TÜVRheinland®
Precisely Right.

Certification Report

W77Q16/32 version C

Sponsor and developer: ***Winbond Electronics Corporation***
No. 8, Keya 1st Rd., Daya Dist.,
Taichung City 428
Taiwan R.O.C

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-0308282-CR**

Report version: **1**

Project number: **0308282**

Author(s): **Jordi Mujal**

Date: **08 September 2021**

Number of pages: **11**

Number of appendices: **0**

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS

Foreword **3**

Recognition of the Certificate **4**

International recognition 4
European recognition 4

1 Executive Summary **5**

2 Certification Results **6**

2.1 Identification of Target of Evaluation 6
2.2 Security Policy 6
2.3 Assumptions and Clarification of Scope 6
2.3.1 Assumptions 6
2.3.2 Clarification of scope 6
2.4 Architectural Information 6
2.5 Documentation 7
2.6 IT Product Testing 7
2.6.1 Testing approach and depth 7
2.6.2 Independent penetration testing 7
2.6.3 Test configuration 8
2.6.4 Test results 8
2.7 Reused Evaluation Results 8
2.8 Evaluated Configuration 8
2.9 Evaluation Results 8
2.10 Comments/Recommendations 8

3 Security Target **10**

4 Definitions **10**

5 Bibliography **11**

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the W77Q16/32 version C. The developer of the W77Q16/32 version C is Winbond Electronics Corporation located in Taichung City, Taiwan and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a Memory Flash IC. The TOE is dedicated to be embedded into systems that need protection of their memory contents. In particular, the TOE is dedicated to the secure storage of the code and data for IoT applications.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 08 September 2021 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the W77Q16/32 version C, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the W77Q16/32 version C are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL2 augmented (EAL2+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 (Flaw Reporting Procedures).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the W77Q16/32 version C from Winbond Electronics Corporation located in Taichung City, Taiwan.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	W77Q [16/32]JW[W/R/SF/SS/ST/SN/SV/ZP/TB/TC/XF/XG/XH/UU/UX/ UZ/BY/BJ/BK]	C

To ensure secure usage a set of guidance documents is provided, together with the W77Q16/32 version C. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The TOE comprises all security functionality necessary to ensure the secure execution of the Memory Flash:

- Secure separation between Test mode and User mode.
- Protection against leakage and physical attacks.
- Confidentiality, Authenticity and integrity of Secret User Data.
- Authenticity and integrity of Authenticated User Data.
- Integrity protection of the flash content by error detection codes.
- Memory Rollback protection, Irreversibility-Anchor and Clone Replace Protection.
- Secure Communication Channel with the host device and a remote operator.
- Memory Access Control of the flash content by implementing an access control policy.
- Protection of the secure boot of the Host Device and secure update process.
- Secure Key Provisioning Mechanism.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

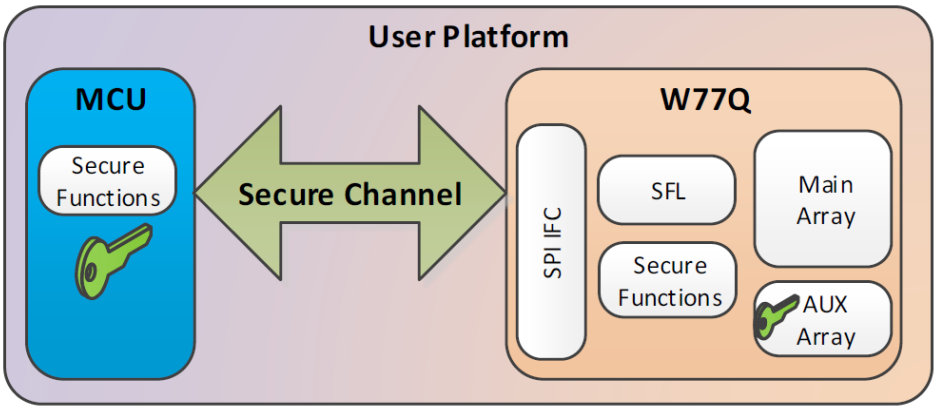
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 3.5 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The architecture of the Memory Flash is described in the figure below. The TOE includes only the W77Q16/32 device. The MCU and SPI bus appearing in this diagram are not part of the TOE.



The TOE consists of the following Hardware components:

- **Main Flash Array**: stores the User data (i.e. the mass data including executable code).
- **Auxiliary array**: contains the TSF data, including: keys, secure configurations, Winbond unique ID (WID), Monotonic Counter etc.
- **Secure Functions:** implements the TSF, including data encryption, command authentication, access privileges management, Secure Channel support.
- **SFL (Standard Flash Logic):** implements datapath for plain access to the unprotected areas of the Main Array (as in standard Flash devices).
- **SPI Interface**: supports communication over the SPI bus.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
W77Q16JW/W77Q32JW Operational User Guidance	C
W77Q16JW/W77Q32JW Preparative Procedure	C
W77Q - Secure Serial NOR Flash Memory Security Manual	A7
W77Q - Secure Serial NOR Flash Memory Data Sheet	A6

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer provided documentation evidence covering several test scenarios. In each of the scenarios several TSFIs were tested. The evaluators examined the tests and all results were as expected.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

2.6.2 Independent penetration testing

To identify potential vulnerabilities, the evaluator performed the following activities:

- The evaluators analysed the TOE guidance, functional specification, TOE design and architecture description in order to identify potential vulnerabilities.
- Publicly available sources of information such as scientific papers, books and online databases were examined. In particular, the CWE database was checked.
- Internal Lab discussions. Previous experience was shared between evaluators during internal discussions
- Vulnerability analysis and attack potential calculations based on *[JIL-AAPS]* was considered.

The total test effort expended by the evaluators was 4 weeks. During that test campaign, 33,3% of the total time was spent on Perturbation attacks, 33,3% on side-channel testing, and 33,3% on logical tests.

2.6.3 Test configuration

The configuration of the sample used for testing and penetration testing was the same as described in the *[ST]*. As a part of the work package the evaluators initialized the TOE as required by the TOE guidance.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

For composite evaluations, please consult the *[ETRfC]* for details.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number W77Q16/32 version C.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents. To support composite evaluations according to *[JIL-COMP]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that must be considered when this TOE is used as platform in a composite evaluation.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the W77Q16/32 version C, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 2 augmented with ALC_FLR.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of the TOE. There are no particular obligations or recommendations for the user apart from following the user

guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: None.

3 Security Target

The W77Q[16/32]JW[W/R/SF/SS/ST/SN/SV/ZP/TB/TC/XF/XG/XH/UU/UX/UZ/BY/BJ/BK] Secure Flash Memory Security Target, Version F *[ST]* is included here by reference.

Please note that, to satisfy the need for publication, a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MCU	MicroController (unit)
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
SFL	Standard Flash Logic
SPI	Serial Peripheral Interface
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[ETR]	Evaluation Technical Report “W77Q16/32 Secure Flash Memory version C” – EAL2+, v6.0, 08 September 2021
[ETRfC]	Evaluation Technical Report for Composition “W77Q16/32 Secure Flash Memory version C” – EAL2+, v5.0, 08 September 2021
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020
[JIL-AM]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)
[JIL-COMP]	Composite product evaluation for Smartcards and similar devices, version 1.5.1, May 2018.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	W77Q[16/32]JW[W/R/SF/SS/ST/SN/SV/ZP/TB/TC/XF/XG/XH/UU/UX/UZ/BY/BJ/BK] Secure Flash Memory Security Target, Version F
[ST-lite]	W77Q[16/32]JW[W/R/SF/SS/ST/SN/SV/ZP/TB/TC/XF/XG/XH/UU/UX/UZ/BY/BJ/BK] Secure Flash Memory Security Target Lite, Version F.
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)