Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1131-V3-2026

for

Sensor 2185 (KITAS 4.0) Revision 1.2.2

from

Continental Automotive Technologies GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, 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-1131-V3-2026 (*)

Digital Tachograph: Motion Sensor

Sensor 2185 (KITAS 4.0)
Revision 1.2.2

from	Continental Automotive Technologies GmbH
PP Conformance:	Digital Tachograph - Motion Sensor (MS PP) Version 1.0, 9 May 2017, BSI-CC-PP-0093-2017
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
valid until:	8 February 2031

SOGIS
Recognition Agreement
for components up to
EAL 4

Common Criteria

he 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 and 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, 9 February 2026

For the Federal Office for Information Security

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

Fabian Hodouschek
Head of Certification

L.S.

Sandro Amendola
Director-General Directorate General S

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - 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 licensing 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 2 December 2025, BGBI. 2025, no. 301, p. 2

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 02 December 2025, Bundesgesetzblatt 2025, no. 301

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 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 and ALC_FLR 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 Sensor 2185 (KITAS 4.0), Revision 1.2.2 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1131-V2-2023. Specific results from the evaluation process BSI-DSZ-CC-1131-V2-2023 were re-used.

The evaluation of the product Sensor 2185 (KITAS 4.0), Revision 1.2.2 was conducted by Deutsche Telekom Security GmbH. The evaluation was completed on 21 January 2026. 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 Technologies GmbH.

The product was developed by: Continental Automotive Technologies 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 evaluated guidance documentation, are observed,
- the product is operated in the environment as specified 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. 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. Therefore the BSI reserves the right to revoke the certificate, especially if a exploitable vulnerability of the certified product gets to known.

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 9 February 2026 is valid until 8 February 2031. 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 Sensor 2185 (KITAS 4.0), Revision 1.2.2 has been included in the BSI list of certified products, which is published regularly in the listing found at the BSI Website https://www.bsi.bund.de/dok/Zertifizierung-Gesamtlisten. Further information can be obtained from BSI-Infoline +49 (0)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 Technologies 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 Sensor 2185 (KITAS 4.0).

The TOE is a second generation Tachograph Motion Sensor. A motion sensor is installed within a road transport vehicle as part of a digital tachograph system. Its purpose is to provide a vehicle unit with motion data that accurately reflects the vehicle's speed and distance travelled. The motion sensor is mechanically interfaced to a moving part of the vehicle, which movement is representative of the vehicle's speed and distance travelled. It may be located in the vehicle's gearbox or in any other part of the vehicle. In the operational phase, the motion sensor is connected to a vehicle unit. A motion sensor meeting the requirements of this ST can be paired and used with second-generation vehicle units, or with first generation vehicle units.

The functional requirements for a Motion Sensor are specified in Annex 1C [15], Chapter 3.2, and the common security mechanisms are specified in Appendix 11 of Annex 1C [16]. Aspects of the electrical interface between the motion sensor and vehicle unit are described in ISO 16844-3 [17].

The Security Target [5] is the basis for this certification. It is based on the certified Protection Profile Digital Tachograph - Motion Sensor (MS PP) Version 1.0, 9 May 2017, BSI-CC-PP-0093-2017 [7].

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 [5] and [8], chapter 6.1. They are all selected from Common Criteria Part 2. Thus the claimed set of SFRs in the ST is CC Part2 conformant.

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

TOE Security Functionality	Addressed issue
TOE_SS.Integrity_Authenticity	The TOE provides this security service of ensuring integrity and authenticity of the TOE.
TOE_SS.Identification_Authentication	The TOE provides this security service of identification and authentication of the vehicle unit before access to data and functions is allowed.
TOE_SS.Accuracy	The TOE provides this security service of accuracy of stored, processed and outputted data.
TOE_SS.Access	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.Audit	The TOE provides this security service of audit service to ensure proper audit data generation. The TOE generates audit records for events impairing its security.

TOE Security Functionality	Addressed issue
TOE_SS.Reliability	The TOE provides this security service of reliability of service to ensure proper operation.
TOE_SS.Secured_Data_Exchange	The TOE provides this security service of secured data exchange with the vehicle unit. This will be supported by a specific security controller that is responsible for all cryptographic algorithms and methods.
TOE_SS.Cryptographic_Support	The TOE provides this security service of cryptographic support using standard cryptographic algorithms and procedures. The TOE consists of a specific security controller that is responsible for all cryptographic algorithms and methods as well as for secure storage of security relevant data
TOE_SS.Software_Update	A software update is not supported by the TOE. If a software change is required, a new security certification of the complete TOE is needed. Old motion sensors must be replaced as required.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [5] and [8], chapter 8.

The assets to be protected by the TOE are defined in the Security Target [5] and [8], 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 [5] and [8], chapter 3.

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 52, 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:

Sensor 2185 (KITAS 4.0), Revision 1.2.2

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Sensor 2185 (KITAS 4.0): configuration 1: Sensor 2185.20 (KITAS 4.0) with an aluminum housing and a plastic connector housing	1.22	Separate unit in a closed case (Manufacturing option)
2	HW	Sensor 2185 (KITAS 4.0): configuration 2: Sensor 2185.32 (KITAS 4.0) with a plastic housing	1.22	Separate unit in a closed case (Manufacturing option)
2	DOC	DE_TB_DTCO-2022-02-07, Continental AG [11]	no version, 2022-02	Paper or PDF-file The guidance for the final customer is transported together with the TOE. OEM customers can order the guidance at a later date.
3	DOC	LF_Kontrollorgane-2022-05-18, Continental AG [10]	Version 2.3, 2022-05-18	Paper or PDF-file The guidance for governance bodies can be requested via mail, email or phone directly from the homologation team of the developer that is responsible for managing this certification

Table 2: Deliverables of the TOE

The manufactured device reaches in delivery condition a sorting station. 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. The seal is applied on the seam between aluminium case and plastic connector.

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 TOE must be paired and calibrated with a certified DTCO. The calibration and the pairing are only allowed to be done in a certified workshop. Therefore, the evaluators assume that the document [11] is available to the workshop. This document is part of the TOE configuration and also a DTCO guidance. The delivery procedures for the document are the same as the ones for the DTCO.

The guidance can be requested by the governance body directly from the developer. Because the governance body are trained by the developer, the evaluators assume that the governance body takes care of the proper restrictive handling of [10].

The authenticity of the TOE can be checked by the customer by comparing the identification data stored in the device with the device data on the type plate, see 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:

- To maintain the integrity of motion data supplied to the vehicle unit;
- To demonstrate its authenticity to the vehicle unit through an authenticated pairing process;
- To detect physical tampering;
- To audit security relevant events and send these to the vehicle unit;
- To provide a secure communication channel between itself and the vehicle unit.

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 [5] and [8], chapter 4.2.

5. Architectural Information

A motion sensor is installed within a road transport vehicle as part of a smart tachograph system. Its purpose is to provide a vehicle unit with motion data that accurately reflects the vehicle’s speed and distance traveled.

The motion sensor is mechanically interfaced to a moving part of the vehicle, which movement is representative of the vehicle’s speed and distance traveled. It may be located in the vehicle’s gear box or in any other part of the vehicle. In the operational phase the motion sensor is connected to a vehicle unit. It may also be connected to specific equipment for management purposes, as defined by the manufacturer.

The application is split to be executed by two controllers. Controlling of external interfaces is done by a standard controller (Application Controller - AppCon). A security Controller (SecCon) is used to execute all security enforcing functions and to control the correct operation of the AppCon (as far as possible).

That leads to three relevant security domains:

- Non-protected external world: outside the TOE housing

- Housing protected Application Domain: AppCon and peripherals
- Hardware protected Secure Domain: SecCon, certified security controller

The communication between SecCon and AppCon is based on SecCon services. These services are called for any security related feature of the application. For any service to be requested on the SecCon, a specific protocol is followed. Services are constructed as sequence of subservice steps. Every message provides serviceId, subserviceId and payload.

To protect the system against physical attacks a combination of several countermeasures is implemented.

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 categorizes the tests into non-functional feature tests (e.g., security parameters, performance, interoperability, stability, reliability) and functional test (e.g., pairing process, signal processing, temperature management, interface behaviour). The test documentation consists of a test coverage and depth of testing analysis, a test plan, test specifications, and test result logs. The particular test specifications show:

- Testing steps
- Test description
- Test preconditions
- Test conduction
- Expected results

The test documentation shows that all TSF subsystem behaviour and interactions according to the TOE design and architecture are tested. This includes all interfaces of SFR-enforcing modules.
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 did not conduct additional independent testing for functional aspects.
The evaluator used information from the last re-evaluation of the TOE. The evaluator then derived attack scenarios which cover potential vulnerabilities that result from preliminary findings. For these scenarios the evaluator created penetration tests, so that every attack scenario is tested by at least one relevant penetration test.

TOE test configurations:
No special configuration is made. According to section 1.2.1 of the Security Target [5] and [8] the TOE has various configurations, which are all covered by tests. The configuration state is not important.

No attack scenario with the attack potential Moderate was successful in the TOE's operational environment as defined in the Security Target [5] and [8], provided that all measures required by the developer are applied.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

Sensor 2185.20 (KITAS 4.0) with an aluminum housing and a plastic connector housing and Sensor 2185.32 (KITAS 4.0) with a plastic housing. Details can be found in the Security Target [5] and [8], chapter 1.2.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [6] 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 Apllication of CC to Integrated Circuits
- The Apllication of Attack Potential to Smartcards

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

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-1131-V2-2023, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the updates of the side audits of two sites and the update of the software to increase the side channel resistance of the crypto implementation.

The evaluation has confirmed:

- PP Conformance: Digital Tachograph - Motion Sensor (MS PP) Version 1.0, 9 May 2017, BSI-CC-PP-0093-2017 [7]
- 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 tables presented in chapter 11 and 12 of the Security Target give 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 the these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 52, 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.

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

- For the checking procedure of the KITAS sensor supervisory bodies must request the appropriate documentation [10] from Continental Automotive GmbH.
- For the correct execution of the checking procedure of the KITAS sensor supervisory bodies must follow the instructions in the appropriate documentation [10] from Continental Automotive GmbH, independent from the vehicle unit.
- The guidance [10] and [11] contains the error message: „Geberstörung – eine Dauer von mehr als zwei Minuten. Dies ist ein Hinweis auf eine Sicherheitsverletzung“. This message requires the supervisory body and trustworthy workshops to check the TOE for potential manipulations in detail. It cannot be excluded that a potential attack is not prevented by the security measures oft he housing. For this case the evaluators recommend an X-ray examination of the TOE from the developer to detect such attacks.

11. Security Target

For the purpose of publishing, the Security Target [8] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [5] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12. Regulation specific aspects (eIDAS, QES)

None.

13. Definitions

13.1. 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
DTCO	Digital Tachograph or Smart Tachograph
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GNSS	Global Navigation Satellite System
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
VU	Vehicle Unit

13.2. 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.

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.

14. 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 licensing (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] Security Target BSI-DSZ-CC-1131-V3-2026, Version 1.32, 13 June 2025, Sensor 2185 (KITAS 4.0) Security Target, Continental Automotive Technologies GmbH (confidential document)

[6] Evaluation Technical Report, Version 3.2, 14 January 2026, Evaluation Technical Report BSI-DSZ-CC-1131-V3, Deutsche Telekom Security GmbH, (confidential document)

[7] Digital Tachograph - Motion Sensor (MS PP) Version 1.0, 9 May 2017, BSI-CC-PP-0093-2017

[8] Security Target lite BSI-DSZ-CC-1131-V3-2026, Version 1.32, 13 June 2025, Sensor 2185 (KITAS 4.0) Security Target Lite, Continental Automotive Technologies GmbH (sanitised public document)

[9] Configuration list for the TOE, Version 1.58, Date 12.09.2025, Developer_2185R1.BL.0467.ConfigurationListHom, Continental AG (confidential document)

[10] Guidance documentation for the TOE, Version 2.3, Date 18.05.2022,LF_Kontrollorgane-2022-05-18, Continental Automotive GmbH

[11] Guidance documentation for the TOE, No Version, Date 02.2022, Digitaler Tachograph – DTCO® 4.0 / 4.0e Technische Beschreibung, Continental Automotive GmbH

[12] Guidance documentation for the TOE, Version 1.3, Date 30.11.2021, Sensor 2185 (KITAS 4.0) – Guidance for VU Manufacturers, Continental AG,

[7] specifically

- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile für Evaluationen nach CC
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- 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 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- 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
- AIS 40, Version 1, Use of Interpretation for Security Evaluation and Certification of DigitalTachographs

[13] Rapport de certification ANSSI-CC-2020/24, ST33G1M2A1 C01 including optional crypto-graphic library NesLib and optional library SFM, Agence nationale de la sécurité des sys-tèmes d’information, 2020-05-14

[14] Evaluation Technical Report for composite evaluation Project: ASTIAM2 2023 / ST33G1M2A1 C04, THALES COMMUNICATIONS & SECURITY SAS, Revision 2.0, 2023-12-08(confidential document)

[15] Commission Implementing Regulation (EU) 2016/799, 18.03.2016, implementing Regulation (EU) No 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, Official Journal of the European Union

[16] Appendix 11 of Annex IC of Council Regulation (EEC) No. 165/2014 [15] - Common security mechanisms

[17] ISO 16844-3, Road vehicles, Tachograph systems, Part 3: Motion sensor interface, First edition, 2004-11-01, Corrigendum 1, 2006-03-01

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-1131-V3-2026

Evaluation results regarding development and production environment

The IT product Sensor 2185 (KITAS 4.0), Revision 1.2.2 (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 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 9 February 2026, 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 Technologies GmbH, Heinrich-Hertz-Str. 45, 78052 Villingen (TOE development, testing and building, delivery)

b) Continental Automotive Technologies GmbH, 300704 Timisoara, Strada Siemens Nr. 1,Romania (SW development and testing)

c) Continental Automotive Components (India) Private Ltd, Gold Hill Supreme Software Park, Plot No 21,22,27,28 Shanthipura Rd Electronics City Phase II, Industrial Area Hosur Road 560100 Bangalor Electronic City, Bengaluru, Karnataka 560100, India (SW development)

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [5] and [8]. 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 [5] and [8]) are fulfilled by the procedures of these sites.

Note: End of report