NASK

Polish IT Security Evaluation and Certification Scheme (PC1)

Certification Report

[2022-1] Certification Report on DTMS-2 EAL4 + ATE_DPT.2 and AVA_VAN.5

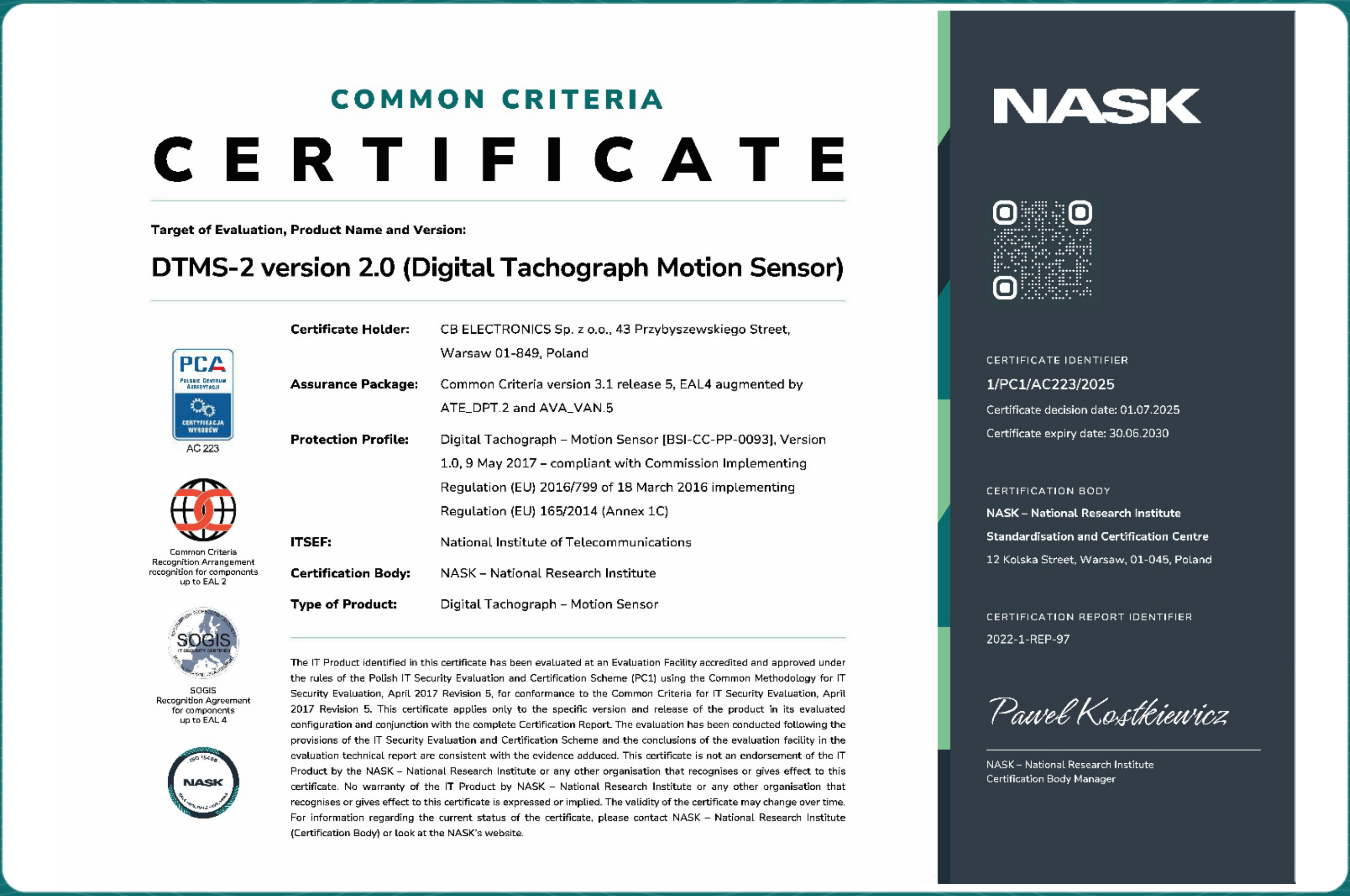
Certification Dossier Code: 2022-1

Certification Report Creation Date: 20th June 2025

Certification Report Code: 2022-1-REP-94 (internal)
2022-1-REP-97 (public)

NASK RWA code: OSiC.8711.1.2022

AC 223



COMMON CRITERIA

CERTIFICATE

Target of Evaluation, Product Name and Version:

DTMS-2 version 2.0 (Digital Tachograph Motion Sensor)

AC 223

Common Criteria Recognition Arrangement recognition for components up to EAL 2

SOGIS Recognition Agreement for components up to EAL 4

Certificate Holder:	CB ELECTRONICS Sp. z o.o., 43 Przybyszewskiego Street, Warsaw 01-849, Poland
Assurance Package:	Common Criteria version 3.1 release 5, EAL4 augmented by ATE_DPT.2 and AVA_VAN.5
Protection Profile:	Digital Tachograph – Motion Sensor [BSI-CC-PP-0093], Version 1.0, 9 May 2017 – compliant with Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 (Annex 1C)
ITSEF:	National Institute of Telecommunications
Certification Body:	NASK – National Research Institute
Type of Product:	Digital Tachograph – Motion Sensor

The IT Product identified in this certificate has been evaluated at an Evaluation Facility accredited and approved under the rules of the Polish IT Security Evaluation and Certification Scheme (PC1) using the Common Methodology for IT Security Evaluation, April 2017 Revision 5, for conformance to the Common Criteria for IT Security Evaluation, April 2017 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and conjunction with the complete Certification Report. The evaluation has been conducted following the provisions of the IT Security Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT Product by the NASK – National Research Institute or any other organisation that recognises or gives effect to this certificate. No warranty of the IT Product by NASK – National Research Institute or any other organisation that recognises or gives effect to this certificate is expressed or implied. The validity of the certificate may change over time. For information regarding the current status of the certificate, please contact NASK – National Research Institute (Certification Body) or look at the NASK's website.

NASK

CERTIFICATE IDENTIFIER

1/PC1/AC223/2025

Certificate decision date: 01.07.2025

Certificate expiry date: 30.06.2030

CERTIFICATION BODY

NASK – National Research Institute

Standardisation and Certification Centre

12 Kolska Street, Warsaw, 01-045, Poland

CERTIFICATION REPORT IDENTIFIER

2022-1-REP-97

Pawel Kostkiewicz

NASK – National Research Institute
Certification Body Manager

Certification
NASK

Table of content

1. **Introduction 4**
2. **Certification overview 4**
   - Recognition of the certificate 5
   - Executive Summary 5
   - Documentation available for users 6
   - Security Target 6
3. **TOE Summary 7**
   - TOE Overview 7
   - Security Assurance Requirements 9
   - Security Functional Requirements 10
   - Security Policy 11
4. **Assumptions and Clarification of Scope 12**
   - Environmental Assumptions 12
   - Clarification of Scope 12
   - Threats 12
5. **Architectural Information 14**
   - Physical scope 14
   - Delivery of the TOE 16
   - Logical scope 16
6. **IT security evaluation 17**
   - Evaluated Configuration 17
   - Functional testing 21
   - Developer testing 21
   - Evaluator testing 21
   - Penetration testing 21
   - Evaluation results and conformity verdicts 24
   - Evaluator Comments/Recommendations 25
7. **Certifier Recommendations 27**
8. **Acronyms 27**
9. **Bibliography 28**
   - References 29
   - List of related documents 30

1. Introduction

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been tested at an approved Laboratory (IT Security Evaluation Facility) – on the basis of the IT Security Evaluation and Certification Scheme – using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5. This certification report, and its associated certificate, applies only to the identified version and release of the product in its tested and evaluated configuration. The evaluation has been conducted in accordance with the provisions of the IT Security Evaluation and Certification Scheme - PC1, and the conclusions of the Laboratory in the technical evaluation report are consistent with the evidence. This report, and its associated certificate, are not an endorsement of the IT product by the NASK National Research Institute, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the NASK National Research Institute, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration.

2. Certification overview

The NASK's "IT Security Evaluation and Certification Scheme" (Accreditation AC-223 by Polish Centre of Accreditation) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by an approved Laboratory under the oversight of the Certification Body, which is managed by the NASK National Research Institute. Laboratory is a commercial facility that has been approved by the Certification Body to perform Common Criteria based cybersecurity evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025:2018- The General Requirements for the Competence of Testing and Calibration Laboratories. By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. **The consumer of certified IT products should review the Security Target, in addition to this Certification Report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the Laboratory**. The Certification Report, Product Certificate and Security Target are posted to the Certified Products List for the IT Security Evaluation and Certification Scheme published by NASK National Research Institute.

Recognition of the certificate

European Recognition of 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 up to EAL4. A higher recognition levels are provided for IT-Products related to certain SOGIS Technical Domains only.

The current list of signatory nations and approved certification schemes can be found on https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations. This certificate is recognized under SOGIS-MRA up to EAL4.

International Recognition of CC Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the Common Criteria (Common Criteria Recognition Arrangement, CCRA-2014) became effective in September 2014. It covers Common Criteria certificates based on: collaborative Protection Profiles, assurance components up to EAL2 augmented by ALC_FLR and certificates for PP and cPP.

The current list of signatory nations and of collaborative Protection Profiles can be found on https://www.commoncriteriaportal.org .

The CCRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition. This certificate is recognized under CCRA-2014 up to EAL2 augmented by ALC_FLR.

Executive Summary

This document constitutes the Certification Report for the certification file of the product: **DTMS-2**

TOE Version:	2.0
Developer:	CB ELECTRONICS Sp. z o.o.
Sponsor:	CB ELECTRONICS Sp. z o.o.
Security Target:	Security Target for **DTMS-2**, version 1.6, date of issue 2025-06-12
Protection Profile:	Security Target claims strict conformance to the following Protection Profile: • Digital Tachograph – Motion Sensor [BSI-CC-PP-0093], Version 1.0, 9 May 2017 – compliant with Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 (Annex 1C).

Laboratory/ITSEF: Information Technology Security Evaluation Facility of National Institute of Telecommunications - ITSEF NIT

Evaluation Level: Common Criteria version 3.1 release 5, Evaluation Assurance Level EAL 4+ ATE_DPT.2 and AVA_VAN.5

Evaluation end date: June 2025 (Final ETR ver.1.1, issue date 12.06.2025)

Expiration Date: 30.06.2030

Documentation available for users

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

[EXT-1360] [EVD-ST-V1.6]	**Security Target DTMS-2, v. 1.6, issue date 12.06.2025** **(confidential document – LITE version available)**
[EXT-1312] [EVD-AGD_PRE_v1.6]	**AGD_PRE EAL4+ for Digital Motion Sensor 2 (DTMS-2), Version 1.6, issue date 07.04.2025 (confidential document)**
[EXT-1311] [EVD-AGD_OPE_v1.6]	**AGD_OPE EAL4+ for DTMS-2 Digital Motion Sensor (DTMS-2), Version 1.6, issue date 07.04.2025 (confidential document)**

Security Target

Along with this certification report, the complete Security Target of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

DTMS-2 SECURITY TARGET version 1.6, issue date 2025-06-12

The public version of this document is published along with this certification report on the Certification Body website.

3. TOE Summary

TOE Overview

The TOE is a second generation tachograph motion sensor compliant with Protection Profile [BSI-CC-PP-0093[6]] in the sense of [7] Annex 1C, intended to be used in the digital tachograph system. The Digital Tachograph system additionally contains a VU, tachograph cards, an external GNSS module (if applicable) and remote early detection communication readers. The motion sensor is mounted directly into the gearbox and collects the motion data that accurately reflects the vehicle's speed and distance travelled. In the operational phase the motion sensor is connected to a VU and this data is captured from the rotating wheels inside the gearbox via a sensor and transmitted in an encrypted form and plain analog form to the authenticated VU of the Digital Tachograph system.

A motion sensor can be paired and used with second generation VU's and with first generation VU's as well [BSI-CCPP-0093[6]]. The functional requirements for a Motion Sensor are specified in [7] Annex 1C, Chapter 3.2, and the common security mechanisms are specified in Appendix 11. Aspects of the electrical interface between the motion sensor and VU are described in ISO 16844-3 [8]. In case of failure in self-tests or during pairing and normal operation, the TOE generates and stores the audit record, to be read by the VU o its request. The accuracy of motion data is checked by functional tests during the development and after its production. The reliability of the TOE service is provided by sending motion data to the VU via 2 independent channels –analogue line (the electric pulses) and data line (number of pulses sent on analogue line-encrypted), which are compared by the VU. In case of difference the audit record is generated by VU, hence the motion data manipulation is detected. The simplified block scheme of typical motion sensor is described in the Figure 1.

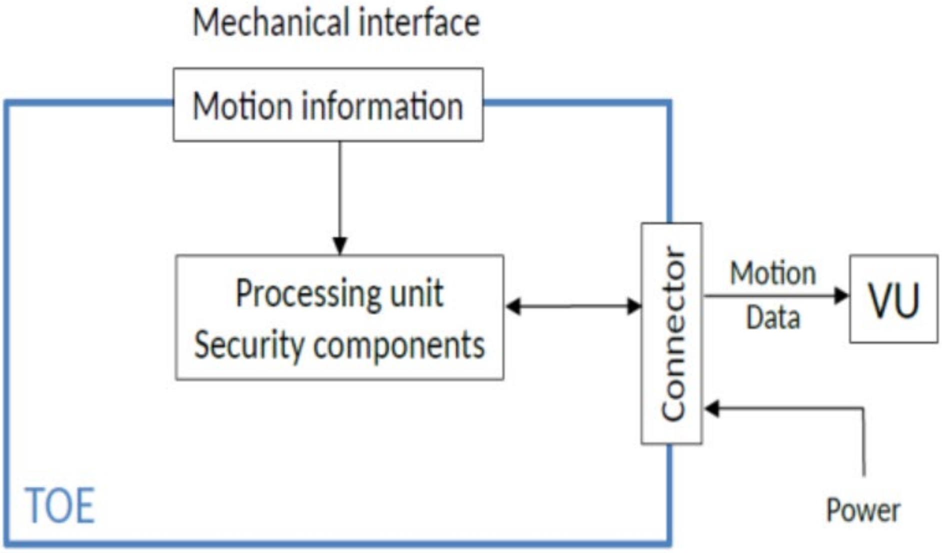


Figure 1: Motion sensor

The TOE physically consists of the following elements (see figure 2):

- a Hall Motion Sensor (HMS) that converts magnetic field changes of the rotating element of the gear into electrical pulses that allow the VU to derive speed and distance,
- a microcontroller processes the electrical pulses from the sensor in real-time and transmits the real time speed analog pulses to the VU and encrypted and authenticated motion data only to the authenticated VU,
- a Security Module (EAL 6+ certified [9]) stores key material and encrypts/decrypts data transmitted to and from the VU,
- elements such as voltage regulator and buffers are required such that the TOE can fulfill its function according to [8]).

A schematic overview of the TOE is shown in Figure 2. The connector (1) connects the motion sensor with the cable to the VU. It also contains the interface to the VU (data interface) and the power supply. The crimping (2) links the connector with the body (3). Inside the body the Printed Circuit Board PCB (4) performs the logical security functions of the TOE (described below). It is connected with the Hall Motion Sensor (HMS) for motion detection (speed signal interface, 5).

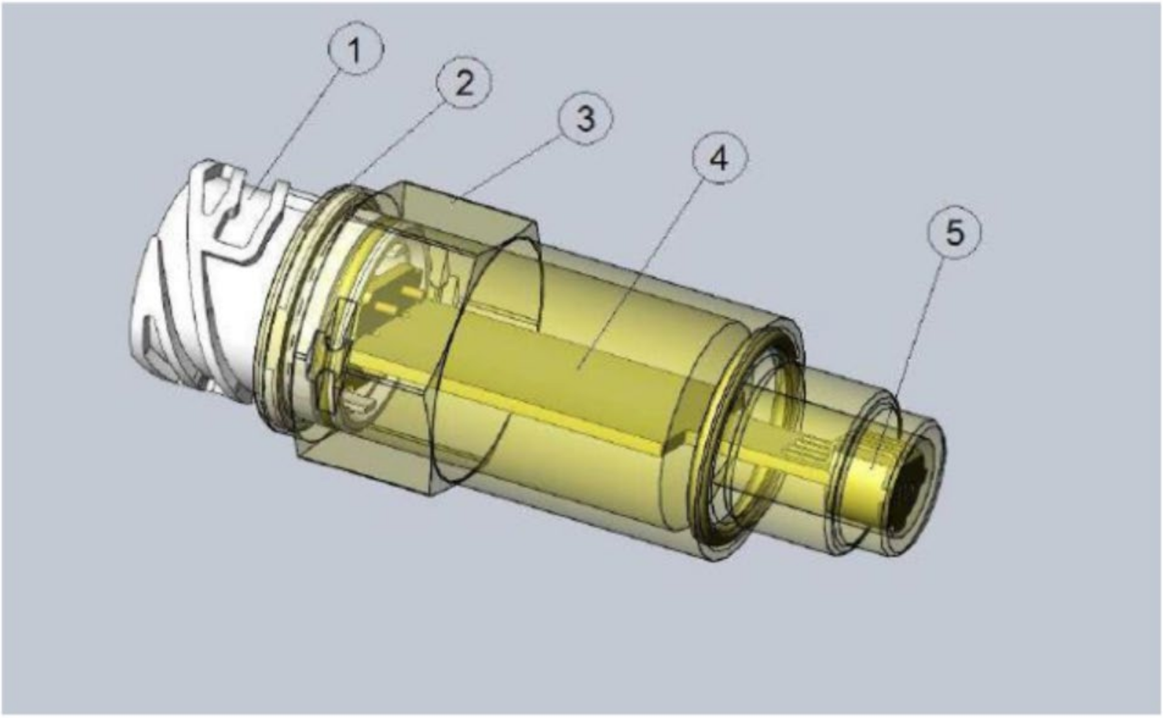


Figure 2: Schematic TOE overview (proximity type)

Figure 2 shows a motion sensor proximity type DTMS-2 distinguishes models with different lengths, see Table 1 for details of the identification system) which has an aluminium body and a socket (connector) for the cable (see Figure 3, right). The motion sensor rotary type DTMS-2 is equipped with a rotating element inside the body (see Figure 3, left).

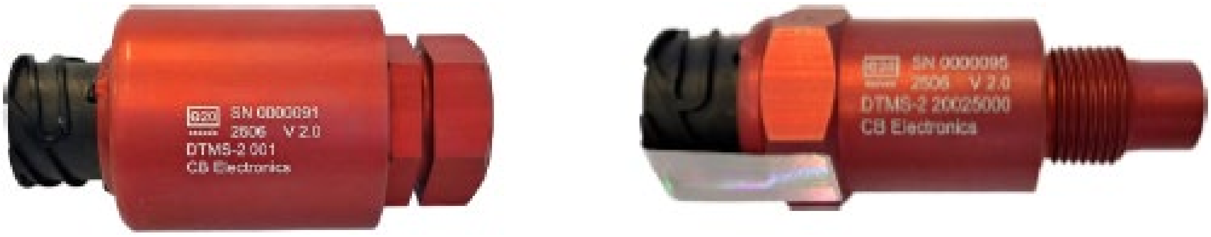


Figure 3. From left to right: DTMS-2 – Rotary, DTMS-2 – Proximity

Security Assurance Requirements

The product was evaluated with all the evidence required to fulfil the evaluation level EAL 4+ ATE_DPT.2 and AVA_VAN.5, according to Common Criteria v3.1 Revision 5.

Assurance Class	Assurance Component
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
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.2 Analysis of coverage
	ATE_DPT.2 Testing: security enforcing modules
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample

Assurance Class	Assurance Component
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

Security Functional Requirements

Functional requirement	Description
FAU: Security audit	FAU_GEN.1 Audit data generation
	FAU_STG.1 Protected audit trail storage
	FAU_STG.4 Prevention of audit data loss
FCS: Cryptographic support	FCS_COP.1 Cryptographic operation
	FCS_CKM.4 Cryptographic key destruction
FDP: User Data Protection	FDP_ACC.1 Subset access control
	FDP_ACF.1 Security attribute based access control
	FDP_ETC.1 Export of user data without security attributes
	FDP_ETC.2 Export of user data with security attributes
	FDP_ITC.1 Import of user data without security attributes
	FDP_SDI.2 Stored data integrity monitoring and action
FIA: Identification and authentication	FIA_AFL.1 Authentication failure handling
	FIA_ATD.1 User attribute definition
	FIA_UAU.2 - User authentication before any action
	FIA_UAU.3 Unforgeable authentication
	FIA_UID.2 User identification before any action
FPT: Protection of the TSF	FPT_FLS.1 Failure with preservation of secure state
	FPT_PHP.2 Notification of physical attack
	FPT_PHP.3 Resistance to physical attack
	FPT_TST.1 TSF testing
	FPT_TDC.1 Inter-TSF basic TSF data consistency
FRU: Resource utilization	FRU_PRS.1 Limited priority of service
FTP: Trusted path/channels	FTP_ITC.1 Inter-TSF trusted channel

Security Policy

TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

OSP.CRYPTO: The cryptographic algorithms and keys described in [7] Annex 1C, Appendix 11 shall be used where data confidentiality, integrity and authenticity need to be protected.

4. Assumptions and Clarification of Scope

Environmental Assumptions

The 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 to determine if the identified vulnerabilities can be exploited.

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 Security Target [EVD-ST-V1.6] makes 3 assumptions on the environment of the TOE:

A.Approved_Workshops: It is assumed that the Authority States (Member State) approve, regularly control and certify trusted fitters and workshops to carry out installations, checks, inspections and repairs.

A.Controls: It is assumed that the law enforcement controls of the TOE will be performed regularly and randomly and must include security audits (as well as visual inspection of the TOE).

A. Type Approved: It is assumed that the motion sensor will only be operated together with a VU being type approved according to [7] Annex 1C[1].

Clarification of Scope

Threats

The Security Target [EVD-ST-V1.6] defines threats which have been taken into consideration during the evaluation process.

T.Access: Access control – a VU or other device (under control of an attacker) could try to use functions not allowed to them, and thereby compromise the integrity or authenticity of motion data (MOD).

T.Design: Design knowledge - an Attacker could try to gain illicit knowledge of the motion sensor design (TOE design and software code (TDS)), either from manufacturer's material (e.g. through theft or bribery) or from reverse engineering, and thereby more easily mount an attack to compromise the integrity or authenticity of Motion data (MOD).

[1] Type approval requirements include Common Criteria certification against the relevant digital tachograph protection profile

T.Environment: Environmental attacks – an attacker could compromise the integrity or authenticity of motion data (MOD) through physical attacks on the motion sensor (thermal, electromagnetic, optical, chemical, mechanical).

T.Hardware: Modification of hardware -An attacker could modify the motion sensor hardware (THW), and thereby compromise the integrity or authenticity of motion data (MOD).

T.Mechanical: Interference with mechanical interface –an attacker could manipulate the motion sensor input, for example, by disconnecting the sensor from the gearbox, such that motion data (MOD) does not accurately reflect the vehicle’s motion.

T.Motion_Data: Interference with motion data - an attacker could add to, modify, delete or replay the vehicle’s motion data, and thereby compromise the integrity or authenticity of motion data (MOD).

T.Security_Data: Access to security data - an attacker could gain illicit knowledge of secret cryptographic keys (SDK) during security data generation or transport or storage in the equipment, thereby allowing an Other Device to be connected.

T.Software: Attack on software -an attacker could modify motion sensor software (TDS) during operation, and thereby compromise the integrity, availability or authenticity of motion data (MOD).

T.Test: An attacker use of non-invalidated test modes or of existing back doors could permit manipulation of motion data (MOD).

T.Power_Supply: Invalid test modes -an attacker could vary the power supply to the motion sensor, and thereby compromise the integrity or availability of motion data (MOD).

Security Policy

TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

OSP.CRYPTO: The cryptographic algorithms and keys described in [7] Annex 1C, Appendix 11 shall be used where data confidentiality, integrity and authenticity need to be protected.

5. Architectural Information

Physical scope

The physical scope of the TOE is presented on Figure 2. Physically TOE consists of:

- the connector (connecting the motion sensor with the cable to the VU and contains the data interface to the VU and the power supply);
- the crimping (linking the connector with the body);
- the body containing the Printed Circuit Board PCB with microcontroller;
- the Hall sensor (HMS) for motion detection (speed signal interface),

The physical boundary of the TOE is defined by the MS casing, the mechanical interface with the gearbox and the 4-pin connector [ISO 15170-1[10]].

Only the data signal in/out (pin 4) has integrity authenticity and confidentiality protection by the use of cryptographic support. The real-time analogue signal (pin 3) has not.

The different models of the motion sensor only differ by their length (to be able to fit in different kinds of vehicles) and the nature of operation (see Table 1 below).

The identification system for appropriate variants of motion sensors is as follows:

1. First digit indicates the motion sensor type: (0-Rotary; 2 - Proximity; 3-Sprinter).

2. Depending on the type of motion sensor:

    a. Applicable for the Rotary or Proximity types of motion sensors:

        i. Second digit indicates the connector type,

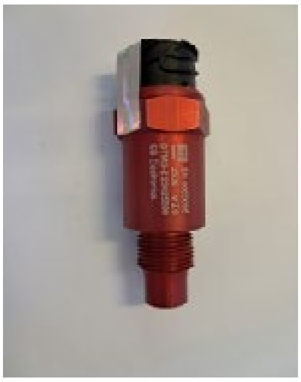
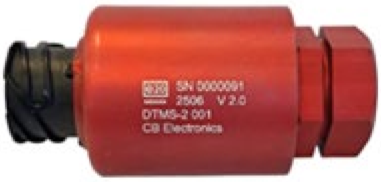
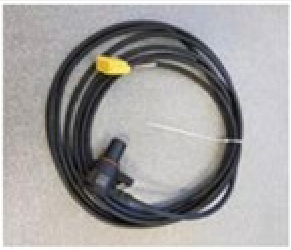
        ii. Third digit indicates the thread type,

    b. Applicable for the Sprinter type of motion sensor:

        i. All consecutive digits express the cable length in millimetres,

    c. Applicable for the proximity type of motion sensors:

        i. Next digits represent the motion sensor length expressed in tenth of millimetres.

No.	Description	Variant	Length	Images
1.	Digital Motion Sensor MS TYPE Proximity Standard ISO 15170 connector M 18x1,5	DTMS-2 200180	18,0 mm	
		DTMS-2 200186	18,6 mm	
		DTMS-2 200198	19,8 mm	
		DTMS-2 200238	23,8 mm	
		DTMS-2 200250	25,0 mm	
		DTMS-2 200338	33,8 mm	
		DTMS-2 200350	35,0 mm	
		DTMS-2 200620	62,0 mm	
		DTMS-2 200632	63,2 mm	
		DTMS-2 200888	88,8 mm	
		DTMS-2 200900	90,0 mm	
		DTMS-2 2001138	113,8 mm	
		DTMS-2 2001150	115,0 mm	
		DTMS-2 2001368	136,8 mm	
2.	Digital Motion Sensor MS TYPE Rotary Standard ISO 15170 connector Internal thread M22x1,5 Right	DTMS-2 001	Not applicable	
3.	Digital Motion Sensor MS TYPE Sprinter Sensor with proximity detector and armored cable	DTMS-2 3224	Cable length 224 mm	
		DTMS-2 3230	Cable length 230 mm	
		DTMS-2 3410	Cable length 410 mm	

Delivery of the TOE

The TOE ready for pairing (software embedded in the hardware with user data and security data) is delivered to the thrusted Workshop by courier delivery. The TOE documentation (Installation Manual and Operational Guidance) is delivered by signed pdf file by e-mail.

No	Type	Description	Name of the archive/file
1.	signed pdf	Installation Manual	AGD_PRE EAL4+ for Digital Motion Sensor (DTMS-2), version 1.6, 07.04.2025
2.	signed pdf	Operational Guidance	AGD_OPE EAL4+ for DTMS-2, version 1.6, 07.04.2025.

Logical scope

The TOE measures the motion data that accurately reflects the vehicle's speed and distance travelled and passes this information along to the VU. The motion sensor provides two types of motion information to the vehicle unit it is connected to the real-time analog speed pulses (pin 3 [8]), and the digital motion data (pin 4 [8]). The following actions are performed. [7]

- Motion data detection and transmission to the VU,
- Pairing with a VU – mutual authentication and the exchange of a session key, KS,
- Sending data at VU request,
- Security audit data generation.

The TOE provides the security features described in 1.3.2 [ST Lite v1.0]. In the context of the TOE logical scope, these security features are as follows:

- Maintenance the integrity of motion data supplied to the VU,
- Demonstration of the TOE authenticity to the VU through an authenticated pairing process,
- Preserving audit data for security relevant events and send these to the VU,
- Detecting physical tampering,
- Providing the secure communication channel between itself and the VU.

6. IT security evaluation

The Evaluation Assurance Level EAL 4+ ATE_DPT.2 and AVA_VAN.5 requires the independent and penetration testing provided by Evaluator and vulnerability analysis for a High attack potential.

The Evaluator has performed an installation and configuration of the TOE and its environment according to the [EVD-ST-V1.5] documentation. Installation and configuration of the TOE for AVA activities are the same as configuration used to execute the independent tests and is consistent with the evaluated configuration according to Security Target.

The Evaluator has examined set of developer test cases and selected test cases for independent testing. The sample has been chosen to cover all relevant TOE functionalities which refer to the Signer. The Evaluator noted that Signer (or any subject claiming to be him) is the only external entity that interacts with the TOE from outside TOE operational environment, which is tightly secured in accordance with security objectives for operational environment specified in the Security Target [EVD-ST-V1.6].

Evaluated Configuration

The test environment consists of following components.

This section includes description of the test environment that has been prepared to repeat developer's tests and perform independent tests by the Evaluator.

The test environment consists of the following components:

a) Driving Unit TC-1/ZN, that simulates gearbox and allows to collect the motion data that reflect the vehicle's speed and distance travelled,

b) TOE rotary type, that is directly connected to the Driving Unit, or

TOE Proximity type connected to the Driving Unit through an adapter, or

TOE sprinter type, that is connected in the same way as TOE Proximity type.

c) MS – VU Interface 01, that converts the TOE's [ISO163844-3] compliant output to the USB standard accepted by the VU emulator software.

d) PC with VU simulator installed (msenstst32.exe, where v31 is the version being for TOE v1.5 tests, while the v35 version is for TOE v2.0 tests.).

e) Power Supply, that is used to power the TOE during tests.

f) An oscilloscope that measures voltage waveforms of the real-time analog speed signal on pulse cable. Moreover, the oscilloscope is also used to observe data flow on the digital line on which encrypted [ISO163844-3] messages are exchanged.

The test environment consists of following 3 test environment setups TS_01, TS_02 and TS_03.

The test setup TS_01 can be applied to any type of the TOE, because the functional tests do not depend on the motion detection mechanism. They can be done with any TOE type, as the behaviour and functionality do not differ because of the same implementation. A schematic design of the test setup TS_01 is shown in Figure 4.

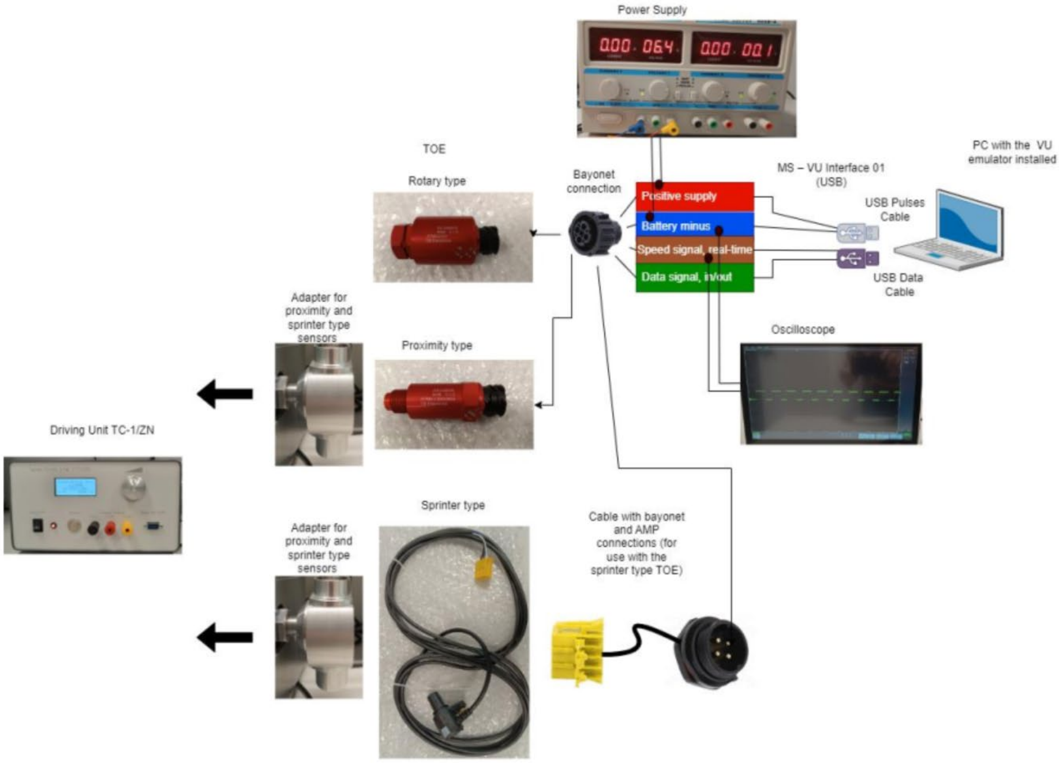

Power Supply
TOE
Rotary type
Bayonet connection
MS – VU Interface 01 (USB)
PC with the VU emulator installed
Positive supply
Battery minus
Speed signal, real-time
Data signal, in/out
USB Pulses Cable
USB Data Cable
Oscilloscope
Adapter for proximity and sprinter type sensors
Proximity type
Driving Unit TC-1/ZN
Sprinter type
Adapter for proximity and sprinter type sensors
Cable with bayonet and AMP connections (for use with the sprinter type TOE)

Figure 4: Test configuration TS_01

The test setup TS_02 can be applied if no oscilloscope is required for tests. A schematic design of the measurement setup TS_02 has been shown in Figure 5.

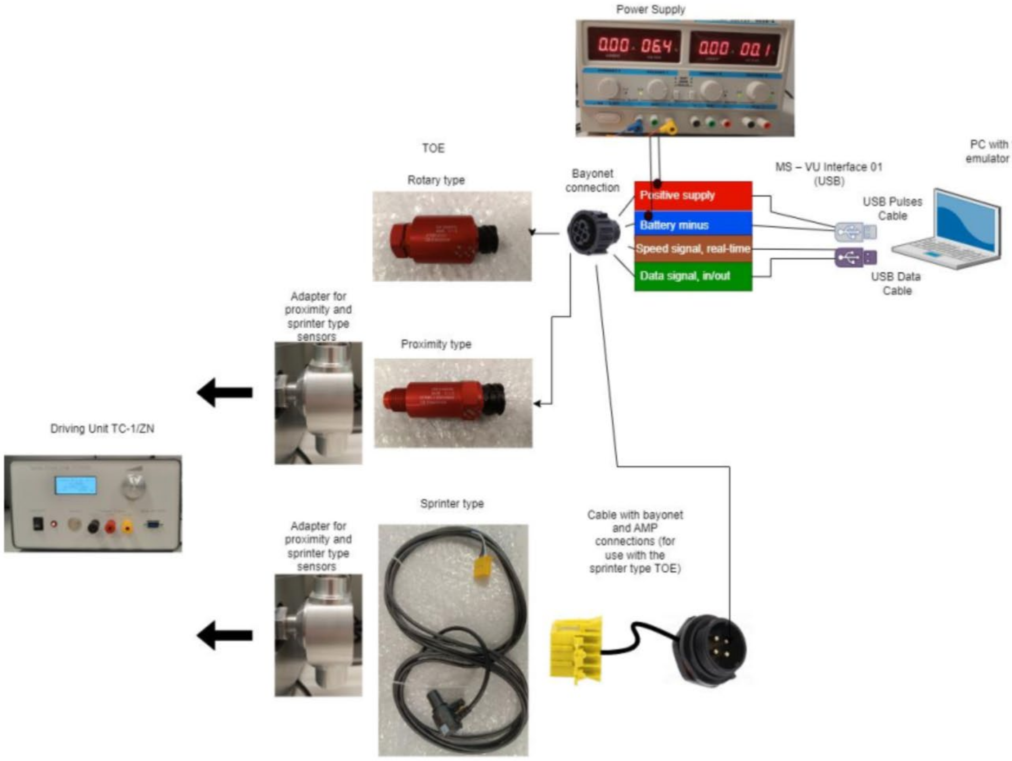

Power Supply
TOE
Rotary type
Bayonet connection
MS – VU Interface 01 (USB)
PC with the VU emulator installed
Positive supply
Battery minus
Speed signal, real-time
Data signal, in/out
USB Pulses Cable
USB Data Cable
Adapter for proximity and sprinter type sensors
Proximity type
Driving Unit TC-1/ZN
Sprinter type
Cable with bayonet and AMP connections (for use with the sprinter type TOE)
Adapter for proximity and sprinter type sensors

Figure 5: Test configuration TS_02

The test configuration TS_03 can be applied for test cases that verify error handling and key destruction procedures. A schematic design of the measurement setup TS_03 has been shown in Test configuration TS_03 (see Figure 6).

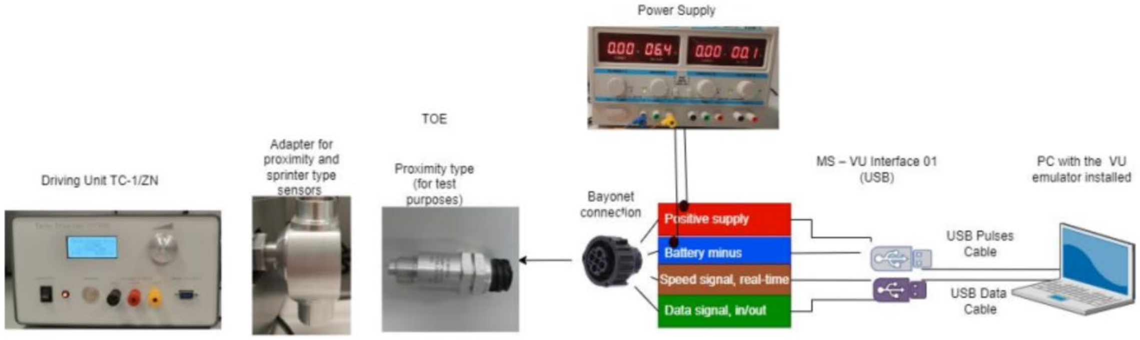


Figure 6: Test configuration TS_03

Table 1 list all test environment components identified by serial numbers.

No.	Test environment component	Serial number		Test configuration
1.	Power supply	20170820760		All test configurations
2.	Oscilloscope	C019641		TS_02
3.	Driving Unit TC-1/ZN	0201/22 (delivered by the Developer)		All test configurations
4.	Adapter	Delivered by the Developer (no serial number)		All test configurations, applied for proximity type motion sensor
5.	Cables	Data cable	Delivered by the Developer (no serial number)	All test configurations
6.		Analog pulses cable	Delivered by the Developer (no serial number)	TS_01
7.		Cable with bayonet and AMP connections (for sprinter type TOE)	Delivered by the Developer (no serial number)	All test configurations
8.	TOE	DTMS-2 Rotary type	See Table 2	TS_01, TS_02[1]
9.		DTMS-2 Proximity type	See Table 2	TS_01, TS_02
10.			See Table 2	TS_03
11.		DTMS-2 sprinter type		TS_01, TS_02
12.	PC with the VU emulator software installed	4JJC4J3		All test configurations

Functional testing

The Evaluation Assurance Level EAL 4+ ATE_DPT.2 and AVA_VAN.5 requires the Developer to deliver design information and test results, consistent with good commercial practise.

The Evaluator’s task is divided into two activities. The Evaluators shall confirm the Developer’s tests results using the sampling strategy described in details by the Common Criteria methodology. Additionally, the Evaluator’s task is to devise and perform their own subset of tests which are intended to be the supplementary for the tests prepared by the Developer.

Developer testing

The Developer’s testing verifies the functionality of their corresponding TSFI either directly or indirectly (using the interface to test other functionality). The correspondence between the test documentation and TSFIs described in the functional specification is accurate.

The Developer prepared 129 tests cases and conducted extensive testing campaign.

All the tests have obtained a PASS verdict.

Evaluator testing

The Evaluator has examined set of developer test cases and selected test cases for independent testing. The evaluators performed a total of 140 tests under ATE_IND, including 129 developer tests and 11 own tests.

The Evaluator considers the selected 129 developer tests as enough to confirm the validity of the developer's test results.

Additionally, the Evaluators independently devised and conducted 11 independent test cases.

The final verdict takes into account the results of the developer's tests that were repeated by the Evaluator and the results of the tests devised by the Evaluator. The final result of Evaluator testing is PASS as all the test cases are assigned a PASS verdict.

All the 140 test cases have obtained a PASS verdict.

Penetration testing

The Evaluation Assurance Level EAL 4+ ATE_DPT.2 and AVA_VAN.5 requires the independent and penetration testing provided by Evaluator and vulnerability analysis for a High attack potential.

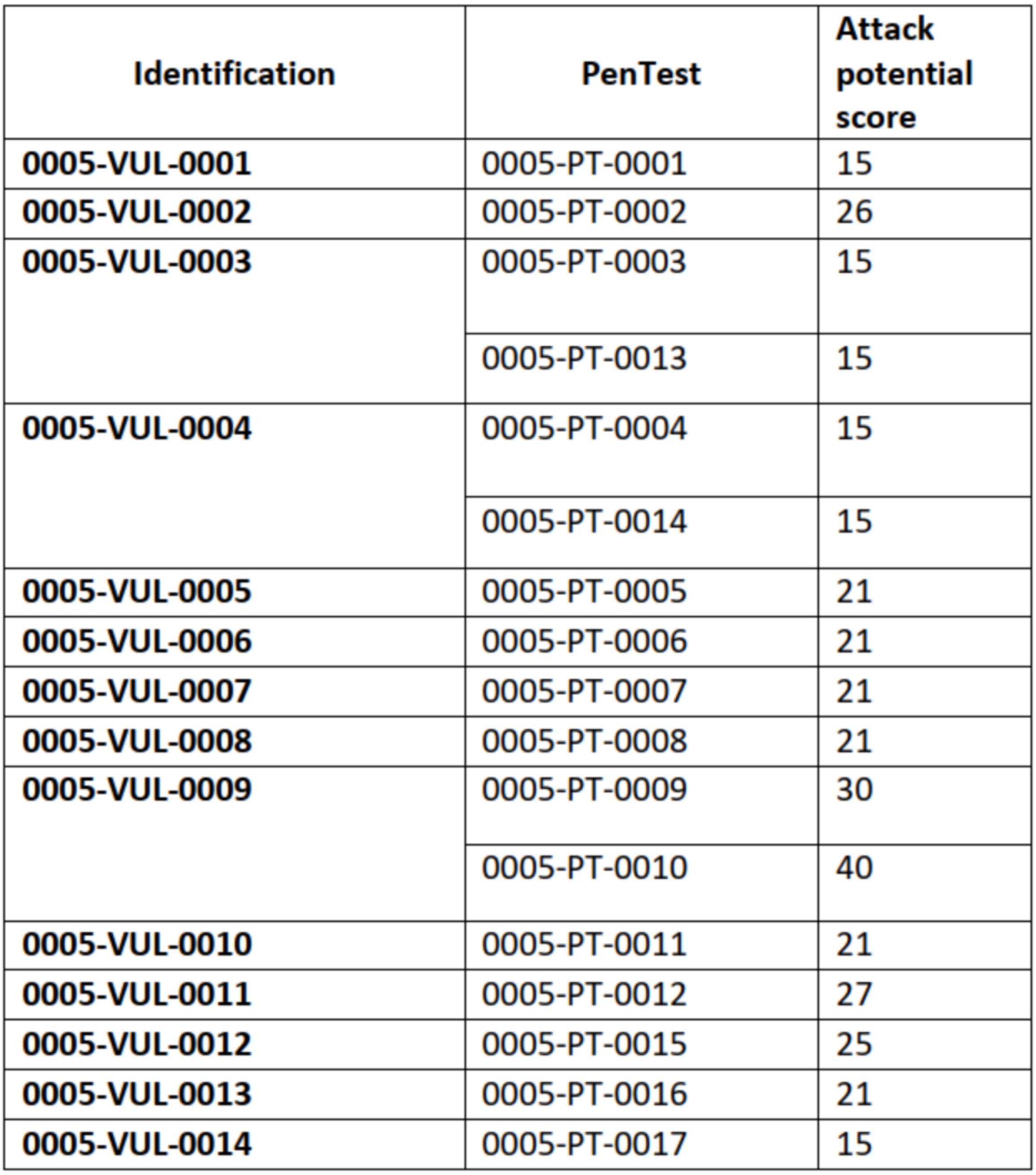
The attack potential used for this evaluation is consistent with EAL 4+ ATE_DPT.2 and AVA_VAN.5: High attack potential. The developed test plan was based on vulnerability survey of the evaluation evidence as well as the information available in the public domain was performed by the Evaluator covers development and operational vulnerabilities. TOE configuration used to execute the penetration test plan was consistent with the evaluated configuration according to the Security Target.

A vulnerability analysis has been completed, based on a structured examination of evidence to identify potential vulnerabilities. This was followed by a set of penetration tests to check whether these vulnerabilities could be exploited in the TOE operational environment.

14 potential vulnerabilities were identified, for which 17 penetration tests were carried out. All penetration tests resulted with FAIL verdict, which is the proof for the resilience of the product and fulfilment of the assumptions of the Security Problem Definition**.**

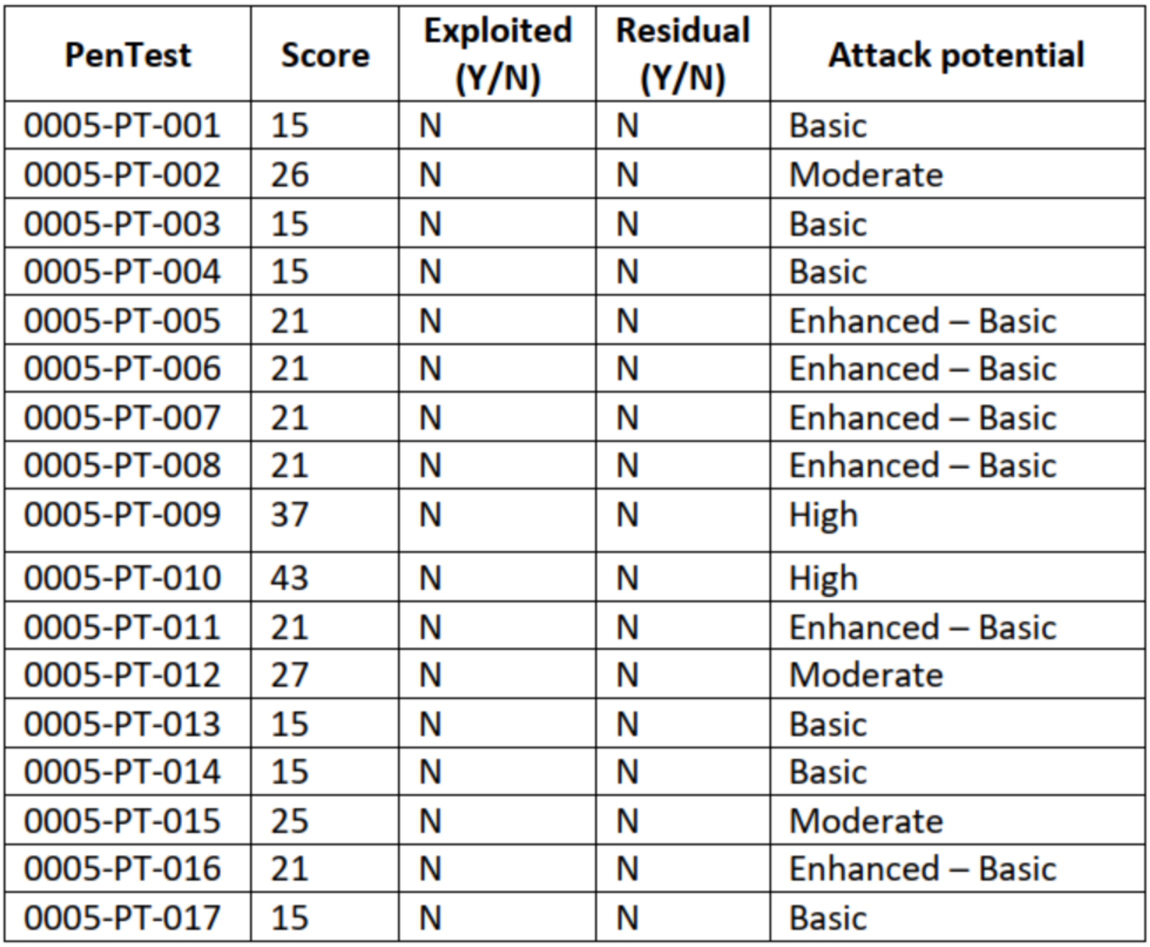
Vulnerabilities and penetration tests summary

The following table describes identified expected potential vulnerabilities which are subject to further processing according to the Vulnerability Analysis, v1.0 and the penetration tests developed to check if the vulnerabilities are exploitable with the required potential attack.



Identification	PenTest	Attack potential score
0005-VUL-0001	0005-PT-0001	15
0005-VUL-0002	0005-PT-0002	26
0005-VUL-0003	0005-PT-0003	15
	0005-PT-0013	15
0005-VUL-0004	0005-PT-0004	15
	0005-PT-0014	15
0005-VUL-0005	0005-PT-0005	21
0005-VUL-0006	0005-PT-0006	21
0005-VUL-0007	0005-PT-0007	21
0005-VUL-0008	0005-PT-0008	21
0005-VUL-0009	0005-PT-0009	30
	0005-PT-0010	40
0005-VUL-0010	0005-PT-0011	21
0005-VUL-0011	0005-PT-0012	27
0005-VUL-0012	0005-PT-0015	25
0005-VUL-0013	0005-PT-0016	21
0005-VUL-0014	0005-PT-0017	15

Table 2: Expected potential vulnerabilities according to the Vulnerability Analysis, v1.0



PenTest	Score	Exploited (Y/N)	Residual (Y/N)	Attack potential
0005-PT-001	15	N	N	Basic
0005-PT-002	26	N	N	Moderate
0005-PT-003	15	N	N	Basic
0005-PT-004	15	N	N	Basic
0005-PT-005	21	N	N	Enhanced – Basic
0005-PT-006	21	N	N	Enhanced – Basic
0005-PT-007	21	N	N	Enhanced – Basic
0005-PT-008	21	N	N	Enhanced – Basic
0005-PT-009	37	N	N	High
0005-PT-010	43	N	N	High
0005-PT-011	21	N	N	Enhanced – Basic
0005-PT-012	27	N	N	Moderate
0005-PT-013	15	N	N	Basic
0005-PT-014	15	N	N	Basic
0005-PT-015	25	N	N	Moderate
0005-PT-016	21	N	N	Enhanced – Basic
0005-PT-017	15	N	N	Basic

Table 3: List of penetration tests and assigned calculated actual attack potential

After providing all planned tests the Evaluator concluded that there were not exploitable vulnerabilities in the TOE operational environment according to the scope of this evaluation.

Evaluation results and conformity verdicts

The Evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation and concluded that the TOE meets the security objectives stated in the Security Target for an attack potential High.

The Certifier reviewed the work of the Evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

Based on the Validation Report (VRE-202) for Final ETR Certifier hereby states that TOE is conformant with the Common Criteria for Information Technology Security Evaluation (CC version 3.1 rev. 5) evaluation assurance level EAL4 augmented with ATE_DPT.2 and AVA_VAN.5.

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class	Assurance Component	Laboratory Verdict	Certification Body Validation
ADV: Development	ADV_ARC.1 Security architecture description	PASS	CONFORMANT
	ADV_FSP.4 Complete functional specification	PASS	CONFORMANT
	ADV_IMP.1 Implementation representation of the TSF	PASS	CONFORMANT
	ADV_TDS.3 Basic modular design	PASS	CONFORMANT
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	PASS	CONFORMANT
	AGD_PRE.1 Preparative procedures	PASS	CONFORMANT
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation	PASS	CONFORMANT
	ALC_CMS.4 Problem tracking CM coverage	PASS	CONFORMANT
	ALC_DEL.1 Delivery procedures	PASS	CONFORMANT
	ALC_DVS.1 Identification of security measures	PASS	CONFORMANT
	ALC_LCD.1 Developer defined life-cycle model	PASS	CONFORMANT
	ALC_TAT.1 Well-defined development tools	PASS	CONFORMANT
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims	PASS	CONFORMANT
	ASE_ECD.1 Extended components definition	PASS	CONFORMANT
	ASE_INT.1 ST introduction	PASS	CONFORMANT
	ASE_OBJ.2 Security objectives	PASS	CONFORMANT
	ASE_REQ.2 Derived security requirements	PASS	CONFORMANT
	ASE_SPD.1 Security problem definition	PASS	CONFORMANT
	ASE_TSS.1 TOE summary specification	PASS	CONFORMANT
ATE: Tests	ATE_COV.2 Analysis of coverage	PASS	CONFORMANT
	ATE_DPT.2 Testing: security enforcing modules	PASS	CONFORMANT
	ATE_FUN.1 Functional testing	PASS	CONFORMANT
	ATE_IND.2 Independent testing - sample	PASS	CONFORMANT
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis	PASS	CONFORMANT

Evaluator Comments/Recommendations

Recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and shall to be considered when using the product.

The following usage recommendations are given:

The evaluators note that the TOE shall be mounted by trusted and approved fitters or workshops (OE.Approved_Worskshops) as indicated in the developer delivered Preparative Procedure [PP1.6]. Moreover, approved fitter shall always adhere strictly to the instructions provided in the Preparative Procedure to ensure proper installation and compliance with regulations. Specifically, the fitters shall securely fasten the sensor to the designated gearbox mounting point, ensuring correct alignment to avoid possibility of interference caused by external magnetic field. Figure 10 of the Preparative Procedure [PP1.6] is particularly useful for correct assembly. The fitter shall verify that all connections are tight and free of debris to maintain reliable data transmission between TOE and VU.

Moreover, the evaluators note that the approved workshop shall follow strictly the sealing procedure ([EXT-1312] [EVD-AGD_PRE-V1.6]). The TOE shall be tightly sealed to prevent unauthorized modification of TOE mounting/installation. Thus, the fitter shall apply and tighten a certified tamper-resistant seal as specified in the Preparative Procedure ([EXT-1312] [EVD-AGD_PRE-V1.6]). Sealing should be carried out strictly in accordance with the instructions in this document.

Once installed in the approved workshop, the TOE should be regularly inspected (OE.Regular_Inspection). During inspections, the following should be ensured: correct mounting of the TOE (TOE properly mounted and tightly sealed to the gearbox), integrity of the TOE housing and TOE seal (OE.Mechanical).

7. Certifier Recommendations

All the assurance components required by the evaluation level EAL 4+ ATE_DPT.2 and AVA_VAN.5 of Common Criteria standard have been assigned a "PASS" verdict. Consequently, the laboratory assigned the "PASS" VERDICT to the whole evaluation due all the evaluation requirements are satisfied for the EAL 4+ ATE_DPT.2 and AVA_VAN.5, as defined by the Common Criteria v3.1 Revision 5 and the CEM v3.1 Revision 5.

Application Note: According to *SOG-IS Crypto Evaluation Scheme: Agreed Cryptographic Mechanisms* [5] encryption and decryption 3DES algorithm is legacy. The current expiration date of 3DES algorithm in [ACM] is 31.12.2024 for 112 bits key size and 31.12.2027 for 168 bits key size.

Considering the obtained and validated evidence during the certification process of the product **DTMS-2** evaluation, **a positive resolution is proposed**.

8. Acronyms

EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ITSEF	Information Technology Security Evaluation Facility
CB	Certification Body
TOE	Target Of Evaluation

9. Bibliography

The following standards and documents have been used for the evaluation of the product:

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

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

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

4. [CEM31] Common Criteria for Information Technology Security Evaluation. Evaluation Methodology, Version 3.1 Revision 5

5. [ACM] SOG-IS Crypto Evaluation Scheme: Agreed Cryptographic Mechanisms, Version 1.3, February 2023

6. Common Criteria Protection Profile, Digital Tachograph – Motion Sensor (MS PP), BSI-CC-PP-0093, Version 1.0, 9 May 2017, DG JRC – Directorate E – Space, Security and Migration Cyber and Digital Citizens’ Security Unit E3

7. Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components

8. ISO 16844-3:2004 Road vehicles – Tachograph systems – Part 3: Motion sensor interface

9. Certification Report JCOP 4.7 SE051, EAL 6 augmented with ASE_TSS.2 and ALC_FLR.1. TÜV Rheinland Nederland B.V. July 2020

10. ISO 15170-1:2001 Road vehicles — Four-pole electrical connectors with pins and twist lock — Part 1: Dimensions and classes of application

References

List of normative documents:

SOG-IS MRA Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, v3.0, 8.01.2010

CCRA Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 02.07.2014

ISO/IEC 15408 Information technology - Security techniques - Evaluation criteria for IT security

ISO/IEC 17025 General requirements for competence of calibration and testing laboratories

ISO/IEC 17065 Conformity assessment - Requirements for bodies certifying products, processes and services

ISO/IEC 18045 Information technology — Security techniques — Methodology for IT security evaluation

ISO/IEC 19790 Information Technology - Security Techniques - Security requirements for cryptographic modules

PC1 v. 2.7 IT Security Evaluation and Certification Scheme

List of related documents

[EXT-1363] [FIN-ETR-V1.1]	**Final Evaluation Technical Report, v1.1, issue date 16.06.2025 (ITSEF confidential document)**
[EXT-1360] [EVD-ST-V1.6]	**DTMS-2 Security Target, v. 1.6, issue date 12.06.2025 (confidential document)**
[EXT-1487] [EVD-ST-V1.0 LITE]	**Security Target for DTMS-2, version 1.0 Lite, issue date 10.09.2025**
[EXT-1312] [EVD-AGD_PRE-V1.6]	**AGD_PRE EAL4+ for Digital Motion Sensor (DTMS-2) v1.6, issue date 07.04.2025 (confidential document)**
[EXT-1311] [EVD-AGD_OPE_v1.6]	**AGD_OPE EAL4+ for Digital Motion Sensor (DTMS-2) v1.6, issue date 07.04.2025 (confidential document)**
[EXT-1307] [EVD-ADV_FSP_v1.2]	**ADV_FSP _v1.2, issue date 07.04.2025 (confidential document)**
[EXT-1306] [EVD-ADV_ARC_v1.1]	**ADV_ARC _v1.1, issue date 07.04.2025 (confidential document)**
[EXT-1308] [EVD-ADV_TDS_v1.2]	**ADV_TDS _v1.2, issue date 07.04.2025 (confidential document)**
[EXT-1349] [EVD-AVA_VAN-v1.0]	**Vulnerability Analysis, v1.0, issue date 12.05.2025 (confidential document)**
[EXT-1348] [EVD-PEN_TEST-v1.0]	**Penetration Tests Plan and Report, v1.0, issue date 12.05.2025 (confidential document)**
[EXT-1359] [EVD-ALC_CMS-V1.3]	**ALC_CMS (DTMS-2), v1.3, issue date 12.06.2025 (confidential document)**
[EXT-1333] [EVD-ALC_CMC-V1.6]	**ALC_CMC (DTMS-2), v1.6, issue date 07.04.2025 (confidential document)**
[EXT-1331] [EVD-ALC_DEL-V1.1]	**ALC_DEL (DTMS-2), v1.1, issue date 30.11.2024 (confidential document)**
[EXT-1340] [TPR-ATE_LAB-V1.0]	**Independent Test Plan and Report CB Electronics DTMS-2, v1.0, issue date 30.04.2025 (confidential document)**
[EXT-1342] [TP-ATE_DEV-V1.4]	**ATE EAL4+ for DigiTal Motion Sensor 2 (DTMS-2), v.1.4, issue date 07.04.2025 (confidential document)**
[EXT-1343] [TPR-ATE_DEV-V1.5]	**ATE01 DTMS-2-Tests cases & results, v.1.5, issue date 07.04.2025 (confidential document)**

Certification
NASK

NASK

PCA
POLSKIE CENTRUM AKREDYTACJI
CERTYFIKACJA WYROBÓW
AC 223

SOGIS
IT SECURITY CERTIFIED