Federal Office
for Information Security

Certification Report

BSI-DSZ-ITSEC-0509-2008

for

Digital Tachograph DTCO 1381, Release 1.3

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-0509-2008

Digital Tachograph DTCO 1381,
Release 1.3

IT Security Certified
SOGIS - MRA

from	Continental Automotive GmbH
Functionality:	according to Appendix 10 of Annex 1(B) of Council Regulation (EEC) No. 3821/85 amended by Council Regulation (EC) No. 1360/2002 and last amended by CR (EC) No.561/2006 and CR (EC) No. 1791/2006 on recording equipment in road transport
Assurance:	Evaluation Level E 3 Strenght of Mechanisms high

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved 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 vehicle unit specific guidance according to “Annex 1B of the European Regulation (EEC) No 3821/85 3 amended by the European Regulation (EEC) No 2135/98 4 and last amended by CR (EC) No.561/2006 and CR (EC) No. 1791/2006 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 4, Para. 3, 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, 17 November 2008
For the Federal Office for Information Security

Joachim Weber L.S.
Head of Division

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - 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

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 setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

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)
- Information Technology Security Evaluation Criteria (ITSEC), version 1.2, June 1991[5]
- Information Technology Security Evaluation Manual (ITSEM), version 1.0, September 1993
- BSI certification: Application Notes and Interpretation of the Scheme (AIS / JIL)

[2] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

[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 on 15.7.1992 in the Gemeinsames Ministerialblatt 1992, p. 546

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

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998.

This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

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

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria 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 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 Digital Tachograph DTCO 1381, Release 1.3 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-ITSEC-0485-2007. Specific results from the evaluation process based on BSI-DSZ-ITSEC-0485-2007 were re-used.

The evaluation of the product Digital Tachograph DTCO 1381, Release 1.3 was conducted by T-Systems GEI GmbH. The evaluation was completed on 13 November 2008. The T-Systems GEI GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

[6] Information Technology Security Evaluation Facility

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.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular 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 Digital Tachograph DTCO 1381, Release 1.3 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http://

www.bsi.bund.de and [4a]). 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-Str. 45
78052 Villingen-Schwenningen

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 [5] 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 Security Target contains a description of the vehicle unit DTCO 1381, Release 1.3 (the TOE), of the threats it must be able to counteract and of the security objectives it must achieve. It specifies the required security enforcing functions. It states the claimed minimum strength of security mechanisms and the required level of assurance for the development and the evaluation.

The security target is based on the Vehicle Unit Generic Security Target, which is described in Appendix 10 [7] of Annex 1B [8] of the European Regulation (EEC) No 3821/85 amended by the European Regulation (EEC) No 2135/98 and last amended by CR (EC) No.561/2006 and CR (EC) No. 1791/2006. The Security Target states the security functions and assumptions on the environment and describes how they are implemented in the vehicle unit DTCO 1381. Wherever it is referred to DTCO 1381, it deals with the current TOE DTCO 1381, Release 1.3.

Requirements referred to in the document, are those of the body of Annex 1B. For clarity of reading, duplication sometimes arises between Annex 1B body requirements and security target requirements.

In case of ambiguity between a security target requirement and the Annex 1B body requirement referred by this security target requirement, the Annex 1B body requirement shall prevail.

Annex 1B body requirements not referred by security targets are not the subject of security enforcing functions.

Unique labels have been assigned to threats, objectives, procedural means and SEF specifications for the purpose of traceability to development and evaluation documentation.

The following table 1 outlines the TOE deliverables:

Item No.	Delivery	Part	Version	Date	Form of Delivery
1	Digital Tachograph DTCO 1381, Release 1.3	entire device as Vehicle Unit (Manufacturing option)	a) SW-Version of the Tachograph Application: 01.03.42, displayed as: 01.03.42 on display, 13.42 on print out, 1342 in download file, 013.042 via diagnostic interface; b) SW-Version of the Software Upgrade	-	separate unit in a closed case (Manufacturing option)

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

Item No.	Delivery	Part	Version	Date	Form of Delivery
			Module (SWUM): 02.01, displayed as: 02.01 on display; c) security module: Variant C4 A2C53358729 (Laser labelling: on bottom = A2C53358470, on top = A2C53332854) Variant C1c A2C53337798 (Laser labelling: on bottom = A2C53332850, on top = A2C53332854) d) HW Version (Type plate): 1381 Rel. 1.3		
2	Documentation: Technical Description Manual [9]	(manufacturing option as well as SW-Upgrade option) Digitaler Tachograph DTCO 1381 (Rel. 1.3), Technische Beschreibung, TD00.1381.00 133 101 – OPM 000 AA, Continental Automotive GmbH, Ausgabe 07/2008	TD00.1381.00 133 101 – OPM 000 AA	Edition 07/2008	Paper or PDF-file
3	Documentation: Operating Instructions for drivers / co-drivers and forwarding companies [10]	(manufacturing option as well as SW-Upgrade option) Digitaler Tachograph DTCO 1381, Betriebsanleitung	BA00.1381.00 130 101 – 40283207 OPM 000 AA	Edition 09/2008	Paper or PDF-file

Item No.	Delivery	Part	Version	Date	Form of Delivery
		Unternehmer & Fahrer, BA00.1381.00 130 101 – 40283207 OPM 000 AA (eingereicht am 12.08.08, 2.711.289 Bytes), Continental Automotive GmbH, Ausgabe 09/2008			
4	Documentation: Operating Instructions for the control authorities and control officers [11]	(manufacturing option as well as SW-Upgrade option) Digitaler Tachograph DTCO 1381, Leitfaden für die Kontrollorgane, BA00.1381.00 230 101 – 40285986 OPM 000 AA (eingereicht am 12.08.08, 3.368.185 Bytes), Continental Automotive GmbH, Ausgabe 09/2008	BA00.1381.00 230 101 – 40285986 OPM 000 AA	Edition 09/2008	Paper or PDF-file
5	Documentation: Software Upgrade Manual [12]	Digitaler Tachograph DTCO 1381, Software Upgrade, TD00.1381.00 600 101 – OPM 000 AB, Siemens VDO Automotive AG, Ausgabe 03/2006	TD00.1381.00 600 101 – OPM 000 AB	Edition 03/2006	Paper or PDF-file

Table 1 Deliverables of the TOE

1.2 Definition of the TOE and Type of Use

The VU (DTCO 1381, Release 1.3) is intended to be installed in road transport vehicles. Its purpose is to record, store, display, print and output data related to driver activities. It is

connected to a motion sensor with which it exchanges vehicle's motion data. Users identify themselves to the VU using tachograph cards. The VU records and stores user activities data in its data memory, it also records user activities data in tachograph cards. The VU outputs data to display, printer and external devices.

1.3 Assumed Operational Environment

The vehicle unit's operational environment while installed in a vehicle is described in the figure 1 of the Security Target [5]. For more details and basic architecture of the DTCO 1381, Release 1.3 refer to the Security Target [5, chapter 5.1]. The VU general characteristics, functions and mode of operations are described in Chapter II of Annex 1B. The VU functional requirements are specified in Chapter III of Annex IB. It must be noted that although the printer mechanism is part of the TOE, the paper document once produced is not.

1.4 Subjects, Objects, Actions

For the TOE the following types of subjects exist:

Subjects:

S1 entities:

S1.1 installation device in the manufacturing process for storing objects in the external data memory of the TOE

S1.2 motion sensor in pairing and operational mode

S1.3 calibration device (programming tools)

S1.4 intelligent dedicated equipment for downloading (e.g. personal computer)

S1.5 tachograph cards

S1.6 management device

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)

S2.5 unknown

Note: The human users S2.1 to S2.4 of the recording equipment in road transport vehicles identify themselves to the TOE using tachograph cards. Authentication and access control for those users is performed by TOE unit by identifying the type of tachograph cards.

Objects:

For the specification of the security functions of the TOE the following objects are relevant. Definitions of data objects are provided in the Appendix 1 [13] of Annex 1(B). For more details about the subjects, objects and actions refer to the Security Target [5, chapter 5.3 and table 1].

1.5 Security Objectives and Threats

Security objectives and threats are described in the Security Target [5, chapter 5.4 and 5.5].

1.6 Security Functions and Mechanisms

The following security functions are implemented in the TOE:

TOE Security Function	Addressed issue
SEF1	Identification and authentication
SEF2	Access control
SEF3	Accountability
SEF4	Audit
SEF5	Object re-use
SEF6	Accuracy
SEF7	Reliability of service
SEF8	Data exchange
SEF9	Cryptographic support

Table 2: overview of the security functions

For more details about the security functions refer to the Security Target [5, chapter 6.4 to 6.9]. A rationale of the security functions is given in the Security Target [5, chapter 10].

The required security mechanisms are specified in Appendix 11 [14]. The TOE implements all necessary security mechanisms.

1.7 Level of Evaluations and Strength of Mechanisms

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

2 Evaluation Results

The TOE provides the functionality according to Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002 [7]. The changes Annex 1B of the European Regulation (EEC) No 3821/85 amended by the European Regulation (EEC) No 2135/98 and last amended by CR (EC) No.561/2006 and CR (EC) No. 1791/2006 are implemented.

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 4, Para. 3, 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 developer identified one operational vulnerability. The analysis of the potential impact of this vulnerability shows that the vulnerability in question cannot be exploited in the intended environment for the TOE because either

the vulnerability is adequately covered by other uncompromised external security measures, or

it could be shown that the vulnerability is irrelevant to the security target or will not be exploitable in practice, or

The instructions for the user have to be followed.

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 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 [7] for the vehicle unit.

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 secuirty 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 vehicle unit microprocessor was 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 unambigously 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 the Companies listed in the following Table 3:

Name of Manufacturer/ Developer	Location	Form of Developing and Manufacturing
Continental Automative GmbH (former Siemens VDO)	78052 Villingen, Heinrich-Hertz-Str. 45, Germany	Developing of Hardware, Software, mechanical Construction and Test of whole TOE
Siemens PSE DE	21079 Hamburg, Harburger Schloßstr. 18, Germany	Developing of Software (Interfaces)
Siemens IT Solutions and Services (formals Siemens PSE)	1031 Wien, Erdberger Lände 26, Austria	Developing of Software Parts
Siemens Information Systems Ltd. (SISL)	No. 84, Keonics Electronics City, Hosur Road, Bangalore - 560 100, India	Test of the Software (Modultest)
Siemens VDO Automotive SRL	300724 Timisoara, Calea Martirilor 1989 Nr. 1, Romania	Developing of the Driver Software and Testing
Siemens CT IC 3	81730 München, Otto-Hahn-Ring 6, Geb. 10, Flur 3, Germany	Developing of Software and Optimisation (RSA, TDES)
Fa. Schweizer Electronic AG (SEAG)	78713 Schramberg, Einsteinstr. 10 and 78655 Dunningen, Porschestrasse	Production of Multilayer Conductor Board for Security Modul
FA. AT&S	A-8700 Leoben, Fabriksgasse 13, Österreich	Production of Multilayer Conductor Board for Security Modul
Fa. Meiko, factory in Nansha	2 Guangsheng Road, Nansha District, Guangzhou 511458, China	Production of Multilayer Conductor Board for Security Modul
Fa. AT&S, Shanghai	No.5000, Jin Du Road, Shanghai 201108, China	Production of Multilayer Conductor Board for Security Modul

Table 3: production sites

2.5 Correctness - Operation - Operational Documentation

2.5.1 User Documentation

The user documentation [10] and [11] describes the security enforcing functions relevant to the unprivilidged user. The description of these 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 vehicle manufactures is considered as the administration documentation [11] 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 following components listed in the Table 1 are provided for a customer, who purchases the TOE. The TOE is labled with its identification number ’DTCO 1381, Release 1.3. For more details please refer to 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 by various self tests and diagnostic procedures of the vehicle unit hardware and software. If an error is detected, a reset is performed or the error is displayed or recorded.

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

3 Instructions for the User

The user has to observe the following instructions:

1. The operator of the digital tachograph system has to make sure, that the organisational measures being relevant for him and defined in [7] (cf. chapter 2.9 of this document) are adequately implemented. These are at least the following measures:
   - M.Sec_Data_Generation[9]
   - M.Sec_Data_Transport[10]
   - M.Card_Availability[11]
   - M.Card_Traceability[12] and
   - M.Approved_Workshops[13].

   Such measures could be defined e.g. by the National Policy (MSA Policy) and enforced by accreditation and audit procedures.
2. It must be assured by organisational measures, that the certificates and key pairs respectively for a successful device authentication are only granted to trustworthy tachograph cards. Furthermore this tachograph cards must be able to protect these secrets in a sufficient manner and they must be evaluated and certified in accordance with [7] and [5] to ITSEC on an evaluation level E3 and with a minimum strength of function high.
3. It must be assured by organisational measures, that the necessary data for the pairing process are only granted to trustworthy motion sensors. Furthermore the motion sensors must be able to protect these data in a sufficient manner and they must be evaluated and certified in accordance with [7] and [5] to ITSEC on an evaluation level E3 and with a minimum strength of function high.
4. The evaluator advises the operator of the digital tachograph system, that the control officers will be fit out with equipment, which can download data from the tachograph and then analyse it efficiently. Such automated data analysis will remarkably facilitate the search of important events.
5. The evaluator advises the operator of the digital tachograph system that he should recommend to forwarding companies using of such Fleet Management Systems which ensure completeness of the 'Company Activity Data' in their own event logs at the remote data download.
   The background of this recommendation is the fact that the current specification [Digital Tachograph, Specification for remote company card authentication and remote data downloading, Index H, Heavy Truck Electronic Interfaces Working Group – DTCO,

[9] Security data generation algorithms must be accessible to authorised and trusted persons only.

[10] Security data must be generated, transported, and inserted into the VU, in such a way to preserve its appropriate confidentiality and integrity.

[11] Tachograph cards must be available and delivered to authorised persons only.

[12] Card delivery must be traceable (white lists, black lists) , and black lists must be used during security audits.

[13] Installation, calibration and repair of recording equipment must be carried by trusted and approved fitters or workshops.

31.01.2008] does not arrange either for reading the ‘Card Identification’ from the remotely connected Company Card with subsequent storing the 'Company Activity Data’ in the Vehicle Unit event log or for writing the 'Company Activity Data’ back to the remotely connected Company Card at the remote data download.

4 Definitions

CAN	Controller Area Network
DTCO	Digital Tachograph
LC Display	Liquid Crystal Display
PIN	Personal Identification Number
ROM	Read Only Memory
RTC	Real Time Clock
SEF	Security Enforcing Function
TBD	To Be Defined
TOE	Target Of Evaluation
VU	Vehicle Unit
Digital Tachograph	Recording Equipment.
Entity	A device connected to the VU (specific definition see S1).
Management Device	A dedicated device for software upgrade of theTOE
Motion data	The data exchanged with the VU, representative of speed and distance travelled
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 vehicle unit that are distributed in the vehicle as opposed to physical components gathered into the vehicle unit casing.
Security data	The specific data needed to support security enforcing functions (e.g. crypto keys).
SW-Upgrade	SW-Upgrade installs a new version of software in the TOE.
SW-Upgrade Modul (SWUM)	A component of software in the TOE which is responsible for the realization and control of the software upgrade System Equipment, people or organisations, involved in any way with the recording equipment.
Tachograph cards	Smart cards intended for use with the recording equipment. Tachograph cards allow for identification by the recording equipment of the identity (or identity group) of the cardholder and allow for data transfer and storage. A tachograph card may be of the following types: driver card, control card, workshop card, company card.

User	Users are to be understood as human user of the equipment. Normal users of the VU comprise drivers, controllers, workshops and companies (specific definition see S2).
User data	Any data, other than security data, recorded or stored by the VU.
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 this regulation.

5 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)

[4a] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Website

[5] Security Target DTCO 1381, Release 1.3, Digital Tachograph – Vehicle Unit, Version 1.15 vom 14.11.2007, Siemens VDO Automotive AG

[6] Technischer Evaluationsbericht, Digital Tachograph DTCO 1381, Release 1.3, Continental Automotive (vormals Siemens VDO), Version 6.02 vom 12. November 2008 (confidential document)

[7] Appendix 10 of Annex 1B of Council Regulation (EEC) No. 3821/85 - Generic Security Targets

[8] Annex 1B of Council Regulation (EEC) No. 3821/85 amended by CR (EC) No. 1360/2002, CR (EC) No. 432/2004 and corrigendum dated from 13.03.2004 (OJ L 77) and last amended by CR (EC) No.561/2006 and CR (EC) No. 1791/2006

[9] Digitaler Tachograph DTCO 1381 (Rel. 1.3), Technische Beschreibung, TD00.1381.00 133 101 – OPM 000 AA, Continental Automotive GmbH, Ausgabe 07/2008

[10] Digitaler Tachograph DTCO 1381, Betriebsanleitung Unternehmer & Fahrer, BA00.1381.00 130 101 – 40283207 OPM 000 AA (eingereicht am 12.08.08, 2.711.289 Bytes), Continental Automotive GmbH, Ausgabe 09/2008

[11] Digitaler Tachograph DTCO 1381, Leitfaden für die Kontrollorgane, BA00.1381.00 230 101 – 40285986 OPM 000 AA (eingereicht am 12.08.08, 3.368.185 Bytes), Continental Automotive GmbH, Ausgabe 09/2008

[12] Digitaler Tachograph DTCO 1381, Software Upgrade, TD00.1381.00 600 101 – OPM 000 AB, Siemens VDO Automotive AG, Ausgabe 03/2006

[13] Appendix 1 of Annex 1B of Council Regulation (EEC) No. 3821/85 - Data Dictionary

[14] Appendix 11 of Annex 1B of Council Regulation (EEC) No. 3821/85 - Common Security Mechanisms

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.