Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1015-V2-2020

for

Digital Tachograph DTCO 1381, Release 3.0a

from

Continental Automotive GmbH

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1015-V2-2020 (*)

Digital Tachograph

Digital Tachograph DTCO 1381, Release 3.0a

from	Continental Automotive GmbH
PP Conformance:	Digital Tachograph - Vehicle Unit (VU PP) Version 1.0, 13 July 2010, BSI-CC-PP-0057-2010
Functionality:	PP conformant Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ATE_DPT.2 and AVA_VAN.5

SOGIS
Recognition Agreement

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045, and according to Commission Regulation (EC) No 1360/2002 Annex 1(B) adapting to Council Regulation (EC) No. 3821/85 amended by Commission Regulation (EC) No 432/2004 of 5 March 2004, Council Regulation (EC) No 1791/2006 of 20 November 2006 and Commission Regulation (EC) No 68/2009 of 23 January 2009, Commission Regulation (EU) No 1266/2009 of 16 December 2009 on recording equipment in road transport.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the 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.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2

Bonn, 16 April 2020

For the Federal Office for Information Security

Bernd Kowalski L.S.
Head of Division

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG1 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.

2. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs [3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.

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

[2] Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

[3] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 3 March 2005, Bundesgesetzblatt I, p. 519

- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. 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.

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

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

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://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 by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2 components.

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

4. 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 3.0a has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1015-2017. Specific results from the evaluation process BSI-DSZ-CC-1015-2017 were re-used.

The evaluation of the product Digital Tachograph DTCO 1381, Release 3.0a was conducted by T-Systems International GmbH. The evaluation was completed on 26 March 2020. T-Systems International GmbH is an evaluation facility (ITSEF)[5] 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.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is 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, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

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-assessment or 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 order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 16 April 2020 is valid until 15 April 2025. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security

[5] Information Technology Security Evaluation Facility

Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

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.

6. Publication

The product Digital Tachograph DTCO 1381, Release 3.0a has been included in the BSI list of certified products, which is published regularly (see also Internet: https://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[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Continental Automotive GmbH
Heinrich-Hertz-Strasse 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. Executive Summary

The Target of Evaluation (TOE) is the digital Tachograph DTCO 1381, Release 3.0a. It is a vehicle unit (VU) in the sense of Annex IB [12] 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 Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Digital Tachograph - Vehicle Unit (VU PP) Version 1.0, 13 July 2010, BSI-CC-PP-0057-2010 [8].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ATE_DPT.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] chapter 6.1. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Services	Addressed issue
TOE_SS.Identification_Authentication	Identification and Authentication The TOE provides this security service of identification and authentication of the motion sensor, of users by monitoring the tachograph cards.
TOE_SS.Access	Security Service of Access Control The TOE provides this security service of access control for access to functions and data of the TOE according to the mode of operation selection rules.
TOE_SS.Accountability	Security Service of Accountability The TOE provides this security service of accountability for collection of accurate data in the TOE.
TOE_SS.Audit	Service of Audit The TOE provides this security service of audit related to attempts to undermine the security of the TOE and provides the traceability to associated users.
TOE_SS.Object_Reuse	Service of Object Reuse The TOE provides this security service of object reuse to ensure that temporarily stored sensitive objects are destroyed.
TOE_SS.Reliability	Service of Reliability of Service The TOE provides this security service of reliability of service: self-tests, no way to analyse or debug software in the field, detection of specified hardware sabotage and deviations from the specified voltage values including cut-off of the power supply
TOE_SS.Accuracy	Security Service of Accuracy of stored Data The TOE provides this security service of accuracy of stored data

TOE Security Services	Addressed issue
	in the TOE.
TOE_SS.Data_Exchange	Security Service of Data Exchange The TOE provides this security service of data exchange with the motion senor and tachograph cards and connected entities for downloading.
TOE_SS.Cryptographic_support	Security Service of Cryptographic Support The TOE provides this security service of cryptographic support using standard cryptographic algorithms and procedures.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.2 to 3.4.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

Digital Tachograph DTCO 1381, Release 3.0a

The following table outlines the TOE deliverables:

No	Identifier	Part	Release	Date	Form of Delivery

1	Digital Tachograph DTCO 1381, Release 3.0a	entire device as Vehicle Unit (Manufacturing option)	a) SW-Version of the Tachograph Application: 03.00.41,
			b) SW-Version of the Software Upgrade Module (SWUM): 03.12;
			c) HW Version (Type plate):
			1381 Rel. 3.0a
				-	separate unit in a closed case (Manufacturing option)

2	Documentation: Technical Descrip-	(manufacturing option as well as SW-Upgrade option)	TD00.1381.30 101 101 – 41038233	Edition 09.2019	Paper or PDF-file

No	Identifier	Part	Release	Date	Form of Delivery
	tion Manual [13]	Digitaler Tachograph – DTCO 1381, Release 3.0a, Technische Beschreibung, TD00.1381.30 101 101 – 41038233 OPM 000 AC, Ausgabe 09.2019	OPM 000 AC		
3	Documentation: Operating Instructions for drivers / co-drivers and forwarding companies [14]	(manufacturing option as well as SW-Upgrade option) Digitaler Tachograph – DTCO 1381, Release 3.0a, Betriebsanleitung Unternehmer & Fahrer, BA00.1381.30 100 101 – 41024304 OPM 000 AA, Ausgabe 05.2017	BA00.1381.30 100 101 – 41024304 OPM 000 AA	Edition 05.2017	Paper or PDF-file
4	Documentation: Operating Instructions for the control authorities and control officers [15]	(manufacturing option as well as SW-Upgrade option) Digitaler Tachograph – DTCO 1381, Release 3.0, Leitfaden für die Kontrollorgane, BA00.1381.30 201 101, Ausgabe 01.2020	BA00.1381.30 201 101	Edition 01.2020	Paper or PDF-file
5	Documentation: Guidance for the software update [16]	(manufacturing option as well as SW-Upgrade option) Digitaler Tachograph – DTCO 1381 ab Release 3.0, Software Upgrade, TD00.1381.40 600 101 – 41265525 OPM 000 AA	TD00.1381.40 600 101 – 41265525 OPM 000 AA	Edition 04/2018	Paper or PDF-file

Table 2: Deliverables of the TOE

The version number and the authenticity of the delivered TOE can be checked after start up. All necessary information will be shown on the display integrated. For this reason please refer to table 2.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

The main security of the VU aims to protect

- the data recorded and stored in such a way as to prevent unauthorized access to and manipulation of the data and detecting any such attempts,
- the integrity and authenticity of data exchanged between the motion sensor and the vehicle unit,
- the integrity and authenticity of data exchanged between the recording equipment and the tachograph cards, and
- the integrity and authenticity of data downloaded (locally and remotely).

For detailed information please refer to ST [6], chapter 9 Annex A.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. Details can be found in the Security Target [6], chapter 4.2.

5. Architectural Information

The TOE comprises the complete digital tachograph. The software includes the whole tachograph application and the software upgrade module running in a distributed environment of three microcontrollers. Firstly this is the SLI97CFX1M00PE produced by Infineon, secondly it is the microcontroller FR81S MB91F526L produced by Scansion and thirdly it is the microcontroller PIC16F689 produced by Microchip. The SFR-enforcing parts of the system are exclusively implemented on the secure microcontroller SLI97CFX1M00PE produced by Infineon. Der FR81S MB91F526L controls the display, the security mikrocontroller und den PIC microcontroller.

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

The evaluators spent adequate testing effort for the desired resistance of the TOE against attackers with a high attack potential. The evaluators spent several days each for analysing the test specification and ensuring that the specification has been correctly implemented in the test scripts,

- for creating ideas for independent evaluator tests,
- for ensuring that the test environment delivers correct test results, and
- for repeating developer tests as well as carrying out independent tests.

TOE test configurations:

For the penetration testing the TOE was tested in its operative state. Modifications of the devices were performed before the TOE was brought into its operative state in order to suppress warnings. The later tests were performed in the operative state of the TOE.

Independent tests:

Independent tests were identified based on the developer tests already available. The developer tests have been compared with the ST, the FSP and the TDS in order to determine the fields of further investigation. Furthermore the evaluator devised tests based on a systematical analysis of the ST.

The evaluators conducted independent testing at the developer's site.

The evaluator tests have been carried out against the following TOE configurations: The TOE was brought in every production control state. A simulator for the motion sensor was used. Furthermore every card type (Driver card, workshop card, control card, and company card) was used. For the company card also the remote authentication was in the focus of the tests.

According to EAL4, functional testing is performed down to the depth of SFR-enforcing module interfaces.

The tests showed that the TOE behaves as expected in all configurations that are considered as part of the evaluation. No deviation was found between the expected and the actual test results. The depth of testing is adequate for the evaluation assurance level chosen (EAL4+). The TOE has successfully passed independent testing.

The evaluator reports the evaluator penetration testing effort, outlining the testing approach, configuration, depth and results.

Penetration Tests:

The penetration testing was performed using the developer’s testing environment.

All configurations of the TOE being intended to be covered by the current evaluation were tested.

On the basis of the methodical vulnerability analysis some potential vulnerabilities have been identified by the evaluator. These potential vulnerabilities have been analysed, if they are exploitable in the planned operational environment. For every potential vulnerability which was identified to be a candidate to be exploitable in the planned operational environment the evaluator devised and conducted penetration tests.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential High was actually successful in the TOE’s operational environment as defined in [6] provided that all measures required by the developer are applied.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

The TOE Digital Tachograph DTCO 1381, Release 3a is an electronic device, consisting of hardware and software, and additionally of documentations (see table 2). The TOE was tested with the following software versions:

- Tachographenapplikation, Version 03.00.41 (AppCon Software V03.00.41 und SecCon Software V03.00.41)
- BattCon-Software, Version 03.00-02-00
- Software Update Module, Version 03.12

The software which includes the whole tachograph application and the software upgrade module are running in a distributed environment of three microcontrollers: SLI97CFX1M00PE, FR81S MB91F526L und PIC16F689. The SFR-enforcing parts of the system are implemented exclusively on the secure microcontroller SLI97CFX1M00PE produced by Infineon.

There is only one configuration of the vehicle unit that is delivered to the approved workshops. The configuration at delivery, as well as the further steps to be taken in order to activate and calibrate the TOE in a vehicle are described in [13]. The correct input of the calibration parameters is guaranteed by the trustworthiness of the accredited work shops (see [6] A.Approved_Workshops).

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL 5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

- The Application of CC to Integrated Circuits
- The Application of Attack Potential to Smartcards

(see [4], AIS 25, AIS 26, AIS 32, AIS 34, AIS 36) were used.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ATE_DPT.2 and AVA_VAN.5 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-1015-2017, re-use of specific evaluation tasks was possible.

The evaluation has confirmed:

● PP Conformance:	Digital Tachograph - Vehicle Unit (VU PP) Version 1.0, 13 July 2010, BSI-CC-PP-0057-2010 [8]
● for the Functionality:	PP conformant Common Criteria Part 2 conformant
● for the Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ATE_DPT.2 and AVA_VAN.5

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines the standard of application where its specific appropriateness is stated.

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application
Secure messaging TOE <-> Motion Sensor TOE_SS.Identification_Authentication TOE_SS.Data_Exchange TOE_SS.Cryptographic-support	Triple-DES in CBC mode	[32], [35] [31], sec. 7.6	112	[31], sec. 7.6
Secure messaging authenticated mode TOE <-> tachograph card TOE_SS.Identification_Authentication TOE_SS.Data_Exchange TOE_SS.Cryptographic-support	Retail-MAC	[37] [30], sec. 2.2.3 and ANSI X9.19	112	[30], sec. 5.3
Secure messaging encrypted mode TOE <-> tachograph card TOE_SS.Data_Exchange TOE_SS.Cryptographic_support	Triple-DES in CBC mode	[32], [35] [30], sec. 2.2.3	112	[30], sec. 5.4
Mutual authentication TOE <-> tachograph card TOE_SS.Identification_Authentication TOE_SS.Cryptographic_support	RSA	[36] [30], sec. 2.2.1	1024	[30], CSM_020
Digital signature for downloading to external media TOE_SS.Data_Exchange TOE_SS.Cryptographic_support	RSA	[36] [30], sec. 2.2.1	1024	[30], CSM_034
Mutual authentication TOE <-> tachograph card digital signature for downloading to external media TOE_SS.Identification_Authentication TOE_SS.Data_Exchange TOE_SS.Cryptographic_support	SHA-1	[33] [30], sec. 2.2.2	n/a	[30], CSM_020 [30], CSM_034
De-/encrypting the transport key of the upgrade file (SWUM) TOE_SS.Crypto-graphic_support	RSA	[36] [30], sec. 2.2.1	2048	n/a
Digital signature of the upgrade file for the software upgrade TOE_SS.Crypto-graphic_support	ECC	[38]	256	brainpoolP256r1
Authentication of the management device TOE_SS.Identification_Authentication, TOE_SS.Cryptographic_support	ECC	[38]	256	brainpoolP256r1
Confidentiality of the upgrade file Protection of the SWUM.SK, the SecDev.PK, the curve parameters of the underlying elliptic curve and the CBC-MAC key itself	AES	[35], [34]	128	n/a

Table 3: TOE cryptographic functionality

The strength of the these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). An explicit validity period is not given.

[30] Appendix 11 of Annex I (B) of Council Regulation (EEC) No. 1360/2002 - Common Security Mechanisms

[31] ISO 16844-3 Road Vehicles Tachograph Systems — Part 3: Motion Sensor Interface – First edition, 2004-11-01, Corrigendum 1, 2006-03-01

[32] FIPS PUB 46-3 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION DATA ENCRYPTION STANDARD (DES) Reaffirmed 1999 October 25

[33] FIPS PUB 180-4 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Secure Hash Standard (SHS), March 2012

[34] FIPS PUB 197 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, ADVANCED ENCRYPTION STANDARD (AES), National Institute of Standards and Technology, 2001 November 26

[35] NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques , National Institute of Standards and Technology, U.S Department of Commerce, 2001

[36] PKCS #1: RSA Cryptography Specifications, Version 2.0. RSA Laboratories, September 1998

[37] ISO/IEC 9797-1, Information technology -- Security techniques -- Message Authentication Codes (MACs), 2011

[38] RFC 5639 Elliptic Curve Cryptography (ECC) — Brainpool Standard Curves and Curve Generation, 2010

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

In addition, the following aspects need to be fulfilled when using the TOE:

The operator of the digital tachograph system has to make sure, that the organisational measures being relevant for him and defined in [11], chapter 4.2 are adequately implemented. These are at least the following measures:

- OE.Sec_Data_Generation[7],
- OE.Sec_Data_Transport[8],
- OE.Sec_Data_Strong[9]

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

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

[9] Security data inserted into the TOE shall be cryptographically strong as required by [1].

- OE.Card_Availability[10],
- OE.Card_Traceability[11],
- OE.Approved_Workshops[12], and
- OE.SW_Upgrate[13]

Such measures could be defined e.g. by the National Policy (MSA Policy) and enforced by accreditation and audit procedures.

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 be evaluated and certified in accordance with [11] and [12].

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 [11] and [12].

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.

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, 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.

The evaluator advises the operator of the digital tachograph system, that tachograph cards being used with the TOE must be configured by their issuer in that way that the card expiry date does not exceed the expiry date of all certificates to be verified.

The evaluator advises the operator of the digital tachograph system, that the control officers will verify that the seals are not broken or have been tampered.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

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

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

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

[13] Software revisions shall be granted security certification before they can be implemented in the TOE.

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Definitions

12.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
VU	Vehicle Unit

12.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

13. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[14] https://www.bsi.bund.de/AIS

[14] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2, Reuse of evaluation results

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-1015-V2-2020, Version 1.2, Date: 03.02.2020, Digital Tachograph DTCO 1381 Security Target, Continental Automotive GmbH (public document)

[7] Evaluation Technical Report, Version 4.03, Date: 20.20.2020, Evaluation Technical Report Digital Tachograph DTCO 1381, Release 3.0a, T-Systems International GmbH – Prüfstelle für IT-Sicherheit, Lab-Name, (confidential document)

[8] Digital Tachograph - Vehicle Unit (VU PP) Version 1.0, 13 July 2010, BSI-CC-PP-0057-2010

[9] Configuration list for the TOE, Version 1.8.1.5, Date: 16.02.2020, Konfigurationsliste zu DTCO 1381 Release 3.0a, Continental Automotive GmbH (confidential document)

[10] Annex I (B) of Council Regulation (EEC) No. 1360/2002 „Requirements for construction, testing, installation, and inspection“, 05.08.2002 and last amended by CR (EC) No. 1266/2009

[11] Appendix 10 of Annex I (B) of Council Regulation (EEC) No. 1360/2002 - Generic Security Targets

[12] 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 1B, Version 1.12, June 2003

[13] Digitaler Tachograph – DTCO 1381, Release 3.0, Technische Beschreibung, TD00.1381.30 101 101 – 41038233 OPM 000 AC, Ausgabe 09.2019

[14] Digitaler Tachograph – DTCO 1381, Release 3.0, Betriebsanleitung Unternehmer & Fahrer, BA00.1381.30 100 101 – 41024304 OPM 000 AA, Ausgabe 05.2017

[15] Digitaler Tachograph – DTCO 1381, Release 3.0a, Leitfaden für die Kontrollorgane, BA00.1381.30 201 101, Ausgabe 01.2020

[16] Digitaler Tachograph – DTCO 1381 ab Release 3.0, Software Upgrade, TD00.1381.40 600 101 – 41265525 OPM 000 AA, Ausgabe 04/2018

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailled definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development
and production environment

Annex B of Certification Report BSI-DSZ-CC-1015-V2-2020

Evaluation results regarding development and production environment

The IT product Digital Tachograph DTCO 1381, Release 3.0a (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations, and by advice of the Certification Body for components beyond EAL 5 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 16 April 2020, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1) are fulfilled for the development and production sites of the TOE listed below:

Company	Site	Activity
Continental Automotive GmbH	78052 Villingen, Heinrich-Hertz-Str. 45	HW development SW development HW and SW tests Manufacturing the final TOE Delivery of the final TOE
Continental Automotive GmbH	300724 Timisoara, Calea Martirilor 1989 Nr. 1, Romania	Specification Implementation Module tests
Continental Automotive Components (India) Private Ltd.	6th-11th Floor, Road 560100 Bangalor, Elec-tronic City, Bengaluru, Karnataka, 560100, India	SW development SW tests
Siemens CT IC 3	81730 München, Otto-Hahn-Ring 6, Geb. 53, Flur 6	SW development
Infineon Technologies AG Automotive, Industrial & Multimarket, Chipcard & Security IC´s	85579 Neubiberg, am Campeon 1-12, Germany	IC hardware SW libraries

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6]) are fulfilled by the procedures of these sites.