Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0726-2012

for

Digital Tachograph EFAS-4.0, Version 02

from

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-0726-2012

Digital Tachograph EFAS-4.0
Version 02

from	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, AVA_VAN.5

Common Criteria Recognition Arrangement for components up to EAL 4

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 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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.

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, 9 January 2012

For the Federal Office for Information Security

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

Bernd Kowalski
Head of Department

L.S.

for components up to EAL 4

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

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

Contents

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 European Recognition of ITSEC/CC – Certificates (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 technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp.E3 (basic). In Addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

[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 a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

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

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

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom.Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

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

2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of September 2011 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. 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 nations listed above.

This evaluation contains the components ATE_DPT.2 and AVA_VAN.5 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4 components of these assurance families are relevant.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Digital Tachograph EFAS-4.0, Version 02 has undergone the certification procedure at BSI.

The evaluation of the product Digital Tachograph EFAS-4.0, Version 02 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 19 December 2011. The SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: intellic GmbH.

The product was developed by: intellic GmbH.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

4 Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

[6] Information Technology Security Evaluation Facility

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report and in the Security Target.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods 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-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.

5 Publication

The product Digital Tachograph EFAS-4.0, Version 02 has been included in the BSI list of the 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 GmbH
Fernitzerstraße 5
A-8071 Hausmannstätten
Österreich

This page is intentionally left blank.

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 “EFAS-4.0 V02” provided by intellic Germany GmbH. This is a Vehicle Unit (VU for short) in the sense of Annex 1 B of the Commission Regulation (EC) No 1360/2002 and last amended by CR (EC) No. 68/2009 and CR (EU) No. 1266/2009 on recording equipment in road transport [9]. It is intended to be installed in road transport vehicles and will be used within the Tachograph System to store, display, print and output data related to driver activities in accordance with the requirements of [9].

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 [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, AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 8.1. 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 Functionalities:

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 9.1.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 5.1. 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 5.2 to 5.4.

This certification covers the following configuration of the TOE: EFAS-4.0 V02, Hardware/Software, for delivery configurations see chapter 8.

The vulnerability assessment results as stated within this certificate does 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-4.0, Version 02

The following table outlines the TOE deliverables:

No	Type	Delivery	Identification	Date	Form of Delivery
1	HW/SW	Vehicle Unit EFAS-4.0 with software version V02	The TOE's reference "EFAS-4.0 V02" is shown on the machine readable label. The software version can be displayed or printed as "02.00".	-	The VU is delivered as entire device (packed together with its accessories and the Operating Manual). The possible variants of the VU are a combination of non-security relevant options as described below.
2	DOC	Operating Manual ("Bedienungsanleitung Digitaler Tachograph EFAS")	German version document number: 1030-130-SEC-DE02 file name: 1030-130-SEC-DE02_APPR_E4-BDA.pdf	2011	The Operating Manual is delivered in paper form (together with the VU) or in electronic pdf-form.
3	DOC	Service and Installation Manual ("Digitaler Tachograph EFAS-4.0 Werkstatt-Handbuch" for work-shop personnel)	German version document number: 1030-131-SEC-DE04 file name: 1030-131-SEC-DE04_APPR_E4-WH.pdf	2011	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 (EFAS-4.0 V02) 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 sealed. The TOE is packed together with its accessories and the Operating Manual. The Service and Instruction Manual will be delivered generally in electronic form as pdf-file embedded into a pgp-encrypted file secured by password via email. 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 any more 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 (V02) is stored within the

Security Controller, can be read out from outside and is readable on the print outs. The consumer orders the TOE by the intellic Germany GmbH. In case of an order the consumer 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 features stated above are 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).

Detailed information is given in [6], chapter 8.1.

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:

a) Design environment

OE.Development
VU developers shall ensure that the assignment of responsibilities during development is done in a manner which maintains IT security.

b) Manufacturing environment

OE.Manufacturing
VU manufacturers shall ensure that the assignment of responsibilities during manufacturing is done in a manner which maintains IT security and that during the manufacturing process the VU is protected from physical attacks which might compromise IT security.

OE.Sec_Data_Generation
Security data generation algorithms shall be accessible to authorised and trusted persons only.

OE.Sec_Data_Transport
Security data shall be generated, transported, and inserted into the TOE, in such a way to preserve its appropriate confidentiality and integrity.

OE.Delivery
VU manufacturers, vehicle manufacturers and fitters or workshops shall ensure that handling of the TOE is done in a manner which maintains IT security.

OE.Software_Upgrade
Software revisions shall be granted security certification before they can be implemented in the TOE. The software parts for updates have to be secured during the generation and transport to the VU.

OE.Sec_Data_Strong
Security data inserted into the TOE shall be as cryptographically strong as required by [10].

OE.Test_Points
All commands, actions or test points, specific to the testing needs of the manufacturing phase of the VU shall be disabled or removed before the VU activation by the VU manufacturer during the manufacturing process.

Please note that the design and the manufacturing environments are not the intended usage environments for the TOE. The security objectives for these environments being due to the current security policy (OE.Development, OE.Manufacturing, OE.Test_Points, OE.Delivery) are the subject to the assurance class ALC. Hence, the related security objectives for the design and the manufacturing environments do not address any potential TOE user and, therefore, cannot be reflected in the documents of the assurance class AGD.

The remaining security objectives for the manufacturing environment (OE.Sec_Data_Generation, OE.Sec_Data_Transport, OE.Sec_Data_Strong and

OE.Software_Upgrade) are subject to the ERCA and MSA Policies and, therefore, are not specific for the TOE.

c) Workshops environment

OE.Activation Vehicle manufacturers and fitters or workshops shall activate the TOE after its installation before the vehicle leaves the premises where installation took place.

OE.Approved_Workshops Installation, calibration and repair of recording equipment shall be carried by trusted and approved fitters or workshops.

OE.Faithful_Calibration Approved fitters and workshops shall enter proper vehicle parameters in recording equipment during calibration.

d) End-user environment

OE.Card_Availability Tachograph cards shall be available to TOE users and delivered by Member State Authorities to authorised persons only.

OE.Card_Traceability Card delivery shall be traceable (white lists, black lists), and black lists must be used during security audits.

OE.Controls Law enforcement controls shall be performed regularly and randomly, and must include security audits.

OE.Driver_Card_Uniqueness Drivers shall possess, at one time, one valid driver card only.

OE.Faithful_Drivers Drivers shall play by the rules and act responsibly (e.g. use their driver cards; properly select their activity for those that are manually selected).

OE.Regular_Inspections Recording equipment shall be periodically inspected and calibrated.

OE.Type_Approved_MS The Motion Sensor of the recording equipment connected to the TOE shall be type approved according to Annex I B.

Details can be found in the Security Target [6], chapter 6.2.

5 Architectural Information

The TOE is a composite product. It is composed from 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 Plattform) as Main Controller (MC) including its soft-ware, MC-Flash ROM as well as MC-RAM, power supply, Case Open Supervision (COS) and Real Time Clock (RTC).

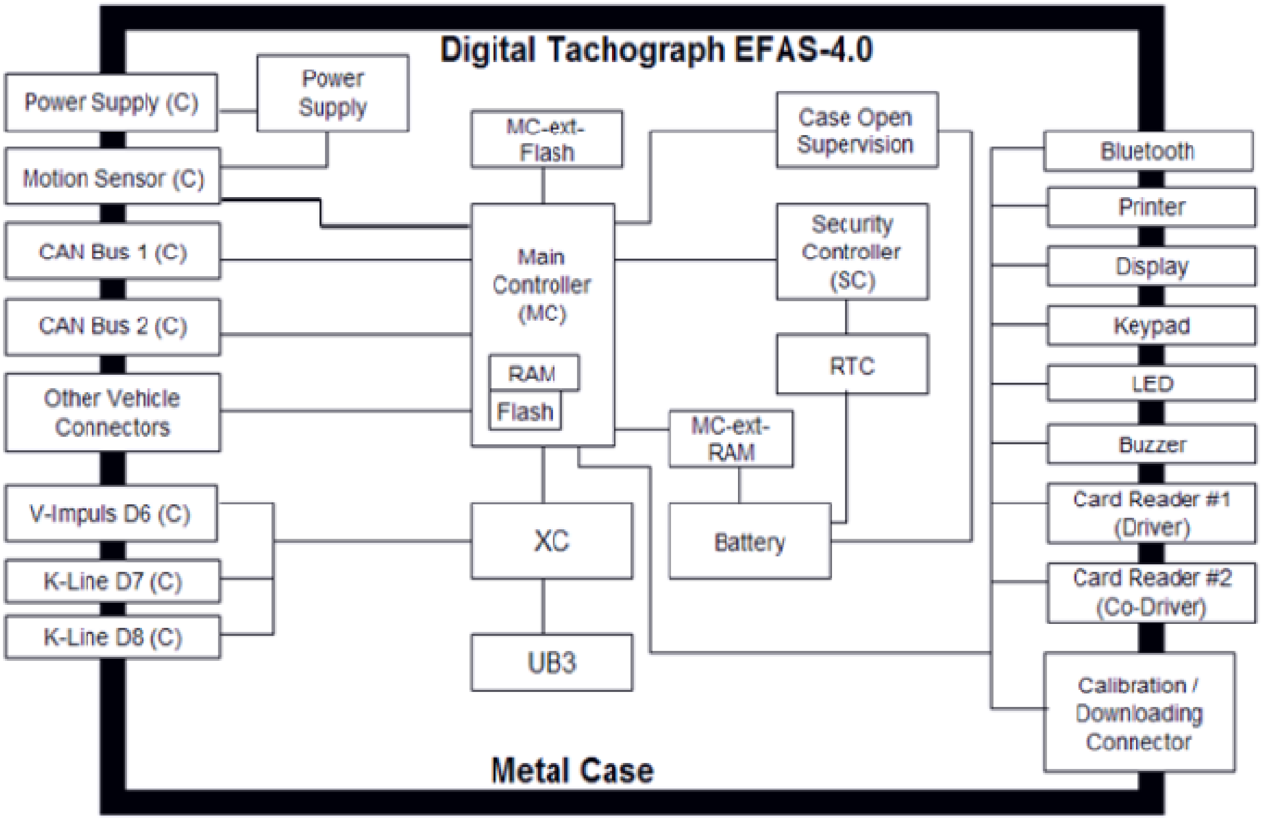

Figure 1 - External Interfaces EFAS 4.0

For details concerning the CC evaluation of the Infineon Security Controller (SC-HW) see the evaluation documentation under the certification ID BSI-DSZ-CC-0727-2011.

Figure 1 shows the external interfaces of the TOE: power supply connector, connector to the motion sensor, CAN connectors, K-line connector, info interface connector, other vehicle connectors, calibration/downloading connector, interface to card readers for tachograph cards and user interface. Only the subsystem (VU Platform) has externally visible interfaces.

Besides the mentioned physical interfaces/connectors the following logical interfaces are defined:

- vehicle connection to power supply
- vehicle connection to motion sensor
- external interfaces to calibration/diagnosis equipment, company server, local downloading equipment, visual instruments and other vehicle connections
- tachograph card readers
- user interface (display, keypad and printer, LED and buzzer as warning elements)

The security functionality is enforced by the SC subsystems and supported by the VU platform. The following Figure 2 shows the decomposition of the TOE into subsystems. It shows the interfaces between the subsystems and that the sub-systems depend on each other.

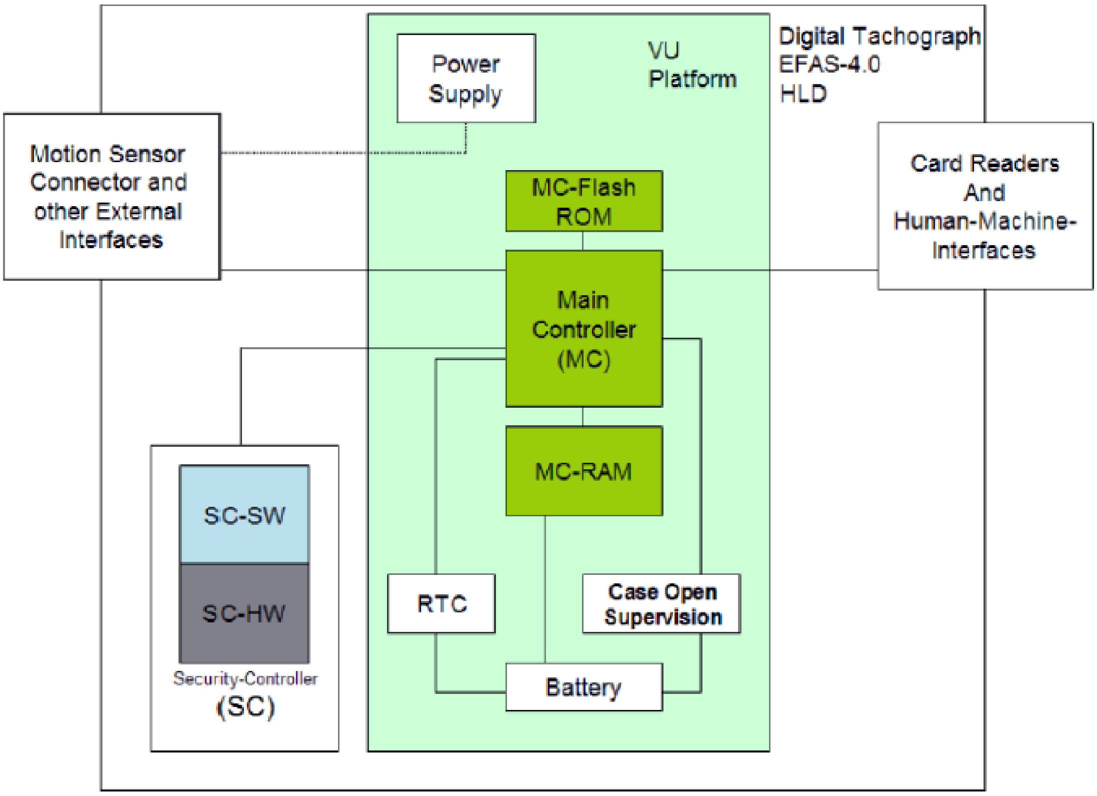

Figure 2 - High Level Design EFAS-4.0

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 Test Configuration

The developer used for their tests a simulated environment (including motion sensor and tachograph cards and different software tools for simulation of their behaviour).

7.2 Tests of the Developer

The test configuration is based on the TOE as described in [6]. For testing the developer provided two software versions, namely release versions R419 and R422. The tests conducted are based on R419 except the additional PSWUPDATE tests. The TOE's software version V02.00 is identical to the actual and proved release version R422.

The developer's tests can be categorised into tests according to the requirements of [10] (functional tests) and tests of the security requirements which are described in the test specification. The behaviour of each security function is covered by test cases using these different approaches.

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. Therefore the relevant classes of the TOE are analysed and commented by the developer. The third type of tests is debug-testing. They are conducted with a special version of the TOE software where the developer can use break-points and hooks.

7.3 Independent Evaluator Tests

The independent testing of the TOE was performed using the developer’s testing environment. All configurations of the TOE being intended to be covered by the current evaluation were tested. The overall test result is that no deviations were found between the expected and the actual test results.

Independent testing approach:

The independent evaluator tests were conducted at SRC in Bonn using the test equipment of the developer. The components – hardware and software – used for testing as well as the configuration of the test environment and the TC-Card Simulation are described within the developer's documents. Furthermore these documents contain examples of use of the 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 permanently available
- Audit capabilities in case of security breaches
- Object re-use of temporary storage objects
- Reliability on the availability of data
- Cryptographic support

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

The TOE EFAS-4.0 V02 is an electronic device, consisting of hardware and software, and additionally of documentations.

The hardware components include the Main Controller (ET-AUT040E-3IN) with Flash and RAM, the Security Controller (SLE78CFX1600P), the Real Time Clock (DS3234SN), the Case Open Supervision, the Card Readers #1 and #2 (C702 10M008 925 4), the Printer (ELM 208-LV-EFK), the Display, the Keypad, LED and Buzzer, the Power Supply hardware and the battery as well as the metal case.

The TOE software V02 is divided into the following three parts:

- SC Software EUSC, identifier "V2.00_00027"
- MC Boot Software EUBootcode, identifier "V2.00_00032"

- MC Application Software EUApplication, identifier "V2.00_00024" (which includes EUBaseSoftware, identifier "V0.05_00024")

Possible variants of the Vehicle Unit EFAS-4.0 V02 may be derived through combinations of the following non-security relevant options:

Code	Option	Description
OP_NOACCEL	Acceleration sensor	The 3-axis acceleration sensor is not populated.
OP_D6OCL	D6 as Open-Collector	The Pin D6 is configured as Open-Collector
OP_D7INF	D7 as Info-Interface	The Pin D7 is configured as Info-Interface
OP_SPI	SPI Interface	The plug for the SPI-Interface is populated
OP_FJPRN	Fujitsu Printing Device	The Mainboard is populated for use of a Fujitsu Printing Device
OP_SCNOHT	SC without heating	No heating for Security Controller
OP_D6HWD	D6 hard-wired with B6/B7	Impulse at D6 = B6/B7 (no scaling factor possible)
OP_NOCANAD	No CAN_A-Bus inductor	No CAN-Bus inductor at CAN_A
OP_NOCANCD	No CAN_C-Bus inductor	No CAN-Bus inductor at CAN_C

Table 3: Variant options

Code	Color Display	Color Keyboard
CL_YY	Yellow	Yellow
CL_AA	Amber	Amber
CL_GG	Green	Green
CL_BR	Blue	Red

Table 4: Color options

These options may be combined freely on demand of a customer. Whenever such a variant is to be manufactured on demand of a customer, a Product Code is assigned to the variant. The following example shows combinations of options:

Produkt name	Product code	Color code	OP_NOACCEL	OP_D6OCL	...
E4 AMO Standard	PCE400001	CL_YY	-	-	...
E4 AMO w/o 2nd Source internal	PCE400002	CL_YY	X	-	...
	PCE400003				...

Table 5: Combinations of options

The TOE includes all possible combinations of options.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [8] 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 used up to EAL4 extended by advice of the Certification Body for components beyond EAL 4 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

(see [4], AIS 25, AIS 27, AIS 36) were used.

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

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

The evaluation has confirmed:

● PP Conformance:	Digital Tachograph - Vehicle Unit (VU PP) Version 1.0, 13 July 2010, BSI-CC-PP-0057-2010 [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 evaluation facility has examined that the analysis of used cryptographic algorithm (Triple DES, AES and RSA) meets all the requirements with regard to the specification of Annex 1B defined by the European Commission [9]. The cryptographic algorithms, mentioned above, are used by the TOE to enforce its security policy. For more details (e.g. key length) please refer to Security target [6], chapter 9. For further information please refer to [10] to [14].

The strength of the 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 policies 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 for the TOE is required and thus requested from the sponsor of the certificate.

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
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
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionalities
VU	Vehicle Unit

12.2 Glossary

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

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

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

Informal - Expressed in natural language.

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

Protection Profile - An implementation-independent statement of security needs for a TOE type.

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 - A set of software, firmware and/or hardware possibly accompanied by guidance.

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 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 3, July 2009

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8].

[5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-CC-0726-2012, Version 18, 10.11.2011, Security Target EFAS-4.0, intellic Germany GmbH

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

[8] Evaluation Technical Report, Version 1.1, 02.12.2011, SRC Security Research & Consulting GmbH, (confidential document)

[9] Annex 1B of Council Regulation (EEC) No. 3821/85 amended by CR (EC) No. 1360/2002, CR (EC) No. 432/2004 and corrigendum dated from 13.03.2004 (OJ L 77) and last amended by CR (EU) No.1266/2009

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

[11] Federal Information Processing Standards Publication 197 (FIPS PUB 197). Advances Encryption Standard (AES), 2001

[12] NIST. Recommendation for Block Cipher Modes of Operation: Methods and Techniques, Special Publication SP800-38A, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 2001

[13] NIST. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication SP800-38B, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 2001

[14] ISO 16844-3 Road vehicles. Tachograph systems. Motion Sensor Interface . WD 3-20/05/99. and ISO 16844-4 Road vehicles, Tachograph systems. CAN interface

[8] specifically

- AIS 25, Version 6, 7 September 2009, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 7, 3 August 2010, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 32, Version 6, 3 August 2010, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 36, Version 3, 19 October 2010, Kompositionsevaluierung including JIL Document and CC Supporting Document

C Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - CC Part 3 extended - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation

Assurance Class	**Assurance Components**
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Assurance Class	**Assurance Family**	**Assurance Components by Evaluation Assurance Level**						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 8.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 8.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

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

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0726-2012

Evaluation results regarding development and production environment

The IT product Digital Tachograph EFAS-4.0, Version 02 (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 guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 9 January 2012, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1)

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

a) intellic Germany GmbH, Voltastr. 5, 13335 Berlin (Development)

b) Funkwerk Dabendorf GmbH, Märkische Str. 15806, Dabendorf (Production)

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.

This page is intentionally left blank.