Reference: 2019-21-INF-3323-v1
Target: Público
Date: 03.12.2020

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

CERTIFICATION REPORT

Dossier #	**2019-21**
TOE	**Winbond Data Secure Flash Memory W77F32WWAW\W77F32WQ3W version B**
Applicant	**22099218J - Winbond Electronics Corporation**
References	

[EXT-4957] Certification Request

[EXT-6156] Evaluation Technical Report

Certification report of the product Winbond Data Secure Flash Memory W77F32WWAW\W77F32WQ3W version B, as requested in [EXT-4957], and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-6156] received on 18/08/2020.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Winbond Data Secure Flash Memory W77F32WWAW\W77F32WQ3W version B.

The TOE is a Memory Flash IC.

Developer/manufacturer: Winbond Electronics Corporation

Sponsor: Winbond Electronics Corporation.

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: Applus Laboratories.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 EAL2.

Evaluation end date: 15/10/2020.

Expiration Date[1]: 03/12/2025

All the assurance components required by the evaluation level EAL2 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 EAL2, 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 Data Secure Flash Memory W77F32WWAW\W77F32WQ3W version B, a positive resolution is proposed.

TOE SUMMARY

The TOE is a Memory Flash IC designed to be embedded into devices that will embed secure applications. The TOE is dedicated to the secure storage of the code and application's data.

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 HW the Memory Flash is built for.

[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.

- 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 EAL2, according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ADV	ADV_ARC.1
	ADV_FSP.2
	ADV_TDS.1
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.2
	ALC_CMS.2
	ALC_DEL.1
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
ATE	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.2

SECURITY FUNCTIONAL REQUIREMENTS

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

SECURITY FUNCTIONAL REQUIREMENTS
FRU_FLT.2
FAU_FLS.1
FMT_LIM.1
FMT_LIM.2
FDP_SDC.1
FDP_ITT.1
FPT_ITT.1

FDP_IFC.1
FDP_UCT.1
FDP_UIT.1
FTP_TRP.1
FPT_FLS.1
FDP_RIP.1
FDP_SDC.1

IDENTIFICATION

Product: Winbond Data Secure Flash Memory W77F32WWAW\W77F32WQ3W version B

Security Target: Security Target of W77F32WWAW\W77F32WQ3W Data Secure Flash Memory (version H).

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 EAL2.

SECURITY POLICIES

The use of the product Winbond Data Secure Flash Memory W77F32WWAW\W77F32WQ3W version B 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 (Organizational 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) not suppose a risk for the product Winbond Data Secure Flash Memory W77F32WWAW\W77F32WQ3W version B, although the agents

implementing attacks have a basic attack potential according to assurance level EAL2 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;
- Confidentiality protection of the flash content by memory scrambling with diversified key;
- State machine protection to counter fault injection;
- Dual Flip-Flops to counter fault injection and leakage attacks;
- Failure counter to detect and react to tamper attempts;

The logical interface of the TOE is made of Flash commands. The TOE consists of four subsystems and fifteen modules, which are related as shown in the table below.

PHYSICAL ARCHITECTURE

The TOE consists of the following Hardware components

- Auxiliary array contains the flash specific data.
- Flash array stores the User data and translates SPI commands into Flash operations.
- SFF (Secure Flash Front-end) which implements encrypted interface for Flash operation and supports Flash memories up to 4GB.

DOCUMENTS

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

- Winbond Technology Ltd., W77F32W Secure Flash Datasheet (version D).
- Winbond Technology Ltd., W77F32W Operational User Guide (version D).
- Winbond Technology Ltd., W77F32W Preparative User Guide (version F).
- Winbond Technology Ltd., SFI Library User Guide (version D).

PRODUCT TESTING

The tests performed by both the evaluator and the developer are based on the TSFIs description included in the functional specification and the SFRs description included in the Security Target [ST].

The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included in the installation and operation manuals. The TOE configuration used to execute the independent tests is consistent with the evaluated configuration according to the Security Target [ST].

The evaluator has repeated all the cases specified by the developer in the test documentation and has compared the obtained results with those obtained by the developer and documented in each associated report. The test repetition performed by the evaluator has demonstrated that the test plan and report provided by the vendor contains information enough to make a reader able to repeat all tests included. Additionally, after the repetition, the evaluator has obtained the same results as the expected ones. The independent testing has covered 100% of SFRs of the [ST] and TSFIs defined in the functional specification for the TOE, sampling has not been performed. The test cases have taken into account critical parameters values, searching that the TOE behaves in a non-expected manner. There has not been any deviation from the expected results under the environment defined in the Security Target [ST].

PENETRATION TESTING

The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included in the installation and operation manuals. The TOE does NOT present exploitable vulnerabilities under the environment defined in the Security Target [ST]. All identified vulnerabilities can be considered closed if the TOE is installed and operated according to the Security Target [ST] and related documentation. The overall test result is that no deviations were found between the expected and the actual test results taking into account that environment. No attack scenario with the attack potential "Basic" has been successful in the TOE's operational environment as defined in the Security Target [ST] when all measures required by the developer are applied.

EVALUATED CONFIGURATION

The TOE is defined by its commercial name and version number: Data Secure Flash W77F32WWAW\W77F32WQ3W version B.

The acceptance procedure for the evaluated configuration of the TOE is described in section 2.1 "Acceptance procedure" of the preparative user guidance Winbond Technology Ltd., W77F32W Preparative User Guide (version F).

The identifiers used to mark the evaluated configuration are:

NO.	TYPE	IDENTIFIER	FORM OF DELIVERY	VERSION
1	HW	Package top marking	Packaged device	W77F32WWAW/ W77F32WQ3W
2	HW	Die marking	Known Good Die	AAG073
3	DOC	W77F32W Preparative User Guide	PDF file	Version F
4	DOC	W77F32W Operational User Guide	PDF file	Version D
5	DOC	W77F32W Secure Flash Datasheet	Hard copy \ PDF file	Version D
6	SW	SFI Library	7zip file	Version 0.2.8
7	DOC	SFI Library User Guide	Hard copy \ PDF file	Version D

EVALUATION RESULTS

The product Winbond Data Secure Flash Memory W77F32WWAW\W77F32WQ3W version B has been evaluated against the Security Target "Security Target of W77F32WWAW\W77F32WQ3W Data Secure Flash Memory (version H)".

All the assurance components required by the evaluation level EAL2 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 EAL2, 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.

- The evaluator encourages the users to follow the product guidance provided by the developer

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” of [OPE_D] and section 3 of [PRE_F] and to observe the operational environment requirements and assumptions defined in the applicable security target.

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.

[PRE_F] W77F32W Preparative User Guide, Version F.

[OPE_D] W77F32W Operational User Guide, Version D.

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:

- Security Target of W77F32WWAW\W77F32WQ3W Data Secure Flash Memory (version H).

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:

- Security Target of W77F32WWAW\W77F32WQ3W Data Secure Flash Memory (version I).

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.org.

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 selected.