Winbond Electronics Corporation

TrustMe © W77Q64/128/256/512/1024/2048Mb & TrustMe © W77T64/128/256/512/1024/2048Mb Sub-Chip

FIPS 140-3 Non-Proprietary Security Policy

Document Version RevA2
June 2025

Prepared by:

jtsec BEYOND IT SECURITY

www.jtsec.es

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 TrustMe © W77Q64/128/256/512/1024/2048Mb & TrustMe © W77T64/128/256/512/1024/2048Mb Sub-Chip Cryptographic Module, hereafter referred to as, "the module". It contains the security rules under which the module must operate and describes how the module meets the requirements as specified in FIPS PUB 140-3 for an overall Security Level 1 cryptographic module.

1.2 Security Levels

The table below describes the individual security areas of FIPS 140-3, as well as the Security Levels of those individual areas.

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	1
10	Self-tests	1
11	Life-cycle assurance	1
12	Mitigation of other attacks	N/A
	Overall Level	1

Table 1: Security Levels

The Module has an overall security level of 1.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The module is defined as a purely hardware sub-chip cryptographic module (as stated in FIPS 140-3 IG 2.3.B) running on the single-chip TrustMe © secure flash memory. The cryptographic service provided by the module is the message digest calculation based on the SHA2-256 cryptographic algorithm.

Module Type: Hardware

Module Embodiment: Single Chip

Module Characteristics: SubChip

Cryptographic Boundary:

The cryptographic boundary of the module is the sub-chip, as shown in the figure below, since it is the only part of the device with cryptographic operation capability.

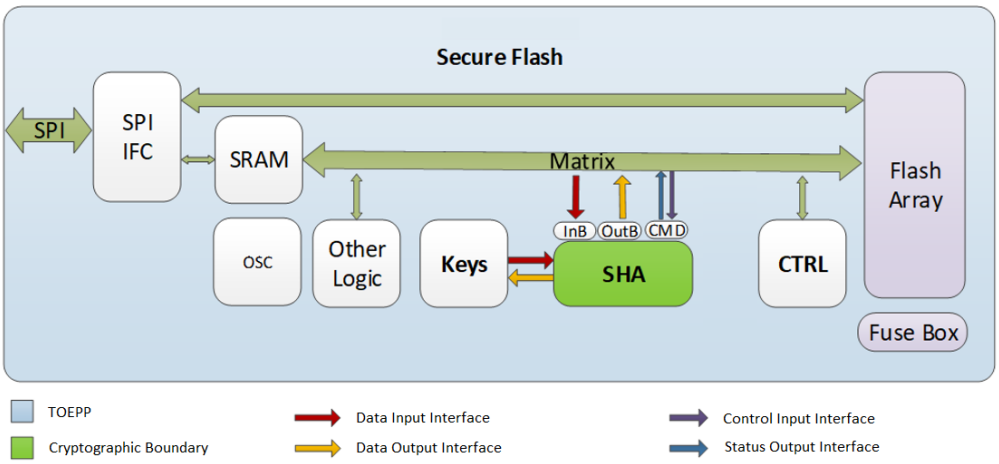

Figure 1: Cryptographic Module (Block Diagram)

Tested Operational Environment's Physical Perimeter (TOEPP):

The TOEPP of the module is defined as the TrustMe © secure flash memory in which the module operates. It is composed of the following main components:

- SRAM: Input/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
- Keys: Session control parameters
- OSC: Internal Clock Oscillator
- SPI IFC: SPI front-end

Figure 2: TrustMe © secure flash memory (Front)

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
TrustMe © W77[Q/T]64/128/256/512/1024/2028Mb	0001 (1h)	N/A	N/A	

Table 2: Tested Module Identification – Hardware

The sub-chip cryptographic module version consists of the four bits (HASH_VER) with the value "1" in hexadecimal (the penultimate value of the hardware version), which is the same for all TrustMe © secure flash memories listed in the table above.

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

There are no components within the cryptographic boundary that are excluded from the FIPS 140-3 security requirements.

2.4 Modes of Operation

Modes List and Description:

The table below details the Modes of Operation supported by the module.

Mode Name	Description	Type	Status Indicator
Approved Mode	Operation mode where the module executes approved services	Approved	The status indicator is the one associated to the internal READY state, composed of the following signals: CMVP_DONE = 1; CMVP_PASS = 1; SHA_BUSY = 0; SSR_STATE = WORK value (01x)

Table 3: Modes List and Description

The module implements only one mode of operation, the Approved Mode, in which the approved services are available. No configuration is necessary for the module to operate and remain in the Approved Mode.

After passing all self-tests on start-up, the module automatically transitions to the Approved Mode.

2.5 Algorithms

Approved Algorithms:

The table below lists all the Approved Algorithms supported by the module.

Algorithm	CAVP Cert	Properties	Reference
SHA2-256	A6518	Message Length - Message Length: 0-768 Increment 1	FIPS 180-4

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

The module does not support any Vendor-Affirmed Algorithms in the Approved Mode of operation.

N/A for this module.

Non-Approved, Allowed Algorithms:

The module does not support any Non-Approved, Allowed Algorithms in the Approved Mode of operation.

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

The module does not support any Non-Approved, Allowed Algorithms with No Security Claimed in the Approved Mode of operation.

N/A for this module.

Non-Approved, Not Allowed Algorithms:

The module does not support any Non-Approved Algorithms that are not Allowed in the Approved Mode of operation.

N/A for this module.

2.6 Security Function Implementations

The table below lists the Security Function Implementations supported by the module.

Name	Type	Description	Properties	Algorithms
Message Digest	SHA	Compute a message digest		SHA2-256: (A6518)

Table 5: Security Function Implementations

2.7 Algorithm Specific Information

There is no algorithm specific information.

2.8 RBG and Entropy

N/A for this module.

N/A for this module.

2.9 Key Generation

The module does not implement any key generation methods.

2.10 Key Establishment

The module does not implement any automated key establishment methods.

2.11 Industry Protocols

The module does not implement any industry protocols.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The table below details the module Ports and Interfaces.

Physical Port	Logical Interface(s)	Data That Passes
Matrix-In-Data	Data Input	Data input (32b)
Matrix-In-Addr	Data Input	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	Data Input	Direct Data-input (128b) from KEYS function
Matrix-Out-Addr	Data Output	Address of the output data to read from (3b) select which 32b data-out word is accessed (out of 32B)
Matrix-Out-Data	Data Output	Data output (32b) from the SHA result
Keys-Data-Out	Data Output	Direct Data-output (128b) to KEYS function (from Hash result)
Reset	Control Input	Reset/Initialize the SHA module and internal states
SHA-Start	Control Input	Start execution of SHA Iteration
HASH-VER	Status Output	Indicates the module version
CMVP-DONE	Status Output	If set, indicates the self-tests execution is complete
CMVP-PASS	Status Output	If set, indicates the self-tests are passed with success
SHA-BUSY	Status Output	If set, indicates that the SHA operation is being performed. Otherwise, the calculation is complete and module is idle
N/A	Power	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 6: Ports and Interfaces

4 Roles, Services, and Authentication

4.1 Authentication Methods

The module does not support authentication for roles.

N/A for this module.

4.2 Roles

The module supports two roles that an operator may assume: Crypto Officer (CO) role and User role. Roles are assumed implicitly based on the service accessed. The table below lists the Roles supported by the module.

Name	Type	Operator Type	Authentication Methods
User	Role	User	None
Crypto Officer	Role	CO	None

Table 7: Roles

4.3 Approved Services

The table below lists all Approved Services supported by the module. The abbreviations of the access rights to keys and SSPs have the following interpretation:

G = Generate: The module generates or derives the SSP.

R = Read: The SSP is read from the module (e.g., the SSP is output).

W = Write: The SSP is updated, imported, or written to the module.

E = Execute: The module uses the SSP in performing a cryptographic operation.

Z = Zeroize: The module zeroizes the SSP.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Module Initialization	Secure initialization of the module	N/A	None	None	None	Crypto Officer
Message Digest	SHA2-256 hash computation	"Busy Bit" set to 1	Message	Hash value	Message Digest	User
Show Version	Return the module version	None	None	Module version	None	Crypto Officer
Show Status	Return the module status	None	None	Module status	None	Crypto Officer
On-Demand Self-test	Initiate on-demand self-tests	"Busy Bit" set to 1	CMVP_BIST command that is executed after a module Reset/Reboot	Pass or Fail	Message Digest	Crypto Officer
Zeroisation	Zeroise all SSPs	None	Flush command	None	None	Crypto Officer

Table 8: Approved Services

According to FIPS 140-3 IG 2.4.C, the module shall indicate when an approved cryptographic algorithm is being used, either by executing an approved security function or during the self-tests. Moreover, the FIPS 140-3 IG 2.4.C states that it is possible to define a static global indicator to provide this indication which in this case is the “Busy Bit” (SHA_BUSY).

4.4 Non-Approved Services

The module does not support any Non-Approved Services.

N/A for this module.

4.5 External Software/Firmware Loaded

The module does not load external software or firmware.

5 Software/Firmware Security

5.1 Integrity Techniques

The module does not need to comply with this section because it is a purely hardware sub-chip cryptographic module defined into the TrustMe © secure flash memory.

5.2 Initiate on Demand

As stated above, the module does not implement any integrity test that can be invoked on demand because it is a purely hardware sub-chip cryptographic module defined into the TrustMe © secure flash memory.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Non-Modifiable

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Hard and opaque enclosure	No actions are required to maintain the physical security of the module	No actions are required to maintain the physical security of the module

Table 9: Mechanisms and Actions Required

The module is a sub-chip module implemented as part of a single-chip embodiment composed of production-grade components with a hard, opaque enclosure that is the TOEPP defined by the entire TrustMe © secure flash memory.

8 Non-Invasive Security

Currently, the ISO/IEC 19790:2012 non-invasive security area is not required by FIPS 140-3 (see NIST SP 800-140F). The requirements of this area do not apply to the module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

The module does not store any SSP.

N/A for this module.

9.2 SSP Input-Output Methods

The module does not support SSP entry and output.

N/A for this module.

9.3 SSP Zeroization Methods

Although the module does not support SSP generation, SSP establishment, SSP entry and output, or SSP storage, the zeroization is implemented as required by the FIPS 140-3 standard to remove any information residues related to the message digest calculations by using the FLUSH command.

Zeroization Method	Description	Rationale	Operator Initiation
FLUSH command	FLUSH command is automatically executed by the module after completing the message digest operation.	Remove any residual information related to the message digest calculation.	Automatically done by the module.

Table 10: SSP Zeroization Methods

9.4 SSPs

The only cryptographic operation supported by the module is the computation of the message digest based on the SHA2-256 cryptographic algorithm, so the module does not use any SSP.

N/A for this module.

N/A for this module.

10 Self-Tests

This section specifies the pre-operational and conditional self-tests performed by the module. The pre-operational and conditional self-tests ensure that the module is not corrupted and that the cryptographic algorithms work as expected.

10.1 Pre-Operational Self-Tests

Pre-operational Self-Tests are run upon the power-up/initialization of the module. The module transitions to the operational state only after the pre-operational self-tests are passed successfully.

The design of the module ensures that all data output, via the data output interface, is inhibited whenever the module is in a pre-operational self-test condition. Because the module is purely hardware and contains neither software nor firmware, it implements the CAST as pre-operational self-tests.

N/A for this module.

10.2 Conditional Self-Tests

Conditional Self-Tests are run when an applicable security function or process is invoked. The Conditional Self-Tests are detailed in the table below.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-256	256-bit hash	KAT	CAST	Successful initialization of the module	Message digest	Module Initialization

Table 11: Conditional Self-Tests

The module performs self-tests on all approved cryptographic algorithms supported in the Approved Mode of operation, using the tests shown in the table above. To ensure all conditional CASTs are performed before the first operational use of the associated algorithm, all CASTs are performed during the module's initial power-up sequence.

Services are not available, and data output (via the data output interface) is inhibited during self-tests. If any of these tests fail, the module transitions to the error state.

10.3 Periodic Self-Test Information

All self-tests can be run on-demand, for periodic testing, by rebooting/resetting the module.

N/A for this module.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-256	KAT	CAST	On demand	By rebooting/resetting the module

Table 12: Conditional Periodic Information

10.4 Error States

If any of the Pre-operational Self-Tests or Conditional Self-Tests fail, the module will output an error status and enter an error state, where all data output is inhibited. Upon entering an error state, an operator can attempt to clear the error state by resetting the module.

The table below shows the different causes that lead to the Error States and the status indicators reported.

Name	Description	Conditions	Recovery Method	Indicator
Error	The module's error state	CAST	Module reboot/reset	Error Code (CMVP_DONE = 1, CMVP_PASS = 0, and SHA_BUSY = 0)

Table 13: Error States

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

No configuration of the module or installation steps are required by the operator. When the TrustMe © secure flash memory is powered on, the module also powers on and starts performing its power-up self-tests without any operator intervention. The module enters Approved Mode automatically if the power-up self-tests are completed successfully (the signals *CMVP_DONE* and *CMVP_PASS* will be set). If any of the self-tests fail during power-up, the module transitions to an Error state.

The operator can verify that the module is in the Approved Mode of operation and that the FIPS-validated version is being used, by checking the module version and comparing it against the versioning information on the module certificate.

The sub-chip cryptographic module version is contained into the HW_VER Register, which contains the TrustMe © secure flash memory hardware version, specified by using four bits in hexadecimal format (the penultimate value of the HW_VER Register):

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

11.2 Administrator Guidance

None

11.3 Non-Administrator Guidance

None

11.4 Design and Rules

When the module is securely installed and initialized as detailed above, it initializes in Approved Mode which is the only mode of operation that complies with the following rules:

1. The module is initialized in the Approved Mode of operation automatically after the power-on self-tests are completed successfully.
2. Once the module is powered on, the power-on self-tests are executed automatically without any operator intervention.
3. All data output interfaces are inhibited during self-tests, zeroization, and error states.
4. The module does not support random number generation, SSP generation, SSP establishment, SSP entry and output, or SSP storage.
5. The module does not implement critical security functions to be tested during the self-test.
6. The module does not support a maintenance interface or maintenance role.
7. The module does not provide bypass capability.
8. The module does not implement authentication mechanisms.
9. The module is a purely hardware sub-chip that does not contain any software nor firmware, therefore, it executes the CAST during the pre-operational self-tests.
10. The module allows the CO to execute the self-test on-demand either by sending the *CMVP_BIST* command to the module or by rebooting/resetting the module.
11. If the module is in an error state, the cryptographic operativity will be disabled.
12. The normal operation of the module can be resumed from an error state by resetting the module.
13. The module does not implement non-invasive security measures.
14. The module does not implement mitigation of other attacks.

11.5 End of Life

The module does not require sanitization because it does not store any SSP and in addition, all the residues related to the message digest calculations are erased once the calculation is finished.

12 Mitigation of Other Attacks

The module does not offer mitigation of other attacks and therefore this section is not applicable.