Security Target for <*W75F32WWJB\W75F32WWJC Secure Flash Memory* >

Version <*1.3*>, dated <*2020-09-15*>

<*Winbond Electronics Corporation*>

Version Control

Version	Date	Description
1.0	*2020-04-07*	*First release*
1.1	*2020-05-29*	*Section 3.1.7 updated adding the flaw reporting procedure*
1.2	*2020-08-04*	*Updated section 1.3 with new documentation version; updated section 3.2 by rewriting security rules; updated section 3.1.7 adding flow remediation process for third parties; updated section 3.2.1 regarding the TOE identification; updated section 3.2.4 rewording the TOE protections; updated section 5 by adding SESIP-GP specifications and updated documents.*
1.3	*2020-09-15*	*Updated Section 3.1.7 and added the communication channel to report corrective actions; updated sections 3.2.4, 3.2.9 and 3.2.11 to reword Security Function Requirements.*

Table of Contents

1 Introduction

The Security Target describes the Platform (in this chapter) and the exact security properties of the Platform that are evaluated against [GP-SESIP] (in chapter 3) and that a potential consumer can rely upon the product upholding if they fulfill the objectives for the environment (in chapter 2).

1.1 ST reference

See title page.

1.2 Platform reference

TOE name	*SpiFlash® TrustME™ Secure Flash Memory*
TOE version	*A*
TOE identification	*W75F32WWJB\W75F32WWJC*
TOE Type	*Memory Flash IC*

1.3 Included guidance documents

The following documents are included with the platform:

Reference	**Name**	**Version**
[OPE_JB]	*W75F32WWJB Secure Flash Operational User Guidance* *Doc ID: S6065-AAG078.11*	*Version I*
[OPE_JC]	*W75F32WWJC Secure Flash Operational User Guidance* *Doc ID: S6065-AAG078.12*	*Version I*
[PRE_JB]	*W75F32WWJB Secure Flash Preparative User Guidance* *Doc ID: S6065-AAG078.13*	*Version H*
[PRE_JC]	*W75F32WWJC Secure Flash Preparative User Guidance* *Doc ID: S6065-AAG078.14*	*Version H*
[SFI_FS_8.9]	*SFI IP Functional Specification Doc ID: S6065-AAG078.9* *(HW_VER) 0000h*	*Version D*
[SFI_FS_8.10]	*SFI IP Functional Specification Doc ID: S6065-AAG078.10* *(HW_VER) 0010h*	*Version D*
[Datasheet]	*TrustME™ W75xxBx/W75xxCx* *1.8V 32M-BIT SECURE SERIAL FLASH Datasheet*	*Version D*

1.4 Platform functional overview and description

The TOE consists of:

- HW IC Part number (name W75F32WWJB\W75F32WWJC version A) delivered in good die form via Courier.
- Set of associated IC dedicated documentation (see section 1.3) delivered in PDF via e-mail.

TOE description

The TOE is a dedicated external memory. The memory is intended to be embedded into highly critical hardware devices such as smart card, secure element, USB token, secure micro SD, etc. These devices will embed secure applications such as financial, telecommunication, identity (e-Government), etc. and will be working in a hostile environment. In particular, the TOE is dedicated to the secure storage of the code and data of critical applications.

The security needs for the TOE consist in:

- Maintaining the integrity of the content of the memories and the confidentiality of the content of protected memory areas as required by the critical HW products (e.g. Security IC) the Memory Flash is built for;
- Providing a secure communication with the Host device that will embed the TOE in a secure HW product such as Security IC;

The main security features of the TOE are as follows:

- Secure separation between Test mode and User mode. More precisely,
    - The switch from User mode to Test mode can only be done after completely erasing the flash content.
    - The confidentiality and the integrity of the flash content are protected in both Test mode and User mode.
- The confidentiality and the integrity of the transmitted data from/to the Host device are protected by a secure channel;
- Integrity protection of the flash content by error detection codes (CRC-32);
- Confidentiality protection of the flash content by memory scrambling with diversified key;
- Security sensors or detectors including power glitch detector and out-of-specified operating conditions (voltage, temperature, clock frequency);
- Active Shields against physical intrusive attacks (e.g. reverse-engineering, probing);
- State machine protection to counter fault injection;
- Dual Flip-Flops and bus encoding to counter fault injection and information leakage;
- Failure counter to detect and react to tamper attempts;

TOE scope

The TOE scope is depicted in Figure 1. The TOE is delimited by the Red box. Parts outside the red box are outside of the evaluated scope. The out of scope part comprises:

- The Host device that will embed the TOE and will be needed to run the TOE in order to stimulate the TSF. It is assumed that all components (Hardware or Software) of the Host Device are appropriately protected in the TOE security environment
- SPI Bus for the communication between the Host device and the TOE

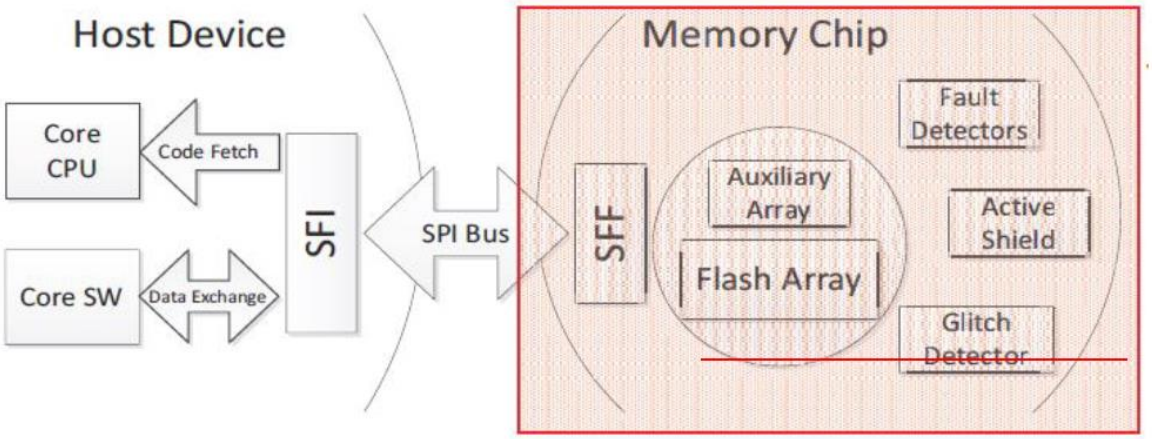

Figure 1 TOE scope

- Auxiliary array contains the flash specific data: the binding key (and its digest value), the failure and session counters;
- Flash array stores the User data (i.e. the mass data including executable codes) and translates SPI commands into Flash operations;
- SFF (Secure Flash Front-end) which implements encrypted and authenticated interface for Flash operation and supports Flash memories up to 4GB;
- Detectors of abnormal operating conditions;

The physical interface of the TOE with the external environment is the entire surface of the Memory Flash module. The electrical interface of the TOE with the external environment is made of the chip's pads including the data pins for SPI bus:

- Standard SPI: CLK, /CS, DI_IO0, DO_IO1
- Quad SPI: CLK, /CS, DI_IO0, DO_IO1, IO2, IO3
- Octal: CLK, /CS, DI_IO0, DO_IO1, IO2, IO3, IO4, IO5,
- IO6, IO7

The TOE physical scope consists of the TOE documentation (user guidance) as listed in section 1.3 and the following Hardware components:

Component	Name	Version
HW IC part	*SpiFlash® TrustME™ Secure Flash Memory (W75F32WWJB\W75F32WWJC)*	*Version* A
Document	*Associated IC dedicated documentation as listed in section 1.3*	*N/A*

The logical scope includes the logical interface of the TOE that is made of Flash commands and described in user guidance listed in in section 1.3.

TOE features

The TOE can be delivered in two different configurations. Depending on the TOE configuration, the applicable documentation is different. Details are as listed in section 1.3:

Part Number	Density	Binding Method	Note
W75F32WWJB	*32 Mbit*	*Single-Phase*	*Requires to be done in secured environment*
W75F32WWJC	*32 Mbit*	*Two-Phase*	*Support secure binding to be completed in non-secure environment*

The TOE can be operated in two different modes:

TEST mode	USER mode
In TEST mode, the TOE provides access to both the auxiliary and flash arrays. However, there are some restrictions in the Test mode: • The Binding Key (Kb) cannot be read out; • The auxiliary array can only be erased if a complete erase has been done after the last reset; • The read and write commands do not read and write effective values of the flash;	In USER mode, the access to the flash arrays is authenticated and controlled via the flash commands. There is no interface to access to the auxiliary array. TOE cannot switch back from USER mode to TEST mode without erasing all the memory.

The TOE physical characteristics are described as follows:

Performance

- 50MHz Standard/Quad/Octal SPI clocks
- 20.5MB/S continuous encrypted and authenticated data transfer rate
- More than 100,000 erase/program cycles
- More than 20-year data retention

Efficiency

- 16-byte burst read
- Data Integrity Check

Allows secure execution in place (S-XIP) operation

Operating conditions

- Single 1.65 to 1.95V supply
- 20mA active current, <1µA Power-down (typ.)
- -40°C to +105°C operating range

4KB-block Architecture

Uniform Block Erase (4K-bytes)

Program 1 to 16 byte in a single command

Erase/Program Suspend & Resume

2 Security Objectives for the operational environment

In order for the TOE to fulfill its security requirements, the operational environment (technical or procedural) must fulfil the following objectives.

Secure communication with the TOE
The authorized Host device shall support the trusted communication channel with the TOE by protecting the confidentiality and the integrity of the transmitted data.

In particular, the host device shall correctly protect the secure channel in order to prevent data modification, disclosure, insertion, deletion and replaying.

Protection during Binding process
Security procedures shall be used after the TOE delivery to maintain confidentiality and integrity of the TOE (to prevent any possible copy, modification, retention, theft or unauthorized use).

In addition, the host device shall provide a secure random source for generating a fresh Binding key (Kb) for the TOE.

In order to fulfil these security objectives, several security rules shall be followed as explained in Appendix 2 of [OPE_JB] and [OPE_JC].

3 Security requirements and implementation

3.1 Security Assurance Requirements

The claimed assurance requirements package is: **SESIP3** as defined in [GP-SESIP]

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 [ADV_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 Complete mapping of the implementation representation of the TSF to the SFRs (ADV_IMP.3)

In accordance with the requirement for a complete mapping of the implementation representation of the TSF to the SFRs (ADV_IMP.3), the developer provided the implementation representation for the entire TSF in the form of Verilog and System Verilog files. Thereby, the TSF is defined to a level of detail such that the TSF can be generated without further design decisions.

In order to support the implementation representation, the developer also provides an excel file [ADV_IMP] to match the Verilog modules with the modules described in sections **2**, **3** and **4** of [ADV_TDS]. Moreover, some descriptions of the design identified as design elements in [ADV_TDS], are matched with the implementation in tab **"ADV tables mapping"** of [ADV_IMP].

3.1.3 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 for both TOE configurations [OPE_JB] and [OPE_JC]. Such 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 TOE 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 TOE (TEST mode and USER mode).

- Security rules to be followed in order to fulfil the security objectives for the operational environment.

3.1.4 Preparative procedures (AGD_PRE.1)

In accordance with the requirement for preparative procedures (AGD_PRE.1), the developer provided the Preparative User Guides for both TOE configurations [PRE_JB] and [PRE_JC]. Such guides include the following information:

- Necessary steps for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
- Necessary steps for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment.

3.1.5 Labelling of the TOE (ALC_CMC.1)

In accordance with the requirement for the labelling of the TOE (ALC_CMC.1), the developer provided the document “Configuration Management Capabilities” [ALC_CMC], where it is explained how:

- It is ensured that the TOE is labelled with its unique reference;
- It is ensured that the TOE is correct and complete before it is sent to the customer;
- It is ensured that no configuration items are missed during evaluation;
- It is prevented unauthorized modification, addition, or deletion of configuration items.

3.1.6 TOE CM Coverage (ALC_CMS.1)

In accordance with the requirement for the TOE CM coverage (ALC_CMS.1), the developer provided the document “Configuration Management Capabilities” [ALC_CMC], where it is explained how:

- It is ensured that changes on the TOE are managed at the implementation level;
- It is ensured that the tracking of problems on the TOE is also controlled;
- It is ensured that the tools used for the development of the TOE are controlled as well, since they have a significant impact on the final quality of the TOE;
- The configuration item list includes the TOE itself and uniquely identifies all configuration items.

3.1.7 Flaw Reporting Procedure (ALC_FLR.2)

Due to the TOE type (Memory Flash IC), and due to the fact that the TOE 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 TOE are not possible.

In case of any suspected security issue detection, please contact https://www.winbond.com/hq/support/technical-support/?__locale=en as a supporting point.

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

- Reporting: Identified flaws can be communicated to Winbond through the URL defined above.
- Evaluation: Winbond follows an analysis with the following steps:
  - Customer Return (Flaw Analysis) FA flow
  - FA Task Procedure
  - FA Report – 8D methodology
  - FA cycle time
  - FA cycle time - AG
- Solution: Winbond will provide the FA report to the customer with the concluded corrective action.
- Communication: In case corrective actions are identified, an Engineering Change Notice (ECN) will be distributed to the customers by email.

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 aforementioned URL.

3.1.8 Independent testing: conformance (ATE_IND.1)

In accordance with the requirement for Independent testing: conformance (ATE_IND.1), the developer provides the TOE (both configurations), the experimental set-up and the related documentation for testing ([ATE_vE], [ATE_COV_vE], [ATE_CTDvB] and [ATE_TSTL]).

3.1.9 Focused Vulnerability Analysis (AVA_VAN.3)

In accordance with the requirement for a Focused Vulnerability Analysis (AVA_VAN.3), the developer provides the TOE (both configurations) and the necessary experimental set-up for testing.

3.2 Security Functional Requirements

The platform fulfills the following security functional requirements:

3.2.1 Identification of platform type

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

1. Tamper evidence for package integrity and package level for the correct version of the product **W75F32WWJB/ W75F32WWJC**.
2. Verify that the version on the die marking on the Known Good Die is correct (**AAG078A**).
3. Run ‘GET_STATUS’ command to get the TOE product type:
   a. BIT EMPTY (2) = **1**: The device is W75F32WWJB.
   b. BIT EMPTY (2) = **0**: The device is W75F32WWJC.

Self-assessment:

The TOE (part of a platform) provides the secure acceptance procedures [PRE_JB] and [PRE_JC] (see section 1.3), where the expected version numbers for all delivered parts of the TOE are given (AAG078A die marking, W75F32WWJB/ W75F32WWJC version A).

Moreover, a procedure is described in order to identify the TOE through testing (Secure installation/configuration).

~~3.2.2 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.~~

3.2.3 Identification of individual platform

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

Self-assessment:

Only in TOE configuration W75F32WWJC, the Secure Flash Device is provided with a pre-programmed secret (pre-Binding Key) that is unique per Secure Flash Device. The pre-programmed secret is provided to the User in a database that maps a device's Unique Device ID hash (HUID) to its pre-Binding Key (see section 2.1 Package contents in [PRE_JC]).

This unique ID is necessary in order to perform the binding process in this particular TOE configuration (W75F32WWJC). See section 2.2 in [OPE_JC] for the full details.

3.2.4 Secure communication support

The platform provides the support to establish a secure communication channel(s) against threats as detailed below.

The secure communication channel authenticates **the host and the TOE** and protects against **disclosure (plaintext data disclosure by probing), modification (Man-in-the-Middle), hammering** (a.k.a. brute-forcing) **and replay** of messages between the endpoints, using **a SPI bus and the security measures:**

- a fresh session key is used for each session;
- for update operations (write/erase): the payload (access address and data) is encrypted (by a stream cipher) and a MAC digest is added to ensure integrity;
- for reading operation: 8 transport integrity check bits are added to each 32 bit long word, providing a progressive authentication of the transmitted data;
- session and transaction counters are also used to protect against replaying;
- Failure counter is used to protect against authentication brute force.

Self-assessment:

The confidentiality and the integrity of the communication between the TOE and the Host-Device is protected against disclosure (plaintext data disclosure by probing), modification (Man-in-the-Middle), hammering and replay attacks. In particular, as described above.

The TSF enables in-place execution of the code stored in the TOE. For this purpose, each data-word sent by TOE is separately encrypted by applying a cascade of a stream ciphering operation and a mixing operation that cryptographically maps input bits to output bits.

Furthermore, to maintain the throughput needed for the in-place execution, the data sent by TOE is authenticated by a sequence of authentication bytes interleaved with the data-words so that each given byte cumulatively authenticates the data words that were authenticated by a previous byte in the sequence and the data words transmitted between the previous byte and the given byte.

This implementation can be assessed through testing.

3.2.5 Secure communication enforcement

The platform ensures the application can only communicate with **the memory flash IC (TOE)** over the secure communication channel(s) supported by the platform.

Self-assessment:

The TSF ensures that only an authorized Host device (i.e. a Host device that knows the Binding key Kb) can open a secure channel to communicate with the TOE.

More precisely, the TSF provides a mutual authentication between the Host device and the TOE by verifying that both of them share the same Binding key. A failed authentication increases the Failure counter: if this counter reaches a pre-defined value, then the TOE is locked.

This implementation can be assessed through testing. See guidance documents for full details (section 1.3).

3.2.6 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, ensuring that the other functional requirements are not compromised.

Self-assessment:

The TSF protects the TOE against physical manipulation (including the TOE probing) by implementing the following security mechanisms:

- Failure counter: this counter is incremented after each tamper-detection and the TOE is locked if the counter reaches a pre-defined value.
- Active Shielding: The Active Shield detection is filtered using a counter, when that number reaches a preset threshold, the Active Shield raises a tamper alarm.

- Dual flip-flops: A difference in the state of two joint flip-flops indicates a fault and raises the Fault Injection Alarm output signal. This mechanism is designed to detect perturbation attacks like Laser or Electro-Magnetic fault injections.
- Clock-tree protection: The 0-1 pattern spreads in a dedicated shift register with every clock pulse provided all clock signals are active. This mechanism is designed to ensure that the clock-tree is intact.
- State machine monitoring: The TOE implements Tamper Detectors that detects abnormal conditions and reports a fault state.
- Bus Encoding: Command bus to the Flash array is encoded, such that more than 1-bit flip distinguishes between any two commands. Furthermore, some of the bits of the command are used as qualifiers for internal analog processes within the Flash array.

Moreover, the TSF detects abnormal operation conditions (voltage, temperature, clock frequency, power glitch) using the corresponding sensors. If an abnormal operation condition happens, then the TSF disturbs the cryptographic computations, interrupts data interchange and inform the host.

The TSF also protects the TOE against the inherent or intentional leak of the TOE operations by the following security mechanisms:

- Advanced stream cipher using long linear feedback shift registers: the calculations are protected against timing and power consumption leak;
- Anti-leakage measures for the hash functions that are used for stream-ciphering and MAC digest: masking input data and undisclosed intermediate output values;
- Session setup: the logic is protected against timing and power consumption leak;

The implementation of these security measures can be assessed through testing.

3.2.7 Software attacker resistance: isolation of platform

The platform provides isolation between the application and itself, such that an attacker able to run code as an application on the platform cannot compromise the other functional requirements.

Self-assessment:

The TOE is physically isolated from the Host. The communication between them can only be performed through the SPI bus via a secure channel established during the binding process. Therefore, only an authenticated host can perform read, write and erase operations.

This implementation can be assessed through testing.

3.2.8 Cryptographic keystore

The platform provides the application with a way to store **the binding key** 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 **to establish the secure channel**.

Self-assessment:

The binding key and its digest value are stored in the auxiliary array.

In user mode, there is no way to access to the auxiliary array.

In test mode, the binding key cannot be read out.

The only way to switch from user mode to test mode is by erasing all memory contents (including the binding key).

This implementation can be assessed through testing.

3.2.9 Secure encrypted storage

The platform ensures that all data stored by the application, with the exception of **nothing**, is encrypted as specified below with a platform instance unique key of key length 80 bits.

Self-assessment:

The TSF protects the integrity of the User Data (including executable codes) stored in the flash array using **CRC-32 error detecting code**. All User data can be protected by CRC-32 error detecting code but the integrity verification is performed only if the access is done via an authenticated read (i.e. AUTH_READ command).

If an inconsistency is detected between the User data and its error detecting code, then the TSF informs the Host-Device about the error.

In addition, the TSF also sends pseudo-randomly chosen of the CRC-32 error detecting code to the Host-Device in a secure way so that the host can independently verify data integrity**.**

Moreover, the TSF protects the confidentiality of the User Data stored in the flash array by a **memory scrambling** mechanism that is based on diversified keys. Both the addresses and the memory content are scrambled but by a key that is unique for each instance of the TOE.

Furthermore, the TSF protects the User data against disclosure by manipulating the binding key. In particular, the Flash array is completely erased before:

- A new Binding key is set, or
- the current Binding key is erased.

In addition, the current Binding key is stored in the Auxiliary array and cannot be read out by the Flash commands. The integrity of the Binding key is protected by a digest value: if an illegal modification is detected on the Binding key, then the TOE is locked and can only be unlocked in Test mode (and the Flash array has been erased).

The implementation of these security mechanisms can be assessed through testing.

3.2.10 Residual information purging

The platform ensures that **the flash array and the auxiliary array** are erased by using a non-Authenticated Read and then sending a GET_STATUS command (as specified in **the operational guidance**) before the memory is (re)used by the platform or application again and before an attacker can access it.

Self-assessment:

The TSF enforces the complete erasure of the Flash content before a new Binding key is set or the current Binding key is erased.

This can be assessed through testing.

3.2.11 Secure debugging

The platform only provides **the host** authenticated as specified in Secure Communication Support with debug functionality**.**
The platform ensures that all data stored by the application is made unavailable.

Self-assessment:

As explained in section 2.6 of the functional specification [ADV_FSP], specific actions need to be carry out to enter to TEST mode. The TSF ensures that the User Data is not disclosed or manipulated via the features available in the TEST mode. In particular, the Flash array is completely erased before switching to TEST mode. Furthermore, the access to User data is also restricted in the Test mode. More precisely:

- The Binding Key (Kb) cannot be read out by the Flash commands;
- The Binding key cannot be erased unless a complete erase has been done after the last reset;
- The read and write commands do not read and write effective values of the Flash array;

This implementation can be assessed through testing.

4 Mapping and sufficiency rationales

4.1 SESIP3 sufficiency

Assurance Class	Assurance Families	Covered by	Rationale
ASE: Security Target evaluation	ASE_INT.1 ST Introduction	Section Introduction “and “Title”	The ST reference is in the Title, the TOE reference in the “Platform reference”, the TOE 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 in Security Objectives for the operational environment refers to the guidance documents.
	ASE_REQ.3 Listed Security requirements	Section “Security Functional Requirements”.	All SFRs in this ST are taken from [GP-SESIP]. “Identification of platform type” is included. “~~Secure update of platform~~” not included (justification in ALC_FLR.2)
	ASE_TSS.1 TOE Summary Specification	Section “Security requirements and implementation”	All SFRs are listed per definition, and for each SFR the implementation and verification is defined in “Security Functional Requirements”.
ADV: Development	ADV_FSP.4 Complete functional specification	Document [ADV_FSP]	[ADV_FSP] provides an accurate and complete instantiation of the SFRs. All TSFIs are described.
	ADV_IMP.3 Complete mapping of the implementation representation of the TSF to the SFRs	Verilog and system Verilog files. Documents [ADV_TDS] and [ADV_IMP]	The implementation representation defines the TSF to a level of detail such that the TSF can be generated without further design decisions.
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	Documents [OPE_JB] and [OPE_JC]	Description of secure operation of the TOE and security rules to fulfil with security objectives for the operational environment.

	AGD_PRE.1 Preparative procedures	Documents [PRE_JB] and [PRE_JC]	Description of secure acceptance procedures and installation.
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE	Document [ALC_CMC]	Section 2 of [ALC_CMC] describes how the TOE is uniquely labelled.
	ALC_CMS.1 TOE CM coverage	Document [ALC_CMC]	Section 2 and section 4 of [ALC_CMC] describes how the configuration item list identifies the TOE itself and uniquely all items.
	ALC_FLR.2 Flaw reporting procedures	Document “Flaw Reporting Procedure (ALC_FLR.2)”.	The flaw reporting and remediation procedure is described in [ALC_FLR]. Since updates to the TOE are not possible , the for SFR “Secure update of platform” is removed.
ATE: Tests	ATE_IND.1 Independent testing: conformance	Documents [ATE_vE], [ATE_COV_vE], [ATE_CTDvB] and [TS_TL_July]	The TOE (both configurations), the experimental set-up and the test plan has been delivered for the laboratory independent testing.
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis	All delivered documentation, TOE and experimental set-up	Evidence delivered is the input for the vulnerability analysis to be performed by the laboratory.

5 References

[GP-SESIP] Security Evaluation Standard for IoT Platforms (SESIP), version 1.0, March 2020, GP_FST_070.

[OPE_JB] W75F32WWJB Secure Flash Operational User Guidance Doc ID: S6065-AAG078.11, Version I

[OPE_JC] W75F32WWJC Secure Flash Operational User Guidance Doc ID: S6065-AAG078.12, Version I

[PRE_JB] W75F32WWJB Secure Flash Preparative User Guidance Doc ID: S6065-AAG078.13, Version H

[PRE_JC] W75F32WWJC Secure Flash Preparative User Guidance Doc ID: S6065-AAG078.14, Version H

[SFI_FS_8.9] SFI IP Functional Specification Doc ID: S6065-AAG078.9 (HW_VER) 0000h, Version D

[SFI_FS_8.10] SFI IP Functional Specification Doc ID: S6065-AAG078.10 (HW_VER) 0010h, Version D

[Datasheet] TrustME™ W75xxBx/W75xxCx 1.8V 32M-BIT SECURE SERIAL FLASH Datasheet, Version D

[ADV_FSP] W75FxxWKDJ-B/C Secure Serial Flash Memory Functional Specification, S6065-AAG078.5, Rev G

[ADV_TDS] W75FxxWKDJ-B/C Secure Serial Flash Memory Design Specification, S6065-AAG078.6, Rev F

[ADV_IMP] W75F32W_ADV_IMP_G.xlsx

[ALC_CMC] Secure Flash: Configuration Management Capabilities, S6065-AAG078.19, Rev I

[ALC_FLR] W75F FA flow, Rev A

[ATE_vE] W75FxxWKDJ-B/C Secure Serial Flash Memory ATE Document, S6065-AAG078.18, Rev E

[ATE_COV_vE] W75F32WKDJB\W75F32WKDJC Secure Serial Flash Memory ATE Tests Mapping Table, S6065-AAG078.17, Rev E

[ATE_CTDvB] W75F32WKDJB\W75F32WKDJC Secure Serial Flash Memory ATE Countermeasures Tests Description, S6065-AAG078.X, Rev B

[ATE_TSTL] Test_Suite_and_Test_Logs_July, 2019