Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1055-2018

for

Digital Tachograph EFAS-4.8 V03.50

from

intellic Germany GmbH

sponsored by

Intellic 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-1055-2018 (*)

Digital Tachograph EFAS-4.8 V03.50

from	intellic Germany GmbH
sponsored by	Intellic 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 und AVA_VAN.5

SOGIS
Recognition Agreement

Common Criteria

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR

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 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 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 4

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.

Bonn,

For the Federal Office for Information Security

Joachim Weber
Head of Branch

L.S.

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

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[2]
- BSI Certification and Approval Ordinance[3]
- BSI Schedule of Costs[4]
- 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 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

3 Ordinance on the Procedure for Issuance of 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

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

- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [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.sogisportal.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: http://www.commoncriteriaportal.org.

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

[5] 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 EFAS-4.8, V03.50 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0980-2017. Specific results from the evaluation process BSI-DSZ-CC-0980-2017 were re-used.

The evaluation of the product Digital Tachograph EFAS-4.8, V03.50 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 31 July 2018. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor is: Intellic GmbH.

The applicant of the certification and the developer of the product is: intellic Germany 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 August 2018 is valid until 13 August 2023. 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 Target and user guidance documentation mentioned herein to

[6] Information Technology Security Evaluation Facility

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 EFAS-4.8, V03.50 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[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] intellic Germany GmbH
Innungsstraße 40
13509 Berlin

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 “EFAS-4.8 V03.50” is a vehicle unit (VU) in the sense of Annex I B [9] intended to be installed in road transport vehicles and which is designed in accordance with the Tachograph Specification [9]. Its purpose is to record, store, display, print and output data related to driver activities. The VU records and stores user activities data in its internal data memory, it also records user activities data in tachograph cards. The VU outputs data to display, printer and external devices. 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 und AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 7.1. 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 Functionality	Addressed issue
SF.ACS	Security Attribute Based Access Control
SF.SECAUDIT	Audit
SF.EX_CONF	Confidentiality of Data Exchange
SF.EX_INT	Integrity and Authenticity of Data Exchange
SF.GEN_SKEYS	Generation of Session Keys
SF.GEN_DIGSIG	Generation of Digital Signatures optionally with Encryption
SF.VER_DIGSIG	Verification of Digital Signatures optionally with Decryption
SF.DATA_INT	Stored Data Integrity Monitoring and Action
SF.IA_KEY	Key Based User / TOE Authentication
SF.INF_PROT	Residual Information Protection
SF.FAIL_PROT	Failure and Tampering Protection
SF.SELFTEST	Self Test
SF.UPDATE	VU Software Upgrade

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 8.1.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 4.1. 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 4.2, 4.3 and 4.4.

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 EFAS-4.8, V03.50

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/ SW	EFAS-4.8 V03.50	EFAS-4.8 Hardware version 80 Software version V03.50	The VU is delivered as entire device (packed together with its accessories and the Operating Manual [12]). The possible variants of the VU are a combination of non-security relevant options as described below.
2	DOC	Operating Manual [12] (“Bedienungsanleitung Digitaler Tachograph EFAS-4.8”)	German version document number: 1030-130-SEC-DE05 file name: 1030-130-SEC-BDA_E4_8.pdf	The Operating Manual is delivered in paper form (together with the VU) or in electronic pdf-form.
3	DOC	Service and Installation Manual [13] (“Werkstatt-Handbuch Digitaler Tachograph EFAS-4.8” for workshop personnel)	German version document number: 1030-131-SEC-DE15_WHB_E4_8 file name: 1030-131-SEC-DE15_WHB_E4_8.pdf	The Service and Installation Manual is delivered in paper form or in electronic pdf-form.

Table 2: Deliverables of the TOE

The delivery of the TOE from the production facility to the customer which is a distributor or a workshop is described briefly in the following: At delivery the TOE is completely assembled and the TOE's case is leaded. The TOE is packed together with its accessories and the Operating Manual [12]. The Service and Instruction Manual [13] will be delivered usually in electronic form as pdf-file embedded into a pgp-encrypted file secured by password via download from the intellic-website portal. The TOE is marked with a machine readable label which shows the TOE’s reference, the serial number and the configuration. The serial number is also fixed within the TOE and can be read out from outside. The firmware of the Security Controller and the Main Controller cannot be modified anymore except by means of an update procedure based on VU specific and EU secrets (loaded into the Security Controller during personalisation). The TOE software version (V 03.50) is

stored within the Security Controller, can be read out from outside and is readable on the print outs. The customer orders the TOE from the intellic GmbH. In case of an order the customer is informed about the delivery process by fax or by email. The information about the delivery process contains the serial numbers of the Vehicle Units sent to the consumer. Furthermore, the consumer is informed that he has to compare the serial numbers after receipt.

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 data to be measured (the physical data measurement is performed by the motion sensor which is not part of this TOE) and recorded and then to be checked by control authorities must be available and reflect fully and accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed.

It concretely means that security of the VU aims to protect

a) 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,

b) the integrity and authenticity of data exchanged between the motion sensor and the vehicle unit,

c) the integrity and authenticity of data exchanged between the recording equipment and the tachograph cards, and

d) the integrity and authenticity of data downloaded (locally and remotely).

The main security feature stated above is provided by the following major security services:

a) Identification and authentication of motion sensor und tachograph cards,

b) Access control to functions and stored data,

c) Accountability of users,

d) Audit of events and faults,

e) Object reuse for secret data,

f) Accuracy of recorded and stored data,

g) Reliability of services,

h) Data exchange with motion sensor, tachograph cards and external media (download function).

‘Identification and Authentication’ as well as ‘data exchange’ directly require cryptographic support according to [6], sec. 7.1.

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. The following topics are of relevance:

Secure development and manufacturing environment, secure data generation and cryptographically strong security data, secure transport procedures, secure delivery processes, secure upgrade process, removal of test points in final TOE, availability and traceability of tachograph cards, law enforcement controls and regular inspections, faithful drivers that possess only one driver card and type approval of motion sensors. Details can be found in the Security Target [6], chapter 5.2.

5. Architectural Information

The TOE is a composite product. It is composed of the Security Controller hardware including crypto library provided by INFINEON (Subsystem SC-HW), the software of the Security Controller developed by intellic Germany GmbH (Subsystem SC-SW), and all other components of the TOE (Subsystem VU Platform) as Main Controller (MC) including its software, MC-Flash ROM as well as MC-RAM, power supply, Case Open Supervision (COS) and Real Time Clock (RTC).

More detailed information can be found in the Security Target [6], chapters 2.1 to 2.3.

For details concerning the CC evaluation of the INFINEON Security Controller (SC-HW) see the evaluation documentation under the certification ID BSI-DSZ-CC-0891-V3.

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

7.1. Developer Testing

The test configuration is based on the TOE as described in [6]. For testing the developer provided the release version R003. The tests conducted are based on R003. The TOE's software version V03.50 is identical to the actual and proved release version R003.

There are three different kinds of test procedures used by the developer. The first procedure is to test the TOE through a python script which automatically starts the tachograph card simulator and triggers all operations. The second procedure is to prove the behaviour of the TOE by conducting a code review. The third type of tests is debug-testing. They are conducted with a special version of the TOE software where the developer can use breakpoints and hooks.

The evaluators have verified that all descriptions and interactions are tested. All SFR-enforcing descriptions and interactions are mapped to appropriate tests. By mapping each subsystem and module to at least one test case every subsystem except of SC-HW is covered. The subsystem SC-HW is tested implicitly because it comprises the utilised Security Controller which is tested functionally by all tests.

The tests covered all TSFIs as well as each subsystem and module.

All test results were as expected.

7.2. Independent Evaluator Testing

The evaluators repeated a wide range of the developer tests in the lab of the ITSEF and defined some additional independent tests, which were executed by the developer because they required the debug test environment.

The evaluators centred their test activities with tests on

- commands and operations / sequences according to the identification and authentication process,
- access control according to rights to functions,
- accountability by holding identification data permanent available,
- audit capabilities in case of security breaches,
- object re-use of temporary storage objects,
- reliability on the availability of data,
- cryptographic support.

The overall test result is that no deviations were found between the expected and the actual test results.

7.3. Penetration Testing

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 test results showed that the TOE in its operational environment is resistant against attackers with high attack potential

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

The TOE EFAS-4.8 V03.50 is an electronic device, consisting of hardware and software, and additionally of documentations.

The hardware components include the Main Controller (STM32F429) with Flash and RAM, the Security Controller (SLE78CFX3000P), the Real Time Clock (PCF2127T), the Case Open Supervision, the Card Readers #1 and #2 (C702 10M008 925 4), the Printer (ELM208-V10-LV), the Display, the Keypad, LED and Buzzer, the Power Supply hardware and the battery as well as the metal case.

The TOE software V03.50 is divided into the following four parts:

- EUApplication, identifier "V3.50_00003"
- EUBootcode, identifier "V3.50_00003"
- LangEu, identifier "V3.50_00002"
- EUSC, identifier "V3.50_00002"

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, [4] (AIS 34), and guidance specific for the technology of the product.

The following guidance specific for the technology was used regarding the composite aspect:

(i) The Application of CC to Integrated Circuits

(ii) The Application of Attack Potential to Smartcards

(iii) JIL 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 [14, 15]) have been applied in the TOE evaluation.

(see [4], AIS 25, AIS 26, 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 und 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-0980-2017, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the new main controller, the STM32F429 with Cortex-M4 core by STMicroelectronics.

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 und 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 strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded

as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

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	Validity Period
Decryption and data integrity protection	AES in CBC and COUN-TER mode and CMAC	[FIPS 197] (AES), [NIST SP800-38A] (AES CBC mode), [NIST SP800-38B] (AES CMAC), [NIST SP800-38D] (COUNTER)	128 bits	TR-02102-1	The related commission regulation [9] does not make any restrictions
Encryption, decryption, Retail-MAC	Triple DES in CBC and ECB modes	[ISO16844] for the Mo-tion Sensor and [CSM] for the Tachograph Cards	112 bits	[9]	See above
Decryption, verifying for the Tachograph Cards authen-tication and signing for downloading to external media	RSA	[CSM], CSM_020 for the Tachograph Cards authentication and [CSM], CSM_034 for down-loading to external media	1024 bits	[9]	See above

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).

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

AES	Advanced Encryption Standard
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
CBC	Cipher Block Chaining
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CMAC	Cipher-Based Message Authentication Code
COS	Case Open Supervsion
cPP	Collaborative Protection Profile
CSM	Common Security Mechanism
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
ECB	Electronic Code Book (an operation mode of a block cipher)
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MC	Main Controller
PP	Protection Profile
RSA	Rivest-Shamir-Adleman Algorithm
RTC	Real Time Clock
SAR	Security Assurance Requirement
SC	Security Controller
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TR	Technische Richtlinie / Technical Guideline

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
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, http://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[8] 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-1055-2018, Version 35, 30.05.2018, Security Target EFAS-4.8, intellic Germany GmbH

[7] Evaluation Technical Report, Version 1.8, 26.07.2018, SRC Security Research & Consulting GmbH, (confidential document)

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

[9] Annex I B of Commission Regulation (EC) No. 1360/2002 'Requirements for construction, testing, installation and inspection', 05.08.2002 and last amended by CR (EC) No. 432/2004 and corrigendum dated as of 13.03.2004 (OJ L 77)

[10] Appendix 11 of Annex I B of Commission Regulation (EEC) No. 1360/2002 – Common Security Mechanisms

[11] EFAS-4.8 V03.50 Konfigurationsliste, Version 07, 03.04.2018 file name: 1220-111-SEC-DE07_APPR_Konfigurationsliste.docx, intellic Germany GmbH (confidential document)

[12] Bedienungsanleitung Digitaler Tachograph EFAS-4.8, Copyright 2017 Intellic GmbH, Hausmannstätten, Österreich, file name: 1030-130-SEC-BDA_E4_8.pdf

[13] Werkstatt-Handbuch Digitaler Tachograph EFAS-4.8, Copyright 2011-2017 Intellic GmbH, Hausmannstätten, Österreich file name: 1030-131-SEC-DE15_WHB_E4_8.pdf

[14] Certification Report BSI-DSZ-CC-0891-V3-2018 for Infineon Security Controller, M7892 Design Steps D11 and G12, with specific IC dedi-cated firmware and optional software, BSI, 09.01.2018

[15] Evaluation Technical Report for Composite Evaluation (ETR COMP) - M7892 G12 and D11 - BSI-DSZ-CC-0891-V3, TÜV Informationstechnik GmbH, Version 1, 2017-11-29 (confidential document)

[8] 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 38, Version 2.9, Reuse of evaluation results

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 http://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-1055-2018

Evaluation results regarding development and production environment

The IT product Digital Tachograph EFAS-4.8, V03.50 (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 14 August 2018, 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) intellic Germany GmbH, Innungsstraße 40, 13509 Berlin (Tegel), Germany (Development)

b) BAŞARI TEKNOLOJİK SİSTEMLER SAN. VE TİC. A.Ş. Alcı (OSB) Mahallesi 2030. Cadde No:8 06930 Sincan Ankara TÜRKİYE (Production, Delivery)

c) Bosch Car Multimedia Portugal S.A. Rua Max Grundig, 35 Lomar, Apartado 2458, 4705 820 Braga PORTUGAL (Production, Delivery)

d) For the development and production sites of the underlying HW platform SLE78CFX3000P please see Annex B of the Certification Report BSI-DSZ-CC- 0891-V3-2018 for Infineon Security Controller [14]

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.

Note: End of report