Federal Office
for Information Security

Certification Report

BSI-DSZ-ITSEC-0681-2011

for

KITAS 2171 Motion Sensor, Version 1.11

from

Continental Automotive GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-ITSEC-0681-2011

KITAS 2171 Motion Sensor, Version 1.11

from	Continental Automotive GmbH
Functionality:	according to Appendix 10 of Annex IB of Council Regulation (EEC) No. 3821/85 amended by Council Regulation (EC) No. 1360/2002 and last amended by Council Regulation (EC) No. 69/2009 and by CR (EU) No. 1266/2009 on recording equipment in road transport
Assurance:	E3 Strength of Mechanisms: high

for components up to E3

The IT product identified in this certificate has been evaluated at an approved evaluation facility evaluation facility using the Information Technology Security Evaluation Criteria (ITSEC), version 1.2, June 1991 and the Information Technology Security Evaluation Manual (ITSEM), version 1.0, September 1993. extended by motion sensor specific guidance according to Appendix 10 of Annex IB of Council Regulation (EEC) No. 3821/85 amended by Council Regulation (EC) No. 1360/2002 and last amended by Council Regulation (EC) No. 69/2009 and by CR (EU) No. 1266/2009 on recording equipment in road transport.

The rating of the strength of mechanisms does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The confirmed evaluation level only applies on the condition that all stipulations regarding generation, configuration and operation as far as specified in the Certification Results are kept and that the product is operated in the environment described, where one is specified.

This certificate is only valid in conjunction with the complete Certification Report.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 13 January 2011
For the Federal Office for Information Security

Bernd Kowalski L.S.
Head of Department

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

Contents

A Certification.....7

1 Specifications of the Certification Procedure.....7

2 Recognition Agreements.....8

2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA).....8

2.2 International Recognition of CC – Certificates (CCRA).....8

3 Performance of Evaluation and Certification.....9

4 Validity of the certification result.....9

5 Publication.....10

B Certification Results.....11

1 Security Target and Scope of the Evaluation.....12

1.1 Executive Summary of the Security Target.....12

1.2 Subjects.....13

1.3 Objects.....14

1.4 Security Objectives and Threats.....15

1.5 Security Functions and Mechanisms.....15

1.6 Level of Evaluations and Strength of Mechanisms.....15

2 Evaluation Results.....15

2.1 Effectiveness – Construction.....16

2.2 Effectiveness - Operation.....17

2.3 Correctness - Construction - Development Process.....18

2.4 Correctness - Construction - Development Environment.....19

2.5 Correctness - Operation - Operational Documentation.....20

2.6 Correctness - Operation - Operational Environment.....20

3 Obligations and Notes for the Usage of the TOE.....21

4 Abbreviations.....22

5 Definitions.....22

6 Literature and References.....24

C Excerpts from the Criteria.....25

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [4]
- Information Technology Security Evaluation Criteria (ITSEC), version 1.2, June 1991[5] [1]
- Information Technology Security Evaluation Manual (ITSEM), version 1.0, September 1993 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS / JIL) [3]

[2] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

[5] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic).

The new agreement was initially signed by the national bodies of Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom.

Within the terms of this agreement the German Federal Office for Information Security (BSI) recognises

- for the basic recognition level certificates issued as of April 2010 by the national certification bodies of France, The Netherlands, Spain and the United Kingdom.
- for the higher recognition level in the technical domain Smart card and similar Devices certificates issued as of April 2010 by the national certification bodies of France, The Netherlands and the United Kingdom.

In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

Historically, the first SOGIS-Mutual Recognition Agreement Version 1 (ITSEC only) became initially effective in March 1998. It was extended in 1999 to include certificates based on the Common Criteria (MRA Version 2). Recognition of certificates previously issued under these older versions of the SOGIS-Mutual Recognition Agreement is being continued.

2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 has been signed in May 2000 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC.

As of February 2007 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations resp. approved certification schemes can be seen on the web site: http:\\www.commoncriteriaportal.org

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product KITAS 2171 Motion Sensor, Version 1.11 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-ITSEC-0271-2004. Specific results from the evaluation process based on BSI-DSZ-ITSEC-0271-2004 were re-used.

The evaluation of the product KITAS 2171 Motion Sensor, Version 1.11 was conducted by T-Systems GEI GmbH. The evaluation was completed on 13 January 2011. The T-Systems GEI GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Continental Automotive GmbH.

The product was developed by: Continental Automotive GmbH.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

The confirmed evaluation level and minimum strength of mechanisms is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report.

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

For the meaning of the evaluation levels and the confirmed strength of mechanisms, please refer to the excerpts from the criteria at the end of the Certification Report.

4 Validity of the certification result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report and in the Security Target.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product KITAS 2171 Motion Sensor, Version 1.11 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Continental Automotive GmbH
Heinrich-Hertz-Strasse 45
78052 Villingen
Germany

B Certification Results

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.

1 Security Target [8] and Scope of the Evaluation

The complete Security Target [6] of the target of evaluation (TOE) is used for the evaluation. The following chapter gives a brief summary.

1.1 Executive Summary of the Security Target

The Target of Evaluation (TOE) is KITAS 2171 Motion Sensor, Version 1.11. This TOE is a product intended to be installed in road transport vehicles. Its purpose is to provide a VU with secured motion data representative of vehicle's speed and distance travelled. The Motion Sensor is mechanically interfaced to a moving part of the vehicle, which movement can be representative of vehicle's speed or distance travelled. It may be located in the vehicle's gear box or in any other part of the vehicle. It may also be connected to specific equipment for management purposes. In the case of the KITAS 2171 Motion Sensor, it will only be connected to specific equipment during the manufacturing process to initialise the device. In the field no specific equipment will be connected. Also workshops will not perform any management or repair operations but replace a faulty Motion Sensor by a new one.

For more details please refer to Security Target [6, chapter 5.1].

This is a re-certification based on BSI-DSZ-ITSEC-0271-2004. The main reason for the re-certification was the Council Regulation (EC) No. 69/2009 and CR (EU) No. 1266/2009 on recording equipment in road transport.

The Security Target is based on the Motion Sensor Generic Security Target [12], which is described in Appendix 10 of Annex IB [10] of Council Regulation (EC) No. 1360/2002 - Generic Security Targets.

The following figure shows the basic architecture of the actual TOE, the Motion Sensor KITAS 2171 (**KI**enzle **TA**chograph **S**ensor) and of the Motion Sensor of the DTCO (**D**igital **T**a**C**h**O**graph).

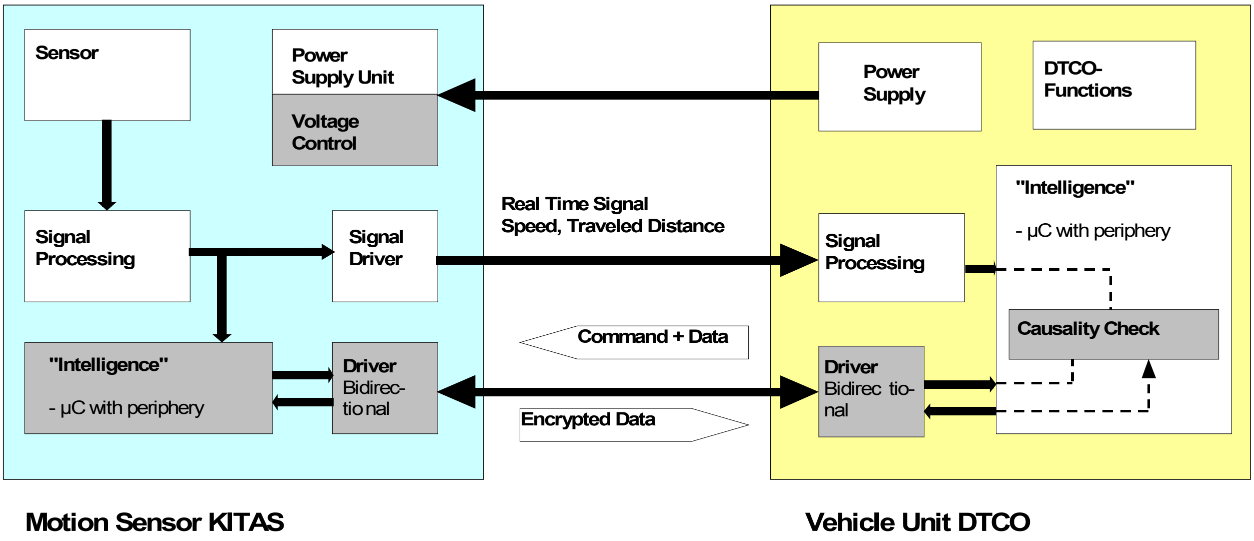

Figure 1 Architecture of the TOE

[8] The security target was made available by the sponsor.

There is a microcontroller integrated in the Motion Sensor KITAS 2171, Version 1.11. One of the two signalling channels carries the sensor signal (speed, travelled distance) to the DTCO in real time. The other one acts as a bi-directional channel. The distance signal is added to an impulse counter in both the Motion Sensor and the DTCO.

The value of the impulse counter in the Motion Sensor KITAS 2171 is transmitted encrypted on a periodic request of the DTCO. It is decrypted and checked for equality in the DTCO. A deviation is interpreted as manipulation. The DTCO acts as master and controls the integrity/completeness of the plaintext signal.

The KITAS Motion Sensor has been equipped with cryptographic functions for data transfer. In this context the standardised procedure Triple-DES (Data Encryption Standard) with 2 keys is used.

Authentication information for an unequivocal assignment between the KITAS Motion Sensor and the DTCO is stored during the initialisation phase. The authenticity of signals transferred over the bi-directional channel is proved with this information.

Cases of manipulation of the power supply or one of the two signalling channels are detected by the system. A substitution of the Motion Sensor is also detected, since the DTCO and the KITAS Motion Sensor are unequivocally assigned during the initialisation phase.

The real time signal (speed and travelled distance) itself is being transferred in plaintext, since there are no requirements for confidentiality of the signal itself.

The physical construction of the Motion Sensor KITAS is of a way that opening the KITAS box isn't possible without destroying it. This way a manipulation gets obvious. Furthermore the Motion Sensor is sealed at the gearbox.

For further information refer to Security Target [6, chapter 5.2].

The following Table 1 outlines the TOE deliverables:

No	Type	Description	Version	Type of delievery
1	Hardware Motion Sensor	Motion Sensor KITAS 2171, Version 1.11	V1.11	Hardware
2	Software	COP08	V1.09	Software
3	Software	2. Microcontroller (with dynamic und static detection of the magnet manipulation)	V2.0	Software
4	Documentation	KITAS 2171 Weg- und Geschwindigkeitsgeber – Installationsbeschreibung, Version 1.3, Continental Automotive GmbH, 26.03.2010	V1.3	as paper

Table 1: Deliverables of the TOE

1.2 Subjects

For the Motion Sensor KITAS 2171 the following types of subjects exist:

S1: Entities:

S1.1: Installation device in the manufacturing process
S1.2: Vehicle unit in pairing and operational mode with the Motion Sensor

S2: Users:

S2.1: Drivers and co-drivers (in operational mode)
S2.2: Workshop staff, fitters and staff of vehicle manufacturers (in calibration mode)
S2.3: Control officers from national control authorities (in control mode)
S2.4: Staff of the respective haulage company (in company mode)

Note: The human users S2.1 to S2.4 of the recording equipment in road transport vehicles are subjects of the vehicle unit in the tachograph system and have not direct access to the Motion Sensor. They will access it indirectly through the vehicle unit only. So any authentication and access control function for those users is performed by the vehicle unit. The Motion Sensor itself does not need to know which human user currently accessing the system.

1.3 Objects

For the specification of the security functions of the Motion Sensor KITAS 2171. the following objects are relevant. Definitions of data objects are provided in the Appendix 10 and 11([12] and [13]) of Annex IB [9].

O1: motion data representative of vehicle's speed and distance travelled:

O1.1: impulses (real time signal)
O1.2: impulse counter

O2: Data of file No. 0 (Error messages for audit records)

O2.1: Actual random number
O2.2: Kind of error (EEPROM error, authentication failure, self testing errors ...) for audit records

O3: Data of file No. 1 (Operating system identifier)

O3.1: SensorOSIdentifier (Identifier of the operating system – Firmware version - of the Motion Sensor)

O4: Data of file No. 2 (First pairing information)

O4.1: SensorPairingDateFirst
O4.2: FirstVUApprovalNumber
O4.3: FirstVUSerialNumber

O5: Data of file No. 3 (Current pairing information)

O5.1: SensorPairingDateCurrent
O5.2: CurrentVUApprovalNumber
O5.3: CurrentVUSerialNumber

O6: Data of file No.4 (Extended serial number N_s)

O6.1: SerialNumber (Serial number for the Motion Sensor, unique for the manufacturer, the type and the month below)
O6.2: MonthYear (Date of production)
O6.3: Type (type of the Motion Sensor)
O6.4: ManufacturerCode (numerical code of the manufacturer of the equipment)

O7: Data of file No. 5 (Security identifier)

O7.1: SensorSCIdentifier (Identifier of the security component - processor part-type - of the Motion Sensor)

O8: Data of file No. 6 (Approval number)

O8.1: SensorApprovalNumber (type approval number of the sensor)

O9: Security data to be stored in the Motion Sensor

O9.1: K_p (sensor specific pairing key)

O9.2: $e_k(N_s)$ (extended serial number of the Motion Sensor encrypted with the Master key)

O9.3: $e_k(K_p)$ (sensor specific pairing key encrypted with the Master key)

O10: Security data to generate and to be stored in the Motion Sensor

O10.1: K_s (session key)

O11: Security data not stored in the Motion Sensor

O11.1: K (Master key)

1.4 Security Objectives and Threats

Security objectives and threats are described in the Security Target [6, chapter 5.5 to 5.7].

1.5 Security Functions and Mechanisms

The following security functions are implemented in the TOE:

TOE Security Functions	Addressed issue
SEF1	Identification and authentication [6, chapter 6.1]
SEF2	Access control [6, chapter 6.2]
SEF3	Accountability [6, chapter 6.3]
SEF4	Audit [6, chapter 6.4]
SEF5	Accuracy [6, chapter 6.5]
SEF6	Reliability of service [6, chapter 6.6]
SEF7	Data exchange [6, chapter 6.7]
SEF8	Cryptographic support [6, chapter 6.8]

Table 2: Overview of the security functions

For more details about the security functions refer to the Security Target [6, chapter 6]. A rationale of the security functions is given in the Security Target [6, chapter 10].

The required security mechanisms are specified in Appendix 11 [13]. The TOE implements all necessary security mechanisms.

1.6 Level of Evaluations and Strength of Mechanisms

The minimum strength of the Motion Sensor security mechanisms is **high**, as defined in ITSEC [1]. The target level of assurance for the Motion Sensor is ITSEC level **E3**, as defined in ITSEC [1].

2 Evaluation Results

The TOE provides the functionality according to Appendix 10 of Annex IB of Regulation (EC) no. 1360/2002 [10].

2.1 Effectiveness – Construction

2.1.1 Analysis of Suitability of the Functionalities

The suitability analysis assigns the security enforcing functions and mechanisms to the threats which have been identified in the Security Target and detailed design and which it counteracts. It also shows how the security enforcing functions and mechanisms counteract the identified threats and that there are no identified threats which are not adequately counteracted by one or more of the listed security enforcing functions.

The evaluation facility has examined, that the suitability analysis meets all the requirements with regard to content, presentation and evidence and that the analysis has used all the relevant information.

2.1.2 Analysis of the Binding of the Functionalities

This analysis of the binding concerns all the possible relationships between the security enforcing functions and mechanisms. It shows that a security enforcing function or mechanism cannot be made to conflict with or counteract the tasks of other security enforcing functions or mechanisms.

The evaluation facility has examined, that the analysis of the binding meets all the requirements with regard to content, presentation and evidence and that the analysis has used all the relevant information.

2.1.3 Analysis of the Strength of Mechanisms

The ability of the mechanisms to counteract direct attacks has been evaluated.

The analysis of the strength of mechanisms lists all security enforcing mechanisms as critical within the TOE. It contains analyses of the algorithms and principles underlying these mechanisms. The analysis of the strength of mechanisms has shown, that all mechanisms identified as critical, fulfil the claimed strength of mechanism.

The evaluation facility has examined, that all critical mechanisms have been identified as such. The evaluation facility has examined, that analysis of the strength of mechanisms, as submitted, meets all the requirements with regard to content, presentation and evidence and that the analysis has used all the relevant information. The evaluation facility has examined, that all mechanisms identified as critical, fulfil the claimed strength of mechanism.

The rating of the strength of mechanisms does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

2.1.4 Constructional Vulnerabilities

The developer has provided a list of known vulnerabilities. These known vulnerabilities have been assessed to determine whether they could in practice compromise the security of the TOE as specified by the Security Target.

The analysis of the potential impact of each known vulnerability shows that the vulnerabilities in question cannot be exploited in the intended environment for the TOE because either the vulnerability is adequately covered by other uncompromised security mechanisms or it could be shown that the vulnerability is irrelevant to the Security Target, will not exist in practice or can be countered adequately by documented technical, personnel, procedural or physical security measures outside the TOE. These external security measures have been defined within the appropriate documentation.

The evaluation facility has examined, that the list of known vulnerabilities meets all the requirements with regard to content, presentation and evidence and that the analysis has used all the relevant information. The evaluation facility has performed an independent vulnerability analysis. It has checked that all combinations of known vulnerabilities have been addressed. It has checked that the analyses of the potential impact of vulnerabilities contain no undocumented or unreasonable assumptions about the intended environment. It has checked that all assumptions and requirements for external security measures have been appropriately documented.

2.2 Effectiveness - Operation

2.2.1 Ease of Use Analysis

The TOE cannot be configured or used in a manner which is insecure but which an administrator or user of the TOE would reasonably believe to be secure.

The evaluation facility has examined, that the ease of use analysis provided meets all the requirements with regard to content, presentation and evidence and that the analysis has used all the relevant information. The analysis has been checked for undocumented or unreasonable assumptions about the intended environment. The evaluation facility has checked that all assumptions and requirements for external security measures have been appropriately documented. The procedure for configuration has been assessed to examine, that the TOE can be configured and used in a secure manner.

2.2.2 Operational Vulnerabilities

The evaluation facility has examined, that the list of known operational vulnerabilities meets all the requirements with regard to content, presentation and evidence and that the analysis has used all the relevant information. The evaluation facility has performed an independent vulnerability analysis under consideration of the listed vulnerabilities and those found during the evaluation process. It has checked that all combinations of known vulnerabilities have been addressed. It has checked that the analyses of the potential impact of vulnerabilities contain no undocumented or unreasonable assumptions about the intended environment. It has checked that all assumptions and requirements for external security measures have been appropriately documented.

2.3 Correctness - Construction - Development Process

2.3.1 Security Target

The Security Target [6] describes the security enforcing functions provided by the TOE. They contain specifications identifying the way in which the product is used, the intended operational environment and the threats assumed for this operational environment. The security enforcing functions listed in the Security Target are specified using an informal notation. The Security Target explains, why the functionality is appropriate for this type of use and how it counteracts the threats.

The Security Target correspond fully to the generic Security Target [12] for the Motion Sensor.

The evaluation facility has examined, that the information provided meets all the requirements with regard to content, presentation and evidence and that there are no inconsistencies within the Security Target.

2.3.2 Architectural Design

The architectural design describes the general structure and all external interfaces of the TOE. It describes the separation of the TOE into security enforcing and other components and how the security enforcing functions are provided.

The evaluation facility has examined, that the information provided meets all the requirements with regard to content, presentation and evidence.

2.3.3 Detailed Design

The detailed design describes the realisation of all security enforcing and security relevant functions. It specifies all basic components, identifies all security mechanisms and maps the security enforcing functions to mechanisms and components. All interfaces of the security enforcing and security relevant components are documented together with their purposes and parameters. Specifications for the mechanisms have been provided. These specifications are suitable for the analysis interrelationships between the mechanisms employed. The detailed design describes how the security mechanisms realise the security enforcing functions as specified in the Security Target.

The evaluation facility has examined, that the information provided meets all the requirements with regard to content, presentation and evidence.

2.3.4 Implementation

The test documentation contains the test plan, test objectives, test procedures and test results. The library of test programs contains test programs and test tools which are suitable for repeating all the tests described in the test documentation. This documentation describes the correspondence between the tests and

- the security enforcing functions as described in the Security Target,
- the security relevant and security enforcing functions and mechanisms as defined in the detailed design,
- and the security mechanism as described in the source code.

All tests show the expected results.

A description of correspondence describes the correspondence between source code and basic components of the detailed design.

The evaluation facility has examined, that the information provided meets all the requirements with regard to content, presentation and evidence. The library of test programs was used to check by sampling the test results. The evaluation facility has examined, that the tests cover all security enforcing and security relevant functions. Additional tests were performed to search for errors.

2.4 Correctness - Construction - Development Environment

2.4.1 Configuration Control

The development process is supported by a tool based configuration control system and an acceptance procedure. The configuration list provided enumerates all basic components of the TOE. The TOE, its basic components and all documents that have been supplied, including the manuals and the source code, have unique identification. This identification is used in references. The configuration control system ensures that the TOE corresponds to the documentation which has been supplied and that only authorised changes are possible.

The information on the configuration control system describe the use of the system in practice and how it can be used in the development process together with the vendor’s quality management procedure.

The evaluation facility has examined, that the documented procedures are applied and that the information provided meets all the requirements with regard to content, presentation and evidence.

2.4.2 Programming Languages and Compilers

For the implementation of the TOE C compiler and the assembler for the Motion Sensor microprocessors were used. All used instructions and statements of the assembler are completely and clearly defined so that the meaning of all instructions and statements used in the source code are unambiguously defined.

The evaluation facility has examined, that the information provided meets all the requirements with regard to content, presentation and evidence.

2.4.3 Security in the Developer’s Environment

The document on the security of the developer’s environment describes the measures taken to protect the integrity of the TOE and the confidentiality of the relevant documents. Descriptions of the physical, personnel and procedural security measures as used by the developer were provided.

The evaluation facility has examined, that the documented procedures are applied and that the information provided meets all the requirements with regard to content, presentation and evidence. The evaluation facility has searched for errors in the procedures.

The TOE was developed and manufactured by: Continental Automotive GmbH, Heinrich-Hertz-Strasse 45, 78052 Villingen, Germany

2.5 Correctness - Operation - Operational Documentation

2.5.1 User Documentation

The user documentation [8] and [9] describes the usage and the security enforcing functions relevant to the unprivileged user. The description of the functions is provided in a way understandable for the user.

The evaluation facility has examined that the information provided meets all the requirements with regard to content, presentation and evidence.

2.5.2 Administrators Documentation

The technical product documentation targeted to the authorised workshop staff, fitters and Motion Sensors manufactures is considered as the administration documentation [7] in this case. This documentation is structured, internally consistent, and consistent with all other documents supplied for this level.

The evaluation facility has examined, that the information provided meets all the requirements with regard to content, presentation and evidence.

2.6 Correctness - Operation - Operational Environment

2.6.1 Delivery and Configuration

The procedure for delivery is described. A procedure approved by BSI for this evaluation level is applied to guarantee the authenticity of the delivered TOE. The information supplied describes how the described procedures maintain security.

The evaluation facility has examined, that the information provided meets all the requirements with regard to content, presentation and evidence.

The TOE deliverables are listed in the Table 1.

2.6.2 Start-up and Operation

Secure start-up and operation is guaranteed by the secure state of the TOE at start-up and operation.

The evaluation facility has examined, that the information provided meets all the requirements with regard to content, presentation and evidence.

3 Obligations and Notes for the Usage of the TOE

In addition all aspects of assumptions, threats physical personnel and procedural means as outlined in the Security Target are not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The evaluators recommend in line with periodical checkups to obey following recommendations:

- Following the documentation [9, chapter 8, p. 77], the control officer or fitter has to check the graving of the metal case.
- As described in [9, chapter 8, p. 77], the lead sealing shall be checked.
- By the electrical checking, a break of voltage should be checked (check of voltageflag [9, chapter 8, p. 111]). A break of voltage could occur when vehicles has been set disused for a time or it also could be a sign for manipulation.

One or more abnormalities which can’t be explained should lead to a detailed checking of the complete system to detect potential attack efforts. In this case the motion sensor should be taken out of the gearbox by a qualified workshop for detailed check, e.g. with magnifier, e.g. cable check to motion sensor as described in [16. chapter 11, p. 215]. KITAS parameters should be screened by the qualified workshop for inconsistencies, as described [16. chapter 11, p. 215] a recalibration of the KITAS has to be done in case of inconsistencies.

4 Abbreviations

DTCO	Digital Tachograph
e	encrypted
K	Master key
K_p	sensor-specific pairing key
K_s	session key
KITAS	Kienzle Tachograph Sensor
N_s	Extended Serial-Number
ROM	Read Only Memory
SEF	Security Enforcing Function
TBD	To be defined
TOE	Target of Evaluation
VU	Vehicle Unit

5 Definitions

Digital Tachograph Recording Equipment

Entity A device connected to the motion sensor (specific definition see subject S1, Chapter 1.2)

Motion data The data exchanged with the VU, representative of speed and distance travelled (specific definition see object O1, Chapter 1.3)

Motion Sensor Part of the recording equipment, providing a signal representative of vehicle speed and/or distance travelled.

Physically separated parts Physical components of the motion sensor that are distributed in the vehicle as opposed to physical components gathered into the motion sensor casing

Recording Equipment The total equipment intended for installation in road vehicles to show, record and store automatically or semi-automatically details of the movement of such vehicles and of certain work periods of their drivers

Security data The specific data needed to support security enforcing functions (e.g. crypto keys). (specific definition see objects O9, O11)

System Equipment, people or organisations involved in any way with the recording equipment

User A human user of the motion sensor (when not used in the expression “user data”, specific definition see subject S2)

User data Any data, other than motion or security data, recorded or stored by the motion sensor. (specific definition see objects O2, O3, O4, O5, O6, O7, O8)

Vehicle Unit The recording equipment excluding the motion sensor and the cables connecting the motion sensor. The vehicle unit may either be a single unit or be several units distributed in the vehicle, as long as it complies with the security requirements of Appendix 10 [12] of Annex IB [10] of Council Regulation (EC) No. 1360/2002

6 Literature and References

[1] Information Technology Security Evaluation Criteria (ITSEC), version 1.2, June 1991

[2] Information Technology Security Evaluation Manual (ITSEM), Version 1.0, September 1993

[3] ITSEC Joint Interpretation Library (ITSEC JIL), Version 2.0, November 1998

[4] BSI certification: Procedural Description (BSI 7125, Version 5.1, January 1998)

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Website

[6] Security Target, KITAS 2171, Version 1.11, Digital Tachograph - Motion Sensor, Version 1.5, 2011-01-10, Continental Automotive GmbH

[7] Digitaler Tachograph DTCO 1381, Technische Beschreibung, TD00.1381.00 120 101-OPM 000 AA, Siemens VDO Automotive

[8] KITAS 2171 Weg- und Geschwindigkeitsgeber – Installationsbeschreibung, Version 1.3, Continental Automotive GmbH, 2010-03-26

[9] Digitaler Tachograph – DTCO 1381, Leitfaden für die Kontrollorgane, Version 09.08, Continental Automotive GmbH

[10] Appendix 10 of Annex IB of Council Regulation (EEC) No. 3821/85 amended by Council Regulation (EC) No. 1360/2002 and last amended by Council Regulation (EC) No. 69/2009 and by CR (EU) No. 1266/2009 on recording equipment in road transport

[11] Appendix 8 of Annex IB of Council Regulation (EC) No. 1360/2002 – Calibration Protocol

[12] Appendix 10 of Annex IB of Council Regulation (EC) No. 1360/2002 - Generic Security Targets

[13] Appendix 11 of Annex IB of Council Regulation (EC) No. 1360/2002 – Common Security Mechanisms

[14] Joint Interpretation Library (JIL): Security Evaluation and Certification of Digital Tachographs, JIL interpretation of the Security Certification according to Commission Regulation (EC) 1360/2002, Annex IB, Version 1.12, June 2003

[15] Technischer Evaluationsbericht, Geschwindigkeits- und Weggeber KITAS 2171, Version 1.11 Continental, Version 1.2, 2011-01-12, T-Systems (Confidential document)

[16] Digitaler Tachograph DTCO 1381, Dokument: TD00.1381.00 133 101 – OPM 000 AA, Release 1.3, Continental Automotive GmbH, Ausgabe 07/2008

C Excerpts from the Criteria

The following quotes from the ITSEC and ITSEM describe the requirements for the specified product and explain the assurance levels achieved.

Six levels for correctness and effectiveness are defined for assessment of the assurance. E1 designates the lowest level and E6 designates the highest level defined here.

The abbreviation TOE (Target Of Evaluation) used means the certified product. The Section numbers have been taken from the ITSEC rsp. ITSEM.

1 Effectiveness

ITSEC:

”Assessment of effectiveness involves consideration of the following aspects of the TOE:

a) the suitability of the TOE’s security enforcing functions to counter the threats to the security of the TOE identified in the security target;

b) the ability of the TOE’s security enforcing functions and mechanisms to bind together in a way that is mutually supportive and provides an integrated and effective whole;

c) the ability of the TOE’s security mechanisms to withstand direct attack;

d) whether known security vulnerabilities in the construction of the TOE could in practice compromise the security of the TOE;

e) that the TOE cannot be configured or used in a manner which is insecure but which an administrator or end-user of the TOE would reasonably believe to be secure;

f) whether known security vulnerabilities in the operation of the TOE could in practice compromise the security of the TOE.”

2 Correctness

ITSEC:

”The seven evaluation levels can be characterised as follows:”

Level E0

4.4 This level represents inadequate assurance.

Level E1

4.5 At this level there shall be a security target and an informal description of the architectural design of the TOE. Functional testing shall indicate that the TOE satisfies its security target.

Level E2

4.6 In addition to the requirements for level E1, there shall be an informal description of the detailed design. Evidence of functional testing shall be evaluated. There shall be a configuration control system and an approved distribution procedure.

Level E3

4.7 In addition to the requirements for level E2, the source code and/or hardware drawings corresponding to the security mechanisms shall be evaluated. Evidence of testing of those mechanisms shall be evaluated.

Level E4

4.8 In addition to the requirements for level E3, there shall be an underlying formal model of security policy supporting the security target. The security enforcing functions, the architectural design and the detailed design shall be specified in a semiformal style.

Level E5

4.9 In addition to the requirements for level E4, there shall be a close correspondence between the detailed design and the source code and/or hardware drawings.

Level E6

4.10 In addition to the requirements for level E5, the security enforcing functions and the architectural design shall be specified in a formal style, consistent with the specified underlying formal model of security policy.”

3 Classification of Security Mechanisms

ITSEM:

”6.C.4 A type A mechanism is a security mechanism with a potential vulnerability in its algorithm, principles or properties, whereby the mechanism can be overcome by the use of sufficient resources, expertise and opportunity in the form of a direct attack. An example of a type A mechanism would be an authentication program using a password: if the password can be guessed by attempting all possible passwords in succession, the authentication mechanism is of type A. Type A mechanisms often involve the use of a ”secret” such as a password or cryptographic key.

6.C.5 All type A mechanisms in a TOE have a strength, which corresponds to the level of resources, expertise and opportunity required to compromise security by directly attacking the mechanism.

6.C.7 A type B mechanism is a security mechanism which, if perfectly conceived and implemented, will have no weaknesses. A type B mechanism can be considered to be impregnable to direct attack regardless of the level of resources, expertise and opportunity deployed. A potential example of a type B mechanism would be access control based on access control lists: if perfectly conceived and implemented, this type B mechanism cannot be defeated by direct attack. However, these type B mechanisms can be defeated by indirect attacks which are the subject of other effectiveness analyses.”

4 Minimum Strength of the Security Mechanisms

ITSEC:

”3.5 All critical security mechanisms (i.e. those mechanisms whose failure would create a security weakness) are assessed for their ability to withstand direct attack. The minimum strength of each critical mechanism shall be rated either basic, medium or high.

3.6 For the minimum strength of a critical mechanism to be rated basic it shall be evident that it provides protection against random accidental subversion, although it may be capable of being defeated by knowledgeable attackers.

3.7 For the minimum strength of a critical mechanism to be rated medium it shall be evident that it provides protection against attackers with limited opportunities or resources.

3.8 For the minimum strength of a critical mechanism to be rated high it shall be evident that it could only be defeated by attackers possessing a high level of expertise, opportunity and resources, successful attack being judged to be beyond normal practicality."

This page is intentionally left blank.