Reference: 2019-48-INF-3811- v1
Target: Limitada al expediente
Date: 06.06.2022

Created by: CERT11
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2019-48**
TOE	**Winbond SpiFlash TrustME Secure Flash Memory W75F40WBYJEG version A**
Applicant	**22099218J - Winbond Electronics Corporation**
References	

[EXT-5414] Certification Request

[EXT-7686] Evaluation Technical Report

Certification report of the product Winbond SpiFlash TrustME Secure Flash Memory W75F40WBYJEG version A, as requested in [EXT-5414] dated 08/10/2019, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-7686] received on 08/04/2022.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Winbond SpiFlash TrustME Secure Flash Memory W75F40WBYJEG version A.

The Target of Evaluation is a Memory Flash IC.

Developer/manufacturer: Winbond Electronics Corporation

Sponsor: Winbond Electronics Corporation.

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Applus Laboratories.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 EAL5 + ALC_DVS.2 + AVA_VAN.5.

Evaluation end date: 05/05/2022.

Expiration Date[1]: 07/06/2027.

All the assurance components required by the evaluation level EAL5 (augmented with ALC_DVS.2 + AVA_VAN.5) have been assigned a "PASS" verdict. Consequently, the laboratory Applus Laboratories assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL5 + ALC_DVS.2 + AVA_VAN.5, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product Winbond SpiFlash TrustME Secure Flash Memory W75F40WBYJEG version A, a positive resolution is proposed.

TOE SUMMARY

The TOE is a memory flash IC designed 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 main function is the secure storage of the code and data of critical applications.

The security needs for the TOE consist in:

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

- 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.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL5 and the evidences required by the additional components ALC_DVS.2 and AVA_VAN.5, according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE.TSS.1
ADV	ADV_ARC.1
	ADV_FSP.5
	ADV_IMP.1
	ADV_INT.2
	ADV_TDS.4
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.4
	ALC_CMS.5
	ALC_DEL.1
	ALC_DVS.2
	ALC_LCD.1
	ALC_TAT.2
ATE	ATE_COV.2
	ATE_DPT.3
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.5

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R5:

SECURITY FUNCTIONAL REQUIREMENTS
FDP_IFC.1
FDP_ITT.1
FDP_RIP.1
FDP_SDC.1
FDP_SDI.2
FDP_UCT.1
FDP_UIT.1
FMT_LIM.1
FMT_LIM.2
FPT_FLS.1/Binding Key
FPT_FLS.1/Detectors
FPT_ITT.1
FPT_PHP.3
FPT_TRP.1
FRU_FLT.2

IDENTIFICATION

Product: Winbond SpiFlash TrustME Secure Flash Memory W75F40WBYJEG version A

Security Target: W75F40WBYJEG Secure Flash Memory Security Target (Version E).

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 EAL5 + ALC_DVS.2 + AVA_VAN.5.

SECURITY POLICIES

The use of the product Winbond SpiFlash TrustME Secure Flash Memory W75F40WBYJEG version A shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in [ST], chapter 3.4 (Organisational Security Policies).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The assumptions detailed in [ST], chapter 3.5 (Assumptions) are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

CLARIFICATIONS ON NON-COVERED THREATS

The threats detailed in [ST], chapter 3.3 (Threats) do not suppose a risk for the product Winbond SpiFlash TrustME Secure Flash Memory W75F40WBYJEG version A, although the agents implementing attacks have the attack potential according to the High of EAL5 + ALC_DVS.2 + AVA_VAN.5 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are detailed in [ST], chapter 4.2 (Security Objectives for the Operational Environment).

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

ARCHITECTURE

LOGICAL ARCHITECTURE

The main security features of the TOE are described as follows:

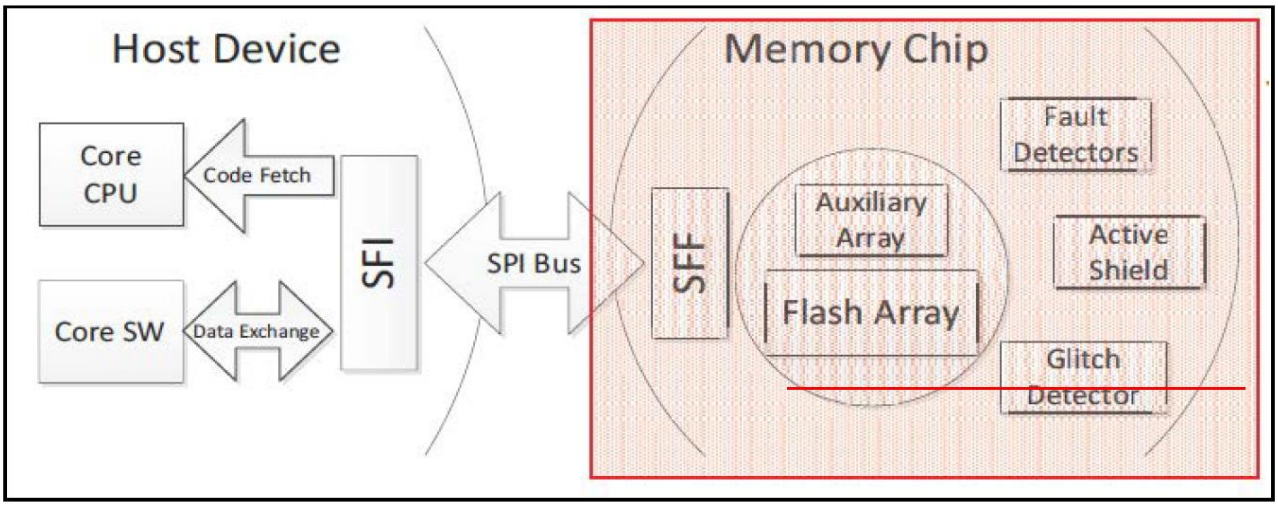
- Secure separation between Test mode and User mode. More precisely:
  - The switch from User mode to Test mode can only be done after completely erasing the flash content.
  - The confidentiality and the integrity of the flash content are protected in both Test mode and User mode.

- 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.

The logical interface of the TOE is made of Flash commands.

PHYSICAL ARCHITECTURE

The physical architecture is depicted in the following figure. The TOE is delimited by the red box.



The TOE consists of the following Hardware components:

- 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.
- Dual SPI: CLK, /CS, DI_IO0, DO_IO1.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

- W75F40WBYJEG Preparative User Guide (version I).
- W75F40WBYJEG Operational User Guide (version F).
- W75F40 Secure Flash Datasheet (version A).
- SFI Library User Guide (versión E).

PRODUCT TESTING

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.

During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluator has applied sampling strategy and has concluded that the information is complete and coherent enough to reproduce tests and identify the functionality tested.

In addition, the lab has devised a test for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that

this variation neither represents any security problem nor a decrease in the functional capacity of the product.

PENETRATION TESTING

Based on the list of potential vulnerabilities applicable to the TOE in is operational environment [JILAAPS], the evaluation team has devised vulnerability analysis and attack scenarios for penetration testing according to JIL supporting documents [JILAAPS] and [JILADVARCS]. Within these activities all aspects of the security architecture which were not covered by functional testing have been considered.

No attack scenario with the attack potential High according to Common Criteria v3.1 R5 has been successful in the TOE's operational environment as defined in the security target and the operational guidance [OPE_F] when all security measures required by the developer are applied.

EVALUATED CONFIGURATION

The TOE is defined by its commercial name and version number:

- Winbond SpiFlash® TrustME™ W75F40WBYJEG Secure Flash Memory version A.

The acceptance procedure for the evaluated configuration of the TOE is described in section 2 "Acceptance procedure" of the preparative user guidance [PRE_I].

The identifiers used to mark the evaluated configuration of the TOE are:

No	Type	Identifier	Version	Delivery Method
Form of delivery : Packaged Device				
1	HW	IC Part number	W75F40WBYJEG	Via Courier
Form of delivery : Associated IC Dedicated Documentation				
1	PDF	W75F40WBYJEG Preparative User Guide	Version I	Encrypted mail
2	PDF	W75F40WBYJEG Operational User Guide	Version F	Encrypted mail
3	PDF	W75F40 Secure Flash Datasheet	Version A	Mail
4	PDF	SFI Library User Guide	Version E	Encrypted mail

EVALUATION RESULTS

The product Winbond SpiFlash TrustME Secure Flash Memory W75F40WBYJEG version A has been evaluated against the Security Target W75F40WBYJEG Secure Flash Memory Security Target (Version E).

All the assurance components required by the evaluation level EAL5 + ALC_DVS.2 + AVA_VAN.5 have been assigned a "PASS" verdict. Consequently, the laboratory Applus Laboratories assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL5 + ALC_DVS.2 + AVA_VAN.5, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

- To follow the security guidance's of the TOE strictly
- To keep the TOE under personal control and set all other security measures available from the environment.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Applus Laboratories, a positive resolution is proposed.

The certifier strongly recommends to the TOE consumer to strictly follow the security recommendations that can be found on Appendix 1 "Security rules and Recommendations" of [OPE_F] and to observe the operational environment requirements and assumptions defined in the applicable Security Target.

Additionally, it should be noted that the SFI Library provided by the manufacturer in order to enable the interaction between the user and the TOE is part of the operational environment and, as a consequence, it has not been tested by the laboratory.

GLOSSARY

CCN Centro Criptológico Nacional

CNI Centro Nacional de Inteligencia

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

OC Organismo de Certificación

TOE Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[JILAAPS] Application of Attack Potential to Smartcards. Joint Interpretation Library. Version 3. April 2019. Joint Interpretation Library

[JILADVARCS] Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices, version 2.0. January 2012. Joint Interpretation Library.

[CCDB-2006-04-004] ST sanitising for publication. CCMC. April 2006.

[ST] W75F40WBYJEG Secure Flash Memory Security Target (version E).

[ST Lite] W75F40WBYJEG Secure Flash Memory Security Target Lite (version E1).

[PRE_I] W75F40WBYJEG Preparative User Guide (version I).

[OPE_F] W75F40WBYJEG Operational User Guide (version F).

[DS_A] W75F40 Secure Flash Datasheet (version A).

[SFI_UG_E] SFI Library User Guide (versión E).

SECURITY TARGET / SECURITY TARGET LITE

Along with this certification report, the complete security target of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

- W75F40WBYJEG Secure Flash Memory Security Target (version E).

The public version of this document constitutes the ST Lite. The ST Lite has also been reviewed for the needs of publication according to [CCDB-2006-04-004], and it is published along with this certification report in the Certification Body and CCRA websites. The ST Lite identifier is:

- W75F40WBYJEG Secure Flash Memory Security Target Lite (version E1).

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components up to EAL2 and ALC_FLR.