REF: 2016-26-INF-1864 v1	Created by: CERT11
Target: Público	Revised by: CALIDAD
Date: 30.05.2017	Approved by: TECNICO

CERTIFICATION REPORT

File: 2016-26 Winbond Secure Serial Flash Memory W75F32W version D

Applicant: Winbond Electronics Corporation

References:

[EXT-3010] Certification request of Winbond Secure Serial Flash Memory W75F32W version D

[EXT-3335] Evaluation Technical Report of Winbond Secure Serial Flash Memory W75F32W version D.

The product documentation referenced in the above documents.

Certification report of the product Winbond Secure Serial Flash Memory W75F32W version D, as requested in [EXT-3010] dated 01/05/2016, and evaluated by the laboratory Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-3335] received on 03/04/2017.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

TABLE OF CONTENTS

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Winbond Secure Serial Flash Memory W75F32W version D.

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: No.

Evaluation Level: Common Criteria v3.1 R4 - EAL5 + ALC_DVS.2 + AVA_VAN.5.

Evaluation end date: 03/04/2017.

All the assurance components required by the evaluation level EAL5 (augmented with augmented with AVA_VAN.5 *Advanced methodical vulnerability analysis* and ALC_DVS.2 *Sufficiency of security measures*) 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 R4 and the Common Methodology for Information Technology Security Evaluation v3.1 R4.

Considering the obtained evidences during the instruction of the certification request of the product Winbond Secure Serial Flash Memory W75F32W version D, a positive resolution is proposed.

TOE SUMMARY

The Target of Evaluation is a Memory Flash IC. The TOE is dedicated 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.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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 R4.

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.5 Complete semi-formal functional specification with additional error information
	ADV_IMP.1 Implementation representation of the TSF
	ADV_INT.2 Well-structured internals
	ADV_TDS.4 Semiformal modular design
AGD: Guidance documents	AGD_OPE.1 Preparative procedures
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.5 development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.2 Compliance with implementation standars
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE:Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.3 Testing: modular design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	**AVA_VAN.5 Advanced methodological vulnerability analysis**

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R4:

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

TOE Security Functional Requirements	Description
FRU_FLT.2	Limited fault tolerance
FPT_FLS.1/Detectors	Failure with preservation of secure state
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FDP_SDC.1	Stored data confidentiality
FDP_SDI.2	Stored integrity monitoring and action
FPT_PHP.3	Resistance to physical attack
FDP_ITT.1	Basic internal transfer protection
FPT_ITT.1	Basic internal TSF data transfer protection
FDP_IFC.1	Subset information flow control
FDP_UCT.1	Basic data exchange confidentiality
FDP_UIT.1	Data exchange integrity
FTP_TRP.1	Trusted path
FPT_FLS.1/Binding_Key	Failure with preservation of secure state
FDP_RIP.1	Subset residual information protection

IDENTIFICATION

Product: Winbond Secure Serial Flash Memory W75F32W version D

Security Target: Security Target of W75F32W 32M-bit Secure Serial Flash Memory, version 1.18. 30/03/2017.

Protection Profile: No.

Evaluation Level: Common Criteria v3.1 R4 - EAL5 + ALC_DVS.2 + AVA_VAN.5.

SECURITY POLICIES

The use of the product Winbond Secure Serial Flash Memory W75F32W version D shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target. In short, it establishes the need of implementing organisational policies related to the following aspects.

Policy 01: A.Secure-Channel External protection during the secure channel

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

It is assumed that U.Host-Device supports the trusted communication channel with the TOE by protecting the confidentiality and the integrity of the transmitted data.

In particular, U.Host-Device is assumed to correctly protect the secure channel in order to prevent data modification, disclosure, insertion, deletion and replaying.

Policy 02: A.Binding-Process Protection during Binding process

It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer to maintain confidentiality and integrity of the TOE (to prevent any possible copy, modification, or unauthorised use).

This means that the binding process (i.e. generating a unique and random key Kb for U.Host-Device and the TOE) is assumed to be done in a secure environment where the communication between U.Host-Device and the TOE is protected.

Furthermore, U.Host-Device is assumed to provide a secure random source for generating a fresh Binding key (Kb) for the TOE.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following 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.

Assumption 01: A.Secure-Channel External protection during the secure channel

It is assumed that U.Host-Device supports the trusted communication channel with the TOE by protecting the confidentiality and the integrity of the transmitted data.

In particular, U.Host-Device is assumed to correctly protect the secure channel in order to prevent data modification, disclosure, insertion, deletion and replaying.

Assumption 02: A.Binding-Process Protection during Binding process

It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer to maintain confidentiality and integrity of the TOE (to prevent any possible copy, modification, or unauthorised use).

This means that the binding process (i.e. generating a unique and random key Kb for U.Host-Device and the TOE) is assumed to be done in a secure environment where the communication between U.Host-Device and the TOE is protected.

Furthermore, U.Host-Device is assumed to provide a secure random source for generating a fresh Binding key (Kb) for the TOE.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Winbond Secure Serial Flash Memory W75F32W version D, 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.

The threats covered by the security properties of the TOE are categorized below.

Threat 01: T.Phys-Manipulation Physical Manipulation

An attacker may physically modify the Memory Flash in order to

- modify User Data stored in the TOE;
- modify TSF Data stored in the TOE;
- modify or deactivate the security services of the TOE (provided by TSF logic);
- modify the security mechanisms of the TOE (provided by TSF logic) to enable attacks disclosing or manipulating User Data, for example the integrity protection mechanism.

Threat 02: T.Phys-Probing Physical Probing

An attacker may perform physical probing of the TOE in order to disclose User Data and TSF Data while stored in Memory Flash.

Threat 03: T.Malfunction Malfunction due to Environmental Stress

An attacker may cause a malfunction of TSF logic by applying environmental stress in order to deactivate or affect security mechanisms of the TOE. This enables attacks disclosing or manipulating User Data.

This may be achieved by operating the Memory Flash outside the normal operating conditions.

Threat 04: T.Abuse-Func Abuse of Functionality

An attacker may use functions of the TOE which may not be used after TOE Delivery in order to

- disclose or manipulate User Data (user data or code stored in the TOE) or
- enable an attack disclosing or manipulating User Data.

Threat 05: T.Leak-Inherent Inherent Information Leakage

An attacker may exploit information which is leaked from the TOE during usage of the Memory Flash in order to disclose confidential User Data.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

Threat 06: T.Leak-Forced Forced Information Leakage

An attacker may exploit information which is leaked from the TOE during usage of the Memory Flash in order to disclose confidential User Data even if the information leakage is not inherent but caused by the attacker.

Threat 07: T.Abuse-Communication Communication Probing and Manipulation

An attacker may probe and modify the communication between the TOE and U.Host-Device in order to manipulate User/TSF Data or disclose User/TSF Data read from the TOE.

Threat 08: T.Host-Forging Forge the functionality of an authorized Host device

An attacker may access to the User data currently stored in the TOE by:

- illegally establishing a secure channel with the TOE (e.g. by tampering the Binding key or by forging the secure channel without knowing the Binding key) in order to execute the Flash commands;
- binding the TOE with another Host device in order to execute the Flash commands;

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 categorized below.

Environment objective 01: OE.Secure-Channel Secure communication with the TOE

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

In particular, U.Host-Device shall correctly protect the secure channel in order to prevent data modification, disclosure, insertion, deletion and replaying.

Environment objective 02: OE.Binding-Process 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 unauthorised use).

In addition, U.Host-Device shall provide a secure random source for generating a fresh Binding key (Kb) for the TOE.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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 Path-Differential signaling to counter fault injection and side-channel attacks;
- Failure counter to detect and react to tamper attempts;

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

PHYSICAL ARCHITECTURE

The architecture of the Memory Flash is described in Figure 1. The TOE is delimited by the Red box.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

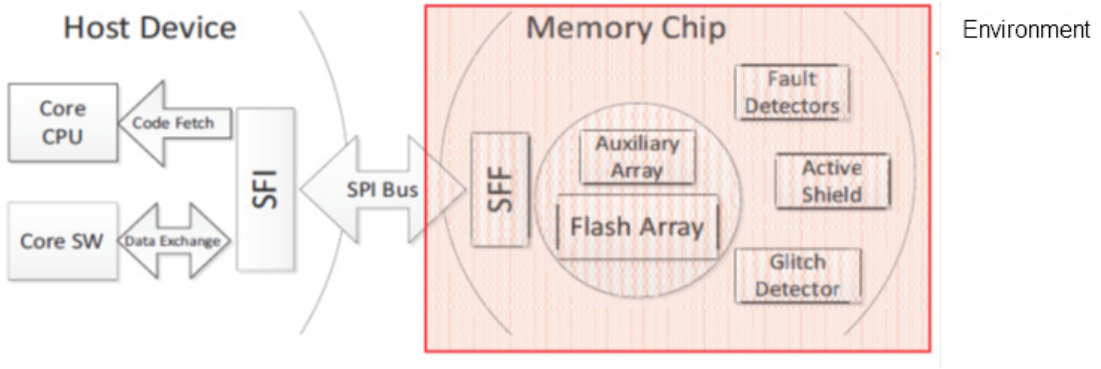

FIGURE 1. TOE ARCHITECTURE AND BOUNDARIES

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
- 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 comprises:

- All security functionality necessary to ensure the secure execution of the Memory Flash,

The guidance for the secure usage of the TOE:

- Operational User Guidance [OPE]
- Preparative Procedure [PRE]
- Datasheet [DTS].

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

DOCUMENTS

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

- [OPE] TrustME™ W75F32W Secure Flash Operational User Guidance, revision F. 02/04/2017.
- [PRE] TrustME™ W75F32W Secure Flash Preparative User Guidance, revision G. 02/04/2017.
- [DTS] TrustME™ 1.8V 32M-BIT Secure Serial Flash Memory With Octal SPI Interface, revision B. 01/04/2015.

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. Moreover, the evaluation team has planned and executed additional tests independently of those executed by the developer.

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 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.

PENETRATING 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 penetrations testing according to JIL supporting documents

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

[JILAAPS] and [JILAVDARC]. 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 CC v3.1 R4 has been successful in the TOE's operational environment as defined in the security target and the operational guidance [OPE] when all security measures required by the developer are applied.

EVALUATED CONFIGURATION

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

- Winbond Secure Serial Flash Memory W75F32W version D.

The acceptance procedure for the evaluated configuration of the TOE is described in section 2 "Acceptance procedure" of the preparative user guidance [PRE]. The identifiers used to mark the evaluated configuration of the TOE are:

Type	Identifier	Form of delivery	Identifier
HW	Package top marking	Known Good Die	W75F32W
HW	Die Marking	Known Good Die	AAG0546PDCC (corresponds to TOE)
SW	SFI IP RTL	Tar file	Version 0

The TOE also includes the documents identified in section DOCUMENTS of this certification report that shall be distributed and made available together to the users of the evaluated version.

EVALUATION RESULTS

The product Winbond Secure Serial Flash Memory W75F32W version D has been evaluated against the Security Target Security Target of W75F32W 32M-bit Secure Serial Flash Memory, version 1.18. 30/03/2017.

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 R4 and the Common Methodology for Information Technology Security Evaluation v3.1 R4.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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.

1. The evaluator encourages users to follow the SECURITY RULES AND RECOMMENDATIONS specified in the operational guidance.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Winbond Secure Serial Flash Memory W75F32W version D, 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] 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
IT	Information Technology
OC	Organismo de Certificación
PP	Protection Profile
SFF	Secure Flash Front-End
SPI	Serial Peripheral Interface
TOE	Target Of Evaluation
TSC	TSF Scope of Control
TSFI	TSF Interface
TSP	TOE Security Policy

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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, Revision 4, September 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 4, September 2012.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012.

[JILAAPS] Applications of Attack Potential to Smartcards, version 2.9. Jan. 2013. Joint Interpretation Library.

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

[OPE] TrustME™ W75F32W Secure Flash Operational User Guidance, revision F. 02/04/2017. Winbond Electronics Corporation.

[PRE] TrustME™ W75F32W Secure Flash Preparative User Guidance, revision G. 02/04/2017. Winbond Electronics Corporation.

[DTS] TrustME™ 1.8V 32M-BIT Secure Serial Flash Memory With Octal SPI Interface, revision B. 01/04/2015. Winbond Electronics Corporation.

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

SECURITY TARGET

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 W75F32W 32M-bit Secure Serial Flash Memory, version 1.18. 30/03/2017. Winbond Electronics Corporation.

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 Lite of W75F32W 32M-bit Secure Serial Flash Memory, version B. April 2017. Winbond Electronics Corporation.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es