CERTIFICATION REPORT

Certification file:	**TUVIT-TSZ-9262-2016**
Product / system:	motion sensor for a digital tachograph BogArt Motion Sensor, Version 01
Product manufacturer:	BogArt Sp. z.o.o. Nowa Wieś Mała 40 11-040 Dobre Miasto, Poland
Customer:	see above
Evaluation body:	TÜV Informationstechnik GmbH TÜV NORD GROUP Evaluation Body for IT security Langemarckstraße 20 45141 Essen, Germany
Evaluation report:	*Version 3 as of 2016-06-24* project-number: *8111395598* authors: Ludger Knobel, Ulrich Heitkötter
Result:	EAL4+ augmented by ATE_DPT.2
Evaluation stipulations:	none
Certifier:	Dr. Silke Keller
Certification stipulations:	none
Date:	2016-06-29

……..……..……..……	……..……..……
Dr. Christoph Sutter	Dr. Silke Keller
Head of Certification Body	Certifier

Contents

Part A

Certificate and Background of the Certification

Part A presents a copy of the issued certificate and summarizes

- information about the certification body,
- the certification procedure, and
- the performance of evaluation and certification.

1 The Certificate

Certificate

The certification body of TÜV Informationstechnik GmbH hereby awards this certificate to the company

BogArt Sp. z.o.o.
Nowa Wieś Mała 40
11-040 Dobre Miasto, Poland

to confirm that its motion sensor for a digital tachograph

BogArt Motion Sensor, Version 01

has been evaluated at an accredited and licensed/approved evaluation facility according to the Common Criteria (CC), Version 3.1 Rev. 4 using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 and fulfils the requirements of

Common Criteria, Version 3.1 R4
EAL 4 augmented.

The appendix to the certificate is part of the certificate and consists of 3 pages.

The certificate is valid only in conjunction with the complete certification report for the evaluated configurations and intended operating environment.

CC V3.1 R4 TÜViT 2016 Trusted Product
Certificate ID: 9262.16

Certificate valid until 2021-06-30

Essen, 2016-06-29
Dr. Christoph Sutter
Head of Certification Body

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Langemarckstr. 20
45141 Essen, Germany
www.tuvit.de

DAkkS Deutsche Akkreditierungsstelle D-ZE-12022-01-00

2 Certification Body – CERTÜViT

The Certification Body of *TÜV Informationstechnik GmbH*[1] – TÜV NORD GROUP – was established in 1998 and offers a variety of services in the context of security evaluation and validation.

TÜViT is accredited for certification of IT security products according to ITSEC and Common Criteria by *Deutsche Akkreditierungsstelle GmbH under* registration no. D-ZE-12022-01-00 and performs its projects under a quality management system certified against ISO 9001.

3 Specifications of the Certification Procedure

The certification body conducts the certification procedure according to the criteria laid down in the following:

- DIN EN ISO/IEC 17065
- TÜViT Certification Scheme
- TÜViT Certification Conditions
- Common Criteria for Information Technology Security Evaluation (CC) part 1-3, version 3.1 revision 4, September 2012.
- Common Methodology for Information Technology Security Evaluation (CEM), version 3.1 revision 4, September 2012.
- Application Notes and Interpretations of the Scheme (AIS), published by BSI.

4 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The motion sensor for a digital tachograph BogArt Motion Sensor, Version 01 has undergone the certification procedure at TÜViT certification body.

The evaluation of the motion sensor for a digital tachograph BogArt Motion Sensor, Version 01 was conducted by the evaluation body for IT-security of TÜViT and concluded on June 24, 2016. The TÜViT evaluation body is recognised by BSI.

Sponsor as well as the developer is BogArt Sp. z.o.o. Distributor of the product is BogArt Sp. z.o.o..

[1] in the following termed shortly TÜViT

The certification was concluded with

- the comparability check and
- the preparation of this certification report.

This work was concluded on June 29, 2016. The confirmation of the evaluation assurance level (EAL) only applies on the condition that:

- all stipulations regarding generation, configuration and operation, as given in part B of this report, are observed,
- the product is operated – where indicated – in the environment described.

This certification report applies only to the version of the product indicated here. The validity of the certificate can be extended to cover new versions and releases of the product, provided the applicant applies for re-certification of the modified product, in accordance with the procedural requirements, and provided the evaluation does not reveal any security deficiencies.

This certificate is not an endorsement of the IT product by the TÜV Informationstechnik GmbH or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Informationstechnik GmbH or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

In order to avoid an indefinite usage of the certificate when evolved attack methods require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 29 June 2016 is valid until 30 June 2021. The validity date can be extended by re-assessment or re-certification.

With regard to the meaning of the evaluation assurance levels (EAL), please refer to part C of this report.

Within the last two years, the certifier did not render any consulting or other services for the company ordering the certification and there was no relationship between them that might have an influence on his assessment.

The certifier did not participate at any time in test procedures for the product, which forms the basis of the certification.

5 Publication

The following Certification Results consist of pages B-1 to B-17. The certification report and the certificate for product BogArt Motion Sensor, Version 01 will be included in the TÜViT certification list (http://www.certuvit.de).

Further copies of this certification report may be ordered from the sponsor of the product. The certification report may also be obtained in electronic form at the internet address of CERTÜViT as stated above.

Part B

Certification Result

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the Certification Result

1 Executive Summary

The target of evaluation (TOE) is the motion sensor for a digital tachograph ***BogArt Motion Sensor, Version 01*** including the models

- BogArt Motion Sensor type DTMS 00x - Rotary Version 01 and
- BogArt Motion Sensor type DTMS 200xxxxx- Proximity, Version 01.

The TOE architecture is described in chapter 5. The motion sensor has to be integrated in a digital tachograph system. The digital tachograph system consists of a gearbox, the motion sensor and the vehicle unit. The motion sensor is mounted directly into the gearbox and collects data that represents the vehicle speed and distance. The data is captured inside the gearbox via a sensor and transmitted in an encrypted form to the authenticated vehicle unit. The gear box, the vehicle unit and the tachograph cards are not part of the TOE.
It provides the following functionality:

- collecting of data representing vehicle speed and distance,
- transmission of the data to vehicle unit,
- encrypting the data for the transmission,
- authenticating the vehicle unit,
- control of access to the TOE security functions and data.

The security target is the basis of this certification. It is not based on a certified protection profile.

The TOE security assurance requirements are based entirely on the assurance components and classes defined in part 3 of Common Criteria (see part C of this report or [CC] Part 3 for details). The TOE meets the assurance requirements of assurance level EAL 4+ (Evaluation Assurance Level 4+) augmented by ATE_DPT.2 (testing: security enforcing modules).

The TOE's security functional requirements were taken from CC part 2 (i. e. the set is CC part 2 conformant) [CC]. They can be categorized in the following eight logical security functions:

Security Function	Description
Identification and authentication	The TOE identifies and authenticates a connected vehicle unit or management device that is used to manage the TOE, e. g. for updating other devices.
Access control	The TOE controls access to its logical security functions and data.
Accountability	The TOE stores accountability data and outputs it to authenticated entities.

Security Function	Description
Audit	The TOE records audit events and sends them to the vehicle unit.
Accuracy	The TOE derives motion data from sensor mechanical input and checks stored user data for integrity errors.
Reliability of service	The TOE runs self-tests to detect internal errors. It is furthermore resistant to physical and logical sabotage.
Data exchange	The TOE exports data to the vehicle unit such that it can be verified for integrity and authenticity.
Cryptographic support	The TOE performs cryptographic functions in accordance with the specified algorithms and methods.

A more detailed description of the TOE security functions can be found in section 6.1 of the public ST, which is attached as part E of this certification report.
Assets for the TOE comprise the motion data collected by the motion sensor and transmitted to the vehicle unit, the authentication data of the vehicle unit and the security functions and data of the TOE.
The 12 threats comprise threats to access control policies, design related threats and operation related threats.
There are no organisational security policies for the TOE.
A more detailed description of the threats and assumptions can be found in sections 3.1 and 3.3 of the public ST, which is attached as part E of this certification report. The certification covers the configurations of the TOE as outlined in chapter 8.

2 Identification of the TOE

The Target of Evaluation (TOE) is the BogArt Motion Sensor, Version 01. The following TOE models are comprised

- BogArt Motion Sensor type DTMS00**T** - Rotary, Version 01
  T: thread, possible values:
  - 1 (internal thread M22*1,5 right) ,
  - 2 (external thread M22*1,5 left),
  - 3 (internal thread 7/8” 18 UNS 2B),
  - 7 (internal thread M18*1,5 right)

- BogArt Motion Sensor type DTMS200**LG** - Proximity, Version 01
  L: length, possible values:
  - 198 (19,8 mm),
  - 250 (25,0 mm),
  - 350 (35,0 mm),
  - 632 (63,2 mm),
  - 900 (90,0 mm),
  - 115 (115,0 mm),
  - 137 (136,8 mm)

  G: gasket, possible values:
  - 00 (no gasket),
  - 12 (gasket 1,2 mm),
  - 18 (gasket 1,8 mm)

The TOE delivery consists of the following parts:

1. TOE Documentation (see chapter 6)
2. BogArt Motion Sensor

The TOE is delivered by courier. The integrity of the delivered TOE has to be checked comparing the type, version and serial number indicated on the product's plate with those mentioned on the packing letter. The TOE authenticity and integrity must be verified by checking the hologram foil, which should not be damaged or scratched.

The installation guidance is delivered by BogArt by e–mail. The integrity of the Installation Guidance has to be checked by comparing the hash sum of received document with the hash sum in this certification report (see chapter 6).

The TOE is identified by the label engraved in the product plate on the case of the TOE DTMS00T yymm V01 or DTMS200LG yymm V01 (DTMS00T/DTMS200LG: as indicated above; yymm: year and month of manufacturing; V01: TOE version 01).

3 Security Policy

The security policy is expressed by the set of security functions of the security target derived from the generic ST.

Following properties must be maintained by the security policy:

- the integrity and authenticity of the motion data exchanged with the vehicle unit,
- the confidentiality of the specific data needed to support the security enforcing functions (e. g. cryptographic keys)
- the integrity and authenticity of the user data recorded or stored by the motion sensor.

Specific details concerning the different security policies can be found in section 6.1 of the public ST, which is attached as part E of this certification report.

4 Assumptions and Clarification of Scope

The assumptions defined in the Security Target and some aspects of threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled and physical, personnel or procedural measures to be taken. The following topics are of relevance:

- Motion sensor developers must ensure that the assignment of responsibilities during development is done in a manner which maintains IT security.
- Motion sensor manufacturers must ensure that the assignment of responsibilities during manufacturing is done in a manner which maintains IT security, and that during the manufacturing process the motion sensor is protected from physical attacks which might compromise IT security.
- Motion sensor manufacturers, vehicle manufacturers and fitters or workshops must ensure that handling of the motion sensor is done in a manner which maintains IT security.
- Security data generation algorithms must be accessible to authorised and trusted persons only.
- Security data must be generated, transported, and inserted into the motion sensor, in such a way to preserve its appropriate confidentiality and integrity.
- Installation, calibration and repair of recording equipment must be carried by trusted and approved fitters or workshops.
- Means of detecting physical tampering with the mechanical interface must be provided (e. g. seals).

- Recording equipment must be periodically inspected and calibrated.
- Law enforcement controls must be performed regularly and randomly, and must include security audits.
- Software revisions must be granted security certification before they can be implemented in a motion sensor.

5 Architectural Information

The TOE physically consists of:

Name of Element	Description
Hall Sensor	converts magnetic field changes of the rotating element of the gear into electrical pulses that allow the vehicle unit to derive speed and distance
microcontroller	processes the electrical pulses from the sensor in real-time and transmits the data to the authenticated vehicle unit
secure element	stores key material and encrypts/decrypts data transmitted to and from the vehicle unit
Hall Sensor for attack detection	detects external magnetic fields to prevent magnetic attacks on the TOE
supporting elements	such as voltage regulator, buffers, and interference suppressors are required such that the TOE can fulfill its function

6 Documentation

The following documentation is provided with the product by the developer to the consumer:

- BogArt Motion Sensor AGD Documentation, version 15, 2016-06-15,
  file name: BogArt Motion Sensor AGD v15.pdf, SHA-256 checksum:
  7de9cd481be3cc5cd14804146b013c058588ead9f49a4c619d7fae952d433941

7 IT Product Testing

The developer's testing approach was to systematically test the TOE security functionality / TSFI, i.e. the following security functionalities as defined in [ST] have been tested:

- Identification and Authentication,
- Access Control,
- Accountability,
- Audit,
- Accuracy,
- Reliability of service,
- Data exchange,
- Cryptographic support.

The evaluator's objective was to test the functionality of the TOE systematically against the security functionality description in [ST] and [ADV]. In order to do this, the evaluation body performed the following tasks:

- Repeat the developer's tests,
- Devise and execute own functional tests.
- Based on a list of potential vulnerabilities applicable to the TOE in its operational environment the evaluators devised the attack scenarios for penetration tests when they were of the opinion, that those potential vulnerabilities could be exploited in the TOE's operational environment. While doing this, also the aspects of the security architecture description were considered for penetration testing. All other evaluation input was used for the creation of the tests as well.

8 Evaluated Configuration

The TOE is delivered in one fixed configuration and no further generation takes place.
The Security Target [ST] has identified solely one configuration of the TOE under evaluation. The TOE consists only of one part besides the guidance but there are different types of the TOE depending on the model, the thread, the length, and the gasket (see chapter 2). For both TOE models proximity and rotary all possible lengths were tested.
The operational environment of the TOE in its evaluated configuration can be summarized as follows:
To fulfil its function the TOE must be integrated in a Digital Tachograph system. The vehicle unit and the tachograph cards don't belong to the TOE. Additional hardware, software or firmware beyond that is not necessary for the TOE.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report [ETR] was provided by TÜViT's evaluation body according to the requirements of the Scheme, the Common Criteria [CC], the Methodology [CEM] and the Application Notes and Interpretations of the Scheme [AIS].
As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL4 package including the class ASE as defined in the CC (see also part C of this report).
- The component ATE_DPT.2 augmented for this TOE evaluation.

The verdicts for CC, part 3 assurance classes and components (according to EAL4+ augmented by ATE_DPT.2 and the class ASE for the Security Target Evaluation) are summarised in the following table:

Assurance classes and components			**Verdict**
	Development	**ADV**	**PASS**
	Security architecture description	ADV_ARC.1	PASS
	Complete functional specification	ADV_FSP.4	PASS
	Implementation representation of the TSF	ADV_IMP.1	PASS
	Basic modular design	ADV_TDS.3	PASS
	Design compliance with the platform certification report, guidance and ETR_COMP	ADV_COMP.1	PASS
	Guidance documents	**AGD**	**PASS**
	Operational user guidance	AGD_OPE.1	PASS
	Preparative procedures	AGD_PRE.1	PASS
	Life-cycle support	**ALC**	**PASS**
	Production support, acceptance procedures and automation	ALC_CMC.4	PASS
	Problem tracking CM coverage	ALC_CMS.4	PASS
	Delivery procedures	ALC_DEL.1	PASS
	Identification of security measures	ALC_DVS.1	PASS
	Developer defined life-cycle model	ALC_LCD.1	PASS
	Well-defined development tools	ALC_TAT.1	PASS
	Integration of the application into the underlying platform and Consistency check for delivery and acceptance procedures	ALC_COMP.1	PASS

Assurance classes and components			Verdict
	Security Target evaluation	**ASE**	**PASS**
	Conformance claims	ASE_CCL.1	PASS
	Extended components definition	ASE_ECD.1	PASS
	ST introduction	ASE_INT.1	PASS
	Security objectives	ASE_OBJ.2	PASS
	Derived security requirements	ASE_REQ.2	PASS
	Security problem definition	ASE_SPD.1	PASS
	TOE summary specification	ASE_TSS.1	PASS
	Consistency of Security Target	ASE_COMP.1	PASS
	Tests	**ATE**	**PASS**
	Analysis of coverage	ATE_COV.2	PASS
	Testing: security enforcing modules	ATE_DPT.2	PASS
	Functional testing	ATE_FUN.1	PASS
	Independent testing - sample	ATE_IND.2	PASS
	Composite product functional testing	ATE_COMP.1	PASS
	Vulnerability Assessment	**AVA**	**PASS**
	Focused vulnerability analysis	AVA_VAN.3	PASS
	Composite product vulnerability assessment	AVA_COMP.1	PASS

9.2 Results of the cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see [BSIG], section 9, para. 4, clause 2). But Cryptographic Functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from [TR-02102].

Any Cryptographic Functionality that is marked with 'No' in column 'Security Level above 100 Bits' of the following table achieves a security level of lower than 100 Bits (in general context).

No.	Purpose	Cryptographic Mechanism	Implementation Standard	Key Size in Bits	Security Level above 100 Bits	Comments
1.	encryption / decryption	Triple DES	ECB mode as specified in [ISO/IEC 10116]	112	No	Security level is 80 bits (BSI AIS 46, Review Protocol of

No.	Purpose	Cryptographic Mechanism	Implementation Standard	Key Size in Bits	Security Level above 100 Bits	Comments
						(Krypto-) AVA-KickOff, chapter 12.1)
2.	encryption of data files	Triple DES	CBC mode as specified in [ISO/IEC 10116]	112	No	Security level is 80 bits (BSI AIS 46, Review Protocol of (Krypto-) AVA-KickOff, chapter 12.1)

A Security Level above 100 bits is required by AVA_VAN.5. The Security level reached is not above 100 bits due to the fact that it is required by the ISO 16844-3 to use the 2Key Triple DES encryption. Furthermore there was an investigation of ISO16844-3 and the C source msavrnxp implementing the ISO-commands. There is no way getting bigger samples of pairs plain/cipher text encrypted with pairing key or session key. The security level of 80 bits is sufficient for AVA_VAN.3.

10 Evaluation Stipulations, Comments, and Recommendations

The evaluation technical report contains no stipulations or recommendations.

The evaluation technical report contains the following comment:

The ETR for composition is the following one:

[ETR_COMP]

The date of this ETR for composition is August 4th, 2014. This means that the ETR_COMP is older than 18 month. There are some arguments for accepting this fact:

1. The attack potential is only „enhanced basic“ (AVA_VAN.3).
2. The motion sensor is filled with epoxy resin and sealed before delivery.

3. The motion sensor is sealed to the gear box during installation.
4. The logical access to the NXP chip is only possible via the main processor as shown in figure 1 in [ADV, 3.1]. There is no direct physically or logically access to the NXP chip. (This is the difference to the use of the chip on a smart card.)
5. The TOE uses only few security functions of the platform as shown in table 2 in [ST, 2.5.2].
6. Outside of the composite procedure which is actually only applicable for “smart cards and similar devices” the certificate for the NXP chip is still valid up to August 2018 and was not removed because of security problems.

These arguments are sufficient to accept the ETR for composition even it is about 4 months older than it should be.

11 Certification Stipulations and Notes

There are no stipulations or notes resulting from the certification report.

12 Security Target

The security target [ST] for *BogArt Motion Sensor, Version 01* is included in part E of this certification report.

13 Definitions

13.1 Acronyms

AGD	Guidance Documents
CC	Common Criteria for Information Technology Security Evaluation (referenced to as [CC])
CEM	Common Methodology for Information Technology Security Evaluation (referenced to as [CEM])
EAL	Evaluation Assurance Level
EEPROM	Electrical Erasable and Programmable Read Only Memory
ES	Embedded Software
EU	European Union
FSP	Functional Specification
HLD	High-level Design
DTSM	Digital Tachograph Motion Sensor
IC	Integrated Circuit
IF	Interface
IGS	Installation, Generation and Start-up
OS	Operating System
OSP	Organisational Security Policy
PP	Protection Profile
RSA	Signature Algorithm of Rivest, Shamir, Adleman
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SIF	Sub-interface
SOF	Strength of Function
SS	Sub-system
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Function Interfaces
TSP	TOE Security Policy
VLA	Vulnerability Analysis

13.2 Glossary

Augmentation	The addition of one or more assurance component(s) from Part3 to an EAL or assurance package.
Extension	The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.
Formal	Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.
Informal	Expressed in natural language.
Object	An entity within the TSC that contains or receives information and upon which subjects perform operations.
Protection Profile	An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
Security Function	A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.
Security Target	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
Semiformal	Expressed in a restricted syntax language with defined semantics.
Strength of Function	A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.
Subject	An entity within the TSC that causes operations to be performed.
Target of Evaluation	An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
TOE Security Functions	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TOE Security Policy	A set of rules that regulate how assets are managed, protected and distributed within a TOE.
TSF Scope of Control	The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

14 Bibliography

[AGD]	BogArt Motion Sensor AGD Documentation, version 15, 2016-06-15, BogArt Sp. z o.o.
[AIS]	Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE, Bundesamt für Sicherheit in der Informationstechnik

[AIS1]	Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 1, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers, Version 13, 2008-08-14, Bundesamt für Sicherheit in der Informationstechnik.
[AIS11]	Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 11, Programmiersprachen und Compiler, Version 2.0, 1998-02-02, Bundesamt für Sicherheit in der Informationstechnik.
[AIS14]	Anwendungshinweise und Interpretationen zum Schema, AIS 14: Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 2010-08-03, Bundesamt für Sicherheit in der Informationstechnik.
[AIS19]	Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 19, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 9, 2014-11-03, Bundesamt für Sicherheit in der Informationstechnik.
[AIS23]	Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 23, Zusammentragen von Nachweisen der Entwickler, Version 3, 2013-04-15, Bundesamt für Sicherheit in der Informationstechnik.
[AIS23_JIL-CDE]	Joint Interpretation Library - Collection of Developer Evidence, Version 1.5, January 2012.
[AIS32]	Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 32, CC-Interpretationen im deutschen Zertifizierungsschema, Version 7, 2011-06-08, Bundesamt für Sicherheit in der Informationstechnik.
[AIS36]	Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 36, Kompositionsevaluierung, Version 4, 2013-05-15, Bundesamt für Sicherheit in der Informationstechnik.
[AIS36_CCDB-COMP]	CC Supporting Document, Mandatory Technical Document, Composite product evaluation for Smart Cards and similar devices, Version 1.2, 2012-04, CCDB-2012-04-001.
[AIS36_CCDB-COMP_ETR_TEMPL]	CC Supporting Document, Guidance, ETR template for composite evaluation of Smart Cards and similar devices, Version 1.0, Revision 1, September 2007, CCDB-2007-09-002.
[AIS36_JIL-COMP]	Joint Interpretation Library – Composite product evaluation for Smart Cards and similar devices, Version 1.2, 2012-01.
[AIS36_JIL-COMP_ETR_TEMPL]	Joint Interpretation Library – ETR for composite evaluation, Version 1.0, 2007-09.
[AIS36_JIL-Open_SC]	Joint Interpretation Library – Certification of “open” smart card products, Version 1.1, 2013-02-04.

[AIS40]	Application Notes and Interpretation of the Scheme (AIS), AIS 40, Use of Interpretation for Security Evaluation and Certification of Digital Tachographs, Version 1, 2005-06-28, Bundesamt für Sicherheit in der Informationstechnik.
[AIS42]	Application Notes and Interpretation of the Scheme (AIS), AIS 42, Guidelines for the Developer Documentation, Version 1, 2008-05-21, Bundesamt für Sicherheit in der Informationstechnik.
[AIS46]	Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 46, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, Version 3, 2013-12-04, Bundesamt für Sicherheit in der Informationstechnik.
[AIS46_AVATMP]	Review-Protokoll zum AVA-KickOff Meeting, Date: 2014-03-03, Bundesamt für Sicherheit in der Informationstechnik.
[CC]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Part 1: Introduction and general model, Revision 4, September 2012 Part 2: Security functional requirements, , Revision 4, September 2012 Part 3: Security assurance requirements, , Revision 4, September 2012
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, September 2012
[ETR]	Evaluation Technical Report, TÜV Informationstechnik GmbH, version *3*, *2016-06-24*, project-number: 8111395598
[ETR_COMP]	ETR for Composite Evaluation NXP J3E081_M64, J3E081_M66, J2E081_M64, J3E041_M66, J3E016_M66, J3E016_M64, J3E041_M64 Secure Smart Card Controller Revision 3 EAL5+, Version 3.0, August 13th 2014, Brightsight
[Generic-ST, 3.6]	EC 1360/2002, Appendix 10: Motion sensor generic security target, European Communities
[ISO16844-3]	Road vehicles – Tachograph systems – Part 3: Motion sensor interface (Technical corrigendum 1 applied), ISO 16844-3:2004(E)
[Platform_Cert]	NXP J3E081 M64, J3E081 M66, J2E081 M64, J3E041 M66, J3E016 M66, J3E016 M64, J3E041 M64 Secure Smart Card Controller Revision 3, Certification Report, NSCIB-CC-13-37761-CR, Version 1, August 5th, 2013, TÜV Rheinland Nederland B.V.
[ST]	BogArt Motion Sensor Security Target, Version 18.0, 2016-06-14 BogArt Sp. z o.o.
[TR-02102]	BSI - Technische Richtlinie TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen (consisting of [TR-02102-1]/[TR-02102-2]/[TR-02102-3])

[TR-02102-1] BSI - Technische Richtlinie TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2014-01, 2014-02-10, Bundesamt für Sicherheit in der Informationstechnik.

[TR-02102-2] BSI - Technische Richtlinie TR-02102-2, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS), Version 2014-01, 2014-02-12, Bundesamt für Sicherheit in der Informationstechnik.

[TR-02102-3] BSI - Technische Richtlinie TR-02102-3, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2), Version 2014-01, 2014-02-12, Bundesamt für Sicherheit in der Informationstechnik.

Part C

Excerpts from the Criteria

The excerpts from the criteria are dealing with

- conformance results
- assurance categorization
- evaluation assurance levels
- strength of security function
- vulnerability analysis

CC Part 1:

Conformance Claim

The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:

  CC Part 2 conformant - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or

  CC Part 2 extended - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:

  CC Part 3 conformant - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or

  CC Part 3 extended - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e. g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a pre-defined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e. g. CC Part 2 conformant.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

- **PP Conformant** - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- **Conformance Statement** (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.

CC Part 3:

Class APE: Protection Profile evaluation

Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition

Class ASE: Security Target evaluation

Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation."

Assurance Class	Assurance Components	
Class ASE: Security Target evaluation	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_SPD.1	Security problem definition
	ASE_OBJ.1	Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1	Extended components definition
	ASE_REQ.1 ASE_REQ.2	Stated security requirements Derived security requirements
	ASE_TSS.1 ASE_TSS.2	TOE summary specification TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“ “Each assurance class contains at least one assurance family.” “Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition:

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internalsADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures

Assurance Class	Assurance Components
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle mode ALC_LCD.2 Measurable life-cycle mode
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts

Assurance Class	Assurance Components
ATE Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels

The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.

Evaluation assurance level (EAL) overview

The above table represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in

assurance from EAL to EAL is accomplished by *substitution* of a hierarchically higher assurance component from the same assurance family (i. e. increasing rigour, scope, and/or depth) and from the *addition* of assurance components from other assurance families (i. e. adding new requirements).
These EALs consist of an appropriate combination of assurance components as described in chapter 2 of CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.
While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation“ allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component“ is not recognised by the CC as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Evaluation assurance level 1 (EAL1) - functionally tested

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL 1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL 1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL 1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.
An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.

Evaluation assurance level 2 (EAL2) - structurally tested

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.
EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability

of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.

Evaluation assurance level 3 (EAL3) - methodically tested and checked

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.
EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.
EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.

Evaluation assurance level 5 (EAL5) - semiformally designed and tested

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.
EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.
EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.

Evaluation assurance level 7 (EAL7) - formally verified design and tested

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical

application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**
	ADV_IMP				**1**	1	**2**	2
	ADV_INT					**2**	**3**	3
	ADV_SPM						**1**	1
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**
Guidance documents	AGD_OPE	**1**	1	1	1	1	1	3
	AGD_PRE	**1**	1	1	1	1	1	1
Live cycle support	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD			**1**	1	1	1	**2**
	ALC_TAT				**1**	**2**	**3**	3
Security Target Evaluation	ASE_CCL	**1**	1	1	1	1	1	1
	ASE_ECD	**1**	1	1	1	1	1	1
	ASE_INT	**1**	1	1	1	1	1	1
	ASE_OBJ	**1**	**2**	2	2	2	2	2
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	**1**	1	1	1	1	1	1
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**3**	3	4
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability Assessment	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5

Evaluation assurance level summary

Class AVA: Vulnerability assessment

The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.

Vulnerability analysis (AVA_VAN)

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e. g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.

Part D

Evaluation Results regarding development and production environment

The IT product BogArt Motion Sensor, Version 01 has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM) Version 3.1 extended by Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification dated 29 June 2016 the following results regarding the development and production environment apply. ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1) are fulfilled for the development and production sites of the TOE listed below:

Name of site / Company name	Address	Type of site	Date of last audit	New audit / reused audit / n.r.
BogArt Dobre Miasto / BogArt Sp. z o. o.	Nowa Wieś Mała 40, Dobre Miasto, Poland	Development/ Testing/ Production	2016-04-20/21	new audit

For development and production sites regarding the platform please refer to the certification report NSCIB-CC-13-37761-CR [Platform-Cert].

For the site listed above, the requirements have been specifically applied in accordance with the Security Target [ST]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery as stated in the Security Target [ST] are fulfilled by the procedures of this site.

Part E

Security Target

Attached is the public version of the Security Target: “BogArt Motion Sensor Security Target, Version 18.0, BogArt Sp. z o.o.”
Author: BogArt Sp. z.o.o.
Date: 2016-06-14
Version: 18

BogArt Motion Sensor Security Target

Version: 18.0

Date: 2016-06-14

This page intentionally left blank.

Contents

List of Tables

List of Figures

1 ST Introduction

1.1 ST Reference

ST Title: BogArt Motion Sensor Security Target
ST Version: 18
Certification ID: TUVIT-TSZ-9262

1.2 TOE Reference

TOE Name: BogArt Motion Sensor
TOE Models: BogArt Motion Sensor type DTMS 00x - Rotary, Version 01
BogArt Motion Sensor type DTMS 200xxxxx- Proximity, Version 01

Each 'x' in the type identifiers denotes a numeric character. The use of the types depends on the gear box type. The 00x type is equipped with a mechanical rotating element for motion detection, whereas the 200xxxxx type is not equipped with a rotating element but it detects the motion of an external rotating element such as a tooth wheel of the gear box. This external rotating element is not part of the TOE.

1.3 TOE Overview

The TOE is a motion sensor for a Digital Tachograph system.

A security certification of the motion sensor is required in conformance with Annex 1B of EC regulation 1360/2002 [EC 1360/2002]:

> "In order to achieve the system security, the recording equipment shall meet the security requirements specified in the motion sensor and vehicle unit generic security targets (Appendix 10)."

The motion sensor is mounted directly into the gearbox and collects the data that represents the vehicle speed and distance. This data is captured from the rotating wheels inside the gearbox via a sensor and transmitted in an encrypted form to the authenticated vehicle unit (VU) of the Digital Tachograph system. The vehicle unit and the tachograph cards are not part of the TOE. However, the TOE has to be integrated in a Digital Tachograph system in order to fulfill its function. Besides that, the TOE does not need any additional hardware, software or firmware.

The TOE is capable of cryptographically protecting the motion data as defined in [Generic-ST, 2.2] after it has been stored in the TOE and while it is being transmitted from the motion sensor to the

authenticated vehicle unit. Furthermore, the TOE authenticates the vehicle unit and controls access to TOE security functions and data. An overview of the logical security functions of the TOE is given in Table 1.
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, hence the motion data manipulation is detected.

Further information on the product type can be found in [Generic-ST, 3].

1.4 TOE Description

The TOE physically consists of the following elements:

- A Hall sensor 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 data to the authenticated vehicle unit.
- A secure element stores key material and encrypts/decrypts data transmitted to and from the vehicle unit.
- A second Hall sensor detects external magnetic fields to prevent magnetic attacks on the TOE.
- Supporting elements such as voltage regulator, buffers, and interference suppressors are required such that the TOE can fulfill its function.

A schematic overview of the TOE is shown in Figure 1. The connector (1) connects the motion sensor with the cable to the vehicle unit. It also contains the interface to the vehicle unit (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 sensor for motion detection (speed signal interface, 5).

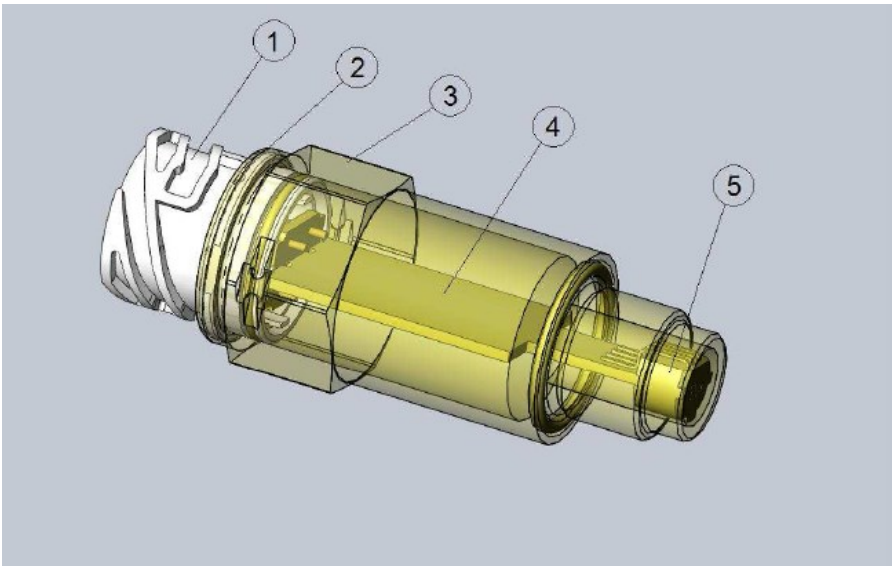

Figure 1: Schematic TOE Overview

Figure 1 shows a motion sensor type DTMS 200xxxxx which has an aluminum body and a socket (connector) for the cable. The motion sensor type DTMS 00x is equipped with a rotating element inside the body. Please see Figure 2 for photographs of both types.

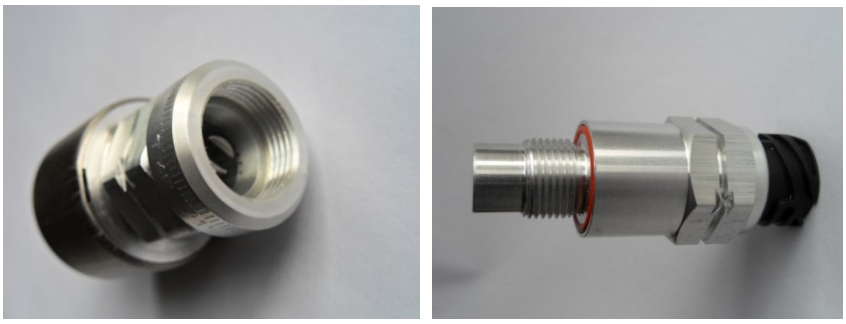

Figure 2: From left to right: DTMS 00x – Rotary, DTMS 200xxxxx – Proximity

Beside the physical motion sensor, the TOE also comprises the guidance documentation for its integration and operation [AGD].

Table 1 lists the logical security functions of the TOE together with a brief description of each function.

Logical Security Function [Generic-ST]	Description
Identification and authentication	The TOE identifies and authenticates a connected VU or management device.

Logical Security Function [Generic-ST]	Description
Access control	The TOE controls access to its logical security functions and data.
Accountability	The TOE stores accountability data and outputs it to authenticated entities.
Audit	The TOE records audit events and sends them to the VU.
Accuracy	The TOE derives motion data from sensor mechanical input and checks stored user data for integrity errors.
Reliability of service	The TOE runs self-tests to detect internal errors. It is furthermore resistant to physical and logical sabotage.
Data exchange	The TOE exports data to the VU such that it can be verified for integrity and authenticity.
Cryptographic support	The TOE performs cryptographic functions in accordance with the specified algorithms and methods.

Table 1: Logical Security Functions

2 Conformance Claims

2.1 CC Conformance Claim

The ST and the TOE claim conformance to [CC]. The TOE is CC Part 2 conformant and CC Part 3 conformant.

2.2 PP Claim

The ST does not claim conformance to a PP.

2.3 Package Claim

The ST claims conformance to Evaluation Assurance Level (EAL) 4 augmented by ATE_DPT.2 as defined in [CC, Part 3].

2.4 Conformance Rationale

A conformance rationale is not required because the ST does not claim conformance to a PP.

2.5 Statement of Compatibility

The TOE contains a secure element that has been certified according to Common Criteria at EAL 5 augmented with ALC_DVS.2, AVA_VAN.5, and ASE_TSS.2 [Platform-Cert].

The following subsections formally integrate the secure element (the „platform”) into this Security

Target (the „Composite ST"). First, the relevant platform functionality that is used by the TOE is identified. Afterwards, the compatibility of the Security Problem Definitions and of the Security Objectives of the Platform ST and the Composite ST is analysed.

2.5.1 Compatibility of Relevant Platform SAR

The platform fulfils the SAR of the TOE as stated in chapter 6.2 due to its certification as stated in chapter 2.5. The SAR of the TOE are only a subset of the SAR fulfilled by the platform.

2.5.2 Compatibility of Relevant Platform SFRs

The following Table 2 identifies the SFRs of the Platform ST [Platform-ST] that are relevant in context of the current Composite ST. All other SFRs of the Platform ST that are not listed in Table 2 are not relevant in context of the current Composite ST. The analysis in the table shows that the Relevant Platform SFRs are consistent with the corresponding SFRs in the Composite ST.

Relevant Platform SFR	Correspondence in Composite ST	Result
FCS Cryptographic Support		
FCS_CKM.3 Cryptographic Key Access	FCS_CKM.3 FCS_CKM.4	Access to DES keys is provided by the Platform API.
FCS_COP.1 Cryptographic Operation	FCS_COP.1	Two Key Triple DES encryption and decryption is performed by the Platform in ECB and CBC mode.
FAU Security Audit		
FAU_ARP.1 Security Alarms	FDP_SDI.2 FPT_TST.1	EEPROM failure (detection of broken EEPROM cells) and corruption of check-summed objects are detected by the Platform (see also FPT_FLS.1).
FDP User Data Protection		
FDP_SDI.2 Stored Data Integrity Monitoring and Action	FDP_SDI.2 FPT_TST.1 FAU_GEN.1	The Platform monitors application code, application data and application keys for integrity errors. Upon detection of an integrity error for application keys, the TSF maintains a secure state (lock card session). Upon detection of an integrity error for the application code/data it throws a SecurityException.
FPT Protection of the TSF		
FPT_FLS.1 Failure with Preservation of Secure State	FDP_SDI.2 FPT_TST.1	The Platform TSF preserves a secure state when potential security violations described in FAU_ARP.1 are detected.

Table 2: Compatibility of Relevant Platform SFRs

2.5.3 Compatibility of Relevant Platform Security Objectives

Based on the Relevant Platform SFRs, the following Table 3 identifies the Relevant Platform Security Objectives. The analysis in this table shows that none of the Relevant Platform Security

Objectives is contradictory to a security objective of the Composite ST.

Relevant Platform Security Objective [Platform-ST, 4]	Corresponding Composite Security Objective [Generic-ST, 3.4/3.5]	Result
OT.OPERATE The TOE must ensure continued correct operation of its security functions. Especially, the TOE must prevent the unauthorized use of TOE or use of incorrect or unauthorized instructions or commands or sequence of commands.	O.Processing The motion sensor must ensure that processing of input to derive motion data is accurate O.Reliability The motion sensor must provide a reliable service.	The platform security objective supports the composite security objectives.
OT.RESOURCES The TOE shall control the availability of resources for the applications	No correspondence	No contradiction to Composite ST
OT.ALARM The TOE shall provide appropriate feedback information upon detection of a potential security violation.	O.Audit The motion sensor must audit attempts to undermine its security and should trace them to associated entities	The platform security objective supports the composite security objective.
OT.CIPHER The TOE shall provide a means to cipher sensitive data for applications in a secure way. In particular, the TOE must support cryptographic algorithms consistent with cryptographic usage policies and standards.	O.Secured_Data_Exchange The motion sensor must secure data exchanges with the VU. O.Authentication The motion sensor must authenticate connected entities	The platform security objective supports the composite security objectives.
OT.KEY-MNGT The TOE shall provide a means to securely manage cryptographic keys. This concerns the correct generation, distribution, access and destruction of cryptographic keys.	O.Secured_Data_Exchange The motion sensor must secure data exchanges with the VU. O.Authentication The motion sensor must authenticate connected entities	The platform security objective supports the composite security objectives.
OT.PIN-MNGT The TOE shall provide a means to securely manage PIN objects.	No correspondence	No contradiction to Composite ST

Relevant Platform Security Objective [Platform-ST, 4]	Corresponding Composite Security Objective [Generic-ST, 3.4/3.5]	Result
OT.SCP.IC The SCP[1] shall provide all IC security features against physical attacks.	No correspondence	No contradiction to Composite ST
OT.SCP.SUPPORT The SCP shall support the TSFs of the TOE.	No correspondence	No contradiction to Composite ST

Table 3: Compatibility of Relevant Platform Security Objectives

2.5.4 Compatibility of Relevant Platform Threats

Based on the Relevant Platform Security Objectives, the following Table 4 identifies the Relevant Platform Threats and OSPs. The analysis in this table shows that none of the Relevant Platform Threats/OSPs is contradictory to a threat or OSP of the Composite ST. Table 4 does not contain an OSP from the Platform ST because none of the OSPs were identified to be relevant.

Relevant Platform Threat/OSP [Platform-ST, 3.3]	Corresponding Composite Threats/OSPs [Generic-ST, 3.3]	Result
T.CONFID-APPLI-DATA The attacker executes an application to disclose data belonging to another application.	T.Security_Data Users could try to gain illicit knowledge of security data during security data generation or transport or storage in the equipment	The platform threat is not contradictory to the composite threat (it is more specific).
T.CONFID-JCS-DATA The attacker executes an application to disclose data belonging to the Java Card System.	T.Security_Data Users could try to gain illicit knowledge of security data during security data generation or transport or storage in the equipment	The platform threat is not contradictory to the composite threat (it is more specific).
T.INTEG-APPLI-DATA The attacker executes an application to alter (part of) another application's data.	T.Stored_Data Users could try to modify stored data (security or user data).	The platform threat is not contradictory to the composite threat (it is more specific).
T.INTEG-JCS-DATA The attacker executes an application to alter (part of) Java Card System or API data	T.Stored_Data Users could try to modify stored data (security or user data).	The platform threat is not contradictory to the composite threat (it is more specific).
T.SID.2	No correspondence	No contradiction to

[1] Smart Card Platform

Relevant Platform Threat/OSP [Platform-ST, 3.3]	Corresponding Composite Threats/OSPs [Generic-ST, 3.3]	Result
The attacker modifies the TOE's attribution of a privileged role (e.g. default applet and currently selected applet), which allows illegal impersonation of this role.		Composite ST
T.RESOURCES An attacker prevents correct operation of the Java Card System through consumption of some resources of the card: RAM or NVRAM	No correspondence	No contradiction to Composite ST
T.PHYSICAL The attacker discloses or modifies the design of the TOE, its sensitive data (TSF and User Data) or application code or disables security features of the TOE by physical (opposed o logical) tampering means. This threat includes IC failure analysis, electrical probing, unexpected tearing, and DPA. That also includes the modification of the runtime execution of Java Card System or SCP software through alteration of the intended execution order of (set of) instructions through physical tampering techniques.	T.Design Users could try to gain illicit knowledge of design either from manufacturer's material (through theft, bribery, …) or from reverse engineering. T.Environment Users could compromise the motion sensor security through environmental attacks (thermal, electromagnetic, optical, chemical, mechanical, …) T.Hardware Users could try to modify motion sensor hardware T.Power_Supply Users could try to defeat the motion sensor security objectives by modifying (cutting, reducing, increasing) its power supply T.Software Users could try to modify motion sensor software	The platform threat does not contradict the composite threats (it is more specific).

Table 4: Compatibility of Relevant Platform Threats/OSPs

2.5.5 Significant Platform Assumptions

The following Table 5 lists all assumptions of the Platform ST and analyses their significance for

the Composite ST. Assumptions of the Platform ST that are not relevant or are automatically fulfilled by the Composite ST are not significant.

Platform Assumption [Platform-ST, 3.5]	Significance for the Composite ST
A.APPLET Applets loaded post-issuance do not contain native methods.	These assumptions are automatically fulfilled. Applets that are part of the TOE are examined during the composite evaluation. Other applets cannot be loaded during the operation of the TOE because the TOE is designed such it cannot be opened and the contactless interface of the platform is deactivated.
A.VERIFICATION All the bytecodes are verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time.	
A.USE_DIAG It is assumed that the operational environment supports and uses the secure communication protocols offered by TOE.	These assumptions are automatically fulfilled. They apply to the protection of the communication with the platform. During operation of the TOE this communication is protected because the TOE is designed such that it cannot be opened and the contactless interface of the platform is deactivated. The Motion Sensor does not use any keys for secure communication with the security module. During manufacturing the communication with the security module is examined as part of the evaluation. Further from [Generic-ST, 3.6.3]: Security data must be generated, transported, and inserted into the motion sensor, in such a way to preserve its appropriate confidentiality and integrity. The only key handled outside the TOE is the master key that is covered by this assumption.
A.USE_KEYS It is assumed that the keys which are stored outside the TOE and which are used for secure communication and authentication between Smart Card and terminals are protected for confidentiality and integrity in their own storage environment.	
A.PPROCESS-SEC-IC It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the EXW manufacturer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).	This assumption is automatically fulfilled. The delivery phase from TOE developer to EXW manufacturer is examined during the evaluation of the TOE.

Table 5: Identified Significant Platform Assumptions

2.5.6 Significant Security Objectives for the Operational Environment

None of the platform assumptions has been identified to be significant. Therefore, no analysis of compatibility of significant security objectives for the operational environment is required.

3 Security Problem Definition

3.1 Threats

The threats to the motion sensor are defined in [Generic-ST, 3.3].

3.2 Organizational Security Policies

There are no organizational security policies for the TOE.

3.3 Assumptions

The assumptions for the TOE are not defined in [Generic-ST]. However, they can directly be deduced from the Security Objectives for the Operational Environment:

A.GENERIC_ST It is assumed, that the physical, personnel and procedural requirements to the environment as given in [Generic-ST, 3.6] are fulfilled.

4 Security Objectives

4.1 Security Objectives for the TOE

The main security objective for the motion sensor is defined in [Generic-ST, 3.4 (O.Sensor_Main)] and is further refined by security objectives in [Generic-ST, 3.5].

4.2 Security Objectives for the Operational Environmnet

The security objectives for the operational environment of the motion sensor are defined in [Generic-ST, 3.6].

4.3 Security Objectives Rationale

The security objectives have been directly taken from [Generic-ST]. Thus, a rationale is not required. The security objectives for the operational environment can be directly mapped to A.GENERIC_ST. Furthermore, a mapping of physical, personnel and procedural requirements to threats can be found in [Generic-ST, 8].

5 Extended Components Definition

There are no extended components defined.

6 Security Requirements

Table 6 shows a mapping of Security Enforcing Functions from the Generic Security Target [Generic-ST] to Security Functional Requirements and Security Assurance Requirements from [CC].

Selections within the SFRs are underlined, assignments are printed in **bold**, and refinements are marked with a „Refinement:" , or by ~~crossed-out text~~.

Please see chapter 8 for applicable definitions of terms used in the SFRs and SARs.

6.1 Security Functional Requirements

SEF Identifier [Generic-ST, 4]	Requirement [Generic-ST, 4]	SFR/SAR Identifier [CC, Part 2/3]	Requirement [CC, Part 2/3]
Identification and authentication			
UIA_101	The motion sensor shall be able to establish, for every interaction, the identity of any entity it is connected to.	FIA_UID.2 User identification before any action	FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

UIA_102	The identity of a connected entity shall consist of:
	• an entity group:
	  ○ VU,
	  ○ Management device,
	  ○ Other,
	• an entity ID (VU only).
			Refinement:
			The identity of a connected entity shall consist of:
			• an entity group:
			  ○ VU,
			  ○ Management device,
			  ○ Other,
			• an entity ID (VU only).

UIA_103	The entity ID of a connected VU shall consist of the VU approval number and the VU serial number.		Refinement: The entity ID of a connected VU shall consist of the VU approval number and the VU serial number.
UIA_104	The motion sensor shall be able to authenticate any VU or management device it is connected to: • at entity connection, • at power supply recovery.	FIA_UAU.2 User authentication before any action	FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

SEF Identifier [Generic-ST, 4]	Requirement [Generic-ST, 4]	SFR/SAR Identifier [CC, Part 2/3]	Requirement [CC, Part 2/3]
			Refinement: The motion sensor shall be able to authenticate any VU or management device it is connected to: • at entity connection, • at power supply recovery.
UIA_105	The motion sensor shall be able to periodically re-authenticate the VU it is connected to.	FIA_UAU.6 Re-authenticating	FIA_UAU.6.1 The TSF shall re-authenticate the user ~~under the conditions~~ **when sensor data is exchanged**.
UIA_106	The motion sensor shall detect and prevent use of authentication data that has been copied and replayed.	FIA_UAU.3 Unforgeable authentication	FIA_UAU.3.1 The TSF shall detect, prevent use of authentication data that has been forged by any user of the TSF. FIA_UAU.3.2 The TSF shall detect, prevent use of authentication data that has been copied from any other user of the TSF.
UIA_107	After (TBD by manufacturer and not more than 20) consecutive unsuccessful authentication attempts have been detected, the SEF shall: • generate an audit record of the event, • warn the entity, • continue to export motion data in a non secured mode.	FIA_AFL.1 Authentication failure handling	FIA_AFL.1.1 The TSF shall detect when **1** unsuccessful authentication attempt~~s~~ occur related to **communication**. FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall • **generate an audit record of the event,** • **warn the entity,** • **continue to export motion data in a non secured mode.**

SEF Identifier [Generic-ST, 4]	Requirement [Generic-ST, 4]	SFR/SAR Identifier [CC, Part 2/3]	Requirement [CC, Part 2/3]
Access Control & Accountability			
ACC_101	The motion sensor shall control access rights to function and data.	FDP_ACC.1 Subset access control	FDP_ACC.1.1 The TSF shall enforce the **MS access control SFP** on **subjects: authenticated entities, objects: user, security and accountability data, operations: read and write**.
ACC_102	The motion sensor shall ensure that motion sensor identification data can be written once only (requirement 078).		
ACC_103	The motion sensor shall accept and/or store user data from authenticated entities only.	FDP_ACF.1 Security attribute based access control	FDP_ACF.1.1 The TSF shall enforce the **MS access control SFP** to objects based on the following: **entities and their authentication status, data and their type**.
ACC_104	The motion sensor shall enforce appropriate read and write access rights to security data.		
ACC_105	Application and data files structure and access conditions shall be created during the manufacturing process, and then locked from any future modification or deletion.		FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: • **authenticated entities are allowed to write user data** • **authenticated entities are allowed to read accountability data**
ACT_101	The motion sensor shall hold in its memory motion sensor identification data (requirement 077).		
ACT_102	The motion sensor shall store in its memory installation data (requirement 099).		
ACT_103	The motion sensor shall have a capability to output accountability data to authenticated entities at their request.		FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**. FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

SEF Identifier [Generic-ST, 4]	Requirement [Generic-ST, 4]	SFR/SAR Identifier [CC, Part 2/3]	Requirement [CC, Part 2/3]
		FMT_MSA.3 Static attribute initialisation	• **no subject is allowed to write motion sensor identification data after manufacturing** • **no subject is allowed to write application and data files structure and access conditions after manufacturing** FMT_MSA.3.1 The TSF shall enforce the **MS access control SFP** to provide restrictive default values for security attributes that are used to enforce the SFP. FMT_MSA.3.2 The TSF shall allow ~~the~~ **no role** to specify alternative initial values to override the default values when an object or information is created.
Audit			

AUD_101	The motion sensor shall, for events impairing its security, generate audit records of the events.	FAU_GEN.1 Audit data generation	FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
			a) Start-up and shutdown of the audit functions;
			b) All auditable events for the not specified level of audit; and
			c)
			• **security breach attempts,**
			  ○ **authentication failure,**
			  ○ **stored data**

AUD_102	The events affecting the security of the motion sensor are the following:
	• security breach attempts,
	  ○ authentication failure,
	  ○ stored data integrity error,
	  ○ internal data transfer error,
	  ○ unauthorised case		

SEF Identifier [Generic-ST, 4]	Requirement [Generic-ST, 4]	SFR/SAR Identifier [CC, Part 2/3]	Requirement [CC, Part 2/3]
	opening, ○ hardware sabotage. • sensor fault.		**integrity error,** ○ **internal data transfer error,** ○ **unauthorised case opening,** ○ **hardware sabotage.** • **sensor fault**. FAU_GEN.1.2 The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **no other audit relevant information**. Refinement: The motion sensors sets NARA flag and generates the audit record. The VU checks the NARA flag status on every Command #70 and if the NARA flag is set, the VU reads the audit record on the next command #80. Application Note: When required data is not available, an appropriate default indication shall be given (TBD by
AUD_103	Audit records shall include the following data: • date and time of the event, • type of event, • connected entity identity. When required data is not available, an appropriate default indication shall be given (TBD by manufacturer).		
AUD_104	The motion sensor shall send the generated audit records to the VU at the moment of their generation, and may also store them in its memory.		

SEF Identifier [Generic-ST, 4]	Requirement [Generic-ST, 4]	SFR/SAR Identifier [CC, Part 2/3]	Requirement [CC, Part 2/3]
			manufacturer).
AUD_105	In the case where the motion sensor stores audit records, it shall ensure that 20 audit records will be maintained independent of audit storage exhaustion, and shall have a capability to output stored audit records to authenticated entities at their request.	The motion sensor does not store audit records.	--
Accuracy & Reliability of Service			
ACR_101	The motion sensor shall ensure that motion data may only been processed and derived from sensor mechanical input.	ADV_ARC.1 Security architecture description	ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.
ACR_102	If data are transferred between physically separated parts of the motion sensor, the data shall be protected from modification.	Requirements not applicable. Motion sensor does not make use of physically separated parts.	--
ACR_103	Upon detection of a data transfer error during an internal transfer, transmission shall be repeated and the SEF shall generate an audit record of the event.		
ACR_104	The motion sensor shall check user data stored in its memory for integrity errors.	FDP_SDI.2 Stored data integrity monitoring and action	FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for **integrity errors** on all objects, based on the following attributes: **checksum of bytes**. FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall **generate an audit record**.
ACR_105	Upon detection of a stored user data integrity error, the SEF shall generate an audit record.		

SEF Identifier [Generic-ST, 4]	Requirement [Generic-ST, 4]	SFR/SAR Identifier [CC, Part 2/3]	Requirement [CC, Part 2/3]
RLB_101	All commands, actions, or test points, specific to the testing needs of the manufacturing phase shall be disabled or removed before the end of the manufacturing phase. It shall not be possible to restore them for later use.	ADV_ARC.1 Security architecture description	ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.
RLB_102	The motion sensor shall run self-tests, during initial start-up, and during normal operation to verify its correct operation. The motion sensor self-tests shall include a verification of the integrity of security data and a verification of the integrity of stored executable code (if not in ROM).	FPT_TST.1 TSF testing	FPT_TST.1.1 The TSF shall run a suite of self tests during initial start-up, periodically during normal operation to demonstrate the correct operation of the TSF. FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of **security data**. FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of **stored executable code (if not in ROM)**. Refinement: Upon detection of an internal fault during self-test, the SEF shall generate an audit record (sensor fault).
RLB_103	Upon detection of an internal fault during self-test, the SEF shall generate an audit record (sensor fault).		
RLB_104	There shall be no way to analyse or debug the motion sensor software in the field.	ADV_ARC.1 Security architecture description	ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.
RLB_105	Inputs from external sources shall not be accepted as executable code.	ADV_ARC.1 Security architecture description	ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from

SEF Identifier [Generic-ST, 4]	Requirement [Generic-ST, 4]	SFR/SAR Identifier [CC, Part 2/3]	Requirement [CC, Part 2/3]
			tampering by untrusted active entities.
RLB_106	If the motion sensor is designed so that it can be opened, the motion sensor shall detect any case opening, even without external power supply for a minimum of 6 months. In such a case, the SEF shall generate an audit record of the event (It is acceptable that the audit record is generated and stored after power supply reconnection). If the motion sensor is designed so that it cannot be opened, it shall be designed such that physical tampering attempts can be easily detected (e.g. through visual inspection).	The motion sensor is designed so it cannot be opened. FPT_PHP.1 Passive detection of physical attack	FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF. FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.
RLB_107	The motion sensor shall detect specified (TBD by manufacturer) hardware sabotage.		
RLB_108	In the case described above, the SEF shall generate an audit record and the motion sensor shall: (TBD by manufacturer).		
RLB_109	The motion sensor shall preserve a secure state during power supply cut-off or variations.	ADV_ARC.1 Security architecture description	ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.
RLB_110	In case of a power supply interruption, or if a transaction is stopped before completion, or on any other	ADV_ARC.1 Security architecture description	ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from

SEF Identifier [Generic-ST, 4]	Requirement [Generic-ST, 4]	SFR/SAR Identifier [CC, Part 2/3]	Requirement [CC, Part 2/3]
	reset conditions, the motion sensor shall be reset cleanly.		tampering by untrusted active entities.
RLB_111	The motion sensor shall ensure that access to resources is obtained when required and that resources are not requested nor retained unnecessarily.	ADV_ARC.1 Security architecture description	ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.
RLB_112	If the motion sensor provides applications other than the tachograph application, all applications shall be physically and/or logically separated from each other. These applications shall not share security data. Only one task shall be active at a time.	The motion sensor does not provide other applications	--
Data exchange			
DEX_101	The motion sensor shall export motion data to the VU with associated security attributes, such that the VU will be able to verify its integrity and authenticity.	FDP_DAU.1 Basic Data Authentication	FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **motion data**. FDP_DAU.1.2 The TSF shall provide **VU** with the ability to verify evidence of the validity of the indicated information.
Cryptographic support			
CSP_101	Any cryptographic operation performed by the motion sensor shall be in accordance with a specified algorithm and a specified key size.	FCS_COP.1 Cryptographic operation	FCS_COP.1.1 The TSF shall perform **encryption/decryption** in accordance with a specified cryptographic algorithm **Two Key Triple DES** and cryptographic key sizes **112 bits** that meet the following: **[ISO16844-3, 7.6] and [ANSI X3.92]**
CSP_102	If the motion sensor generates cryptographic keys,	The motion sensor does not	--

SEF Identifier [Generic-ST, 4]	Requirement [Generic-ST, 4]	SFR/SAR Identifier [CC, Part 2/3]	Requirement [CC, Part 2/3]
	it shall be in accordance with specified cryptographic key generation algorithms and specified cryptographic key sizes.	generate cryptographic keys.	
CSP_103	If the motion sensor distributes cryptographic keys, it shall be in accordance with specified key distribution methods.	FCS_CKM.2 Cryptographic key distribution	FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **distribution of pairing key** that meets the following: **[ISO16844-3, 7.4]**.
CSP_104	If the motion sensor accesses cryptographic keys, it shall be in accordance with specified cryptographic keys access methods.	FCS_CKM.3 Cryptographic key access	FCS_CKM.3.1 The TSF shall perform **cryptographic key access** in accordance with a specified cryptographic key access method **key access controlled by Security Module** that meets the following: **none**.
CSP_105	If the motion sensor destroys cryptographic keys, it shall be in accordance with specified cryptographic keys destruction methods.	FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting with new key data** that meets the following: **none**.

Table 6: Mapping of [EC, 1360-2002] requirements to CC requirements

6.2 Security Assurance Requirements

The SARs consist of Evaluation Assurance Level (EAL) 4 augmented by ATE_DPT.2 as defined in [CC, Part 3] which are the following:

- ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3,
- AGD_OPE.1, AGD_PRE.1,
- ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1
- ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1,
- ATE_COV.2, ATE_DPT.2, ATE_FUN.1, ATE_IND.2,

- AVA_VAN.3.

6.3 Security Requirements Rationale

The SARs have been chosen to provide at least the assurance of a vehicle unit which is defined in [VU-PP, 6.2]

The SFRs have been chosen to provide the identical functionality as required by [Generic-ST], see Table 6. A mapping of requirements to threats and objectives can be found in [Generic-ST, 8].

Note that although FMT_MSA.3 has formal dependencies to FMT_MSA.1 (Management of security attributes) and FMT_SMR.1 (Security roles), these dependencies do not need to be fulfilled in this ST as the security attributes of the TOE cannot be changed.

Also, FAU_GEN.1 has a formal dependency to FPT_STM.1 (Reliable time stamps). However, [Generic-ST] explicitly allows to use an appropriate default indication if audit record data is not available. In the current case the TOE is connected to the VU that receives the audit record from the TOE after an audit event has been recorded. The VU provides the mechanism to connect an decidated audit event to an timestamp.

Finally, as the TOE does not import nor generate cryptographic keys during operation, the dependency of FCS_COP.1 and FCS_CKM.2/3/4 to FCS_CKM.1 or FDP_ITC.1/2 need not be fulfilled in the TOE because the TOE is equiped with the required cryptographic key during personalisation at the manufacurer site.

Beyond that, all dependencies of the SFRs and SARs are fulfilled.

7 TOE Summary Specification

The cryptographic protocol between the Motion Sensor and the VU is specified in [ISO16844-3].

The Motion Sensor stores the following data in its non-volatile memory (FDP_ACF.1):

- N_S – extended serial number[2],
- ${}^{e}K_{ID(N_S)}$ – N_S encrypted with the identification key[3]
- K_P – pairing key[4]
- $e_K(K_P)$ – K_P encrypted with master key

It is assumed that BogArt generates the pairing keys and serial numbers and delivers them to MSCA-CSP for encryption. MSCA-CSP provides to BogArt the following personalization data:

- ${}^{e}K_{ID(N_S)}$ – N_S encrypted with the identification key[5]
- $e_K(K_P)$ – K_P encrypted with master key
- the TOE type code (to be a part of N_S)
- Operating System Identifier in the plain text (to be a part of N_S)
- Security Identifier in the plain text (to be a part of N_S)
- Name of the TOE manufacturer in plain text (to be a part of N_S)

It is also assumed that MSCA-CSP follows the personalization data provisioning as described in ALC_DVS, ALC_LCD, ALC_DEL and ALC_CMC.

All keys are Two Key Triple DES keys (112 bits) and all cryptographic operations are Triple DES operations in ECB mode, except the encryption of data files which are performed using the cipher block chaining (CBC) mode as specified in [ISO16844-3, 7.6] (FCS_COP.1).

The keys are stored in the Security Module embedded in the TOE and accessed using an application running on the Security Module (FCS_CKM.3). A session key is destroyed by overwriting it with a new session key (FCS_CKM.4) or by the Security Module software during error detection handling process (see 7.3). The TOE distributes the pairing key K_P in conformance with [ISO16844-3, 7.4] as described in the next section (FCS_CKM.2).

The Logical Security Function „Cryptographic Support" is realized by these cryptographic operations and is used throughout the protocol between motion sensor and vehicle unit which is described next.

[2] The extended serial number is 8 bytes long.
[3] The identification key is derived by xoring the master key with a constant value.
[4] Unique to MS
[5] The identification key is derived by xoring the master key with a constant value.

7.1 Pairing

The result of the pairing is a session key for encrypted data communication agreed between VU and MS. Moreover, pairing data from the VU containing VU specific information is securely transmitted to the MS for accountability reasons. The session key is stored permanently in the non-volatile memory of the motion sensor and is changed at every pairing, i.e. at a VU change [ISO16844-3, 7.4.5.2].

The pairing together with the communication protocol (section 7.2) realizes the Logical Security Function „Identification and Authentication".

The protocol for pairing can be summarized as follows (for details, see [ISO16844-3, 7.4.2, 7.2]):

1. MS → VU: N_S	VU encrypts serial number with identification key
2. VU → MS: ${}^{e}K_{ID(N_S)}$	MS verifies ${}^{e}K_{ID(N_S)}$ with stored value, on success: VU auth'd
3. MS → VU: $e_K(K_P)$	VU decrypts pairing key, encrypts session key w/ pairing key
4. VU → MS: $e_{Kp}(K_S)$, $e_{Kp}(P_D)$	MS decrypts session key and pairing data[6] with pairing key and encrypts paring data with session key
5. MS → VU: $e_{Ks}(P_D)$	VU decrypts pairing data w/ session key, on succ: MS auth'd

The pairing data sent in step 4 by the VU shall contains the VU type approval number and the VU serial number (FIA_UID.2). It is stored for later auditing (FAU_GEN.1). Only after having successfully established a session key any other TSF-mediated action on behalf of the VU is possible. No other entity (e.g. management device) is supported to connect to the MS (FIA_UID.2).

It should be noted that steps 1 and 2 perform a very weak authentication of the VU. A stronger authentication is achieved by the fact that only devices which know the master key e_K can decrypt the pairing key K_P and can use it to agree on the session key K_S and pairing data P_D with the MS (FIA_UAU.2).

If authentication data in step 4 has been forged the MS does not detect the forged data during the pairing. The VU detects the forged data in step 5. Moreover, the MS detects the forged data because of invalid authentication data (encrypted and/or decrypted with an incorrect session key) during the communication (section 7.2), and will stop the communication process, thus preventing the use of forged data (FIA_UAU.3). In this case, the session key must be re-generated by a new pairing process.

After the first unsuccessful authentication attempt (i.e. the pairing fails) the MS generates an audit record and warns the VU by setting the error flag (NARA flag) that triggers the VU to read the audit record. In that case the MS continues to export motion data in a non secured mode (FIA_AFL.1).

[6] The pairing data is 24 bytes long and its value depends on the date of pairing, the N_S and VU serial numbers, a random number, and the VU type approval number [ISO16844-3]. At decryption, the VU checks the validity of the pairing data.

7.2 Communication

Sensor data is exchanged as follows to ensure the confidentiality and authenticity (for details, see [ISO16844-3, 7.5]):

1. VU → MS: $e_{Ks}(D_A)$ MS decrypts and checks auth data[7], on success: VU auth'd
2. MS → VU: $e_{Ks}(D_S)$ VU decrypts and checks sensor data

Thereby, the VU is re-authenticated before each transfer of sensor data from the MS to the VU (FIA_UAU.6), specifically also after entity connection to the same VU and after a power supply recovery (FIA_UAU.2). A MS and a VU which have not been paired before (cf. Section 7.1) do not share the same session key K_S. In that case the authentication of the VU would fail.

The sensor data exchange partially realizes the Logical Security Function „Access Control & Accountability" by allowing only the authenticated VU to read sensor data (FDP_ACC.1, FDP_ACF.1).

Note that the sensor data sent from the MS to the VU contains 4 bytes of integrity check data derived from the auth data as part of the encrypted data of size 8 bytes. Thereby the VU is able to verify the integrity and authenticity of the motion data sent by the MS (FDP_DAU.1).

These part of the protocol realizes the Logical Security Function „Data exchange".

7.3 Read information

File data is exchanged as follows to ensure the confidentiality and authenticity (for details, see [ISO16844-3, 7.6]):

1. VU → MS: $e_{Ks}(D_A)$ MS decrypts and checks auth data (contains file number)
2. MS → VU: $e_{Ks}(D_{FS})$ VU decrypts and checks file data[8]

The file data exchange partially realizes the Logical Security Function „Access Control & Accountability" by allowing only the authenticated VU to write user data (file number 2 and 3) and to read the file. Write operations of sensor identification data are not possible after manufacturing (FDP_ACC.1, FDP_ACF.1).

The access control policy is enforced using restrictive default security attributes which cannot be changed (FMT_MSA.3).

Note that for file data transfer the auth data is used also as the initialization vector for the Two Key Triple DES encryption in CBC mode.

The following file numbers are supported:

[7] Auth data consists of a 4 bytes random number and 4 bytes control information.
[8] File data contains 4 bytes of integrity check data derived from auth data.

- 0 – audit record
- 1 – OS identifier (e.g., firmware version)
- 2 – pairing data of first pairing
- 3 – pairing data of last pairing
- 4 – extended serial number N_S
- 5 – security identifier of motion sensor
- 6 – type approval of motion sensor

The Logical Security Function „Audit" is realized using the file system of the TOE. File number „0" stores the latest audit record. Due to this architecture the audit record is sent to the VU only if the VU requests the file number „0". Beyond that, audit records are not stored in memory (FAU_GEN.1).

This audit record contains the actual random number of the previous instruction and supports the following (error) events (FAU_GEN.1):

- non-volatile memory (stored data integrity error)
- controller RAM (stored data integrity error)
- controller-instruction
- communication (internal data transfer error)
- authentication (authentication failure)
- sensor element (sensor fault)

To detect stored data integrity error, the MS generates a checksum of the stored bytes and compares it with a reference value on every read (FDP_SDI.2).

To detect a sensor fault, the MS runs self-tests during initial start-up and during normal operation. These self-tests verify the integrity of executable code of the main microcontroller that is stored in the non-volatile memory The self-tests also verify the correct operation of the motion sensor. In case a fault is detected a sensor fault audit record is created (FPT_TST.1).

The security module of the MS also monitors application code, application data and application keys for integrity errors. Upon detection of an integrity error for application keys, the security module locks the card session. Upon detection of an integrity error for the application code/data it throws a SecurityException and sets a register bit which is checked by the TOE. The TOE then generates an audit record (sensor fault) and all keys will be deleted (FPT_TST.1, FAU_GEN.1).

An additional Hall sensor detects external magnetic fields. If a magnetic field is detected, the MS is reset.

Please note the following restriction in context of auditing (FAU_GEN.1):

- As only failure events (errors) are logged, the outcome need not be logged explicitely.
- The sensor is designed so it cannot be opened. Therefore a case opening need not be

detected nor logged.

- Hardware sabotage is detected by the sealing of the motion sensor case (FPT_PHP.1).
- As a time source is not available, the actual random number of the instruction when the error is detected is logged.
- The subject identity (VU identity) is available as part of the pairing data (see section 7.1).
- There is no start-up or shutdown of audit functions. The audit functionality is „always on". Therefore the start-up and shutdown of the function cannot be logged.

The self-tests, integrity checks and sealing of the TOE realize Security Function „Accuray & Reliablity of Service".

8 Abbreviations, Terms and Definitions

The abbreviations and definitions of [Generic-ST, 2.1f.] and [CC] apply. All additional abbreviation, terms and definition are listed in the following tables.

Term	Definition
Accountability Data	Pairing data, File 0-6, NARA flag, RESET flag, the pulse counter, the duty cycle
Management device	A management device is used to manage the TOE, e. g. for updating other devices. The TOE does not have this capability and no data to authenticate or identify such devices. Therefore there is no functionality for management devices implemented by the TOE.
User Data	Pairing data, File 0 (reset only)

Abbreviation	Description
DTMS	Digital Tachograph Motion Sensor
PCB	Printed Circuit Board
MSCA-CSP	Member State Certificate Authority – Certification Services Provider

9 References

Reference	Referenced document
ANSI X3.92	ANSI X3.92-1981, Data Encryption Algorithm, American National Standards Institute
EC 1360/2002	COMMISSION REGULATION (EC) No 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport
Generic-ST	[EC 1360/2002, Appendix 10: Motion sensor generic security target]
ISO16844-3	Road vehicles – Tachograph systems – Part 3: Motion sensor interface (Technical corrigendum 1 applyed), ISO 16844-3:2004(E)
CC	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4

VU-PP	Common Criteria Protection Profile, Digital Tachograph – Vehicle Unit (VU PP), BSI-CC-PP-0057, Version 1.0, 13th July 2010
AGD	Guidance documentation for BogArt Motion Sensor, Version 1.0
Platform-ST	NXP J3E081 M64, J3E081 M66, J2E081 M64, J3E041 M66, J3E016 M66, J3E016 M64, J3E041 M64 Secure Smart Card Controller Revision 3 Security Target Lite, Rev. 00.01, 25th July 2013, NXP Semiconductors
Platform-Cert	NXP J3E081 M64, J3E081 M66, J2E081 M64, J3E041 M66, J3E016 M66, J3E016 M64, J3E041 M64 Secure Smart Card Controller Revision 3, Certification Report, NSCIB-CC-13-37761-CR, Version 1, Wouter Slegers, August 5th, 2013