MINISTERIO DE PRESIDENCIA Y PARA LAS AATT
CENTRO NACIONAL DE INTELIGENCIA
CENTRO CRIPTOLÓGICO NACIONAL
ORGANISMO DE CERTIFICACIÓN

REF: 2016-2-INF-1970 v1	Created by: CERT11
Target: Público	Revised by: CALIDAD
Date: 14.07.2017	Approved by: TECNICO

CERTIFICATION REPORT

File: 2016-2 Winbond TrustME Secure Element W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F) version A

Applicant: Winbond Electronics Corporation

References:

[EXT-2870] Certification request of Winbond TrustME Secure Element W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F) version A

[EXT-3467] Evaluation Technical Report of Winbond TrustME Secure Element W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F) version A.

The product documentation referenced in the above documents.

Certification report of the product Winbond TrustME™ Secure Element W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F) version A, as requested in [EXT-2870] dated 09/12/2015, and evaluated by the laboratory Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-3467] received on 10/07/2017.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Winbond TrustME™ Secure Element W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F) version A.

The Target of Evaluation is a Secure Element.

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: Security IC Platform Protection Profile with Augmentation Packages, version 1.0. BSI-CC-PP-0084-2014.

Evaluation Level: Common Criteria version 3.1 Release 4 EAL5 + ALC_DVS.2 + AVA_VAN.5.

Evaluation end date: 10/07/2017.

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 version 3.1 Release 4 and the Common Methodology for Information Technology Security Evaluation version 3.1 Release 4.

Considering the obtained evidences during the instruction of the certification request of the product Winbond TrustME™ Secure Element W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F) version A, a positive resolution is proposed.

TOE SUMMARY

The Target of Evaluation is a Secure Element. The TOE is dedicated to be used in 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 host the code and data of critical applications.

The security needs for the TOE consist in:

- Maintaining the integrity of the content of the Security IC memories and the confidentiality of the content of protected memory areas as required by the application(s) the Security IC is built for;
- Maintaining the correct execution of the software residing on the Security IC;

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL5 + ALC_DVS.2 + AVA_VAN.5 and the evidences required by the additional components ALC_DVS.2 and AVA_VAN.5, according to Common Criteria version 3.1 Release 4.

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 version 3.1 Release 4:

TOE Security Functional Requirements	Description
FRU_FLT.2	Limited fault tolerance
FPT_FLS.1	Failure with preservation of secure state
FMT_LIM.1/Test	Limited capabilities
FMT_LIM.2/Test	Limited availability
FAU_SAS.1	Audit storage
FDP_SDC.1	Stored data confidentiality
FDP_SDI.2	Stored data 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
FCS_RNG.1	Random number generation
FCS_COP.1/TDES	Cryptographic operation
FCS_COP.1/AES	Cryptographic operation
FCS_COP.1/SHA	Cryptographic operation
FCS_COP.1/RSA	Cryptographic operation
FCS_CKM.1/RSA	Cryptographic key generation
FCS_COP.1/ECC	Cryptographic operation
FIA_API.1	Authentication Proof of Identity
FMT_LIM.1/Loader	Limited capabilities
FMT_LIM.2/Loader	Limited availability

IDENTIFICATION

Product: Winbond TrustME™ Secure Element W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F) version A

Security Target: Security Target of W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F) Winbond TrustME™ Secure Element, version J.

Protection Profile: Security IC Platform Protection Profile with Augmentation Packages, version 1.0. BSI-CC-PP-0084-2014.

Evaluation Level: Common Criteria version 3.1 Release 4 EAL5 + ALC_DVS.2 + AVA_VAN.5.

SECURITY POLICIES

The use of the product Winbond TrustME™ Secure Element W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F) version A vA 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 section 3.3. In short, it establishes the need of implementing organisational policies related to the following aspects.

- **P.Process-TOE**: Identification during TOE Development and Production.
- **P.Crypto-Service**: Cryptographic services of the TOE (see application note).
- **P.Lim_Block_Loader**: Limiting and Blocking the Loader Functionality.

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.

- **A.Process-Sec-IC:** Protection during Packaging, Finishing and Personalisation.
- **A.Resp-Appl:** Treatment of user data of the Composite TOE.

The detail of these assumptions is documented in the Security Target section 3.4.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Winbond TrustME™ Secure Element W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F) version A, although the agents implementing attacks have a high attack potential according to the assurance level

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.

- **T.Leak-Inherent:** Inherent Information Leakage.
- **T.Phys-Probing:** Physical Probing.
- **T.Malfunction:** Malfunction due to Environmental Stress.
- **T.Phys-Manipulation:** Physical Manipulation.
- **T.Leak-Forced:** Forced Information Leakage.
- **T.Abuse-Func:** Abuse of Functionality.
- **T.RND:** Deficiency of Random Numbers.
- **T.Masquerade_TOE:** Masquerade the TOE.

The detail of these threats is documented in the Security Target section 3.2.

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.

- **OE.Process-Sec-IC:** Protection during composite product manufacturing.
- **OE.TOE_Auth:** External entities authenticating of the TOE.
- **OE.Lim_Block_Loader:** Limitation of capability and blocking the Loader.

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 in section 4.2.2.

ARCHITECTURE

LOGICAL ARCHITECTURE

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

- Unique identification data
- All Test features are disabled in the User mode;

- True Random Generation which is compliant to AIS31 PTG.2 standard;
- Cryptographic services: TDES, AES, SHA;
- Accelerated RSA and ECC computations;
- Memory protection provide by Secure flash: confidentiality and integrity are protected in data storage and code execution;
- Detection of power glitch and out-of-specified operating conditions (voltage, temperature, clock frequency);
- Active Shields against physical intrusive attacks (e.g. reverse-engineering, probing);
- Protection against side-channel attacks on TDES and AES;

The logical interface of the TOE is made of

- the CPU instruction set
- the IC registers
- the APIs defined by Cryplib OBJ

PHYSICAL ARCHITECTURE

The TOE comprises:

- Hardware
  - A security IC W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F) version IAD0056PDAA
  - Secure flash W75F32W version D
- Associated IC Dedicated Software
  - Booter - ROM code version 1.2.7
  - FlashLib - ROM code version 1.2.7
  - CryptLib OBJ - version 1.0.7
  - Loader - provided as APDUs sequence version 1.0.0
  - Chip Authentication DB (per customer)
- The guidance for the secure usage of the TOE which is referenced at section DOCUMENTS.

The architecture of the TOE is described in Figure 1.

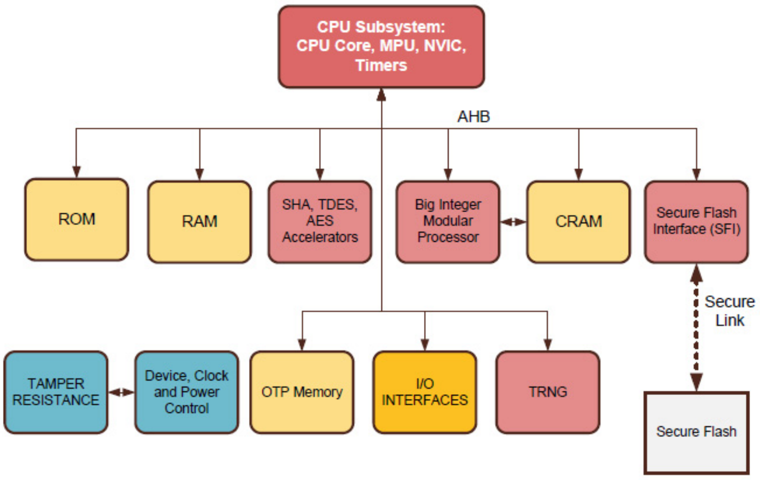
CPU Subsystem: CPU Core, MPU, NVIC, Timers
AHB
ROM
RAM
SHA, TDES, AES Accelerators
Big Integer Modular Processor
CRAM
Secure Flash Interface (SFI)
Secure Link
TAMPER RESISTANCE
Device, Clock and Power Control
OTP Memory
I/O INTERFACES
TRNG
Secure Flash

Figure 1 TOE Architecture

The TOE consists of the following Hardware components

- CPU: ARM SC000-based architecture
- Memories
  - RAM: 32Kbytes
  - ROM: 64Kbytes
  - Secure flash: 4Mbyte
  - OTP memory: 16Kbytes
  - Cryptographic RAM (CRAM): 4Kbytes
- Interfaces
  - Compliant with ISO7816-3
  - Single Wire Protocol (SWP)
  - SPI (master and slave)
  - I2C (master and slave)
  - UART
  - GPIO
- Clock and Power Management
  - Internally generated, self calibrated clock
  - FULL, SAVE, STANDBY and SLEEP operational modes
- Cryprographic Accelators (HW)
  - TDES cryptoprocessor
  - AES cryptoprocessor
  - SHA cryptoprocessor
  - RSA and ECC Big-Integer Modular Processor (BIGIMOD)
  - True Random Number Generator
- Tamper Resistance
  - Out-of-spec detector
  - Glitch detector

- Active shield
- Clock protection

The TOE also includes the following dedicated software components:

- The cryptographic library (Cryplib OBJ) which provides the following features
  - TDES encryption and decryption in CBC and EBC mode with various key sizes: 112 bits and 168 bits;
  - AES encryption and decryption in CBC and ECB mode with various key sizes: 128 bits, 196 bits, and 256 bits;
  - Hash computation by SHA-1 (see FCS_COP.1/SHA application note), SHA-224, SHA-256, SHA-384, SHA-512;
  - RSA encryption and decryption with key sizes up to 4032 bit. Key generation is supported up to 4032 bit.
  - ECC operations such as private scalar multiplication, public scalar multiplication, point validity check, general point addition;
  - Random number generator: interface to the hardware True Random Generation.
- The Flash Loader

DOCUMENTS

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

Reference	Title	Version
[OPEvK]	Winbond TrustME™ Secure Element Operational User Guidance	K
[PREvM]	Winbond TrustME™Secure Element Preparative User Guidance	M
[SFIvE]	Secure Serial Flash Memory Secure Flash Interface (SFI) Specifications and User Guide.	E
[DSvG]	W76Sxx Winbond TrustME™ Secure Element Datasheet	G
[BOOTvE]	W76Sxx Winbond TrustME™Secure Element Booter Interface User Guide	E
[LOADvG]	W76Sxx Winbond TrustME™Secure Element Loader Interface User Guide	G
[FLASHvG]	W76Sxx Winbond TrustME™Secure Element Flash Interface User Guide	G
[CRYPTvF]	W76Sxx Winbond TrustME™Secure Element CryptLib Interface User Guide	F
[ASIPvB]	W76Sxx Winbond TrustME™ Assembly instructions package	B

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 [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 [OPEvK] when all security measures required by the developer are applied.

EVALUATED CONFIGURATION

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

- Winbond TrustME™ Secure Element W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F) version A

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

No	Type	Identifier	Version
Form of delivery : Known Good Die form			
1	HW	Package top marking	• W76S(2/4)MRKD • W75F32W
2	HW	Die Marking	• IAD005 • AAG0546PDCC
Form of delivery : Assembled Parts			
1	HW	Package top marking	W76S(2/4)MR/DN/Q1/Q3/4F
2	HW	IC package	W76S(2/4)MR/DN/Q1/Q3/4F
Form of delivery : Associated IC Dedicated Software			
1	SW (In ROM)	Booter	Version 1.2.7
2	SW (In ROM)	FlashLib	Version 1.2.7
3	SW	CryptLib	Version 1.0.7
4	SW	Loader	Version 1.0.0
5	SW	Chip Authentication DB	N/A, see CADB

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 TrustME™ Secure Element W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F) version A has been evaluated against the Security Target of W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F) Winbond TrustME™ Secure Element, version J.

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 version 3.1 Release 4 and the Common Methodology for Information Technology Security Evaluation version 3.1 Release 4.

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 TrustME™ Secure Element W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F) version A, a positive resolution is proposed.

The certifier strongly recommends to the TOE consumer:

1. to strictly follow all the security rules defined in the TOE operation guidelines [OPEvK] and to observe the operational environment requirements and assumptions defined in the applicable security target.

2. to strictly follow the guidelines related to crypto-algorithms and key lengths established in the documents [CCN-STIC-807] and [ACM], and to observe the recommendations provided by the TOE developer in section "*4.4 Cryptographic Algorithms*" in [OPEvK].

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

BIBLIOGRAPHY

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

TOE:

[ACM] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, version 1.0. SOG-IS Crypto Working Group. May 2016.

[ASIPvB] W76Sxx Winbond TrustME™ Assembly instructions package, version B. Winbond Electronics Corporation.

[BOOTvE] W76Sxx Winbond TrustME™Secure Element Booter Interface User Guide, version E. Winbond Electronics Corporation.

[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.

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

[CCN-STIC-807] Guía de Seguridad de las TIC 807. Criptología de empleo en el Esquema Nacional de Seguridad. Centro Criptológico Nacional. April 2017.

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

[CRYPTvF] W76Sxx Winbond TrustME™Secure Element CryptLib Interface User Guide, version F.

[DSvG] W76Sxx Winbond TrustME™ Secure Element Datasheet, version G. Winbond Electronics Corporation.

[FLASHvG] W76Sxx Winbond TrustME™Secure Element Flash Interface User Guide, version G. Winbond Electronics Corporation.

[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.

[LOADvG] W76Sxx Winbond TrustME™Secure Element Loader Interface User Guide, version G. Winbond Electronics Corporation.

[OPEvK] Winbond TrustME™ Secure Element Operational User Guidance, version K. Winbond Electronics Corporation.

[PREvM] Winbond TrustME™Secure Element Preparative User Guidance, version M. Winbond Electronics Corporation.

[SFIvE] Secure Serial Flash Memory Secure Flash Interface (SFI) Specifications and User Guide, version E. Winbond Electronics Corporation.

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 W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F) Winbond TrustME™ Secure Element, version J.

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:

- W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F) Winbond TrustME™ Secure Element Security Target Lite, revision A. July 2017.