Reference: 2023-23-INF-4410- v1
Target: Limitada al expediente
Date: 12.02.2025

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

CERTIFICATION REPORT

Dossier #	**2023-23**
TOE	**GMV GNSS Cryptographic Module v2.1.7**
Applicant	**ESA-79197356 - GMV Aerospace and Defence, S.A.**
References	

[EXT-8656] 2023-23 GMV GNSS Cryptographic Module - Solicitud de Certificación

[EXT-9230] 2024-09-04_2023-23_ETR_v1.2

Certification report of the product GMV GNSS Cryptographic Module v2.1.7, as requested in [EXT-8656] dated 07/07/2024, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-9230] received on 04/09/2024.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product GMV GNSS Cryptographic Module v2.1.7.

The GMV GNSS Module consists in a software library developed in Linux platform which main purpose is to provide the cryptographic services which could be used in the future for other projects related with GNSS, e.g. the Open Service Navigation Message Authentication (OSNMA) protocol used in Galileo.

Developer/manufacturer: GMV Aerospace and Defence, S.A.

Sponsor: GMV Aerospace and Defence, S.A..

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 EAL2.

Evaluation end date: 31/10/2024

Expiration Date[1]: 21/12/2029

All the assurance components required by the evaluation level EAL2 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, 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 GMV GNSS Cryptographic Module v2.1.7, a positive resolution is proposed.

TOE SUMMARY

The TOE is intended to be implemented in a platform environment that uses Ubuntu 22.04 or above and includes the GNU Multiple Precision Arithmetic Library dependencies. The TOE provides

[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.

the cryptographic primitives to do the cryptographic functions through an Application Program Interface (API). The connection between the application and the GMV GNSS Module implements network sockets that use TCP/IP protocol. Every application using this sockets protocol can connect to the GMV GNSS module.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2 according to Common Criteria v3.1 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
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:

FUNCTIONAL CLASS	FUNCTIONAL COMPONENT
Security Audit (FAU)	Audit data generation (FAU_GEN.1)
	Protected audit trail storage (FAU_STG.1)
Cryptographic Support (FCS)	Cryptographic key destruction (FCS_CKM.4)
	Cryptographic operation (FCS_COP.1)
User Data Protection (FDP)	Import of user data without security attributes (FDP_ITC.2)
	Subset residual information protection (FDP_RIP.1)
	Basic data exchange confidentiality (FDP_UCT.1)
	Subset access control (FDP_ACC.1)
	Security attribute based access control (FDP_ACF.1)
Identification & Authentication (FIA)	Authentication failure handling (FIA_AFL.1)
	User attribute definition (FIA_ATD.1)
	Verification of Secrets (FIA_SOS.1)
	Timing of authentication (FIA_UAU.1)
	Timing of identification (FIA_UID.1)
Security Management (FMT)	Management of security attributes (FMT_MSA.1)
	Static attribute initialisation (FMT_MSA.3)
	Specification of management functions (FMT_SMF.1)
	Security roles (FMT_SMR.1)
Protection of the TSF (FPT)	TSF testing (FPT_TST.1)
	Inter-TSF basic TSF data consistency (FPT_TDC.1)
Resource Utilisation (FRU)	Maximum quotas (FRU_RSA.1)
TOE Access (FTA)	TSF-initiated Termination (FTA_SSL.3)
	User-initiated Termination (FTA_SSL.4)
	TOE session establishment (FTA_TSE.1)
Trusted Path (FTP)	Trusted Path (FTP_TRP.1)

IDENTIFICATION

Product: GMV GNSS Cryptographic Module v2.1.7

Security Target: GMV GNSS Cryptographic Module - Security Target v2.1.7 (28/08/24).

Protection Profile: None.

Evaluation Level: Common Criteria 3.1 R5 EAL2.

SECURITY POLICIES

The use of the product GMV GNSS Cryptographic Module v2.1.7 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 5.3 ("*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 5.4 ("*Assumptions*").

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product GMV GNSS Cryptographic Module v2.1.7, although the agents implementing attacks have the attack potential according to the Basic of EAL2 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 5.2 ("*Threats*").

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

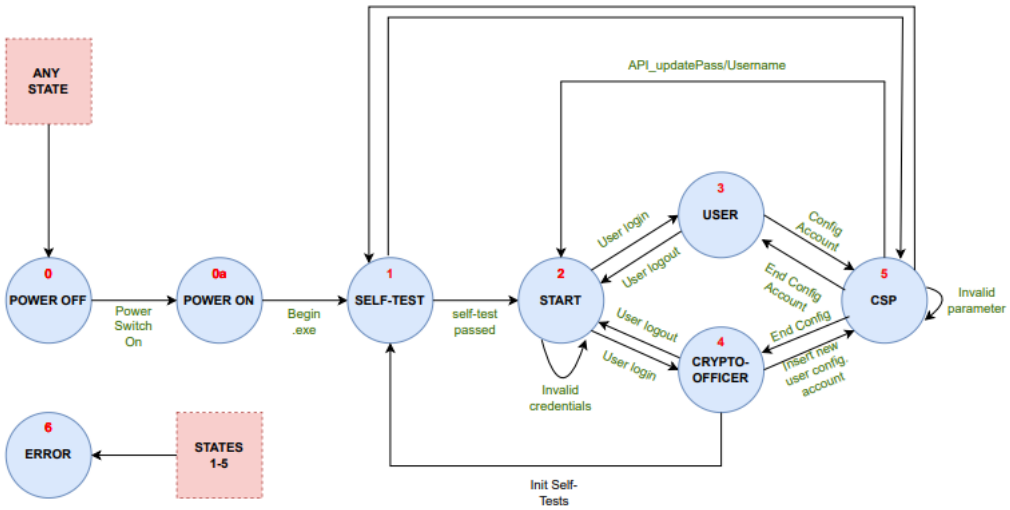
The security objectives declared for the TOE operational environment are those defined in the Protection Profile and they are documented in the Security Target, section 6.2 ("*Security Objectives for the operational Environment*").

ARCHITECTURE

LOGICAL ARCHITECTURE

The TOE is composed of the following software components:

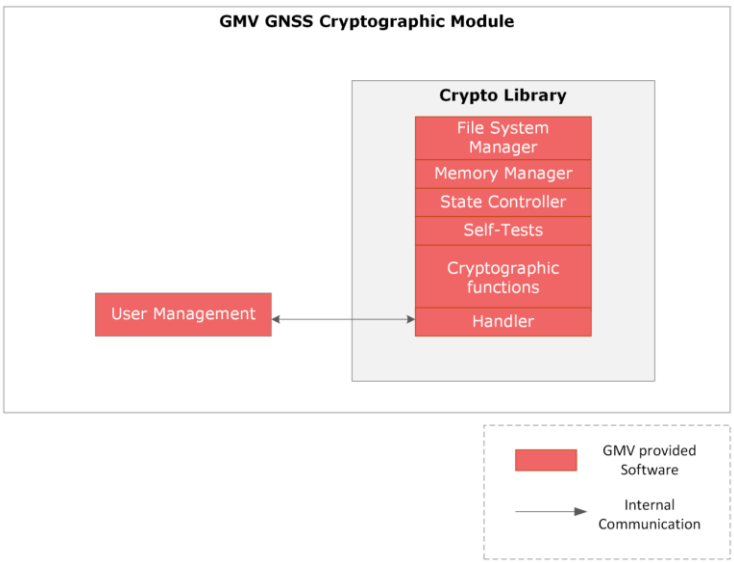
- Crypto library: Component responsible for providing the cryptographic functions and the security services for the TOE (See Table 10). The services offered include the following:
- Memory Manager: This module is designed for the secure management of all data stored and utilized within the system. Key responsibilities encompass the zeroization of data, ensuring that sensitive information is effectively erased and rendered unrecoverable.
- State Controller: Implements the logic to control the state changes of the TOE and the authorized functions for each state. The State Changer function checks that only state changes authorized by the state machine logic is performed. The state logic is specified in the diagram below.



- Self-tests: Tests the integrity of the executable code and the correct operation of the cryptographic functions. For integrity verification, the module computes a hash of the entire executable code and retains it. To validate the effectiveness of the cryptographic functions, it implements FIPS test vectors from the Cryptographic Algorithm Validation Tests (CAVS). These tests are conducted both prior to the module providing services to a client and whenever an authorized user initiates a "self-test operation."
- Timer: The main function of this module is to prevent Denial of Service (DoS) attacks. It achieves this by monitoring socket connections and automatically closing them if a specified time elapses without any operation requests.

- File system manager: This module is responsible for manager the persistence of the system. Its primary function involves ensuring that Role-Based Access Control (RBAC) is applied to all operations, including the addition, modification, and deletion of stored data.
- Handler: Facilitates the management of all internal requests between the module and the crypto library, ensuring the maintenance of the secure channel.
- User Management Module: This module is responsible for user authentication and the comprehensive management of user profiles and their associated data, including usernames, passwords, and roles.

All the components that are included in the scope of this evaluation are in red in the following figure.



PHYSICAL ARCHITECTURE

The TOE, being a software package, is encapsulated within the contents of the provided .zip file.

The TOE comprises three essential components: cryptomodule_1.elf, cryptomodule_2.bin, and cryptomodule_3.bin, along with a comprehensive set of documentation. Upon receipt, a client will obtain a release file including these components compressed into a .zip format, denoted as gmv-gnss-cryptographic-module-v2.1.7.zip, containing:

- [Folder] GMV_GNSS_Cryptographic_Module_v2.1.7: The release TOE file that includes:
  - [File] cryptomodule_1.elf
  - [File] cryptomodule_2.bin
  - [File] cryptomodule_3.bin
  - [Folder] documentation: Folder that includes all the documentation specified in "*GMV GNSS Cryptographic Module - Master Project References Document*", v2.1.7.

- [File] GMV GNSS Cryptographic Module – User Guide.pdf: A comprehensive guide detailing file functionalities and module usage.
- [File] GMV GNSS Cryptographic Module – Functional Spetification.pdf: A comprehensive guide detailing the TOE functionalities, how to build the module packets and more interesting information.
- [File] hashes_file.txt: This file contains the unique hashes for each delivered file, enabling clients to verify their integrity. The hashes included in this file are:

File	Version	Format	SHA-256 Hash
GMV_GNSS_Cryptographic_Module_v2.1.7/ cryptomodule_1.elf	v2.1.7	.elf	8d67bb675277e365296026dc50169b917bf1a80209c7398f03d4c26ba55fb999
GMV_GNSS_Cryptographic_Module_v2.1.7/ cryptomodule_2.bin	v2.1.7	.bin	5095f19589331385d8075f1a9f9e9db49d380a77ee7b6fb483d324af0d4cf419
GMV_GNSS_Cryptographic_Module_v2.1.7/ cryptomodule_3.bin	v2.1.7	.bin	30efedec1fa03b33a00458ac1b263147389e01d2646063a5305c3f86410be27e
GMV_GNSS_Cryptographic_Module_v2.1.7.zip	v2.1.7	.zip	Indicated in hashes_file.txt.

DOCUMENTS

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

File	Version	Format	SHA-256 Hash
GMV GNSS Cryptographic Module – User Guide.pdf	v2.1.7	.pdf	343db2e3d197dfc071d815ece355ea284a171abf5cae2c5cee341a7cc141b762
GMV GNSS Cryptographic Module – Functional Specification.pdf:	v2.1.7	.pdf	1b2a3749606a055f375f4530df7eca1be12bfea4a864af31d9c2ec2d9348cf90

PRODUCT TESTING

The developer has executed tests for the only available TSFI. 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 set of tests for 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 TOE is intended to be implemented in a platform environment that uses Ubuntu 22.04 or above and includes the GNU Multiple Precision Arithmetic Library dependencies. The TOE provides the cryptographic primitives to do the cryptographic functions through an Application Program Interface (API).

The TOE provides this external API that exclusively operates via a TCP/IP socket connection for interfacing with the module. Therefore, any application with the capability to form a socket connection with the TOE is deemed a client of the TOE. The primary hardware and software requirements for such a client are limited to the necessities for setting up this specific socket connection.

EVALUATION RESULTS

The product GMV GNSS Cryptographic Module v2.1.7 has been evaluated against the Security Target GMV GNSS Cryptographic Module - Security Target v2.1.7 (28/08/24).

All the assurance components required by the evaluation level EAL2 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, 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 install the correct version of the TOE 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.
- The fulfilment of the assumptions indicated in the security target is a key point as it implies TOE environment configurations that leave some potential vulnerabilities out of the scope.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidence during the instruction of the certification request of the product GMV GNSS Cryptographic Module v2.1.7, a positive resolution is proposed.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GNSS	Global Navigation Satellite System
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.

[ST] GMV GNSS Cryptographic Module - Security Target v2.1.7 (28/08/24).

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:

- GMV GNSS Cryptographic Module - Security Target v2.1.7 (28/08/24).

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 selected.