EUCC - Certification Report

Certification Report information	
Certification report reference	FCS506_00 EN EUCC GMV_GNSS-Certification Report_v2.0
TOE Identification	GMV GNSS Cryptographic Module version 2.1.7
Evaluation basis	Common Criteria for Information Technology Security Evaluation, version 3.1, revision 5 ([CC31p1], [CC31p2] and [CC31p3]) Common Methodology for Information Technology Security Evaluation, revision 5, version 3.1 ([CEM31])
Evaluation Level	EAL2
Evaluation Technical report (ETR) reference	GMV_GNSS-ETR GMV GNSS Cryptographic Module Evaluation Technical Report version 1.2
CB identification	DEKRA Testing and Certification S.A.U. EUCC CB Body Number at ENISA: CB 3095
Author	Nelson Páramo Valdivielso & Diego Sierra Liras
Date	23/07/2025
EUCC Applicant information	
Applicant identification	GMV Aerospace and Defense S.A.
ITSEF information	
ITSEF identification	DEKRA Testing and Certification S.A.U. ITSEF id at DEKRA: ITSEF-2024-01 Body Number at ENISA: ITSEF 3095

CONTENT

1. Executive Summary

This document is the Certification report of the certification of the **GMV GNSS Cryptographic Module** version **2.1.7** developed on the basis of the Evaluation Technical Report (ETR) GMV_GNSS-ETR.

This report is published together with the corresponding TOE EUCC certificate.

The evaluation was conducted by the ITSEF **DEKRA Testing and Certification S.A.U.** and was finished on **September 4th, 2024** with **PASS** verdict.

The evaluation was conducted in accordance with the Common Criteria (CC) standard, version 3.1 revision 5 (CC V3.1 R5).

The evaluation activities performed during the evaluation correspond to an assurance level of **EAL2**, as specified in [CC31p3] and [CEM31].

The security functionality of the evaluated ICT product is represented by the implementation of the selected components of [CC31p2] and are listed in section **7. SECURITY REQUIREMENTS** of the [ST].

Next, there is a summary of the **threats** and **organisational security policies (OSPs)** addressed by the evaluated ICT product:

- **Threats:**

  Threat agents are defined as external actors, insiders (privileged users), or regular authorised users.

  External actors or insiders could try to alter or disclose critical data through the TOE's functions, file system, or network. Sensitive information could be intercepted or tampered with during transfer, affecting cryptographic performance. Accessing deallocated memory might expose security data. Denial of service (DoS) attacks could disable the TOE, blocking communication. Finally, malicious software could be loaded through the TOE's interfaces or operating system.

- **Organisational Security Policies (OSPs):**

  The TOE implements cryptographic functions that are endorsed by the ESA authority as suitable for user applications. These algorithms, described in detail in Section 2.2 of [GOSNMARG], ensure robust security and compliance with established standards. Additionally, the TOE must generate an audit trail to log security-relevant events. This audit trail includes the fields, details, and subjects associated with each event, providing a reliable mechanism for monitoring and accountability.

The evaluated ICT product usage is recommended given that there are not exploitable vulnerabilities for the evaluated ICT product under its operational environment. The following usage recommendations are given:

- It is mandatory to strictly follow the steps indicated in the installation documentation in order to download and install the correct version of the evaluated ICT product in a proper manner.
- The user guidance must be read and understood in order to operate the evaluated ICT product in an adequate manner according to the security target.
- The fulfilment of the assumptions indicated in the section **4 1. Assumptions and clarification of scope** of this document is a key point as it implies evaluated ICT product environment configurations that leave some potential vulnerabilities out of the scope.

The patch management is out of the scope of the evaluation.

Lastly, the Technical Reviewers' Team provides the following recommendation regarding the certification decision:

Recommendation on Certification Decision		
Recommendation of the Technical reviewers team	**POSITIVE**	Certificate validity period: 5 years

2. Evaluated ICT product / PP

2. Evaluated ICT product	
Name of the evaluated ICT product	GMV GNSS Cryptographic Module version 2.1.7
Enumeration of the ICT product's components that are part of the evaluation	N/A
Version number of the ICT product's components	N/A
ST reference	GMV GNSS Cryptographic Module - Security Target, version 2.1.7, 28/08/2024
Identification of additional requirements to the operating environment of the certified ICT product	There is a single evaluated configuration, consisting of the evaluated ICT product deployed on a platform running Ubuntu 22.04.
Name and contact information of the holder of the EUCC certificate	GMV Aerospace and Defense S.A. Calle de Isaac Newton (Pq. Tecnológico de Madrid), 11 28760, Tres Cantos, Madrid, España Néstor Ganuza Artiles n.ganuza@gmv.com tlf: +34 699888658
Patch management procedure included into the certificate	N/A
Vulnerability handling and Disclosure procedures / assurance continuity	[VUL] EUCC VULNERABILITY MANAGEMENT AND DISCLOSURE PROCEDURES. PAC-PDC Version: 1.0. 27/01/2025
Link to the website of the holder of the EUCC certificate where supplementary cybersecurity information for the certified ICT product in accordance with Article 55 of Regulation (EU) 2019/881 is provided	*https://www.gmv.com/en-es/productos/espacio/gmv-gnss-cryptographic-module#supporting-documents-for-certification*

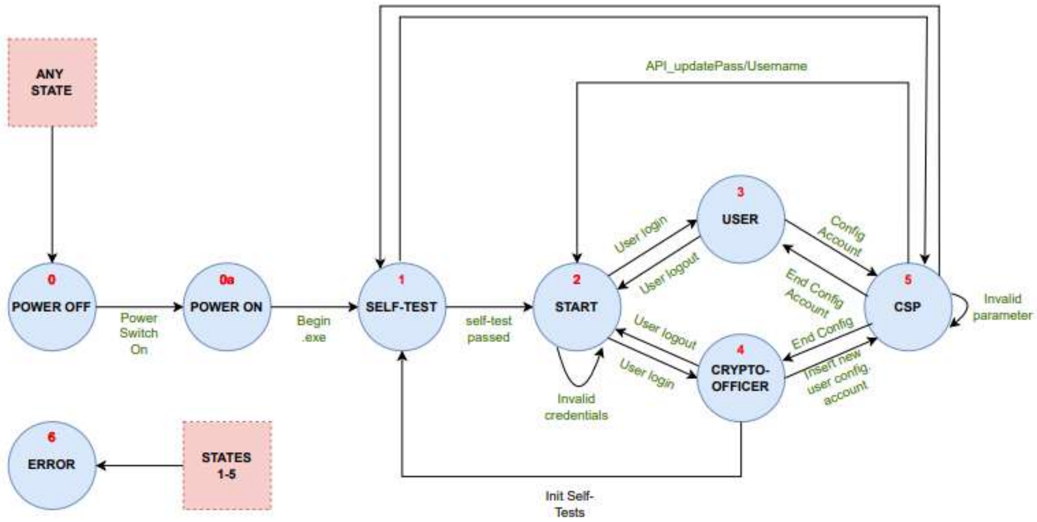
3. Security services

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. 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."

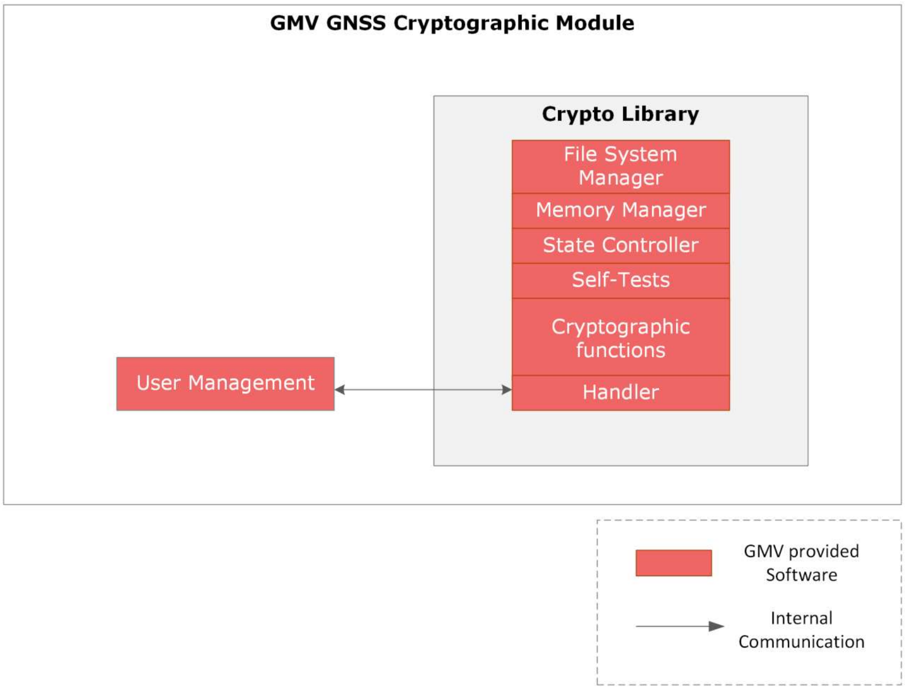
  - **Timer:** The main function of this module is to prevent Denial of Service (DoS) attacks. It achieves this by monitoring socket connections and automatically closing them if a specified time elapses without any operation requests.

  - **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.

The components within the scope of the evaluation are highlighted in red in the following figure.


GMV GNSS Cryptographic Module
Crypto Library
File System Manager
Memory Manager
State Controller
Self-Tests
Cryptographic functions
Handler
User Management
GMV provided Software
Internal Communication

4. Assumptions and clarification of scope

The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and use correctly. The following specific conditions are assumed to exist in an environment where TOE is employed:

Asssumption	Description
A.ADMINISTRATOR **Reliable administrator**	The administrator of TOE will be reliable and will operate the TOE in a secure and correct manner, avoiding any harmful intent to the device or its data.
A.ENVIRONMENT **Environment protection**	The TOE operates in a protected environment that limits physical access to the TOE to authorised Administrators. The TOE environment ensures the confidentiality, integrity, and availability of the security relevant data for the TOE initialisation, start-up, and operation. (e.g. the verification data that allows check the integrity of the TOE software)
A.OPERATING_SYSTEM **Operating System**	The operating system has been selected to provide the functions required by the TOE and the security mechanisms necessary to assure the integrity of TOE code.
A.TIMESTAMP **Operating System Timestamp**	The TOE runs on a platform that provides reliable timestamps.
A.LOG_TRAIL **Availability of log records**	The log records will be accessible to the TOE administrator, who can directly retrieve them from the TOE's persistence system.

5. Architectural information

The product is a software library consisting of two components: the Crypto Library and the User Management Module. Both components are described in Chapter 3.5.2, "TOE Logical Description," of the Security Target [ST].

6. Supplementary cybersecurity information

The manufacturer of the certified ICT product for which an EU statement of conformity has been issued shall make publicly available the following supplementary cybersecurity information:

a) guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ICT products or ICT services;

   https://www.gmv.com/en-es/productos/espacio/gmv-gnss-cryptographic-module#supporting-documents-for-certification:

   1. https://www.gmv.com/en-es/Declaración_de_seguridad_GMV_GNSS_Cryptographic_Module
   2. https://www.gmv.com/en-es/Guía_de_usuario_GMV_GNSS_Cryptographic_Module

b) the period during which security support will be offered to end users, in particular as regards the availability of cybersecurity related updates;

   https://www.gmv.com/en-es/productos/espacio/gmv-gnss-cryptographic-module#supporting-documents-for-certification:

   Vulnerability handling (https://www.gmv.com/en-es/docs/vulnerability-handling):

   GMV has implemented a strategic plan to manage and monitor the cybersecurity of the GMV GNSS Cryptographic Module, for at least 5 years, which includes the following support channels:

   - A vulnerability publication channel. Any new vulnerability identified in the module will be analyzed and published in the NIST National Vulnerability Database (NVD).
   - A specific communication channel through the email eucc@gmv.com, where end users and researchers can report vulnerabilities or request additional information about the security of the product.
   - Product updates and patches will be submitted by GMV to final users when available. GMV GNSS Cryptographic Module users can also request to eucc@gmv.com such updates and patches at any given time.

c) contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers;

   https://www.gmv.com/en-es/contact, available at the bottom of the webpage.

d) a reference to online repositories listing publicly disclosed vulnerabilities related to the ICT product, ICT service or ICT process and to any relevant cybersecurity advisories.

   https://www.gmv.com/en-es/productos/espacio/gmv-gnss-cryptographic-module#supporting-documents-for-certification:

   Vulnerability handling (https://www.gmv.com/en-es/docs/vulnerability-handling)

   GMV has implemented a strategic plan to manage and monitor the cybersecurity of the GMV GNSS Cryptographic Module, for at least 5 years, which includes the following support channels:

   - A vulnerability publication channel. Any new vulnerability identified in the module will be analyzed and published in the NIST National Vulnerability Database (NVD).
   - A specific communication channel through the email eucc@gmv.com, where end users and researchers can report vulnerabilities or request additional information about the security of the product.

7. ICT product testing

The certificate is issued by **DEKRA Testing and Certification S.A.U. EUCC CB (3095)**, under the authority of the Spanish NCCA CCN. The evaluation was performed by **the ITSEF DEKRA Testing and Certification S.A.U.**

The evaluation activities performed for an assurance level of **EAL2**, as specified in [CC31p3] and [CEM31], are summarized in the following table:

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic Design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
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.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability Analysis

There is neither state-of-the-art document nor further security evaluation criteria used in the evaluation.

The evaluated configuration is limited to the ICT product deployed in an environment running Ubuntu 22.04.This specific configuration is established by strictly adhering to the detailed guidance provided [AGD217] and ensuring that all the security objectives for the operational environment are met. The configuration has been verified to align with the intended security posture and functional requirements, ensuring that it operates within the defined environment in a secure and compliant manner.

The [ST] does not claim conformance to any PP.

8. Certificate holder’s lifecycle management processes and production facilities

This section summarizes the configuration management system applied by the holder of the certificate for the identification of the configuration items, its versioning method and change control.

The Configuration Management (CM) scope references all the items that the GMV GNSS Module embraces.

VERSION CONTROL

The GMV GNSS Module is subject to continuous evolution, featuring versions that reflect the addition of new functionalities, the resolution of patches and bugs, or the introduction of new structural configurations.

Version management for the GMV GNSS Module is handled through releases on GitLab, encompassing both the source code and the physical components of the TOE. This comprehensive approach to version control extends to the module's documentation as well. The policy is to synchronize the documentation's version number with that of the source code, ensuring consistency across all elements of the module. This synchronization occurs even in instances where no modifications have been made to the documentation (or vice versa), maintaining a unified versioning scheme that accurately reflects the module's development and status.

- **SEMANTIC VERSIONING**

  These releases are based on semantic versioning. This means that the numbers of the versions are important and contain information about the type of the module release.

  Semantic Versioning is a system used for versioning software that provides a clear and consistent way to communicate changes to a software application. The system consists of a set of rules and requirements that dictate how version numbers are assigned and incremented.

  The version number is typically composed of three parts: **MAJOR.MINOR.PATCH.** Each part represents a different aspect of the software and corresponds to different types of changes made to the software:

  - **MAJOR** version number indicates a significant change that may not be backward compatible with previous versions. This means that any software built on a previous version may require modification to work with the new version.
  - **MINOR** version number indicates a backward-compatible addition of functionality to the software. This means that any software built on a previous version will continue to work with the new version without modification.
  - **PATCH** version number indicates a backward-compatible bug fix or small enhancement to the software. This means that any software built on a previous version will continue to work with the new version without modification.

  In addition to these three parts, Semantic Versioning also allows for pre-release versions to be identified by appending a hyphen and additional identifiers, such as alpha, beta, or rc (release candidate), to the version number. For example, 1.0.0-alpha.1 represents the first alpha release of version 1.0.0.

- **RELEASES**

  The releases are generated through automated means. To issue a release, the following three parameters need to be set:

  - Access Token
  - Semantic versioning name, such as v1.0.1

- A message that describes the new release

The identification of the release is provided both at the TOE documentation and by the TOE itself, accessible through the TOE programmatic interfaces.

9. Evaluation results

The evaluation of the ICT product, has confirmed that it meets the requirements for assurance level 'Substantial' as defined in Article 4 of the EUCC Implementing Regulation and Article 52 of Regulation (EU) 2019/881.

The AVA_VAN.2 component indicates that the product was evaluated to resist attacks from attackers with a BASIC attack potential.

Finally, based on the review of the evaluator's analysis and conclusions for the ASE, ALC, AGD, ADV, ATE, and AVA activities, it can be confirmed that the evaluation was conducted in accordance with the Common Criteria requirements.

ASE:

The findings are well-documented and internally consistent, demonstrating a thorough understanding of the Security Target (ST) and its components. The identified threats, security objectives, and security requirements are appropriately addressed, and the TOE description is both accurate and adequate for the evaluation level. Consequently, the ASE activities fulfill the assurance requirements for EAL2. No issues or deviations were identified that could impact the assurance of the TOE.

ALC:

The findings demonstrate that the TOE's lifecycle processes, covering configuration management, delivery, and related controls, are clearly defined, properly implemented, and aligned with the required assurance level. The submitted evidence supports traceability of changes and the secure handling of the TOE throughout its lifecycle. Accordingly, the ALC activities satisfy the assurance requirements for EAL2, with no issues or deviations identified that could compromise the TOE's security.

AGD:

The evaluation has demonstrated that the guidance documentation is clear, complete, and sufficient to support the secure installation, configuration, and operation of the TOE within its intended environment. The guidance effectively helps prevent common misconfigurations and promotes correct usage. Therefore, the AGD activities fulfill the assurance requirements for EAL2, with no issues or deviations identified.

ADV:

The findings confirm that the design documentation provides sufficient detail to understand the TOE's architecture and security-enforcing functions. The evidence demonstrates clear traceability between the security requirements and the TOE design. Accordingly, the ADV activities meet the assurance requirements for EAL2, with no issues or deviations identified.

ATE:

The testing evidence provided by the developer has been thoroughly reviewed and verified as complete, demonstrating correct implementation of the TOE's specified security functions. This includes validation of cryptographic operations, user data protection, and other security measures to ensure compliance with the defined requirements. The evaluator conducted independent testing to further verify the accuracy and reliability of the developer's claims, executing a comprehensive set of tests that confirmed the TOE operates as intended, with no failures or security vulnerabilities identified.

As a result, the independent testing confirms that the TOE complies with all relevant security requirements specified for the evaluation. The testing process, encompassing both the developer's evidence and the evaluator's independent tests, has been comprehensive and thorough. No issues or deviations were identified during the evaluation, and the testing activities fully satisfy the assurance requirements for EAL2.

AVA:

The evaluation confirmed that the TOE underwent a comprehensive assessment to identify vulnerabilities exploitable with basic attack potential. This assessment included an in-depth analysis of the TOE itself, as well as any third-party components or libraries it depends on. Public known vulnerabilities such as those documented in security databases and related to the TOE's software components were taken into account. The testing process involved simulated attacks using commonly known methods and techniques to evaluate the TOE's resistance to potential exploitation.

Beyond assessing known vulnerabilities, the evaluation also examined the TOE's resilience within its defined operational environment. The analysis confirmed that the TOE maintains robustness against such attacks, with no significant vulnerabilities identified that could undermine its security.

Consequently, the AVA activities were performed in full compliance with the assurance requirements for EAL2, providing a reasonable level of confidence in the TOE's resistance to exploitation.

10. Information of the certificate

Date of Issuance	23/07/2025
Period of Validity	Valid for five years from the date of issuance *The certificate is valid for five (5) years from the date of issuance, inclusive, and remains valid until the end of 22 July 2030, unless suspended or withdrawn earlier*
Unique Identifier of the Certificate	EUCC-3095-2025-07-01
Scheme Name	(EU) 2024/482 - EUCC
Certification Body Accreditation Reference Number	DEKRA Testing and Certification S.A.U. EUCC CB ENAC´s Accreditation number **134/C-PR337** ENISA´s Body number: **3095**

11. Summary of the security target of the ICT product

1. INTRODUCTION

o SECURITY TARGET REFERENCE

Security Target Title	GMV GNSS Cryptographic Module - Security Target
Security Target Version	2.1.7
Date	28/08/24
Author	Esther Godoy, Jorge Juan Tejero, Alberto

o TOE REFERENCE

TOE developer	GMV Aerospace and Defence
TOE version	2.1.7
Date	28/08/24
TOE name	GMV GNSS Cryptographic Module*

o TOE OVERVIEW

The TOE specified in the ST is the GMV GNSS Cryptographic Module.

The GMV GNSS Cryptographic Module is a software library developed on the Linux platform, primarily designed to provide cryptographic services for various future GNSS projects. An example of such a project is the Open Service Navigation Message Authentication (OSNMA) protocol used in Galileo. These cryptographic services utilize algorithms approved by the European Space Agency (ESA) [GOSNMARG].

The TOE is intended to be deployed on a platform environment running Ubuntu 22.04 and depends on the GNU Multiple Precision Arithmetic Library. It offers cryptographic primitives through an Application Programming Interface (API), enabling cryptographic functions. Communication between applications and the GMV GNSS Cryptographic Module is facilitated via network sockets employing the TCP/IP protocol, allowing any application using this socket protocol to connect to the module.

Below is an overview of the services provided by the TOE, along with the associated algorithms and data structures involved.

TOE Service	Algorithm	OSNMA Service Involved
Message Digest	SHA256, Merkle Tree	Public key authentication using Merkle Tree structure with SHA256 hash function
Signature Authentication	ECDSA P-256, ECDSA P-521, SHA256, SHA512, SHA3-256	Signature authentication using public key
Message Authentication	CMAC AES256, HMAC SHA256	Message Authentication Code verification

The GMV GNSS Cryptographic Module recollects and stores logs using a circular log file into the file system to give traceability of the invoked cryptographic services and the users involved.

- **NON-TOE OVERVIEW**

The TOE offers an external API that operates solely through a TCP/IP socket connection to interface with the module. Consequently, any application capable of establishing a socket connection with the TOE is considered a client. The primary hardware and software requirements for such a client are limited to those necessary to establish this specific socket connection.

- **TOE SECURITY FUNCTIONALITY.**

Please refer to section **3 Security services** of the this document.

2. CONFORMANCE CLAIMS

The [ST] claims conformance to [CC31p1], [CC31p2] and [CC31p3].

The [ST] does not claim conformance to any Protection Profile.

The [ST] claims conformance to EAL2 package.

3. SECURITY PROBLEM DEFINITION

- **ASSUMPTIONS:**

Please refer to section **4 Assumptions and clarification of scope** of this document.

- **ASSETS TO BE PROTECTED**

  - **R.USER_DATA:** Data supplied by a client for use in the TOE services. This data requires confidentiality and integrity, in case of users' passwords and integrity in case of the other associated data.
  - **R.OSNMA_KEYS:** Public keys and TESLA keys used by the TOE in support of the cryptographic services. The integrity of these keys must be protected.
  - **R.AES_KEY:** Secret key used to encrypt and decrypt the communication path between the TOE and the user, it must be protected in integrity and confidentiality.
  - **R.INTEGRITY_HASH:** Imported hash to verify the integrity of the embedded code, this data requires integrity.
  - **R.SOFTWARE:** Embedded software of the GMV GNSS Module. The software implements the security mechanisms of the TOE; therefore it must be protected in integrity.

- **THREATS:**

Types	Threats	Description
Threats on critical security parameters	T.KEY_ALTERATION Alteration of keys	TA.EXTERNAL or TA.INSIDER might modify or alter all or part of R.OSNMA_KEYS, R.INTEGRITY_HASH and R.AES_KEY by interaction with the TOE logical functions, the file system in which this information is stored or within the TOE environment. TA.USER with Crypto-officer role might also modify or alter R.AES_KEY since this user has the responsibility to load this data in the GMV GNSS Cryptographic Module.
	T.KEY_DISCLOSE Disclosure of keys	TA.EXTERNAL or TA.INSIDER might disclose all or part of R.OSNMA_KEYS, R.AES_KEY by means of intercept the data in the network communication channel, reading the information

		in the file system or even during the use of the TOE services.
Data Threats	T.DATA_MANIPUL Manipulating data	TA.EXTERNAL, TA.INSIDER or TA.USER could potentially tamper with R.USER_DATA or R.OSNMA_KEYS during their transfer from the client application to the TOE (in the case of TA.EXTERNAL) or within the TOE's persistence system (in the case of TA.INSIDER and TA.USER). Such manipulation might adversely impact the performance of cryptographic functions, as the TOE may not be able to detect the presence of corrupted data.
	T.MEMORY_DUMP_ATTACK Deallocated memory access	TA.EXTERNAL, TA.INSIDER or TA.USER might access to the module's deallocated memory. This may allow access to previous security information such as R.USER_DATA, R.OSNMA_KEYS or R.AES_KEY.
Service Threats	T.BLOCK_SERVICE Blocking of TOE services	TA.EXTERNAL , TA.INSIDER or TA.USER might disable the TOE service through open a socket connection and not operating with the module, or requesting infinite operations. This may hold the communication channel and block another client to connect with the TOE.
	T.MALICIOUS_SW Malicious software	TA.EXTERNAL or TA.INSIDER might modify or alter the R.SOFTWARE by loading malicious software by means of the interaction with the TOE logical interfaces or getting permissions of the operative system in which the TOE is operating.

- **ORGANISATIONAL SECURITY POLICIES (OSPs):**

OSP	Description
P.ALGORITHMS (Approved cryptographic algorithms)	The TOE provides cryptographic functions endorsed by ESA authority as suitable for user implementation.
P.AUDIT (Audit trail generation)	The TOE is required to generate an audit trail of security-relevant events, registering the events fields, details, and the subject associated with the event.

4. SECURITY OBJECTIVES

o SECURITY OBJECTIVES FOR THE TOE

Security Objective	Description
OT.ALGORITHMS (Use of approved cryptographic algorithms)	The TOE offers cryptographic functions provided for users that are validated by the ESA authority as appropriate.
OT.AUDIT (Generation and storage of audit data)	The TOE shall audit the following events: TOE initialization and shutdown, module state changes, self-test operation, user login/logout, cryptographic operations, addition, deletion, and modifications of security attributes and data stored in the TOE,

	zeroization, memory violation, and establishment and disconnection of the secure channel.
OT.DOS.RESPONSE (Denial of Service attack response)	The TOE shall be able to identify a service interruption attack and act so the service can be re-established and operate in the common manner.
OT.RESTRICT.ACCESS (Control access to TOE services)	The TOE shall restrict access to its services based on user roles, allowing access only to those explicitly assigned. Additionally, it shall restrict access when a specific timeout is over.
OT.SEC.CHANNEL (Exchange of encrypted data)	Confidentiality and integrity of the data transferred between the TOE and the user are ensured by a secure communication channel. The TOE shall encrypt data sent through the channel and decrypt received data by the channel.
OT.SEC_DATA (Security of data)	The confidentiality and integrity of the R.USER_DATA, R.AES_KEY and R.INTEGRITY_HASH, in addition to the integrity of the R.OSNMA_KEYS shall be ensured during their whole lifetime.
OT.SEC_STATE (Secure State in case Error is detected)	The TOE shall enter a secure state whenever it detects a failure or an integrity error of software. The secure state shall prevent the loss of confidentiality and integrity of R.USER_DATA, R.AES_KEY and R.INTEGRITY_HASH, and the integrity of R.OSNMA_KEYS
OT.USER_AUTH (Authentication of users interacting with the TOE)	The TOE shall be able to identify and authenticate the users acting with a defined role, before allowing access to any TOE service. Identification shall be password-based, and authentication shall be role-based.

- **SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT**

Security Objectives for the Operational Environment	Description
OE.APPLICATION (Security in Client Application)	The applications which use the TOE shall perform the necessary security checks on the data passes through the secure channel to the TOE. They shall ensure the appropriate format for the communication and operations.
OE.AUDIT_REVIEW (Audit review)	The environment ensures the availability of the generated by the TOE audit trails and provides a review of the audit trail recorded by the TOE.
OE.OPERATING_SYSTEM (OE.OPERATING_SYSTEM Reliable Operating System)	The Operating system in which the TOE is allocated shall enable the correct operation of the TOE services and establish the necessary mechanism to ensure the security of its embedded code. It shall also provide reliable timestamps for the use of the TOE.
OE.PERSONNEL (Reliable Personnel)	The personnel using the TOE shall be aware of the obligations they have to face, depending on their role. The personnel shall be trained on correct usage of the TOE and should be trusted people.
OE.PROTECT_ACCESS (Prevention of unauthorised physical access)	The TOE shall be protected by physical, logical, and organisational protection measures, to prevent any TOE modification, as well as protect assets disclosure. Those measures shall restrict the TOE usage to authorised persons only.

5. SECURITY REQUIREMENTS

The evaluation activities performed for an assurance level of **EAL2**, as specified in [CC31p3] and [CEM31], are summarized in the following table:

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic Design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
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.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability Analysis

The security functionality of the evaluated ICT product is represented by the implementation of the selected components of [CC31p2] listed in the following table:

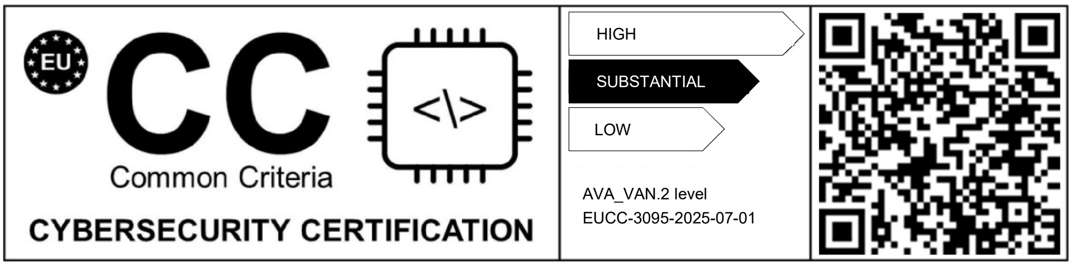
Requirement Class	Requirement component
Security Audit (FAU)	Audit data generation (FAU_GEN.1)
Cryptographic Support (FCS)	Cryptographic Key Destruction (FCS_CKM.4)
	Cryptographic Operation (FCS_COP.1)
User Data Protection (FDP)	Import of user data without security attributes (FDP_ITC.2)
	Subset residual information protection (FDP_RIP.1)
	Inter-TSF user data confidentiality transfer protection (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 initialization (FMT_MSA.3)
	Specification of management functions (FMT_SMF.1)
	Security roles (FMT_SMR.1)
Protection of the TSF (FPT)	TSF self test (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)

6. TOE SUMMARY SPECIFICATION

Section 8 of the TOE Summary Specification of the [ST] outlines the security features of the TOE that enable compliance with the security functional requirements described in the previous section.

12. Mark and label



AVA_VAN.2 level
EUCC-3095-2025-07-01

13. Bibliography

[AGD217] GMV GNSS Cryptographic Module - User Guide, version 2.1.7, August 2024.

[CC31p1] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1, Revision 5

[CC31p2] Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components. Version 3.1, Revision 5

[CC31p3] Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components. Version 3.1, Revision 5

[CEM31] Common Criteria for Information Technology Security Evaluation. Evaluation Methodology. Version 3.1 Revision

[CSA] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[GOSNMARG] Galileo Open Service Navigation Message Authentication (OSNMA) Receiver Guidelines, Version 1.3, January 2024

[IMPACT] Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

[SotA] EUCC SCHEME DRAFT STATE-OF-THE-ART DOCUMENT. ACCREDITATION OF ITSEFs FOR THE EUCC SCHEME. Version 1.6b, June 2024

[ST] GMV GNSS Cryptographic Module – Security Target, v2.1.7, August 2024.

[VUL] EUCC VULNERABILITY MANAGEMENT AND DISCLOSURE PROCEDURES. PAC-PDC Version: 1.0. 27/01/2025.

Signature:

Nelson Páramo Valdivielso
EUCC CB Technical Reviewer

DEKRA Testing and Certification S.A.U.

Signature:

Diego

Diego Sierra Liras
EUCC CB Technical Manager

DEKRA Testing and Certification S.A.U.