Reference: 2023-6-INF-4552- v1
Target: Limitada al expediente
Date: 23.05.2025

Created by: I003
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2023-6**
TOE	**SpiFlash TrustME Secure Flash Memory W75F40W[W/R][I/J/W][B/C] & W75F40W[BY/Q3][I/J/W][C/B]G version AA**
Applicant	**22099218J - Winbond Electronics Corporation**
References	
	[EXT-8336] Certification Request
	[EXT-9493] Evaluation Technical Report

Certification report of the product SpiFlash TrustME Secure Flash Memory W75F40W[W/R][I/J/W][B/C] & W75F40W[BY/Q3][I/J/W][C/B]G version AA, as requested in [EXT-8336] dated 08/02/2023, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-9493] received on 05/03/2025.

CONTENTS

EXECUTIVE SUMMARY 4
TOE SUMMARY 5
SECURITY ASSURANCE REQUIREMENTS 5
SECURITY FUNCTIONAL REQUIREMENTS 6
IDENTIFICATION 6
SECURITY POLICIES 7
ASSUMPTIONS AND OPERATIONAL ENVIRONMENT 7
CLARIFICATIONS ON NON-COVERED THREATS 7
OPERATIONAL ENVIRONMENT FUNCTIONALITY 7
ARCHITECTURE 8
LOGICAL ARCHITECTURE 8
PHYSICAL ARCHITECTURE 8
DOCUMENTS 9
PRODUCT TESTING 9
PENETRATION TESTING 10
EVALUATED CONFIGURATION 10
EVALUATION RESULTS 13
COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM 13
CERTIFIER RECOMMENDATIONS 13
GLOSSARY 13
BIBLIOGRAPHY 14
SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE) 14
ETR FOR COMPOSITION IDENTIFICATION 15
SITE TECHNICAL AUDIT REPORTS (STARs) 15
STAR #1 15
STAR #2 15
STAR #3 16
STAR #4 16

STAR #5 16
RECOGNITION AGREEMENTS 17
European Recognition of ITSEC/CC – Certificates (SOGIS-MRA) 17
International Recognition of CC – Certificates (CCRA) 17

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product SpiFlash TrustME Secure Flash Memory W75F40W[W/R][I/J/W][B/C] & W75F40W[BY/Q3][I/J/W][C/B]G version AA.

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: Nombre Laboratorio.

Protection Profile: None.

Evaluation Level: Common Criteria 3.1 R5 EAL5 + ALC_DVS.2 + AVA_VAN.5.

Evaluation end date: 11/04/2025

Expiration Date[1]: 20/05/2030

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 3.1 R5 and the CEM 3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product SpiFlash TrustME Secure Flash Memory W75F40W[W/R][I/J/W][B/C] & W75F40W[BY/Q3][I/J/W][C/B]G version AA, a positive resolution is proposed.

[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.

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 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.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL5 and the evidence required by the additional component ALC_DVS.2 + AVA_VAN.5 to the table, 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
FRU_FLT.2
FPT_FLS.1/Detectors
FMT_LIM.1
FMT_LIM.2
FDP_SDC.1
FDP_SDI.2
FPT_PHP.3
FDP_ITT.1
FPT_ITT.1
FDP_IFC.1
FDP_UCT.1
FDP_UIT.1
FTP_TRP.1
FPT_FLS.1/Binding_Key
FDP_RIP.1

IDENTIFICATION

Product: SpiFlash TrustME Secure Flash Memory W75F40W[W/R][I/J/W][B/C] & W75F40W[BY/Q3][I/J/W][C/B]G version AA

Security Target: W75F40W[W/R][I/J/W][B/C] & W75F40W[BY/Q3][I/J/W][C/B]G Secure Flash Memory Security Target (version I).

Protection Profile: None.

Evaluation Level: Common Criteria 3.1 R5 EAL5 + ALC_DVS.2 + AVA_VAN.5.

SECURITY POLICIES

The use of the product SpiFlash TrustME Secure Flash Memory W75F40W[W/R][I/J/W][B/C] & W75F40W[BY/Q3][I/J/W][C/B]G version AA 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 3.4 (“Organisational Security Policies”).

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.

The detail of these assumptions is documented in the Security Target, section 3.5 (“Assumptions”).

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product SpiFlash TrustME Secure Flash Memory W75F40W[W/R][I/J/W][B/C] & W75F40W[BY/Q3][I/J/W][C/B]G version AA, 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 those defined in the Security Target, section 3.3 (“Threats”).

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 those defined in the Protection Profile and they are documented in the Security Target, section 4.2 (“Security Objectives for the Operational Environment”).

ARCHITECTURE

LOGICAL ARCHITECTURE

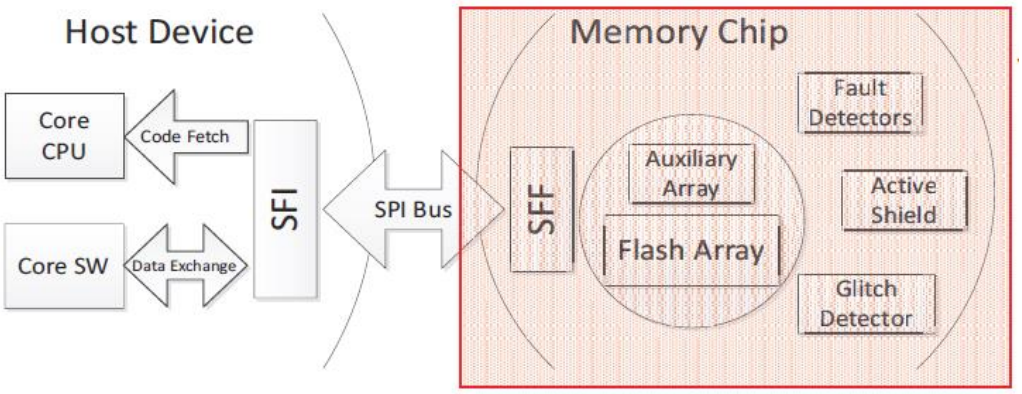
The main security features of the TOE are described as follows:

- Secure separation between Test mode and User mode. The confidentiality and the integrity of the flash content are protected
- 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
- Security sensors Active Shields against physical intrusive attacks

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

PHYSICAL ARCHITECTURE

The physical architecture is depicted in the following figure (the IC is identical for all the part numbers).



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
- Quad SPI: CLK, /CS, DI_IO0, DO_IO1, IO2, IO3

DOCUMENTS

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

- W75F40WxxBx AGD Preparative User Guide (version C).
- W75F40WxxCx AGD Preparative User Guide (version C).
- W75F40WxxBx AGD Operational User Guide (version B).
- W75F40WxxCx AGD Operational User Guide (version B).
- W75F40WxxCx/W75F40WxxBx Secure Flash Datasheet (version A5).
- SFI IP Functional Specification (version A2).
- W75F Pre-Binding Application Note (version B).
- HUID to pre-Binding Key mapping formula

PRODUCT TESTING

The developer has executed tests 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 has 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. Through the tests performed by the Laboratory, it is concluded that 100% of the developer tests were covered.

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. Through the tests performed by the Laboratory it is concluded that 100% of the SFRs and 100% of the TSFI groups defined in the Functional Specification are covered.

PENETRATION TESTING

Based on the list of potential vulnerabilities applicable to the TOE in is operational environment [JIL-ATTPOT], the evaluation team has devised vulnerability analysis and attack scenarios for penetration testing according to JIL supporting documents [JIL-ATTPOT] and [JIL-ARC]. 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 when all security measures required by the developer are applied.

EVALUATED CONFIGURATION

The TOE is defined by its commercial name and version:

- Winbond SpiFlash® TrustME™ W75F40W[W/R][I/J/W][B/C] & W75F40W[BY/Q3][I/J/W][C/B]G Secure Flash Memory version AA.

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

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

No	Type	Identifier	Part Number	Delivery Method	Notes
Form of delivery: Known Good Die Device					
1	HW	IC Part number	W75F40WWIB	Via Courier	4Mb, 1.8V, Wafer Form, Industrial, No Pre-bind, HW SFI
2	HW	IC Part number	W75F40WWJB	Via Courier	4Mb, 1.8V, Wafer Form, Industrial Plus, No Pre-bind, HW SFI
3	HW	IC Part number	W75F40WWWB	Via Courier	4Mb, 1.8V, Wafer Form, Wireless, No Pre-bind, HW SFI
4	HW	IC Part number	W75F40WWIC	Via Courier	4Mb, 1.8V, Wafer Form, Industrial, Pre-bind, HW SFI
5	HW	IC Part number	W75F40WWJC	Via Courier	4Mb, 1.8V, Wafer Form, Industrial Plus, Pre-bind, HW SFI
6	HW	IC Part number	W75F40WWWC	Via Courier	4Mb, 1.8V, Wafer Form, Wireless, Pre-bind, HW SFI
7	HW	IC Part number	W75F40WRIB	Via Courier	4Mb, 1.8V, RDL Wafer Form, Industrial, No Pre-bind, HW SFI
8	HW	IC Part number	W75F40WRJB	Via Courier	4Mb, 1.8V, Wafer Form, Industrial Plus, No Pre-bind, HW SFI
9	HW	IC Part number	W75F40WRWB	Via Courier	4Mb, 1.8V, RDL Wafer Form, Wireless, No Pre-bind, HW SFI
10	HW	IC Part number	W75F40WRIC	Via Courier	4Mb, 1.8V, RDL Wafer Form, Industrial, Pre-bind, HW SFI
11	HW	IC Part number	W75F40WRJC	Via Courier	4Mb, 1.8V, RDL Wafer Form, Industrial Plus, Pre-bind, HW SFI
12	HW	IC Part number	W75F40WRWC	Via Courier	4Mb, 1.8V, RDL Wafer Form, Wireless, Pre-bind, HW SFI
Form of delivery: Assembled Device					
1	HW	IC Part number	W75F40WBYICG	Via Courier	4Mb, 1.8V, WLCSP, Industrial, Pre-bind, HW-SFI, Green package
2	HW	IC Part number	W75F40WQ3ICG	Via Courier	4Mb, 1.8V, QFN32, Industrial, Pre-bind, HW-SFI, Green package
3	HW	IC Part number	W75F40WBYIBG	Via Courier	4Mb, 1.8V, WLCSP, Industrial, No Pre-bind, HW-SFI, Green package
4	HW	IC Part number	W75F40WQ3IBG	Via Courier	4Mb, 1.8V, QFN32, Industrial, No Pre-bind, HW-SFI, Green package
5	HW	IC Part number	W75F40WBYWCG	Via Courier	4Mb, 1.8V, WLCSP, Wireless, Pre-bind, HW-SFI, Green package
6	HW	IC Part number	W75F40WQ3WCG	Via Courier	4Mb, 1.8V, QFN32, Wireless, Pre-bind, HW-SFI, Green package
7	HW	IC Part number	W75F40WBYWBG	Via Courier	4Mb, 1.8V, WLCSP, Wireless, No Pre-bind, HW-SFI, Green package
8	HW	IC Part number	W75F40WQ3WBG	Via Courier	4Mb, 1.8V, QFN32, Wireless, No Pre-bind, HW-SFI, Green package
9	HW	IC Part number	W75F40WBYJCG	Via Courier	4Mb, 1.8V, WLCSP, Industrial plus, Pre-bind, HW-SFI, Green package

No	Type	Identifier	Part Number	Delivery Method	Notes
10	HW	IC Part number	W75F40WQ3JCG	Via Courier	4Mb, 1.8V, QFN32, Industrial plus, Pre-bind, HW-SFI, Green package
11	HW	IC Part number	W75F40WBYJBG	Via Courier	4Mb, 1.8V, WLCSP, Industrial plus, No Pre-bind, HW-SFI, Green package
12	HW	IC Part number	W75F40WQ3JBG	Via Courier	4Mb, 1.8V, QFN32, Industrial plus, No Pre-bind, HW-SFI, Green package

Form of delivery: Associated IC Dedicated Documentation

No	Type	Identifier	Version	Delivery Method	Full Name	Hash	Notes
1	PDF	W75F40WxxBx AGD Preparative User Guide	C	Encrypted mail	W75F40WxxBx_AGD_PRE_RevC_21Nov23.pdf	db882c00381109c682943d5e8529eda73ccbb5f907e52863bdfa4f5641b5966f	
2	PDF	W75F40WxxCx AGD Preparative User Guide	C	Encrypted mail	W75F40WxxCx_AGD_PRE_RevC_21Nov23.pdf	2fab87fc33a77b354c463ac8a90f76472594f163fe697d03e1473d738dba21e2	
3	PDF	W75F40WxxBx AGD Operational User Guide	B	Encrypted mail	W75F40WxxBx_AGD_OPE_RevB_14Jun23.pdf	e07c660c0ccfd1a9ee5b4876441b1f0c501b7f83039e7f1139d454a8ac2adeb2	
4	PDF	W75F40WxxCx AGD Operational User Guide	B	Encrypted mail	W75F40WxxCx_AGD_OPE_RevB_14Jun23.pdf	6b830089fbda5db400d3cdc05378979c5201579b30018a5a83094920df6eb6e2	
5	PDF	W75F40WxxCx/ W75F40WxxBx Secure Flash Datasheet	A5	Mail	W75F40WxxBx_W75F40WxxCx_Datasheet_RevA5_20Nov23.pdf	2bb12f23755aa3690240c8e9817c070d4ca382188668eb095ba5a545d005c17e	For all
6	PDF	SFI IP Functional Specification	A2	Encrypted mail	SFI3_FS_v3.22_RevA2_210728.pdf	85e21393db862cd3c7b51fb4802bcf22ddb91739d7276005aa7c719797da7e34	For all
7	PDF	W75F Pre-Binding Application Note	B	Encrypted mail	W75F Pre-Binding AN RevB 11May23.pdf	4e2063aec42fd25940c16dc497328b2847afc0688034db1369d46a2fb6de6601	
8	PDF	HUID to pre-Binding Key mapping formula	N/A	Encrypted mail	N/A	N/A	

EVALUATION RESULTS

The product SpiFlash TrustME Secure Flash Memory W75F40W[W/R][I/J/W][B/C] & W75F40W[BY/Q3][I/J/W][C/B]G version AA has been evaluated against the Security Target W75F40W[W/R][I/J/W][B/C] & W75F40W[BY/Q3][I/J/W][C/B]G Secure Flash Memory Security Target (version I).

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 3.1 R5 and the CEM 3.1 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 evaluation team makes the following security recommendations:

- 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 SpiFlash TrustME Secure Flash Memory W75F40W[W/R][I/J/W][B/C] & W75F40W[BY/Q3][I/J/W][C/B]G version AA, a positive resolution is proposed.

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.

[JIL-ATTPOT] Application of Attack Potential to Smartcards. Joint Interpretation Library. Version 3.2. November 2022. Joint Interpretation Library.

[JIL-ARC] Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices, version 2.1. July 2021. Joint Interpretation Library.

[START] Joint Interpretation Library. Site Technical Audit Report Template. Version 1.0. February 2018.

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

[ST] W75F40W[W/R][I/J/W][B/C] & W75F40W[BY/Q3][I/J/W][C/B]G Secure Flash Memory Security Target (version I).

[ST Lite] W75F40W[W/R][I/J/W][B/C] & W75F40W[BY/Q3][I/J/W][C/B]G Secure Flash Memory Security Target (version I).

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

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:

- W75F40W[W/R][I/J/W][B/C] & W75F40W[BY/Q3][I/J/W][C/B]G Secure Flash Memory Security Target (version I).

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:

- W75F40W[W/R][I/J/W][B/C] & W75F40W[BY/Q3][I/J/W][C/B]G Secure Flash Memory Security Target (version I1).

ETR FOR COMPOSITION IDENTIFICATION

The evaluation activities carried out in this certification dossier have been summarized in an Evaluation Technical Report for composite evaluation (ETR_COMP). This ETR_COMP has been validated by this Certification Body. The reference of the ETR_COMP is:

- **Report name**: ETR for composite evaluation. W75F40W[W/R][I/J/W][B/C] & W75F40W[BY/Q3][I/J/W][C/B]G version AA.
- **Report ID**: CCEWIN007-EFC-M1.
- **Version**: M1.
- **Issue Date**: 04/03/2025.
- **SHA256**: 2a249e23348d3c74136e283b029f724da7a1fecb3da052b81f76f8e2f6245d52.
- **Issuing ITSEF**: Applus Laboratories.

SITE TECHNICAL AUDIT REPORTS (STARs)

The site visits carried out within this dossier have been summarized in five Site Technical Audit Report (STAR). These STAR reports have been validated by this Certification Body according to [START]. The reference of the STAR are:

STAR #1

- **Report name:** Site technical audit report (STAR). DTF Kitakami and DTF Kawasaki.
- **Report ID:** CCEWIN007-STAR-M0-DTF.
- **Version:** M0.
- **Issue Date:** 16/12/2024.
- **Issuing ITSEF:** Applus Laboratories.
- **Site audit dates:** 05-06/06/2023.

STAR #2

- **Report name:** Site technical audit report (STAR). KSC Kawasaki and KSC Mitaka.
- **Report ID:** CCEWIN007-STAR-M0-KSC.
- **Version:** M0.
- **Issue Date:** 16/12/2024.
- **Issuing ITSEF:** Applus Laboratories.
- **Site audit dates:** 07-08/06/2023.

STAR #3

- **Report name:** Site technical audit report (STAR). Winbond America (WECA).
- **Report ID:** CCEWIN007-STAR-M0-WECA.
- **Version:** M0.
- **Issue Date:** 16/12/2024.
- **Issuing ITSEF:** Applus Laboratories.
- **Site audit dates:** 12/06/2023.

STAR #4

- **Report name:** Site technical audit report (STAR). Winbond Taichung (WECT) and Winbond Jhubei (WEJB).
- **Report ID:** CCEWIN007-STAR-M0-WECT-WEJB.
- **Version:** M0.
- **Issue Date:** 16/12/2024.
- **Issuing ITSEF:** Applus Laboratories.
- **Site audit dates:** 08-11/05/2023.

STAR #5

- **Report name:** Site technical audit report (STAR). Winbond Israel (WTL)
- **Report ID:** CCEWIN007-STAR-M0-WTL.
- **Version:** M0.
- **Issue Date:** 16/12/2024.
- **Issuing ITSEF:** Applus Laboratories.
- **Site audit dates:** 14/05/2023.

These STAR reports constitute evaluation evidence, therefore according to article 25 of Presidential Order PRE/2740/2007 which regulates the CCN Certification Body, written authorization must be requested by Applus Laboratories to the Certification Body to share any information of this certification dossier (including any of the STAR reports) with third parties.

It is expected that if the applicant Winbond Electronics Corporation is willing to share any of these STAR reports with any third party, they may contact Applus Laboratories to perform an authorization request to the CCN Certification Body to distribute this report.

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.