates to the module name “TrustMe © W77Q64/W77Q128 Sub-Chip”.

The version information is continuously shown by the module through the **SHA_VER** signal.
The associated module documentation is manually versioned by appending the date, the major version and minor version on their name as following “W77QAAXXXX_RevYZ” with the following naming convention:

- W77Q – Device model identification.
- AA – Document initials (e.g., The initials for the Security Policy document are SP).
- XXXX – W77Q64/W77Q128 device revision.
- Y – Major revision of the document. It takes alphabetic values (A, B, C, etc.).
- Z – Minor revision of the document. It indicates minor revisions of the document with numerical values.

Note: When a major revision is released, it does not contain the minor revision number associated.
The configuration item list can be consulted in the **WCIL** document.

11.3. Crypto Officer and User Guidance

11.3.1. Installation and Initialization Instructions

Regarding the installation and initialization guidance, once the W77Q64/W77Q128 single-chip device is powered, the module will be also powered and initiated automatically in an approved mode of operation after executing the pre-operational self-tests with success. As detailed in the section 3 "Cryptographic Module Interfaces", when the self-tests are passed, the **CMVP_DONE** and **CMVP_PASS** signals will be set.

There is no specific administrator or non-administrator guidance applicable to this module.

11.3.2. Secure Operation

When the module is initiated as described in the previous section, the module will be in the approved mode and will allow the user to use the authorized services detailed in section "4.2 Services".

11.3.3. Operation Rules

When the module is installed and securely initialized, it is in Approved Mode which is the only mode of operation complying with the following rules:

1. The module is initialized in Approved mode of operation automatically after the self-test is completed successfully.
2. Once the module is powered up, the pre-operational self-tests are executed automatically without requiring any operator additional action to be executed.
3. All data output interfaces except status output interfaces will be inhibited during self-tests, zeroization and error states.
4. The module does not store nor manage any Sensitive Security Parameter; therefore, it does not support random number generation, SSPs generation, SSPs establishment, SSPs entry and output or SSPs storage.
5. The module does not implement critical security functions.
6. The module does not support a maintenance interface or maintenance role.
7. There are no maintenance requirements applicable to this module.
8. The Module does not provide bypass capability.
9. The module does not implement an authentication mechanism because it is a Security Level 1 module.
10. Considering the module is a purely hardware module without containing firmware or software, during the pre-operational self-tests it executes the SHA2-256 KAT instead of firmware/software verification integrity test.
11. The module does not implement conditional self-tests because the only supported cryptographic algorithm is tested during the preoperational self-tests.
12. The module complies with the periodic self-tests requirements by allowing the user and CO to execute the self-tests on demand either by resetting the module or by sending the **CMVP_BIST** command.
13. If the module is in an error state, the cryptographic operativity of the module will be disabled.
14. The normal operation of the Module can be resumed from an Error state by resetting (power cycling) the module.
15. The module does not implement mitigation of other attacks.

11.3.4. End of Life

The module does not require sanitization because it does not store any SSP as detailed in the section “9.5 Sensitive Security Parameter Storage”. All the residues related to the message digest calculations are erased once the calculation is finished as detailed in the section “9.6 Sensitive Security Parameter Zeroization”.

12.Mitigation of Other Attacks

The module is not designed to mitigate other attacks which are outside of the scope of FIPS 140-3.

Glossary and Abbreviations

CO	Crypto Officer
CSP	Critical Security Parameter
FIPS	Federal Information Processing Standard
IUT	Implementation Under Test
KAT	Known Answer Test
Module	TrustME © W77Q64/W77Q128 Sub-Chip Cryptographic Module V1.0
NIST	National Institute of Standards and Technology
PSP	Public Security Parameter
RBG	Random Bit Generator
SHA	Secure Hash Algorithm
SSP	Sensitive Security Parameter

Reference Document

FIPS 140-3 IG	Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program
WSP	W77QSP0200_RevA1.pdf
WCIL	W77QCIL0200_RevA1.pdf
WFSM	W77QFSM0200_RevA1.pdf
WFS	W77QFS0200_RevA1.pdf
FIPS 180-4	Secure Hash Standard (SHS)
SP 800-140F	CMVP Approved Non-Invasive Attack Mitigation Test Metrics

Preliminary Designation

The "Preliminary" designation on a *Winbond* datasheet indicates that the product is not fully characterized. The specifications are subject to change and are not guaranteed. *Winbond* or an authorized sales representative should be consulted for current information before using this product.

Trademarks

Winbond and *TrustME* are trademarks of *Winbond Electronics Corporation.*

All other marks are the property of their respective owner.

Important Notice

Winbond products are not designed, intended, authorized or warranted for use as components in systems or equipment intended for surgical implantation, atomic energy control instruments, airplane or spaceship instruments, transportation instruments, traffic signal instruments, combustion control instruments, or for other applications intended to support or sustain life. Furthermore, *Winbond* products are not intended for applications wherein failure of *Winbond* products could result or lead to a situation wherein personal injury, death or severe property or environmental damage could occur.

Winbond customers using or selling these products for use in such applications do so at their own risk and agree to fully indemnify *Winbond* for any damages resulting from such improper use or sales.

Information in this document is provided solely in connection with Winbond products. Winbond reserves the right to make changes, corrections, modifications or improvements to this document and the products and services described herein at any time, without notice.