Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1158-2020

for

Digital Tachograph DTCO 1381, Release 4.0e

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-CC-1158-2020 (*)

Digital Tachograph: Vehicle Unit

Digital Tachograph DTCO 1381, Release 4.0e

from	Continental Automotive GmbH
PP Conformance:	Digital Tachograph - Vehicle Unit (VU PP) Version 1.0, 9 May 2017, BSI-CC-PP-0094-2017
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ATE_DPT.2 and AVA_VAN.5

SOGIS
Recognition Agreement

Common Criteria

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.

(*) 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 and ALC_FLR
only

Bonn, 14 December 2020

For the Federal Office for Information Security

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

Sandro Amendola
Head of Division

L.S.

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.

Contents

A. Certification

1. 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.

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]
- BMI Regulations on Ex-parte 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]

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 BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.
- 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.

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

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

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 4.0e has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1069-2018. Specific results from the evaluation process BSI-DSZ-CC-1069-2018 were re-used.

The evaluation of the product Digital Tachograph DTCO 1381, Release 4.0e was conducted by Deutsche Telekom Security GmbH. The evaluation was completed on 1 December 2020. Deutsche Telekom Security 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 14 December 2020 is valid until 13 December 2025. Validity can be re-newed by re-certification.

[5] Information Technology Security Evaluation Facility

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 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 4.0e 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 product Digital Tachograph, DTCO 1381, Release 4.0e. The Target of evaluation is a second generation vehicle unit (VU) in the sense of Annex IC [9] 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.

The TOE is providing security functionality conformant to the protection profile "Digital Tachograph – Vehicle Unit (VU PP)" [8]. The software which includes the whole tachograph application and the software upgrade module is running in a distributed environment of four microcontrollers and one ASIC.

There is only one configuration of the vehicle unit that is delivered to the approved workshops.

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, 9 May 2017, BSI-CC-PP-0094-2017 [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. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
TOE_SS.Identification_Authentication	The TOE identifies and authenticates tachograph cards and motion sensors. The TOE identifies and authenticates the workshop user by his card and additionally his PIN.
TOE_SS.Access_Control	The TOE controls access to stored data and functions based on the mode of operation.
TOE_SS.Accountability of users	User activity is recorded such that users can be held accountable for their actions.
TOE_SS.Audit of events and faults	The TOE detects and records a range of events and faults.
TOE_SS.Residual information protection for secret data	Encryption keys and certificates are deleted from the TOE when no longer needed, such that the information can no longer be retrieved
TOE_SS.Integrity and authenticity of exported data	The integrity and authenticity of user data exported (downloaded) to an external storage medium, in accordance with [9], Appendix 7, is assured through the use of digital signatures.
TOE_SS.Stored_Data_Accuracy	Data stored in the TOE fully and accurately reflects the input values from all sources (motion sensor, VU real time clock, calibration connector, Tachograph cards, VU keyboard, external GNSS

TOE Security Functionality	Addressed issue
	facility (if applicable- Note: not applicable)).
TOE_SS.Reliability	The TOE provides features that aim to assure the reliability of its services. These features include but are not limited to self-testing, physical protection, control of executable code, resource management, and secure handling of events.
TOE_SS.Data_Exchange	The TOE provides this security service of data exchange with the motion senor and tachograph cards.
TOE_SS.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 8.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1.1. 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 4.0e

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Digital Tachograph DTCO 1381, Release 4.0	Hardware version: 4.0e Software version: V04-00-72	Separate unit in a closed case (Manufacturing option)
2	DOC	Technical Description Manual [13]	“Ausgabe 7/2020”	Paper or PDF file
3	DOC	Operating Instructions for drivers / co-drivers and forwarding companies [14]	“Ausgabe 07/2020 - A3C0801750000”	Paper or PDF file

No	Type	Identifier	Release	Form of Delivery
4	DOC	Operating Instructions for the control authorities and control officers [12]	“DTCO 4.0/4.0e”	Paper or PDF file
5	DOC	Software Upgrade Manual [15]	“TD00.1381.40 600 101 - A3C0801750000“	Paper or PDF file

Table 2: Deliverables of the TOE

The manufactured device reaches a sorting station in delivery condition. There the device is assigned to the corresponding customer and receives its packaging. After the assembly the TOE is sealed with a factory lead seal including stamped lettering. Neutral lead seals will be supplied as accessories if the sealing occurs outside of the factory. Trucks deliver the TOE in the customer receptacle together with its shipping documents and where appropriate operating manuals and/or operating instructions to the customer. For the activation and calibration of the TOE at the customer, an authentication with the workshop card along with PIN code must be done.

The shipping documents are sent in a customer-specific receptacle together with the TOE via trucks to “fitter + workshop”. Every receptacle contains shipping documents (production order) with all relevant order information as production order number, variant, quantity, and customer data. Per customer order the receptacles are automatically palletized where each pallet also gets a shipping document assigned. The unambiguous material number on the production order guarantees that the materials necessary for a specific configuration at the individual assembly stations are available.

With the loading of the product onto the trucks, a data transmission (DFÜ) of the receipt to the customer is done via SAP R/3 and customer-specific information method (VDA, ODETTE, EDIFACT). After receipt of the pallet in the packing department, the packaging note and appropriate labels (Odette format) are printed according to the shipping documents. The packaging note contains customer-relevant data as customer ordering number of the variant, quantity, weight, and packaging method.

The operating manual for the retail/end user is transported in the receptacle together with the TOE via trucks to „fitter + workshop“. If the package is targeted at commerce, the operating manuals will be packed by the packing department, too. OEM customers order the operating manuals at a later point in time and enclose them with the vehicle papers.

Self-collectors/companies can obtain the DTCO in 1381 only from workshops which are authorized for the calibration of the DTCO 1381 (possession of a valid workshop card necessary). By following the order instructions it is guaranteed that the device delivery was initiated by the manufacturer and not by a third person. In this way it is also guaranteed that the customer receives an approved device.

The hardware of the TOE can be identified by the customer by comparing the identification data stored in the device with the data on the label.

The manuals of the TOE can be identified by calculating the SHA256 of the electronic files and comparing them to the data given in 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:

- protection of data memory in such a way as to prevent unauthorized access to and manipulation of the data and the detection of such attempts,
- confidentiality, integrity and authenticity of data exchanged between the motion sensor and the vehicle unit,
- integrity, authenticity and where applicable, confidentiality of data exchanged between the vehicle unit and the tachograph cards,
- integrity and authenticity of data exchanged between the vehicle unit and the external GNSS facility, if and only if the TOE is connected to an EGF,
- confidentiality, integrity and authenticity of data output through the remote early detection communication for control purposes, and
- integrity, authenticity and non-repudiation of data downloaded.

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 receives motion data from the motion sensor and activity data via the facilities for entry of user's. It stores all this user data internally and can export them to the tachograph cards inserted, to the display, to the printer, and to electrical interfaces. The architecture comprises nine subsystems which are divided into four groups M1, M2, M3, and M4:

- The main system group M1 contains the certified Security Controller hardware including a software library (PSL).
- The main system group M2 contains the main controller of the system.
- The main system group M3 provides the power supply for the other main system groups.
- The main system group M4 contains the GNSS and DSRC Controller, their application code and related hardware components.

The TOE support external connections or interfaces to the following:

- a motion sensor (MS)
- two smart cards
- a power supply unit
- a global navigation system (GNSS)
- a remote early detection communication reader
- other devices used for calibration, data export, software upgrade and diagnostics
- intelligent dedicated equipment for data download

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

Developer tests:

The developer considered the TOE environment as defined in the Security Target.

The developer systematically tested the TOE. For the security tests the developer used two approaches. The first approach is software tests. With this approach the developer tests the software in depth. The developers choose to test single steps in the sequence diagrams used during development. With these tests the SFR-enforcing modules and the interactions between the modules are tested in depth. Using this approach complete test coverage of all important program flows is achieved.

The second approach is the system tests. With this approach the complete system, and especially the TSFI, are tested. The system tests cover all security relevant activities. The focus of these tests is the correct behaviour at the TSFI boundaries and a correct program execution of the complete system. With these tests the results of the software tests are confirmed and additional confidence in the system behaviour is gained.

Furthermore the subsystem SWUM is tested intensively. The approach of the SWUM test is similar to the approach of the software tests.

Using these test approaches high test coverage is achieved. This leads to a high assurance in the correct implementation of the system and especially in its security relevant parts.

The test documentation consists of a test coverage and depth of testing analysis, a test plan, test specifications for each of the security functionalities, and test result logs.

The test result logs show that the tests identified in the test coverage and depth of testing analysis have been executed as expected by the developer.

Evaluator tests:

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 analyzing 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 configuration:

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 TDS in order to determine the fields of further investigation. Furthermore the evaluator devised tests based on a systematically 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.

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

The evaluated version is defined by the document "*1381R3.BOD.0986.Konfigurationsliste_DTCO_1381, Continental AG, Revision 1.20, 2020-11-23*", [11].

The evaluated configuration is 1381.xxxxxxxxxxx with tachograph application version 04.00.72 and software update module version 0405. xxxxxxxxxxx stands for variants of the non-security relevant hardware options. For every variant the softwares tachograph application version 04.00.72 and update module version 0405 are used. The variants are summarized as follows:

- Mainboard: not configurable
- Housing: standard / with spacer / with spacer and cap (black/white)
- DSRC/GNSS plug: DSRC detached antenna or DSRC CAN module / GNSS intern antenna or extern antenna with red or blue connector

- Seal: not configurable
- Additional configurable (optional) parts that have no impact on the security functionality of the TOE

There is only one configuration delivered to accredited workshops which assemble the vehicle unit into vehicles. This configuration as well as further steps for necessary activation and calibration of the TOE in a vehicle is described in [13].

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:

(i) The Application of CC to Integrated Circuits

(ii) The Application of Attack Potential to Smartcards

(iii) Composite product evaluation for Smart Cards and similar devices (see AIS 36). According to this concept the relevant guidance documents of the underlying platform and the documents ETR for Composition from the platform evaluations (i.e. on hardware [Ref Zert-Rep, Ref ETR-Comp] have been applied in the TOE evaluation.

(iv) Terminology and preparation of Smartcard-Evaluations

(v) Use of Interpretation for Security Evaluation and Certification of Digital Tachographs

(see [4], AIS 25, AIS 26, AIS 36, AIS 37, AIS 40).

For RNG assessment the scheme interpretations AIS 20 was used (see [4]).

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-1069-2018, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the SFR-enforcing changes listed below to ensure that the security relevant functionalities remain sound:

- Additional Application on the DSRC Controller (On-board weighing application added)
- Implementation of timeout for a manual entry of data
- Improved multi-manning card handling
- Improved driver identification

- Faster availability of VDO Counter
- Publishing RTM data via DSRC interface
- Improve capability to protect against potential manipulation attacks

The hardware was not changed. Further changes/improvements concern the development environment of the TOE in Timisoara, Villingen and Bangalore.

The evaluation has confirmed:

- PP Conformance: Digital Tachograph - Vehicle Unit (VU PP) Version 1.0, 9 May 2017, BSI-CC-PP-0094-2017 [8]
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- 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 table presented in chapter 12 of the Security Target [6] 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.

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

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.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

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.

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
ASIC	Application-specific integrated circuit
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
CAN	Controller Area Network
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
DFÜ	Datenfernübertragung
DTCO	Digital Tachograph
DSRC	Dedicated Short Range Communication
EAL	Evaluation Assurance Level
EGF	External GNSS Facility
ETR	Evaluation Technical Report
FSP	Functional Specification
GNSS	Global Navigation Satellite System
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MS	Motion Sensor
PIN	Personal Identification Number
PP	Protection Profile
RNG	Random Number Generator
RTM	Remote Tachograph Monitoring
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
SWUM	Software Upgrade Module

TDS	TOE Design
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
VU	Vehicle Unite

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[7] https://www.bsi.bund.de/AIS

[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-1158-2020, Version 1.32, 2020-09-08, Digital Tachograph DTCO 1381 Security Target, Continental Automotive GmbH

[7] Evaluation Technical Report, Version 1.0, 2020-12-01, Digital Tachograph, DTCO 1381, Release 4.0e, Deutsche Telekom Security GmbH, (confidential document)

[8] Protection Profile for Digital Tachograph - Vehicle Unit (VU PP) Version 1.0, 9 May 2017, BSI-CC-PP-0094-2017

[9] *Commission Implementing Regulation (EU) 2016/799* of 18 March 2016 implementing Regulation (EU) 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components, Annex I C last amended by Commission Implementing Regulation (EU) 2018/502 of 28 February 2018

[10] Impact Analysis Report, Continental Automotive GmbH, Revision 1.18, 2020-07-27

[11] Konfigurationsliste zu DTCO 1381 Release 4.0e (Excelsheet), Version 1.20, 23.11.2020, Continental Automotive GmbH (confidential document)

[12] Digitaler Tachograph – DTCO® 4.0 / 4.0e Leitfaden für die Kontrollorgane, BA00.1381.40 202 101, Continental AG, without Version, 2020-11-23 *litv_agd_control*

[13] Digitaler Tachograph DTCO® 4.0 / 4.0e Technische Beschreibung, TD00.1381.40 102 101, Continental AG, Ausgabe 07/2020, 2020-07-09 *litv_agd_technical*

[14] Digitaler Tachograph – DTCO® 4.0e Bedienungsanleitung für Unternehmer & Fahrer, Continental AG, Ausgabe 07/2020, 2020-07-09 *litv_agd_driver*

[15] Technische Beschreibung Digitaler Tachograph DTCO® 1381 – ab Release 4.0 Software Upgrade, Continental AG, Release 4.0, 2020-04-03 *litv_agd_su*

[7] specifically

- 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 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluierungen
- AIS 38, Version 2, Reuse of evaluation results
- AIS 40, Version 1, Use of Interpretation for Security Evaluation and Cerification of Digital Tachographs

[16] Certification Report BSI-DSZ-CC-0827-V8-2020 for Infineon Technologies Smart Card IC (Security Controller) M9900 A22, M9900 C22, M9900 D22,M9900 G11, M9905 A11, M9906 A11 with optional Software Libraries RSA2048, RSA4096, EC, Base,SCL, HCL, PSL and with specific IC dedicated software from Infineon Technologies AG, Bundesamt für Sicherheit in der Informationstechnik, 2020-07-06 *litv_zert_inf*

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 detailed 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-1158-2020

Evaluation results regarding development and production environment

The IT product Digital Tachograph DTCO 1381, Release 4.0e (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 by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 14 December 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.1, ALC_LCD.1, ALC_TAT.1)

are fulfilled for the development and production sites of the TOE listed below:

a) Continental Automotive GmbH, Heinrich-Hertz-Str. 45, 78052 Villingen-Schwenningen, Germany (HW/SW development, HW/SW tests, Manufacturing the final TOE, delivery)

b) Continental Automotive GmbH, 300704 Timisoara, Strada Siemens Nr. 1, Romania (Specification, Implementation, Module tests)

c) Continental Automotive Components (India) Private Ltd, Gold Hill Supreme Park, Shanthipura Main Road, Electronic City Phrase II, Electronic City, Bengaluru, Karnataka 560100, India, 8th-11th Floor, Plot No 21,22,27,28 (SW tests)

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.