Reference: 2022-45-INF-4348- v1
Target: Limitada al expediente
Date: 28.08.2024

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

CERTIFICATION REPORT

Dossier #	**2022-45**
TOE	**V2X subsystem on Transceiver module MQBw version 0353**
Applicant	**107-86-14075 - LG ELECTRONICS INC.**
References	

[EXT-8029] 2022-09-30_2022-YY_solicitud_certificacion

[EXT-9086]2024-06-04_2022-45_ETR_v1.2

Certification report of the product V2X subsystem on Transceiver module MQBw version 0353, as requested in [EXT-8029] dated 30/09/2022, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-9086] received on 04/06/2024.

CONTENTS

EXECUTIVE SUMMARY 3
TOE SUMMARY 3
SECURITY ASSURANCE REQUIREMENTS 4
SECURITY FUNCTIONAL REQUIREMENTS 5
IDENTIFICATION 6
SECURITY POLICIES 6
ASSUMPTIONS AND OPERATIONAL ENVIRONMENT 6
CLARIFICATIONS ON NON-COVERED THREATS 6
OPERATIONAL ENVIRONMENT FUNCTIONALITY 6
ARCHITECTURE 7
LOGICAL ARCHITECTURE 7
PHYSICAL ARCHITECTURE 8
DOCUMENTS 8
PRODUCT TESTING 9
EVALUATED CONFIGURATION 9
EVALUATION RESULTS 9
COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM 10
CERTIFIER RECOMMENDATIONS 10
GLOSSARY 10
BIBLIOGRAPHY 11
SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE) 11
RECOGNITION AGREEMENTS 12
European Recognition of ITSEC/CC – Certificates (SOGIS-MRA) 12
International Recognition of CC – Certificates (CCRA) 12

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product V2X subsystem on Transceiver module MQBw version 0353.

The TOE is a part of the software code that runs on a compatible hardware platform such as the transceiver module and handles the V2X communications via CAM and DEMN messages.

Developer/manufacturer: LG ELECTRONICS INC.

Sponsor: LG ELECTRONICS INC..

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: DEKRA Testing and Certification S.A.U.

Protection Profile: None.

Evaluation Level: Common Criteria 3.1 R5 EAL2 + ALC_FLR.1.

Evaluation end date: 21/06/2024

Expiration Date[1]: 13/08/2029

All the assurance components required by the evaluation level EAL2 (augmented with ALC_FLR.1) have been assigned a “PASS” verdict. Consequently, the laboratory DEKRA Testing and Certification S.A.U. assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL2 + ALC_FLR.1, as defined by the Common Criteria 3.1 R5 and the CEM 3.1 R5.

Considering the obtained evidence during the instruction of the certification request of the product V2X subsystem on Transceiver module MQBw version 0353, a positive resolution is proposed.

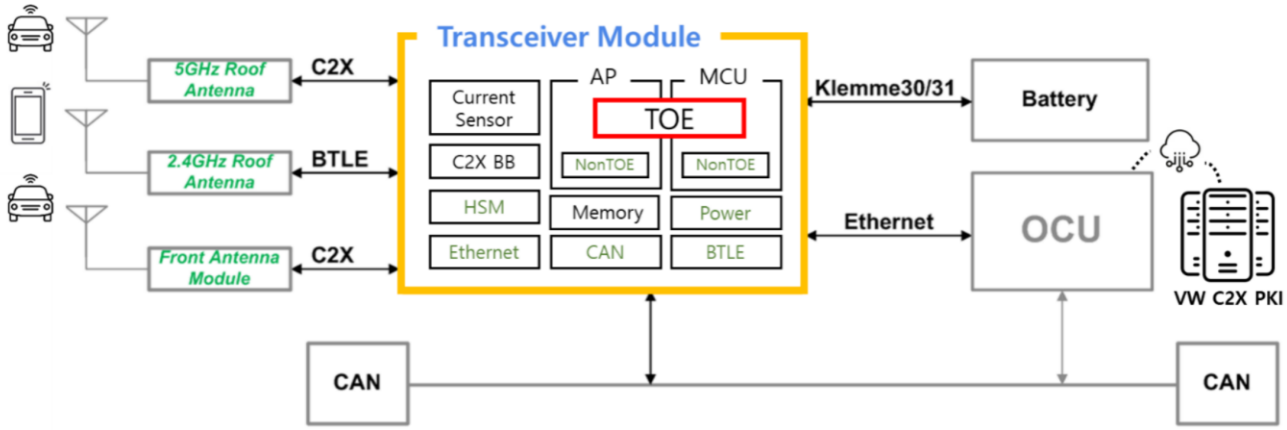
TOE SUMMARY

The TOE is a part of the software code that runs on a compatible hardware platform such as the transceiver module and handles the V2X communications via CAM and DEMN messages.

The TOE has to be deployed in a MQBw UNECE configuration pertaining to combustion vehicle. MQB stands for “*Modularer Querbaukasten*” in German, which translates to “*Modular Transverse Matrix*” in English. Among the various lines of the MQB platform, MQBw UNECE can be considered as the superset of the TOE and is applied to some vehicle models such as Golf and Passat. Thus, the TOE is a software that acts as a communications system placed in the vehicle in order to provide

[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.

different ITS services (active road, co-operative traffic efficiency, co-operative local services, Global Internet services, etc.).



The TOE is used by integrating it into the application processor (AP) and the microcontroller unit (MCU) elements of the transceiver module. The TOE consists of system interface for communication, C2X stack and service layer. Furthermore, they are packaged in one binary file.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2 and the evidence required by the additional component ALC_FLR.1 to the table, according to Common Criteria 3.1 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
	ALC_FLR.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:

Class FPT: Protection of the TSF	
FPT_TDC.1 / Certificates	Inter-TSF basic TSF data consistency
FPT_TDC.1 / Software update	Inter-TSF basic TSF data consistency
Class FCO: Communication	
FCO_NRO.2	Enforced proof of origin
Class FDP: User data protection	
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FDP_ACC.1 / Access control	Subset access control
FDP_ACF.1 / Access control	Security attribute based access control
FDP_ACC.1 / Software update	Subset access control
FDP_ACF.1 / Software update	Security attribute based access control
Class FMT: Security management	
FMT_MSA.1 / Message protection	Management of security attributes
FMT_MSA.3 / Message protection	Static attribute initialisation
FMT_MSA.1 / Access control	Management of security attributes
FMT_MSA.3 / Access control	Static attribute initialisation
FMT_MSA.1 / Software update	Management of security attributes
FMT_MSA.3 / Software update	Static attribute initialisation
FMT_SMF.1 / Trust elements update	Specification of Management Functions
FMT_SMF.1 / Access control	Specification of Management Functions
FMT_SMF.1 / Privacy	Specification of Management Functions
FMT_SMR.1	Security roles
Class FIA: Identification and authentication	
FIA_UID.1	Timing of identification
FIA_UAU.1	Timing of authentication
Class FTP: Trusted path/channels	
FTP_ITC.1	Inter-TSF trusted channel

IDENTIFICATION

Product: V2X subsystem on Transceiver module MQBw version 0353

Security Target: V2X subsystem on Transceiver Module MQBw Security Target, version 1.5 (2024-05-31).

Protection Profile: None.

Evaluation Level: Common Criteria 3.1 R5 EAL2 + ALC_FLR.1.

SECURITY POLICIES

The use of the product V2X subsystem on Transceiver module MQBw version 0353 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 5.4 ("*Organizational 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 5.5 ("*Assumptions*").

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product V2X subsystem on Transceiver module MQBw version 0353, although the agents implementing attacks have the attack potential according to the Basic of EAL2 + ALC_FLR.1 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 5.3 ("*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 Security Target, section 6.2 ("*Security Objectives for the operational Environment*").

ARCHITECTURE

LOGICAL ARCHITECTURE

The logical scope of the TOE consists of the following security features:

V2X Secure Association and Message Protection

- The TOE can establish a secure association with C-ITS stations to send or receive secure messages through CAM and DEMN messages. These messages include the payload, the payload signature and the public key certificate used for signature.
    - TOE uses the HSM in the environment to verify the signature of the messages. The TOE adds a signature generated by the HSM for outgoing messages.
    - The TOE verifies the certificate format, validity and revocation of the certificates included in the CAM and DEMN messages. The TOE also uses the HSM in the environment to verify the certificate signature.
    - The messages include geo-position information and timestamps that are used to verify the validity of the messages.

Privacy

- Provide services supporting the simultaneous change of communication identifiers (station ID, network ID, MAC address) and credentials used for secure communications, within the ITS station.
- The TOE does not communicate identical data values that are linkable to more than one AT.
- The authorization tickets are updated at certain conditions under certain conditions of time and distance of travel.

Access control

- The TOE provides V2X administration capabilities (check CTL, CRL, TLM, RCA, EA, AA and HSM status and disable V2X communication).
- The TOE provides different user roles (EPTI, Basic, Production, Extended, Superuser, E2E) and the corresponding authentication and access control. Protected services can only be executed prior authentication and identification.

Trust elements update

- The TOE provides URLs to connect to the PKI to download appropriate information.

- The TOE verifies the validity of ECTL, CRL, CTL certificates and the valid period of Authorization Tickets.

Software update

- The TOE verifies the software binaries prior the update. The software update is performed only if the signature is valid, and the version is equal or greater than the current version.

HSM communication

- The TOE opens a communication channel with the HSM in the environment to request cryptographic services that are used in the TOE operation.

PHYSICAL ARCHITECTURE

Volkswagen is considered the unique TOE user and the only client for which the TOE is developed. Therefore, the following information is oriented to the Volkswagen employees.

The release package for the TOE consists of a software package and the guidance documents described in the next section. The TOE software package is generated in PDX packaged file form.

Both the software and guidance can be obtained through an internal Volkswagen file exchange platform, DoRIS (Document Retrieval and Information System) that is accessible through a VPN for specific Volkswagen and LGE users who have been granted access.

Type	Delivery Item	Version	Format	SHA256
Software	FL_5QS035741_0353_TMALLORU3_V001_S	0353	.pdx	28921cef2245b1cae9a4eb9865fb6dc2717c5d328272c8f2320635b8caf4370e

DOCUMENTS

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

Type	Delivery Item	Version	Format	SHA256
Guidance	V2X subsystem on Transceiver Module MQBw User Guidance	V1.5	.pdf	468600a647c3a283bd7f9743020ba13c26e612833d9c93383588385ca68f4b6c

Guidance	V2X subsystem on Transceiver Module MQBw DTAB	V0.1	xlsx	fcb2cc9062901a9e46fda85718fe6744c3081f64f309bce9d90754cf81dc8a0c

PRODUCT TESTING

The developer has executed tests for all the TSFIs. 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 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 repeated all the developer functional tests in the developer premises in the testing platform implemented in the evaluation facility.

In addition, the lab has devised a test for each of the TSFI 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.

EVALUATED CONFIGURATION

The evaluated configuration is the production version of the TOE. Although the development version has been used for testing purposes, the evaluated configuration covers the production firmware that is going to be installed in real vehicles. The production version does not include different modes of operations or specific configurations that enable/disable especial functionality.

EVALUATION RESULTS

The product V2X subsystem on Transceiver module MQBw version 0353 has been evaluated against the Security Target V2X subsystem on Transceiver Module MQBw Security Target, version 1.5 (2024-05-31).

All the assurance components required by the evaluation level EAL2 + ALC_FLR.1 have been assigned a "PASS" verdict. Consequently, the laboratory DEKRA Testing and Certification S.A.U. assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL2 + ALC_FLR.1, 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.

- It is mandatory to strictly follow the steps indicated in the installation documentation in order to download and install the correct version of the TOE and the cumulative update in a proper manner.
- The user guidance must be read and understood in order to operate the TOE in an adequate manner according to the security target.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidence during the instruction of the certification request of the product V2X subsystem on Transceiver module MQBw version 0353, a positive resolution is proposed.

GLOSSARY

CAM Cooperative Awareness Message

CCN Centro Criptológico Nacional

CNI Centro Nacional de Inteligencia

DENM Decentralized Environmental Notification Message

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

OC Organismo de Certificación

TOE Target Of Evaluation

V2X Vehicle to other entities

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.

[ST] V2X subsystem on Transceiver Module MQBw Security Target, version 1.5 (2024-05-31).

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- V2X subsystem on Transceiver Module MQBw Security Target, version 1.5 (2024-05-31).

RECOGNITION AGREEMENTS

In order to avoid multiple certifications 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 selected.