Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0474-2008

for

Digital Tachograph EFAS-3 V01

from

EFKON AG

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-0474-2008

Digital Tachograph (Vehicle Unit)

Digital Tachograph EFAS-3 V01

from EFKON AG

Functionality: Product specific Security Target according to Appendix 10 of Annex 1(B) of Council Regulation (EEC) No. 3821/85 amended by Council Regulation (EC) No. 1360/2002 and last amended by CR (EC) No. 432/2004 on recording equipment in road transport;
Common Criteria Part 2 conformant

Assurance: Common Criteria Part 3 conformant,
EAL4 augmented by ADO_IGS.2, ADV_IMP.2, ATE_DPT.2 and AVA_VLA.4;
equivalent to ITSEC E3 high as required by Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002

Common Criteria Arrangement for components up to EAL 4

Common Criteria

The IT product identified in this certificate has been evaluated at an accredited and licensed / approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

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, 19 June 2008

For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Bernd Kowalski
Head of Department

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

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 setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

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 2.3 (ISO/IEC 15408:2005)[5]
- Common Methodology for IT Security Evaluation, Version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

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

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998.

This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

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

---

2 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

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 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria 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 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC.

As of February 2007 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, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations resp. approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

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

This evaluation contains the components ADO_IGS.2, ADV_IMP.2, ATE_DPT.2, AVA_VLA.4 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-3 V01 has undergone the certification procedure at BSI.

The evaluation of the product Digital Tachograph EFAS-3 V01 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 6 June 2008. The SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the applicant is: EFKON AG

The product was developed by: EFKON AG

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

[6] Information Technology Security Evaluation Facility

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

- 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 and the confirmed strength of functions, 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 may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular basis.

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.

5 Publication

The product Digital Tachograph EFAS-3 V01 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// 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] EFKON AG
Andritzer Reichsstrasse 66
8046 Graz
Österreich

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 EFAS-3 V01 is a Digital Tachograph device that operates in road vehicles and is therefore commonly called vehicle unit. The vehicle unit records and stores data related to driver activities of road transport vehicles. It is also able to display, print and output information related to the stored data.

To get information about the vehicle's motion, it is connected to a motion sensor that is mounted in the gearbox of the vehicle. To avoid manipulations, the speed pulses from the motion sensor are secured by an additional encrypted communication path between the motion sensor and the vehicle unit.

To identify themselves to the vehicle unit, the drivers of the vehicle have to use tachograph cards. The driver and the co-driver, if present, have to insert their tachograph cards into the dedicated slots of the vehicle unit when using the vehicle. These tachograph cards are also used by vehicle unit to record and store user activities.

The main hardware components of the vehicle unit are the Main Controller (MC), the Security Controller (SC), the Real Time Clock (RTC) buffered by an internal Battery, a 2 row 16 characters per row LC display, 6 input keys, a thermal printer and two card readers. The main software components of the TOE are the MC software and the SC software. The security functions are concentrated in the SC and its software. As security controller the microcontroller AT90SC144144CT (ATMEL) was chosen.

The Digital Tachograph EFAS-3 V01 is designed to fulfil the requirements to a vehicle unit (VU) of the standardised European Tachograph System described in the Tachograph Specification [13], Annex 1B main body and its appendices. This Security Target reflects the Vehicle Unit Generic Security Target in appendix 10 of the Tachograph Specification [13].

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see part C or [3], part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL4 augmented by ADO_IGS.2, ADV_IMP.2, ATE_DPT.2 and AVA_VLA.4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5.1. They are all selected from Common Criteria Part 2. Thus the TOE is CC part 2 conformant.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6], chapter 5.2.

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

TOE Security Function	Addressed issue
F.ACS	Security Attribute Based Access Control
F.GENAUDIT	Generates records of auditable events
F.IA_KEY	Key Based User / TOE Authentication
F.DATA_INT	Stored Data Integrity Monitoring and Action

TOE Security Function	Addressed issue
F.EX_CONF	Confidentiality of Data Exchange
F.EX_INT	Integrity and Authenticity of Data Exchange
F.INF_PROT	Residual Information Protection
F.FAIL_PROT	Failure and Tampering Protection
F.SELFTEST	Self Test
F.GEN_SKEYS	Generation of Session Keys
F.GEN_DIGSIG	Generation of Digital Signatures optionally with Encryption
F.VER_DIGSIG	Verification of Digital Signatures optionally with Decryption

Table 1: TOE Security Funktions

For more details please refer to the Security Target [6], chapter 6.1.

The claimed TOE's strength of functions 'high' (SOF-high) for specific functions as indicated in the Security Target [6], chapter 6.2 is confirmed. The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security [6], chapter 3.1. Based on these assets the security environment is defined in terms of assumptions, threats and policies. This is outlined in the Security Target [6], chapter 3.

This certification covers the following configurations of the TOE:

- EFAS-3 V01, Hardware/Software, for delivery configurations see chapter 8.
- Operating manual EFAS-3, 5340.029.DOC.D05.FM (German version), 5340.029.DOC.E01.FM (English version), delivered in paper / electronic pdf-form
- Workshop personnel Service and Installation Manual EFAS-3, 5340.028.DOC.D05, delivered in paper / electronic pdf-form
- The hardware components include the Main Controller (MC, AT91SAM7A1-AU) with Flash and RAM, the Security Controller (SC, ATMEL AT90SC320288RCT/A T90SC144144CT), Real Time Clock (M41T81M6F), Case Open Supervision, Card Reader #1 and #2 (C702 10M008 925 4), Printer (ELM 208-LV-EFK), Display, Keypad, LED and Buzzer, Power Supply and Battery as well as the Metal Case.

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-3 V01

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	EFAS-3 Vehicle Unit	V01, delivery configurations: table 4	
2	SW	EFAS-3 Software	V01.01	installed on HW
2	DOC	Operating manual EFAS-3	German: 5340.029.DOC.D05.FM [9,11] English: 5340.029.DOC.E01.FM [10]	paper / pdf
3	DOC	Workshop personnel Service and Installation Manual EFAS-3	5340.028.DOC.D05 [12]	paper / pdf

Table 2: Deliverables of the TOE

The delivery of the TOE (EFAS-3 V01 and Operating manual EFAS-3) from the production facility to the customer which is a distributor or a workshop is described briefly in the following. In case of a workshop the Workshop personnel Service and Installation Manual EFAS-3 is delivered too. At this point of the life cycle the TOE is completely assembled and the TOE case itself and the battery box are leaded. The TOE is marked with a machine readable label which shows the configuration and the serial number. Additionally the serial number is also fixed within the TOE and can be read from outside and the firmware of the security controller cannot be modified anymore. The firmware versions of the security controller and the main controller are fixed and readable from outside. The TOE software version (V01.01) is readable on the print outs. In case of a order the customer is informed about the delivery process by fax or by secured email. The information about the delivery process contains the serial number(-s) of the vehicle units later sent to the customer. Furthermore the customer is informed that an additional information is sent about the shipment of the ordered vehicle units and that the customer has to compare the serial number(-s) after reception.

3 Security Policy

The security policy is expressed by the set of security functional requirements and implemented by the TOE. As a digital tachograph, the VU is installed in a road vehicle. The main tasks of the VU are:

- To record motion data and driver activities for later examination by a control body.
- To support the driver to meet the legal regulations (road speed limits, driving times).
- To transmit the user activities data for recording in tachograph cards or other storage media.

It covers also the issue Access Control. Detailed information is given in [6], chapter 5.1.1.

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:

The assignment of responsibilities during development, responsibilities during manufacturing, handling of non activated EFAS-3, activation, access to security data generation algorithms, confidentiality and integrity of generation transportation and insertion of security data, authorised tachograph cards delivery and availability, uniqueness of driver cards, tracebility of card delivery, trustworthy of fitters and workshops, regularity of inspections, faithful calibration of vehicle parameters, equipment operation by faithful drivers, regular and random law enforcement controls, certification grant of software updates.

Details can be found in the Security Target [6] chapter 4.2.

5 Architectural Information

The TOE is composed of the Security Controller Hardware, including crypto library provided by ATMEL (Subsystem SC-HW), the Software of the Security Controller developed by EFKON AG (Subsystem SC-SW), and all other components of the TOE (Subsystem VU Plattform), i.e. Main Controller (MC) including its software, MC-Flash ROM as well as MC-RAM, Power Supply, Case Open Supervision, Real Time Clock (RTC) and the Battery.

The following figure 1 shows the decomposition of the TOE into subsystems. The figure shows the interfaces between the subsystems and that the subsystems depend on each other.

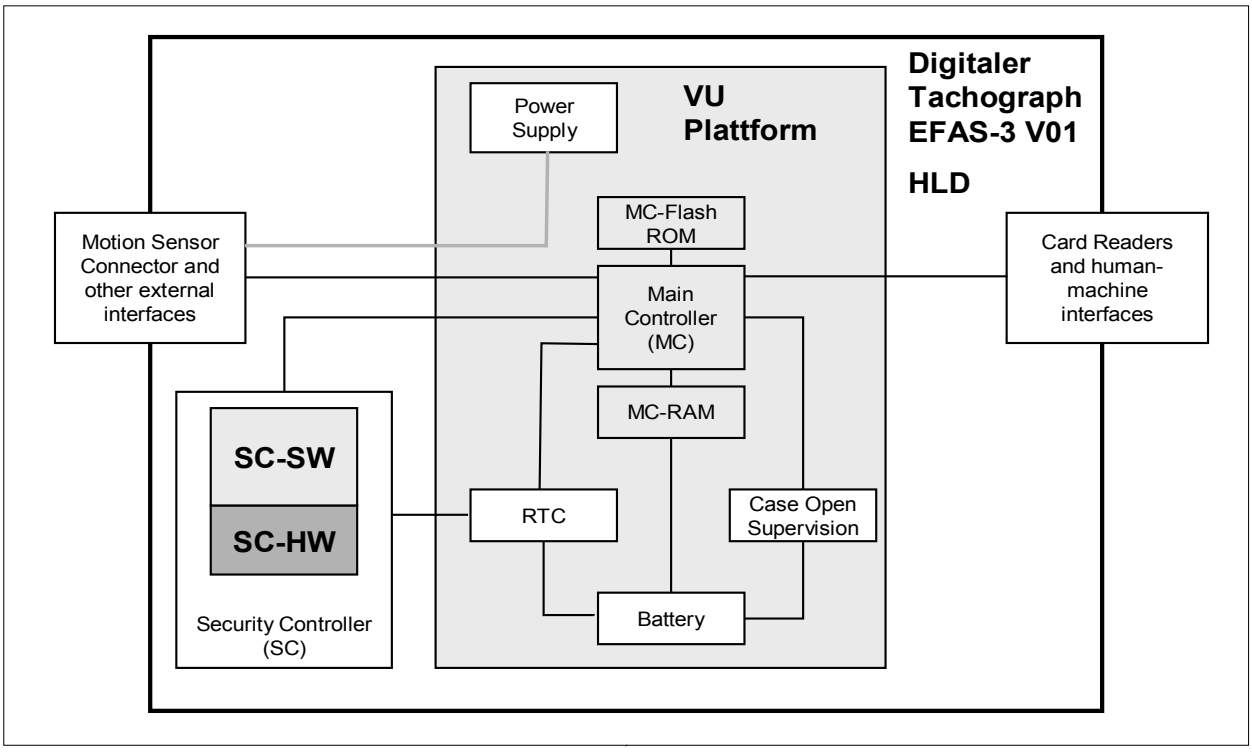

Figure 1: Decomposition of the TOE into its subsystems

Besides the mentioned interfaces/connectors the following input/output interfaces are connected to the Main Controller:

- vehicle connections to the power supply, the motion sensor, and other external connections
- interfaces to tachograph card readers and other human machine interfaces

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 following table displays a mapping of the tools and equipment used for testing:

Tool	Manufacturer	Type	Version
System test specification			
2 non-activated	EFKON mobility	HW	EP000210, SW V01.00 and SW V01.01
2 motion sensors	Siemens VDO	HW	KITAS 2171-50
2 driver cards	Sagem Orga	HW	DR24220FL
2 company cards	Sagem Orga	HW	CP24220FL
2 workshop cards	Sagem Orga	HW	WO24220FL
2 control cards	Sagem Orga	HW	CT24220FL
2 card simulator (MAKInterface with serial cable and a PCB board with card contacts)	Maki GmbH	HW	MAKInterface Pro LP
1 E-Tacho	Siemens VDO	HW	1323.0301
1 Systemtestumgebung	EFKON mobility	HW	01
EFAS Download Tool	EFKON mobility	SW	1.07
Tacho Card Simulator	EFKON mobility	SW	commserver V1.8 tcsimulator V1.10
Software for Systemtestumgebung	EFKON mobility	SW	0.28.0
Test specification security requirements			
2 non-activated	EFKON mobility	HW	EP000210, SW V01.00 and SW V01.01
2 motion sensors	Siemens VDO	HW	KITAS 2171-50
2 driver cards	Sagem Orga	HW	DR24220FL
2 company cards	Sagem Orga	HW	CP24220FL
2 workshop cards	Sagem Orga	HW	WO24220FL
2 control cards	Sagem Orga	HW	CT24220FL
1 Systemtestumgebung	EFKON mobility	HW	01

Tool	Manufacturer	Type	Version
1 card simulator (MAKInterface with serial cable and a PCB board with card contacts)	Maki GmbH	HW	MAKInterface Pro LP
1 Getriebesimulator (gearing simulator)	cb-electronics	HW	ZESPÓŁ NAPĘDOWY TC-1/ZN
1 Card Reader	ChipDrive	HW	CDX330
Motion Sensor Simulator	EFKON mobility	SW	1.1
Tacho Card Simulator	EFKON mobility	SW	commserver V1.8 tcsimulator V1.10
Company Server Simulator	EFKON	SW	0.02.015
Security Server Simulator	EFKON mobility	SW	1.0
EFAS Download Tool	EFKON mobility	SW	1.07
Software for Systemtestumgebung	EFKON mobility	SW	0.28.0

Table 3: mapping of the tools and equipment used for testing

7.2 Tests of the Developer

Tests claimed by the Official Journal of the European Union [13] were performed successfully. The developer provided a test case set which includes a full coverage of all security functionality as well as functional testing of the TOE. There are test cases for every TSF interface. For the execution of these test cases the developer uses real tachograph cards as well as simulated cards within the TC-Card simulation. Additionally the following cathegories were examined:

- Commands and operations / sequences according to the identification and authentication process
- Access control depending on the operating mode
- Data exchange with external devices
- The TOE's reaction due to card conflicts particularly with regard to event data

All commands and all functions are tested with valid and invalid inputs.

7.3 Independent Evaluator Tests

The tests in Bonn were done with the developer's system test environment using a real EFAS-3 which was in an activated state as well as simulated cards within the TC-Card Simulation implemented by the developer.

For the test with the simulator performed by the evaluators, the identification of the correct versions of the electronic data used (Flash and RAM program files, resp. the corresponding sources) is relevant in order to identify the correct version and configuration of the TOE. For this the methods of the configuration management system Microsoft Visual SourceSafe (VSS) were used. The version control mechanism of VSS can guarantee that the design files used for testing are those provided by the developers for a specific version of the TOE.

The evaluators decided to focus their own independent tests on tests with simulated cards within the TC-Card simulation:

- In order to check a specific part of F.ACS, the evaluators decided to check whether an appropriate reaction to unauthorized access takes place.
- In order to check that the TOE enforces the identification and authentication process, the evaluators decided to use test cases where a specific PDU command was tested. Additionally the evaluators checked whether an appropriate reaction to erroneous cards as well as to copied and restored data takes place.
- In order to check the confidentiallity, integrity and authenticity of the data transfer, the evaluators decided to use test cases where the mechanisms of encryption and MAC calculation for secure messaging were used.
- In order to check whether the signature algorithm is calculated correctly and uses the correct keys, the evaluators checked whether an appropriate reaction to an erroneous secret key takes place.
- In order to check that session keys are produced and used accordingly, the evaluators decided to use a test case where PDU commands related to the creation and usage of session keys were used.
- In order to check whether the configuration of the test object complies with the configuration of the TOE of the Security Target, the evaluators checked that it was installed properly and was in the specified state.

Aditionally a DPA analysis for the EFAS-3 was performed in a reproducible way.

The achieved test results correspond to the expected test results.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

- EFAS-3 V01, Hardware/Software, the following delivery configurations are possible in accordance with the corresponding type code:

EFAS-3 V01	**24**	**gg**	**D7**	**A1**	**C0**	**R1**	*Code*	*Meaning*
								R0 = no additional data recording R1 = additional data recording for rpm, speed and status inputs
								C0 = no CAN bus on connector C C1 = CAN bus on connector C with terminating resistor
								A0 = no CAN bus on connector A A1 = CAN bus on connector A with terminating A2 = resistor CAN bus on connector A without terminating resistor
								D7 = K-Line connected to D7 D8 = Info interface connected to D8
								aa = Display, keyboard illumination: amber/amber br = Display, keyboard illumination: blue/red gg = Display, keyboard illumination: green/green yy = Display, keyboard illumination: yellow/yellow
								12 = 12 V power supply 24 = 24 V power supply

Table 4: System of the type code

The TOE variants are necessary to operate in the environment of vehicles from different vehicle manufacturers or different categories of vehicles. Therefore, there are two main hardware versions possible for the VU: EFAS-3 V01 24 and EFAS-3 V01 12 for vehicles with a 24 V resp. a 12 V power supply.

- Operating manual EFAS-3, 5340.029.DOC.D05.FM (German version), 5340.029.DOC.E01.FM (English version), delivered in paper / electronic pdf-form
- Workshop personnel Service and Installation Manual EFAS-3, 5340.028.DOC.D05, delivered in paper / electronic pdf-form
- The hardware components: the Main Controller (MC, AT91SAM7A1-AU) with Flash and RAM, the Security Controller (SC, ATMEL AT90SC320288RCT/A T90SC144144CT [14,15]) covering the main security functionality implementation, the Real Time Clock (M41T81M6F), the Case Open Supervision, the Card Reader #1 and #2 (C702 10M008 925 4), the Printer (ELM 208-LV-EFK), the Display, the Keypad, the LED and the Buzzer, the Power Supply hardware and the battery as well as the Metal Case.
- The VU-software, Ver. V01.01

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 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) Transition from ITSEC to CC

(iii) Composite product evaluation

(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 class ASE
- All components of the EAL4 package as defined in the CC (see also part C of this report)
- The components ADO_IGS.2, ADV_IMP.2, ATE_DPT.2, AVA_VLA.4 augmented for this TOE evaluation.

The evaluation has confirmed:

- for the functionality: Product specific Security Target according to Appendix 10 of Annex 1(B) of Council Regulation (EEC) No. 3821/85 amended by Council Regulation (EC) No. 1360/2002 and last amended by CR (EC) No. 432/2004 on recording equipment in road transport;
  Common Criteria Part 2 conformant
- for the assurance: Common Criteria Part 3 conformant,
  EAL4 augmented by ADO_IGS.2, ADV_IMP.2, ATE_DPT.2 and AVA_VLA.4;
  equivalent to ITSEC E3 high as required by Appendix 10 of Annex 1B of Regulation (EC) no. 1360/2002
- The following TOE Security Functions fulfil the claimed Strength of Function: high

  F.IA_KEY: Key based user / TOE Authentication
  F.GEN_KEYS: Generation of Session Keys
  F.GEN_DIGSIG: The SHA-1 implementation in the function *Generation of Digital Signatures optionally with Encryption.*
  Refer to chapter 9.2 for this rating.
  F.VER_DIGSIG: The SHA-1 implementation in the function F.VER_DIGSIG *Verification of Digital Signatures optionally with Decryption*
  Refer to chapter 9.2 for this rating.

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

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

9.2 Results of cryptographic assessment

The following cryptographic algorithms are used by the TOE to enforce its security policy:

hash functions:

- the SHA-1 implementation in the TOE Security Function F.GEN_DIGSIG (Generation of Digital Signatures optionally with Encryption),
- the SHA-1 implementation in the TOE Security Function F.VER_DIGSIG (Verification of Digital Signatures optionally with Decryption,

algorithms for the encrytion and decryption:

- the RSA implementation in the TOE Security Function F.GEN_DIGSIG (Generation of Digital Signatures optionally with Encryption),
- the RSA implementation in the TOE Security Function F.VER_DIGSIG (Verification of Digital Signatures optionally with Decryption).

The strength of these cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 4, Para. 3, Clause 2) as they are prefined by the Official Journal of the European Union [13] and implemented accordingly.

10 Obligations and notes for the usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered.

- Signature creation and verification using RSA encryption, decryption and key generation with a key length of 1024 bits and the usage of SHA-1 remain valid unless a new version of the Official Journal of the European Union [13] is published. Transition periods shall be considered.

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

- The operational documentation [9,10,11] contains necessary information about the usage of the TOE. For secure usage of the TOE the fulfilment of the assumptions about the environment in the Security Target [6] has to be taken into account. In case of a workshop the Workshop personnel Service and Installation Manual EFAS-3 has to be taken into account too.

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

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

EAL Evaluation Assurance Level

EFAS Elektronischer Fahrtenschreiber (electronic tachograph)

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

PDU Protocol Data Unit

PP Protection Profile

SF Security Function

SFP Security Function Policy

SOF Strength of Function

ST Security Target

TOE Target of Evaluation

TSC TSF Scope of Control

TSF TOE Security Functions

TSP TOE Security Policy

VU Vehicle Unit

12.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance 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 entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

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

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methology for Information Technology Security Evaluation (CEM), Evaluation Methology, Version 2.3, August 2005

[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, BSI 7149), periodically updated list published also on the BSI Website

[6] Security Target BSI-DSZ-0474-2008, Version 05, 04.04.2008, EFAS-3 V01 Security Target, Efkon mobility GmbH

[7] Evaluation Technical Report, Version 1.20, 04.06.2008, Evaluation Technical Report (ETR) EFAS-3 V01, SRC GmbH (confidential document)

[8] Configuration list for the TOE, Version 07, 03.06.2008, EFAS-3 V01 Konfigurationsliste, Efkon mobility GmbH (confidential document)

[9] Operating manual EFAS-3, file 5340.029.DOC.D05 (German version), 2007, EFKON mobility GmbH

[10] Operating manual EFAS-3, file 5340.029.DOC.E01 (English version), 2007, EFKON mobility GmbH

[11] Bedienungsanleitung Korrekturblatt, Dokumentnummer 5345.029.DOC.D00, 2007, Digitaler Tachograph EFAS-3 Bedienungsanleitung, Efkon mobility GmbH

[12] Workshop personnel Service and Installation Manual EFAS-3, file 5340.028.DOC.D05, EFKON mobility GmbH

[13] Official Journal of the European Union: VO (EG) Nr. 1360/2002
Annex 1B of Commission Regulation (EC) No.1360/2002 on recording equipment in road transport: Requirements for Construction, Testing, Installation and Inspection (in: Official Journal of the European Communities, L 207 / 1 ff.), Commission of the European Communities, 05.08.2002
corrected by
Corrigendum dated 13.03.2004 to Commission Regulation (EC) No. 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council

[8] specifically

- AIS 25, Version 3, 6 August 2007, Anwendung der CC auf Integrierte Schaltungen including JIL Document resp. CC Supporting Document
- AIS 26, Version 3, 6 August 2007, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document resp. CC Supporting Document
- AIS 27, Version 2, 23 June. 2005 Transition from ITSEC to CC
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 36, Version 2, 12 November 2007, Kompositionsevaluierung including JIL Document resp. CC Supporting Document

Regulation (EEC) No. 3821/85 on recording equipment in road transport (Official Journal of the European Communities L 207 of 5 August 2002)]

[14] Longbow Security Target – Evaluation of the AT90SC320288RCT/ AT90SC144144CT MCU, Longbow_ST_V1.3 (03 Aug 06), ATMEL

[15] Rapport de certification 2006/20, 16.11.2006, Microcontrôleur sécurisé ATMELAT90SC320288RCT/ AT90SC144144CT rev. G, Secrétariat général de la défense nationale - Direction centrale de la sécurité des systèmes d'information, France

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

- **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
- **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

- **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.”

“Assurance Class	**Assurance Family**
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements ”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.”

“Assurance Class	**Assurance Family**
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

“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 11.1)

“Table 6 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 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 extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“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 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, and that it provides useful protection against identified threats.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

“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 practice. 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 11.5)

“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 practices.

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 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices 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 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices 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 11.8)

“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 11.9)

“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.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim."

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users."

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis."

"Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential."

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 35

Annex B of Certification Report BSI-DSZ-CC-0474-2008

Evaluation results regarding development and production environment

The IT product Digital Tachograph EFAS-3 V01 (Target of Evaluation, TOE) has been evaluated at an accredited and licensed / approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005) .

As a result of the TOE certification, dated 13 June 2008, the following results regarding the development and production environment apply. The Common Criteria assurance requirements

- ACM – Configuration management (i.e. ACM_AUT.1, ACM_CAP.4, ACM_SCP.2),
- ADO – Delivery and operation (i.e. ADO_DEL.2, ADO_IGS.2) and
- ALC – Life cycle support (i.e. ALC_DVS.1, ALC_LCD.1, ALC_TAT.1),

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

a) EFKON mobility GmbH, Voltastraße 5, 13335 Berlin (Development)

b) FLEXAutomotive, FLEXTRONICS, Zrinyi ut 38, H-8900 Zalaegerszeg, Hungary (Production)

For development and production sites regarding the ATMEL chip AT90SC320288RCT/ AT90SC144144CT rev. G refer to [20].

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.