Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0889-2013

for

tru/cos tacho v1.1

from

Trueb 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-0889-2013

Tachograph Card

tru/cos tacho v1.1

from	Trueb AG
PP Conformance:	Protection Profile Digital Tachograph - Smart Card (Tachograph Card), Version 1.02, 15 November 2011, BSI-CC-PP-0070-2011
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ATE_DPT.2 and 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 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1 and according to Commission Regulation (EC) No. 1360/2002 Annex 1(B) adapting to Council Regulation (EC) No. 3821/85 amended by Commission Regulation (EC) No. 432/2004 of 5 March 2004, Council Regulation (EC) No. 1791/2006 of 20 November 2006 and Commission Regulation (EC) No. 68/2009 of 23 January 2009, Commission Regulation (EU) No. 1266/2009 of 16 December 2009 on recording equipment in road transport.

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

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, 28 June 2013

For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED

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 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 EAL 1 to EAL 4 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 EAL 4 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 EAL 4 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 tru/cos tacho v1.1 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0764-2012. Specific results from the evaluation process BSI-DSZ-CC-0764-2012 were re-used.

The evaluation of the product tru/cos tacho v1.1 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 25 June 2013. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Trueb AG.

The product was developed by: Trueb 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, as 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.

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 tru/cos tacho v1.1 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Trueb AG
Hintere Bahnhofstrasse 12
5000 Aarau
Schweiz

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 Tachograph Card product tru/cos tacho v1.1 provided by Trueb AG, based on the hardware platform SLE78CFX2000P from Infineon Technologies AG (Certificate-ID: BSI-DSZ-CC-0782-2012, [12]).

The Tachograph Card is configured and implemented as a driver card, workshop card, control card or company card in accordance with the Tachograph Card specification documents [14] to [18] and conforms with the following standards:

- ISO/IEC 7810 Identification cards – Physical characteristics
- ISO/IEC 7816 Identification cards - Integrated circuits with contacts:
- Part 1: Physical characteristics
- Part 2: Dimensions and location of the contacts
- Part 3: Electronic signals and transmission protocols
- Part 4: Inter-industry commands for interchange
- Part 8: Security related inter-industry commands
- ISO/IEC 10373 Identification cards – Test methods

This Tachograph Card is intended to be used in the Digital Tachograph Systems which contain additionally Motion Sensors and Vehicle Units as recording equipment. The main security features of the TOE are as specified in the Tachograph Card specification [17]:

- The TOE must preserve card identification data and cardholder identification data stored during the card personalisation process.
- The TOE must preserve user data stored in the card by Vehicle Units.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Protection Profile Digital Tachograph - Smart Card (Tachograph Card), Version 1.02, 15 November 2011, BSI-CC-PP-0070-2011 [8].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ATE_DPT.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

Identifier	Addressed issue
SF.PERSO	Card Personalisation
SF.MUT_AUTH	Mutual Authentication
SF.VERIFY	PIN Verification
SF.SM	Secure Messaging
SF.CERT	Certificate Verification and Unwrapping

Identifier	Addressed issue
SF.SIG	Digital Signature Creation and Verification
SF.HASH	Hash Calculation
SF.SES_KEY	Session Key Generation and Limit of Use
SF.ACC	Access Control Mechanism
SF.INTEGRITY	Data Integrity Checks
SF.SELFTEST	Self Test
SF.DATA_ERASURE	Erasure of Data after Usage
SF.HW_PROTECTION	Hardware Protection Mechanisms
SF.SW_PROTECTION	Software Protection Mechanisms

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

This certification covers the following configurations of the TOE: Tachograph Card as driver card, workshop card, control card respective company card. The different configurations of the TOE are described in detail in the Tachograph Card specification [16] and in the guidance documents [9], [10] and [11].

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

tru/cos tacho v1.1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/SW	Initialised module with hardware for contact-based interface. This part of the TOE consists of: Hardware platform: SLE78CFX2000P with its specific IC Dedicated Software and with cryptographic libraries from Infineon Technologies AG IC Embedded Software: Tachograph Operating System (implemented in ROM/EEPROM of the IC) Tachograph Application (as initialisation table and already installed on the TOE)	SLE78CFX2000P (M7892 B11) with ROM mask and initialisation file, for identification data see below	The IC with its Dedicated Software and with the Embedded Software are providing self-protection mechanisms, ensuring confidentiality and integrity during delivery. The delivery does not need additional security measures and can be considered as normal transport.
2	SW	Master Embedding Key (MEK): 3DES key which is unique for each tru/cos tacho v1.1 personalisation agency	---	Item in electronic form, secured against disclosure and modification.
3	DOC	tru/cos tacho v1.1 – Initialization Manual (AGD_PRE) [9]	Version 1.10, 2013-04-22	Document in electronic form.
4	DOC	tru/cos tacho v1.1 – Personalisation Manual (AGD_OPE.Perso) [10]	Version 1.10, 2013-05-23	Document in electronic form.
5	DOC	tru/cos tacho v1.1 – Enduser Manual (AGD_OPE.Enduser) [11]	Version 1.01, 2013-03-15	Document in electronic form.

Table 2: Deliverables of the TOE

To verify that the user has the correct Tachograph Card, it can be identified by the following means as described in the guidance document for the personalisation agent [10], chapter 3.2 and in the guidance document for the end user [11], chapter 2:

The verification of the correct Tachograph Card has to be checked using the GET DATA command which returns the following data:

- The Mask Name equals: ‘43543100000000000000’
- The Mask Version equals: ‘11’
- The Loaded Modules equal: ‘00’
- The Chip Name equals: ‘534C45373843465832303030 50’
- The current life cycle phase equals: ‘04’ (during personalisation phase) or ‘05’ (for end usage phase)
- The ROM EDC matches: ‘A5F7’ (this information is not available for the end user)

In addition, the Tachograph Card can be identified by the ATR Historical Bytes set during the initialisation process. With the ATR, the personalisation agent can check the values of the Equipment Type, Country Personalizer ID, Product Type and Profile ID that were set during the initialisation.

The value for the Equipment Type are set to:

‘00’ = COMPLETE APPLICATION command has not been executed

‘01’ = Driver card

‘02’ = Workshop card

‘03’ = Control card

‘04’ = Company card

The end user can identify the type of the personalised Tachograph Card by the command sequence as described in [11], chapter 2.2:

1. RESET
2. # SELECT MF/DF.TACHOGRAPH

   ‘00 A4 04 0C 06 FF 54 41 43 48 4F’
3. # SELECT EF.APPLICATION ID

   ‘00 A4 02 0C 02 05 0A’
4. # READ BINARY

   ‘00 B0 00 00 01’

The READ BINARY command response can be used to identify the type of the Tachograph Card:

‘01’ = Driver card

‘02’ = Workshop card

‘03’ = Control card

‘04’ = Company card

For the evaluation process the whole life cycle of the TOE was considered during the evaluation as far as the developer/manufacturer of the TOE is directly involved. The module initialisation as part of phase 5 of the TOE's life cycle belongs to the TOE development in the sense of the CC. The TOE is delivered as an initialised module, i.e. it contains all software and at least the data structures as defined in the Tachograph Card specifications [14] to [18], but isn’t embedded in a plastic card and isn’t personalised yet. The TOE can be delivered as already configured initialised module, i.e. as initialised driver card, workshop card, control card respective company card. Alternatively, the TOE can be delivered as initialised module without card configuration, and prior to the personalisation of the product the personalisation agent has to choose and set up the concrete card configuration (by calling the command COMPLETE APPLICATION).

3 Security Policy

The TOE will be used as Tachograph Card and is implemented as the composition of an IC with appropriate Smart Card Embedded Software. A Tachograph Card is intended to be

used in the Digital Tachograph Systems which contain additionally Motion Sensors and Vehicle Units as recording equipment.

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the Digital Tachograph System related issues as outlined in the following.

The main security features of the TOE are as specified in the Tachograph Card specification [17]:

- The TOE must preserve card identification data and cardholder identification data stored during the card personalisation process.
- The TOE must preserve user data stored in the card by Vehicle Units.

The main security features stated above are provided by the following major security services:

- User and Vehicle Unit identification and authentication.
- Access control to functions and stored data.
- Accountability of stored data.
- Audit of events and faults.
- Accuracy of stored data.
- Reliability of services.
- Data exchange with a Vehicle Unit and export of data to a non-Vehicle Unit.
- Cryptographic support for ‘identification and authentication’ and ‘data exchange’ as well as for key generation and distribution in corresponding case according to [18], chapter 4.9.

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:

- OE.Personalisation_Phase: Secure Handling of Data in Personalisation Phase.
- OE.Tachograph_Components: Implementation of Tachograph Components.

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

5 Architectural Information

The TOE is a composite product. It is composed from an Integrated Circuit with its IC Dedicated Software and IC Embedded Software. The latter part contains in particular the Tachograph Card Operating System (realised as native implementation) and the Tachograph Application with its dedicated file system, access rules and cryptographic data for the respective Tachograph Card type.

According to the TOE design and the TOE's global architectural structure the security functionality of the TOE is enforced by the following subsystems:

- Tachograph Application Layer (card type specific file structure, access rules and cryptographic data, as accessible in the TOE's life cycle phase 7).
- Tachograph Card Operating System:
  - S.APP_Level (initialisation, personalisation and end usage phase commands).
  - S.Core_Level (IC platform independent operating system parts).
  - S.HAL_Level (IC platform dependent operating system parts).
- IC Infineon SLE78CFX2000P with its specific IC Dedicated Software and cryptographic libraries.

For details concerning the CC evaluation of the underlying IC see the evaluation documentation under the certification ID BSI-DSZ-CC-0782-2012 [12].

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

The developer tested all TOE security functionality either on real cards or with emulator tests. For all commands and functionality tests, test cases are specified in order to demonstrate its expected behaviour including error cases. Hereby, a representative sample including all boundary values of the parameter set, e.g. all command APDUs with valid and invalid inputs, was tested and all functionality was tested with valid and invalid inputs.

The tests were performed with the composite smartcard product tru/cos tacho v1.1 on the IC Infineon SLE78CFX2000P. All four possible configurations (driver card, company card, control card and workshop card) were tested appropriately. The testing comprises tests in different life cycle states (personalisation, end usage) and with different protocols (T=0 and T=1). The tests of the Tachograph Card product tru/cos tacho v1.1 are based on the comprehensive Collis Tachograph Card test tools. Thereby different Collis test tools are used for testing of functional requirements given in the Tachograph Card specifications [14] to [18] to ensure that a European Digital Tachograph Card is personalised correctly and correct file structure and data are given and to test the T=0 and T=1 protocols. Furthermore, additional test cases are implemented to cover test aspects such as emulator tests, test in the personalisation phase and test power-loss resistance of the Tachograph Card Operating System.

Repetition of developer tests was performed during the independent evaluator tests.

Since much of the security functionality can be tested by APDU command sequences, the evaluators performed these tests with real cards. This is considered to be a reasonable approach because the developer tests include a full coverage of all security functionality. Furthermore, penetration tests were chosen by the evaluators for that security functionality where internal secrets of the card could maybe be modified or observed during testing. During their independent testing, the evaluators covered

- testing APDU commands related to Key Management and Crypto Functions,
- testing APDU commands related to NVM Management and File System,
- testing APDU commands related to Security Management,
- testing APDU commands related to Secure Messaging,
- penetration testing related to verify the Reliability of the TOE,
- source code analysis performed by the evaluators,
- side channel analysis for cryptographic implementations,
- fault injection attacks (laser attacks),
- testing APDU commands for the initialisation, personalisation and usage phase,
- testing APDU commands for the commands using cryptographic mechanisms.

The evaluators tested the TOE systematically against high attack potential during their penetration testing.

The achieved test results correspond to the expected test results.

8 Evaluated Configuration

The TOE tru/cos tacho v1.1 was evaluated in all of its four configurations as described in the Security Target [6]:

- Driver card,
- Control card,
- Company card,
- Workshop card.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL 5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

- Application of CC to Integrated Circuits.
- Smart Card evaluation guidance.
- Application of Attack Potential to Smart Cards.
- Composite product evaluation for Smart Cards and similar devices (see AIS 36). According to this concept the relevant guidance documents of the underlying platform and the documents ETR for Composition from the platform evaluations (i.e. on hardware [12], [13]) have been applied in the TOE evaluation.

- Functionality classes and evaluation methodology of true random number generators.

(See [4], AIS 25, AIS 26, AIS 31, AIS 32, AIS 34, AIS 36, AIS 38.)

For RNG assessment the scheme interpretations AIS 31 was used (see [4]). Refer to BSI-DSZ-CC-0782-2012 [12].

To support composite evaluations according to AIS 36 the document ETR for composite evaluation [13] was provided and approved. This document provides details of this platform evaluation that have to be considered in the course of a composite evaluation on top. The IC Infineon SLE78CFX2000P with its specific IC Dedicated Software and cryptographic libraries from Infineon Technologies AG was certified under BSI-DSZ-CC-0782-2012 [12].

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

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

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0764-2012 [24], re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the following aspects:

- Change of the underlying IC to the IC Infineon SLE78CFX2000P with its specific IC Dedicated Software and cryptographic libraries from Infineon Technologies AG as certified under BSI-DSZ-CC-0782-2012 [12].
- Bugfixing related to the TOE's functionality.
- Integration of existing patch code into the ROM mask.
- Adaptation of the access rules for the file system in the TOE's personalisation phase.
- Update of user guidance documentation due to TOE changes and for editorial corrections.

The evaluation has confirmed:

● PP Conformance:	Protection Profile Digital Tachograph - Smart Card (Tachograph Card), Version 1.02, 15 November 2011, BSI-CC-PP-0070-2011 [8]
● for the Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
● for the Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ATE_DPT.2 and AVA_VAN.5

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

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

9.2 Results of cryptographic assessment

The following cryptographic algorithms are used by the TOE tru/cos tacho v1.1 to enforce its security policy:

Algorithm	Bit Length	Purpose	Security Functionality (Portion of the TSF)	Standard of Implementation	Standard of Usage
Triple DES (3DES) in CBC mode	128 (112 effective)	Encryption / decryption	SF.SM	FIPS PUB 81 [23]	Tachograph Card Specifications [14]-[18]
Retail-MAC	128 (112 effective)	Generation / verification of message authentication code	SF.SM	ANSI X9.19 [19]	Tachograph Card Specifications [14]-[18]
RSA	1024	Encryption / decryption / signature creation / signature verification	SF.MUT_AUTH, SF.SIG	RSASSA-PKCS1-v1_5 [20]	Tachograph Card Specifications [14]-[18]
RSA	1024	Certificate verification	SF.CERT	ISO/IEC 9796-2 [22]	Tachograph Card Specifications [14]-[18]
SHA-1	160	Hash value calculation	SF.HASH	FIPS PUB 180-3 [21]	Tachograph Card Specifications [14]-[18]

Table 3: Deliverables of the TOE

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). According to the Tachograph Card specifications [14] to [18], the algorithms mentioned in table 3 above are considered in the framework of the Digital Tachograph Systems as to be suitable for the calculation of hash values, the creation and verification of digital signatures, the verification of certificates, the authentication protocols and the establishment and execution of a trusted channel between the TOE and the external world. For this reason, an explicit validity period of each algorithm is not defined.

10 Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

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

APDU	Application Protocol Data Unit
AIS	Application Notes and Interpretations of the Scheme
ATR	Answer To Reset
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
DES	Data Encryption Standard
3DES	Triple DES
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read-Only Memory
ETR	Evaluation Technical Report
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MAC	Message Authentication Code
NVM	Non-Volatile Memory
PP	Protection Profile
ROM	Read Only Memory
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

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 - A 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 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 4, September 2012

[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-0889, tru/cos tacho v1.1 Security Target, Version 1.13, 24 June 2013, Trueb AG

[7] Evaluation Technical Report (ETR), Product: tru/cos tacho v1.1, Certification ID: BSI-DSZ-CC-0889, Version 3, Date: 24 June 2013, Evaluation Facility: TÜV Informationstechnik GmbH (confidential document)

[8] Protection Profile Digital Tachograph - Smart Card (Tachograph Card), Version 1.02, 15 November 2011, BSI-CC-PP-0070-2011, Bundesamt für Sicherheit in der Informationstechnik

[9] tru/cos tacho v1.1 – Initialization Manual (AGD_PRE), Version 1.10, 22 April 2013, Trueb AG

[10] tru/cos tacho v1.1 – Personalisation Manual (AGD_OPE.Perso), Version 1.10, 23 May 2013, Trueb AG

[11] tru/cos tacho v1.1 – Enduser Manual (AGD_OPE.Enduser), Version 1.01, 15 March 2013, Trueb AG

[12] Certification Report for BSI-DSZ-CC-0782-2012 for Infineon smart card IC (Security Controller) M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware) from Infineon Technologies AG, 11 September 2012, Bundesamt für Sicherheit in der Informationstechnik

[8] specifically

- AIS 25, Version 7, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 8, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 2.1, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 36, Version 3, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.9, Reuse of evaluation results

[13] ETR for composition according to AIS 36, M7892 B11, BSI-DSZ-CC-0782, Version 2, 11 September 2012, TÜV Informationstechnik GmbH

[14] Annex I(B) of Commission Regulation (EC) No. 1360/2002 ‘Requirements for construction, testing, installation and inspection’, 05.08.2002, adapting to Council Regulation (EC) No. 3821/85 amended by Commission Regulation (EC) No. 432/2004 of 5 March 2004, Council Regulation (EC) No. 1791/2006 of 20 November 2006 and Commission Regulation (EC) No. 68/2009 of 23 January 2009, Commission Regulation (EU) No. 1266/2009 of 16 December 2009 and corrigendum dated as of 13.03.2004 (OJ L 71)

[15] Corrigendum to Commission Regulation (EC) No. 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EC) No. 3821/85 on recording equipment in road transport, Official Journal of the European Communities L 71-86, 13.03.2004

[16] Appendix 2 of Annex I(B) of Commission Regulation (EEC) No. 1360/2002 (refer to [14]) – Tachograph Cards Specification

[17] Appendix 10 of Annex I(B) of Commission Regulation (EEC) No. 1360/2002 (refer to [14]) – Generic Security Targets

[18] Appendix 11 of Annex I(B) of Commission Regulation (EEC) No. 1360/2002 (refer to [14]) – Common Security Mechanisms

[19] ANSI X9.19, Financial Institution Retail Message Authentication, 1986

[20] RFC 3447, J. Jonsson, B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", February 2003

[21] FIPS PUB 180-3, Secure Hash Standard, 2008

[22] ISO/IEC 9796-2:2010 Information technology - Security techniques - Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms

[23] FIPS PUB 81, DES Modes of Operation, 1996

[24] Certification Report for BSI-DSZ-CC-0764-2012 for tru/cos tacho v1.0 from Trueb AG, 28 August 2012, Bundesamt für Sicherheit in der Informationstechnik

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-0889-2013

Evaluation results regarding development and production environment

The IT product tru/cos tacho v1.1 (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 advice of the Certification Body for components beyond EAL 5 and 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, da

ted 28 June 2013, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1)

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

- Trueb AG, Hintere Bahnhofstrasse 12, CH-5000 Aarau, and Suhrenmattstrasse 23, CH-5035 Unterentfelden, Switzerland (Site Certificate BSI-DSZ-CC-S-0011-2012) for chip embedding, TOE initialisation, TOE delivery and documentation generation supported by several service providers charged by Trueb AG with TOE development, testing and documentation generation.
- For development and productions sites regarding the IC Infineon SLE78CFX2000P with its specific IC Dedicated Software and cryptographic libraries from Infineon Technologies AG refer to the certification report BSI-DSZ-CC-0782-2012 [12].

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.