Certification Report

EAL 4+ (ATE_DPT.2 and AVA_VAN.5) Evaluation of

PARS AR-GE ve BİLGİ TEKNOLOJİLERİ LTD. ŞTİ.

PARS Motion Sensor PMS-101 v0.2

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Certificate Number: 21.0.03/TSE-CCCS-50

C.Ç

TABLE OF CONTENTS

c.(

DOCUMENT INFORMATION

Date of Issue	February 15, 2018
Approval Date	February 15, 2018
Certification Report Number	21.0.03/18-003
Sponsor and Developer	Pars Ar-Ge ve Bilgi Teknolojileri Ltd. Şti.
Evaluation Facility	Beam Technology Test Center
TOE	Pars Motion Sensor PMS-101 v0.2
Pages	17

Prepared by	Cem ERDİVAN Common Criteria Inspection Expert
Reviewed by	Zümrüt MÜFTÜOĞLU Common Criteria Technical Responsible (Hardware Product Group)

This report has been prepared by the Certification Expert and reviewed by the Technical Responsible of which signatures are above.

DOCUMENT CHANGE LOG

Release	***Date***	***Pages Affected***	***Remarks/Change Reference***
1.0	February 15, 2018	All	First Release

DISCLAIMER

This certification report and the IT product in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1,revision 4, using Common Methodology for IT Products Evaluation, version 3.1, revision 4. This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

FOREWORD

The Certification Report is drawn up to submit the Certification Commission the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the ITCD Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

The Common Criteria Certification Scheme (CCSS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL = Common Criteria Testing Laboratory) under CCCS' supervision.

CCEF is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by Beam Technology Testing Facility, which is a commercial CCTL.

A Common Criteria Certificate given to a product means that such product meets the security requirements defined in its security target document that has been approved by the CCCS. The Security Target document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the IT product should also review the security target document in order to understand any assumptions made in the course of evaluations, the environment where the IT product will run, security requirements of the IT product and the level of assurance provided by the product.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for PARS Motion Sensor PMS-101 v0.2 whose evaluation was completed on February 13, 2018 and whose evaluation technical report was drawn up by Beam Technology (as CCTL), and with the Security Target document with version no 0.11T of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the ITCD Certified Products List at bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL2. The current list of signatory nations and approved certification schemes can be found on:

http://www.commoncriteriaportal.org.

1 - EXECUTIVE SUMMARY

1.1 TOE Overview

The Target of Evaluation (TOE) addressed by this certification report is a second generation Tachograph Motion Sensor in the sense of Annex 1C *(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)*, intended to be used in the digital tachograph system. The Digital Tachograph system additionally contains a vehicle unit, tachograph cards, an external GNSS module (if applicable) and remote early detection communication readers.

A motion sensor is installed within a road transport vehicle as part of a digital tachograph system. Its purpose is to provide a vehicle unit with motion data that accurately reflects the vehicle's speed and distance travelled.

The motion sensor is mechanically interfaced to a moving part of the vehicle, which movement is representative of the vehicle's speed and distance travelled. It may be located in the vehicle's gear box or in any other part of the vehicle. In the operational phase the motion sensor is connected to a vehicle unit. In its operational phase TOE will not connect any other device.

This motion sensor can be paired and used with second generation vehicle units, and with first generation vehicle units.

The functional requirements for a Motion Sensor are specified in 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 vehicle unit are described in ISO 16844-3.

In its operational mode, the motion sensor is connected to a VU. PMS-101 motion sensor is described in the following figure:

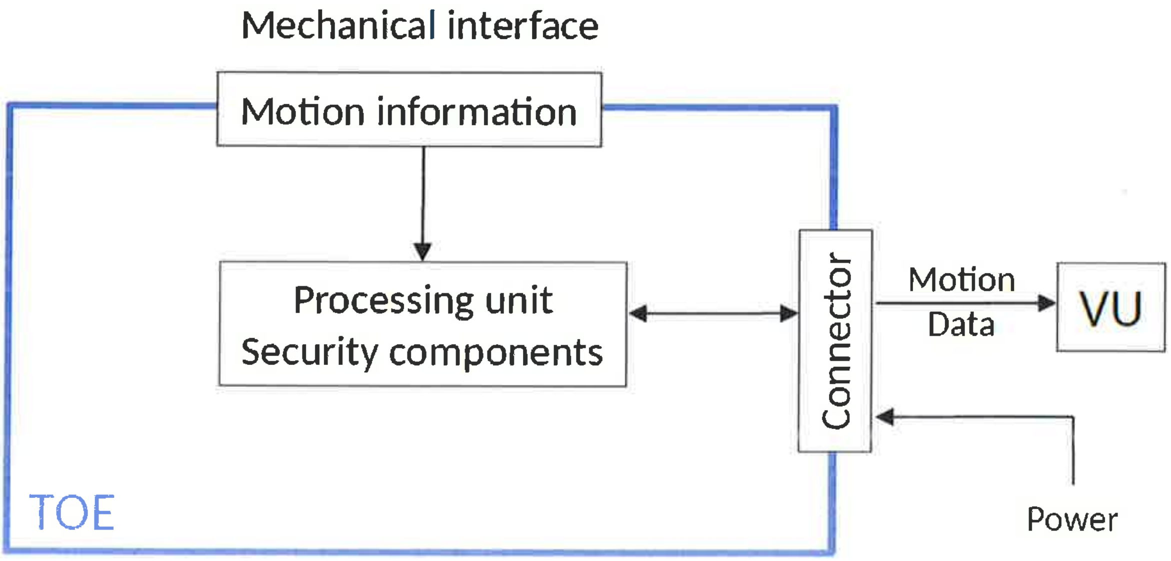

Figure 1 Typical motion sensor

Main objective of the digital tachograph system is given as "The data to be checked by control authorities must be available and reflect fully and accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed". Usage of the motion sensor provides data to the VU so as to allow the VU to determine fully and accurately the movement of the vehicle in terms of speed and distance travelled.

.

1.2 Threats

Threats	Definition
T.Access	Access control – A vehicle unit 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 (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).
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.Tests	Invalid test modes - The use by an attacker of non-invalidated test modes or of existing back doors could permit manipulation of motion data (MOD).
T.Power_Supply	Interference with power supply – An attacker could vary the power supply to the motion sensor, and thereby compromise the integrity or availability of motion data (MOD).

Table 1: Threats

C.Ç

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-50
TOE Name and Version	Pars Motion Sensor PMS-101 v0.2
Security Target Title	Pars Motion Sensor PMS-101 v0.2 Security Target
Security Target Version	V0.11T
Security Target Date	November 14, 2017
Assurance Level	EAL4+ (ATE_DPT.2 & AVA_VAN.5)
Criteria	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 4, September 2012
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
Protection Profile Conformance	• Common Criteria Protection Profile: Digital Tachograph – Motion Sensor (MS PP) v1.0 - BSI-CC-PP-0093
Common Criteria Conformance	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012, extended • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 4, September 2012, conformant
Sponsor and Developer	Pars Ar-Ge ve Bilgi Teknolojileri Ltd. Şti.
Evaluation Facility	Beam Technology Test Center
Certification Scheme	TSE CCCS

2.2 Security Policy

The motion sensor aims to protect data that is stored and transferred in such a way as to prevent unauthorized access to and manipulation of the data, and to detect and report any such attempts.

The main security features of the TOE are as follows:

- To maintain the integrity of motion data supplied to the vehicle unit;

- To demonstrate its authenticity to the vehicle unit through an authenticated pairing process;
- To detect physical tampering;
- To audit security relevant events and send these to the vehicle unit;
- To provide a secure communication channel between itself and the vehicle unit.

The main security features stated above are provided by the following major security services:

- Vehicle Unit identification and authentication;
- Access control to functions and stored data, according to *ISO 16844-3:2004 Road vehicles – Tachograph systems – Part 3: Motion sensor interface, 1 November 2004*;
- Alerting of events and faults;
- Integrity of stored data;
- Reliability of services, including self-testing, physical protection, control of executable code, resource management, and secure handling of events;
- Data exchange with a Vehicle Unit;
- Cryptographic support for VU to motion sensor mutual authentication and secure messaging according to Annex 1C, Appendix 11.

All cryptographic mechanisms for communications with first or second-generation vehicle units, including algorithms and the length of corresponding keys, have to be implemented exactly as required and defined in Annex 1C, Appendix 11, Parts A and B, respectively.

2.3 Assumptions and Clarification of Scope

Policy	Definition
P.Crypto	The cryptographic algorithms and keys described in Annex 1C, Appendix 11 shall be used where data confidentiality, integrity and authenticity need to be protected.

Table 2: Organizational Security Policies

Assumption	Definition
A.Approved_Workshops	Approved Workshops - The Member States approve, regularly control and certify trusted fitters and workshops to carry out installations, checks, inspections and repairs.
A.Controls	Controls - 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	Type Approved VU - The motion sensor will only be operated together with a vehicle unit being type approved according to Annex 1C.

Table 3: Assumptions

C.E

2.4 Architectural Information

2.4.1 Logical Scope

- **Identification and Authentication:** The motion sensor performs an initial authentication of the VU during the pairing process. Authentication is performed by proofing knowledge of a common secret (KM(Master key), KID (derived Master key – identification key)) between the motion sensor and the vehicle unit. During the pairing process a new secret (KS (session key)) common only to the vehicle unit and the motion sensor that performed the pairing is established.
- **Data Exchange:** The motion sensor communicates with the Vehicle Unit. During communication the motion sensor exports sensor data, motion sensor identification data, motion sensor initial security data to the Vehicle Unit and imports motion sensor pairing security data from the Vehicle Unit.
- **Cryptographic Support:** TOE uses Triple-DES (with 2 keys) encryption and decryption operations for first generation digital tachograph systems and AES (128 bit, 192 bit, 256 bit) encryption and decryption operations for second generation digital tachograph systems during data exchange with reading information (from file) instructions (10, 11) and reading sensor data instructions (70, 80).
- **Access Control:** Access controls ensure that access to the TOE functions can be performed only by those authorised to do so. There is only one authorised entity (VU) of the motion sensor at a given time. Access control is performed on the basis of the commands that the vehicle unit is allowed to submit to the motion sensor. As an example;
  - If Vehicle unit is authorised; Motion sensor gives response to Instruction No.41
  - If Vehicle unit is authorised; Motion sensor gives response to Instruction No.11
  - If Vehicle unit is authorised; Motion sensor gives response to Instruction No.80
- **Integrity Protection:** The sensor and the processing unit (uC) of the motion sensor are installed in a box designed so that it cannot be opened and the TOE is a sealed device. So integrity protection of the stored data is provided by design. Beyond that property active stored data integrity checks are performed by data hashing within the TOE for the integrity of stored data in the internal memory.
- **Audit:** The motion sensor generates audit records of the following events and transmits them to the Vehicle Unit:
  - security breach attempts (authentication failure, Stored data integrity error),
  - sensor fault.

  The VU time stamps the audit events which come from the Motion sensor. So motion sensor security functionality does not need to provide a reliable time stamp.
- **Reliability:** The physical construction of the motion sensor is of a way that opening the motion sensor box isn't possible without destroying it. This way a manipulation gets obvious. Furthermore the motion sensor is sealed at the gearbox. The motion sensor contains a power supply unit that controls the voltage and smoothness of the power input. The TOE is designed in a way that each power cut-off or variation results in a reset which provides a secure state in each instance. TOE also provides a sensing element which is immune to magnetic fields. Self testing of the TOE is performed for the accuracy of the integrity of stored data.

2.4.2 Physical Scope

TOE physically consists of the following hardware, software and documentation components;

- **Hardware components:**

C.C

- Sensor (takes motion information from gearbox and sends it to the comparator or directly to the motion sensor connector)
- Comparator (adjusts electrical motion information level for uC)
- Microcontroller (uC) (do/manage motion sensor functionality according to regulations
- K-Line converter (convert serial communication to K-Line communication and vice versa)
- Regulator (regulates voltage received from Vehicle Unit)

- **Software components**
  - Motion sensor software (Runs on the uC)
  - User data (In uC's memory)
  - TSF data (In uC's memory)

- **Documentation**
  - Preparative procedures
  - Operational user guidance

Physically TOE has hardware and software components. Hardware component version is v0.1 and software component version is v0.2.

2.4.3 Hardware/Software environment of TOE

The TOE is the Motion Sensor. It is an independent product, and does not need any additional hardware/software/firmware to ensure the security of the TOE.

In order to be able to supply motion data, the TOE must be paired with a vehicle unit, and must be installed in a motor vehicle.

2.5 Documentation

These documents listed below are provided to customer by the developer alongside the TOE:

Document Name	Version	Release Date
PMS-101 Security Target	v0.11T	November 14, 2018
PARS Motion Sensor Operational User Guidance Document	v0.3T	December 6, 2017
PARS Motion Sensor Preparative Procedures Document	v0.3T	December 6, 2017

2.6 IT Product Testing

- **Developer Testing:** All SFR-Enforcing TSFIs have been tested by developer. Developer has conducted 33 functional tests in total.
- **Evaluator Testing:** Evaluator has chosen all 33 developer tests to conduct by itself. Additionally, evaluator has prepared 16 independent tests. TOE has passed all 49 functional tests to demonstrate that its security functions work as it is defined in the ST.

c.c

- **Penetration Tests:** TOE has been tested against common threats and other threats surfaced by vulnerability analysis. As a result, these penetration tests have been conducted:
  1. Simple Power Analysis
  2. Modifying Audit Data (Encrypted using T-DES) During Its Transfer to Vehicle Unit
  3. Modifying Audit Data (Encrypted using AES) During Its Transfer to Vehicle Unit
  4. Encrypted Data Monitoring When Operational Mode
  5. Encrypted Data Monitoring When Pairing
  6. Brute Force Attack (Via Demonstrating Correct Implementation of Cryptographic Algorithms)
  7. Magnetic Field Test for Motion Sensor
  8. Bypass Tests (For Authentication and Order of Instructions)
  9. Stored Data Integrity Error Generating Test
  10. Physical Tamper Test on Epoxy Case of TOE

2.7 Evaluated Configuration

PMS-101 v0.2 is a motion sensor which is ready to be paired with a compatible digital tachograph-vehicle unit. Thus, during evaluation; TOE is coupled with a modified vehicle unit in order to better understand the test results. This modified vehicle unit is functionally identical to any other vehicle unit but printed results have been made more human-readable.

2.8 Results of the Evaluation

The verdict for the CC Part 3 assurance components (according to EAL4+ (ATE_DPT.2 and AVA_VAN.5) and the security target evaluation) is summarized in the following table:

Class Heading	**Class Family**	**Description**	**Result**
ADV: Development	ADV_ARC.1	Security architecture description	PASS
	ADV_FSP.4	Complete functional specification	PASS
	ADV_IMP.1	Implementation representation of the TSF	PASS
	ADV_TDS.3	Basic modular design	PASS
AGD: Guidance Documents	AGD_OPE.1	Operational user guidance	PASS
	AGD_PRE.1	Preparative procedures	PASS
ALC: Lifecycle Support	ALC_CMC.4	Production support, acceptance procedures and automation	PASS
	ALC_CMS.4	Problem tracking CM coverage	PASS
	ALC_DEL.1	Delivery procedures	PASS
	ALC_DVS.1	Identification of security measures	PASS
	ALC_LCD.1	Developer defined life-cycle model	PASS
	ALC_TAT.1	Well-defined development tools	PASS
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims	PASS
	ASE_ECD.1	Extended components definition	PASS
	ASE_INT.1	ST introduction	PASS
	ASE_OBJ.2	Security objectives	PASS
	ASE_REQ.2	Derived security requirements	PASS
	ASE_SPD.1	Security problem definition	PASS
	ASE_TSS.1	TOE summary specification	PASS

Class Heading	Class Family	Description	Result
ATE: Tests	ATE_COV.2	Analysis of coverage	PASS
	ATE_DPT.2	Testing: security enforcing modules	PASS
	ATE_FUN.1	Functional testing	PASS
	ATE_IND.2	Independent testing - sample	PASS
AVA: Vulnerability Analysis	AVA_VAN.5	Advanced methodical vulnerability analysis	PASS

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of “Pars Motion Sensor PMS-101 v0.2” product, result of the evaluation, or the ETR.

3 SECURITY TARGET

The security target associated with this Certification Report is identified by the following terminology:
Title: Pars Motion Sensor PMS-101 v0.2 Security Target
Version: v0.11T
Date of Document: November 14, 2017

This Security Target describes the TOE, intended IT environment, security objectives, security requirements (for the TOE and IT environment), TOE security functions and all necessary rationale.

C.E

4 ACRONYMS

AES	Advanced Encryption Standard
CA	Certification Authority
CBC	Cipher Block Chaining (an operation mode of a block cipher)
CC	Common Criteria
DES	Data Encryption Standard (see FIPS PUB 46-3)
EAL	Evaluation Assurance Level (a pre-defined package in CC)
EGF	External GNSS Facility
GNSS	Global Navigation Satellite System
MAC	Message Authentication Code
MS	Motion Sensor
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TC	Tachograph Card
TDES	Triple-DES
TOBB	Türkiye Odalar ve Borsalar Birliği
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
VU	Vehicle Unit

5 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012

[3] BTBD-03-01-TL-01 Certification Report Preparation Instructions, Rel. Date: February 8, 2016

[4] ETR v4.2 of PMS-101 v0.2, Rel. Date: February 13,2018

[5] PMS-101 v0.2 Security Target, Version v0.11T, Rel. Date: November 14, 2017