Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1088-2022

for

MTCOS Smart Tachograph V2 / SLE78CFX4000P

from

MaskTech International GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1088-2022(*)

Digital Tachograph: Tachograph Cards

MTCOS Smart Tachograph V2 / SLE78CFX4000P

from	MaskTech International GmbH
PP Conformance:	Digital Tachograph - Tachograph Card (TC PP) Version 1.0, 19 May 2017, BSI-CC-PP-0091-2017
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5

SOGIS
Recognition Agreement

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 Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5, CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1 and in accordance with the COMMISSION IMPLEMENTING REGULATION (EU) 2016/799 and 2021/1228. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 only

Bonn, 3 June 2022

For the Federal Office for Information Security

Sandro Amendola
Head of Division

L.S.

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

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

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

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

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

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

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

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

2. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]

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

[2] Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

[3] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 3 March 2005, Bundesgesetzblatt I, p. 519

- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

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

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

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

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC Part 3 EAL 2+ ALC_FLR components.

4. Performance of Evaluation and Certification

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

The product MTCOS Smart Tachograph V2 / SLE78CFX4000P has undergone the certification procedure at BSI.

The evaluation of the product MTCOS Smart Tachograph V2 / SLE78CFX4000P was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 31 May 2022. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

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

The product was developed by: MaskTech International GmbH.

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

5. Validity of the Certification Result

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

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

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 3 June 2022 is valid until 2 June 2027. Validity can be re-newed by re-certification.

[5] Information Technology Security Evaluation Facility

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product MTCOS Smart Tachograph V2 / SLE78CFX4000P 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[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] MaskTech International GmbH
Nordostpark 45
90411 Nürnberg
Germany

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is the product MTCOS Smart Tachograph V2 / SLE78CFX4000P developed and provided by MaskTech International GmbH.

The TOE is a second generation version 2 Tachograph Card in the sense of COMMISSION IMPLEMENTING REGULATION (EU) 2016/799 [15] and COMMISSION IMPLEMENTING REGULATION (EU) 2021/1228 [17], Annex 1C. It is intended to be used in the 1st generation and 2nd generation version 2 Digital Tachograph Systems, which contain additionally further components as motion sensors (of the 1st or 2nd generation), vehicle units (of the 1st or 2nd generation), remote early detection communication readers and, if applicable, external GNSS modules and remote communication facilities.

The TOE provides different configurations and is implemented in the four different card types as driver card, workshop card, control card and company card in accordance with the Digital Tachograph System specifications given by COMMISSION IMPLEMENTING REGULATION (EU) 2016/799 [15] and COMMISSION IMPLEMENTING REGULATION (EU) 2021/1228 [17], Annex 1C, Appendix 2, Appendix 10 and Appendix 11.

Note: The COMMISSION IMPLEMENTING REGULATION (EU) 2016/799 [15] in its consolidated version covers the COMMISSION IMPLEMENTING REGULATION (EU) 2018/502 [16] and is therefore not mentioned explicitly in the following.

The TOE is interoperable with both Digital Tachograph Systems. It contains two Tachograph Card Applications, the first application being usable within the 1st generation Digital Tachograph System, the second one being usable within the 2nd generation version 2 system. Both applications are fully specified in [15] and [17], Annex 1C and related appendices.

The major security features of the TOE are:

- preservation of card identification data and user identification data stored during the card personalization process (used afterwards by the vehicle unit to identify the human user and to provide functions and data access rights accordingly),
- preservation of user data stored in the card by vehicle units, and
- restriction of certain write operations onto the cards to only authenticated vehicle units.

The TOE MTCOS Smart Tachograph V2 / SLE78CFX4000P is realised as a contact-based smart card and comprises of

- the Infineon Security Controller SLE78CFX4000P (M7892) in design step B11 with its IC Dedicated Software including Test and Support Software from Infineon Technologies AG,
- the IC Embedded Software with the ISO/IEC 7816 compliant and interoperable multi-application smart card operating system MTCOS Pro Smart Tachograph developed by MaskTech International GmbH,
- the Application Layer consisting of the two Tachograph Card Applications for the 1st generation and 2nd generation version 2 Digital Tachograph Systems developed by MaskTech International GmbH,
- the TOE user guidance, and

- configuration scripts for the configuration of the card type.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Digital Tachograph - Tachograph Card (TC PP) Version 1.0, 19 May 2017, BSI-CC-PP-0091-2017 [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 ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [7], chapter 6.1. 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 Functionality:

TOE Security Functionality	Addressed issue
F.IC_CL	This Security Function covers the security functions of the hardware (IC) as well as of the cryptographic library.
F.Access_Control	This Security Function regulates all access by external entities to operations of the TOE which are only executed after this Security Function allowed access.
F.Identification_Authentication	This Security Function provides identification and authentication of user roles.
F.Management	This Security Function provides management and administrative functionalities.
F.Crypto	This Security Function provides a high-level interface to cryptographic functions.
F.Verification	This Security Function addresses TOE internal functions that ensure correct operation.

Table 1: TOE Security Functionality

For more details please refer to the Security Target [6] and [7], chapter 6.1.

The assets to be protected by the TOE are defined in the Security Target [6] and [7], chapter 3.1.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [7], chapter 3.2, 3.3 and 3.4.

This certification covers the configurations of the TOE as outlined in chapter 8.

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

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

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

MTCOS Smart Tachograph V2 / SLE78CFX4000P

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/SW	MTCOS Smart Tachograph V2 / SLE78CFX4000P consisting of:		Delivery as initialised / pre-personalised module (including the operating system and the application layer / file system configured as driver card) Delivery together with delivery note
		1. Hardware Platform: SLE78CFX4000P (M7892) secure dual-interface controller of Infineon Technologies AG in design step B11 (BSI-DSZ-CC-0782-V5 [13]).	SLE78CFX4000P (M7892) in design step B11 with FW version: 78.015.14.2 CL version: 2.07.003	
		2. IC Embedded Software: Operating system MTCOS Pro Smart Tachograph	OS version: 2.5 OS build date: 2022-03-04 Patch version: 0 Patch build date: 2022-03-04	
		3. Application Layer: Tachograph Card applications for the 1st generation and 2nd generation version 2 Digital Tachograph Systems, both configured as driver card	(Revision 394 and 397, 2022-05-10)	
2	DATA	Configuration scripts (for configuration of card type): • Script to remove the application DFs on driver card • Script to create a workshop card • Script to create a company card • Script to create a control card	delete-DriverCard.txt (Revision 367, 2021-11-12) repreperso-WorkshopCard.txt repreperso-CompanyCard.txt repreperso-ControlCard.txt (Revision 385, 2022-04-05)	PGP-encrypted e-mail to issuing authority or the party acting on behalf of it
3	DOC	User Guidance – MTCOS Smart Tachograph V2 / SLE78CFX4000P [11]	Version 1.3	Password-protected download from secure webserver or PGP-encrypted e-mail
4	DATA	Personalisation key	n/a	PGP-encrypted and signed e-mail, via sealed and registered letter or on a smart card via a trustworthy transport service provider

Table 2: Deliverables of the TOE

2.1. Delivery Items and associated Delivery Methods

TOE in development and production phase (before TOE delivery in the sense of the CC): The internal shipment of the TOE and its parts (in particular for flash image production) between MaskTech International GmbH and Infineon Technologies AG makes use of the secure delivery procedures as these are covered by BSI-DSZ-CC-0782-V5 [13].

TOE for personalization: The pre-personalized chips including all software are securely delivered from Infineon Technologies AG to the issuing authority performing the TOE's personalization or party acting on behalf of it. Configuration scripts for the re-configuration of the intended card type are sent via PGP-encrypted e-mail.

Sensitive electronic data: The delivery of sensitive electronic data is performed via PGP-encrypted e-mail. The guidance documentation can alternatively be obtained by password-protected download from the MaskTech International GmbH website (refer to http://www.masktech.com). Transport keys are securely delivered via PGP-encrypted and signed e-mail, via a sealed and registered letter or on a smart card via a trustworthy transport service provider.

2.2. Identification of the TOE by the User

For the customer (personalization agent) to be able to check the correct delivery visually, a delivery note together with the product stating the product type and certification reference number is provided.

The following procedures ensure that the user can unambiguously identify an authentic Tachograph Card (refer to the TOE user guidance [11], chapter 2.2 and chapter 3.4):

- The user can check the correct delivery visually via a delivery note provided together with the product and stating the product type and certification reference number.
- The user can check the chip identification information (in particular concerning the IC and operating system) by means of the command GET CHIP INFORMATION, refer to the TOE user guidance [11], Annex A.6. Please take into account that in [11], Annex A.6 an example for possible response values of the command GET CHIP INFORMATION is provided, whereby the values of chip specific DOs, e.g. the serial number, as well as the option byte and initialization key identifier may vary from the manual. However, the first byte of the ROM-key identifier has to show the same value as the option byte, and the first nibble of the option byte must be a 'C'.
- The user can check the product identifier stored in the file EF.KVC, refer to the TOE user guidance [11], chapter 3.4. The first 8 bytes of the unmodified product identifier are: '92 10 B3 F8 59 08 EF 38'. Please take into account that the value described in [11], chapter 3.4 may have been changed along with the personalization keys; in this case, the value should be passed to the party performing the personalization. The value can be retrieved by using the command READ BINARY within the MF.
- The card type can be determined by using the READ BINARY command on the file EF.Application_Identification.G1/G2.
- The most important check is done implicitly by the correct working of the authentication process using the personalization key stored in the file EF.PERS. The response of the chip to the EXTERNAL / MUTUAL AUTHENTICATION command is verified by using Secure Messaging. Because the personalization keys

are provided by MaskTech International GmbH and can only be changed after authentication against this key, they will work only with the correct product.

2.3. Life-Cycle Model of the TOE

The life-cycle model of the TOE is described in the Security Target [6] and [7], chapter 1.2.4. 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 TOE is securely delivered as an initialised module from Infineon Technologies AG to the issuing authority for personalization or the party acting on behalf of it. Note that the embedding of the chip into the plastic card takes place after TOE delivery and is beyond the scope of the certification. The delivered TOE contains all software and the data structures as defined for a Tachograph Card of type driver card, but is not yet personalised.

The loading of the dedicated embedded and application software (driver card file system) is performed at Infineon Technologies AG and covered by the IC hardware evaluation (BSI-DSZ-CC-0782-V5 [13]). The IC‘s flash loader is deactivated permanently before delivery of the TOE in the sense of the CC.

The TOE is delivered of type driver card, but can be re-configured afterwards prior to its personalization into a card of type workshop, company or control card by using the respective configuration files.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

The TOE is a second generation version 2 Tachograph Card in the sense of COMMISSION IMPLEMENTING REGULATION (EU) 2016/799 [15] and COMMISSION IMPLEMENTING REGULATION (EU) 2021/1228 [17], Annex 1C. It is intended to be used in the 1st generation and 2nd generation version 2 Digital Tachograph Systems, which contain additionally further components as motion sensors (of the 1st or 2nd generation), vehicle units (of the 1st or 2nd generation), remote early detection communication readers and, if applicable, external GNSS modules and remote communication facilities.

The TOE implements physical and logical security functionality in order to protect user data and TSF data stored and operated on the smart card when used in a hostile environment. Due to the nature of its intended application, the TOE will be issued after personalization to end-users and in general might not be directly under the control of trained and dedicated administrators.

Hence, the TOE effectively and securely maintains the integrity and confidentiality of code and data stored in its memories, all modes of operation with the related capabilities for configuration and memory access, the TOE’s correct operation and the integrity and confidentiality of the security functionality provided by the TOE. The TOE's overall policy is to protect against malfunction, leakage, physical manipulation and probing. Besides, the TOE's life cycle is supported as well as the user Identification whereas the abuse of functionality is prevented. Specific details concerning the above mentioned security policy can be found in the Security Target [6] and [7], chapter 7.

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 operational environment. The following topics are of relevance:

Security Objectives for the operational environment defined in ST	**Description according to ST**	**Reference to TOE user guidance**
OE.Personalization_Phase	Secure Handling of Data in Personalization Phase	[11], chapter 3.5.10
OE.Crypto_Admin	Implementation of Tachograph Components	[11], chapter 3.5.10
OE.EOL	End of life	[11], chapter 3.5.10

Table 3: Security Objectives for the operational environment

Details can be found in the Security Target [6] and [7], chapter 4.2.

5. Architectural Information

The TOE is set up as a composite product. In architectural view it is composed of

- the Infineon Security Controller SLE78CFX4000P (M7892) in design step B11 with its IC Dedicated Software including Test and Support Software from Infineon Technologies AG,
- the IC Embedded Software with the operating system MTCOS Pro Smart Tachograph developed by MaskTech International GmbH, and
- the Application Layer consisting of the two Tachograph Card Applications for the 1st generation and 2nd generation version 2 Digital Tachograph Systems developed by MaskTech International GmbH.

Hereby, the TOE makes partly use of the Crypto Libraries of the Infineon hardware platform.

The IC including its Crypto Libraries is certified according to EAL 6 augmented by ALC_FLR.1. For details concerning the CC evaluation of the underlying IC with its cryptographic functionality refer to the evaluation documentation under the Certification ID BSI-DSZ-CC-0782-V5 ([12], [13]).

According to the TOE design the Security Functions of the TOE as listed in chapter 1 are implemented by the following subsystems:

- Application Data: application layer including the Tachograph Card Applications
- Operating System Kernel: HW independent part of the IC Embedded Software
- Hardware Abstraction Layer (HAL): HW dependent part of the IC Embedded Software
- Hardware: HW including libraries (e.g. for cryptographic functionality)

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 [6] and [7].

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 test cases are dedicated to the demonstration of the proper implementation of all security functions, card commands and operating system functionalities. For all commands or functionalities respectively, test cases are specified in order to demonstrate the expected behaviour including error cases. Each security function is covered by at least one test case. From all existing file system setups, a representative subset of configurations was chosen for evaluator testing. The conducted tests can be categorized into two groups: tests with real cards and tests with the emulator. The latter are used for situations where the test result cannot be verified externally (e.g. the secure deletion of data). For the chosen file system setups the evaluators conducted all test cases of the developer’s test suite for non-interactive tests. The evaluators decided to focus their own independent tests on tests with real cards, but emulator tests were also conducted. For these tests the evaluators derived some test ideas from the developer tests under consideration of the described security functionality.

All test cases were executed successfully and ended up with the expected result. No results indicating a wrong implementation could be found.

Concerning penetration testing, all relevant information as well as evaluation documentation were taken into account for the analysis by the evaluators. For the penetration analysis the evaluator analysed the CC deliverables for potential vulnerabilities already during the evaluation work for the corresponding aspects. The evaluators found no exploitable vulnerabilities in the evaluation deliverables.

The evaluators have tested the TOE systematically and thoroughly against high attack potential during their penetration testing. These tests covered in particular side channel analysis, fault (injection) analysis, fuzz testing and source code analysis.

The achieved test results correspond to the expected test results. No attack scenario with the attack potential high was actually successful in the TOE’s operational environment as defined in the Security Target provided that all measures required by the developer are applied.

The overall test result is that no deviations were found between the expected and the actual test results. Potential vulnerabilities cannot be exploited during the personalisation and usage phase.

8. Evaluated Configuration

This certification covers for the TOE

MTCOS Smart Tachograph V2 / SLE78CFX4000P

the following configuration as outlined in the Security Target [6] and [7]:

The TOE consists of

- the Infineon Security Controller SLE78CFX4000P (M7892) in design step B11 with its IC Dedicated Software including Test and Support Software from Infineon Technologies AG,
- the IC Embedded Software with the operating system MTCOS Pro Smart Tachograph developed by MaskTech International GmbH,
- the Application Layer consisting of the two Tachograph Card Applications for the 1st generation and 2nd generation version 2 Digital Tachograph Systems developed by MaskTech International GmbH,
- the TOE user guidance, and
- configuration scripts for the configuration of the card type.

Hereby, in view of the Application Layer with the Tachograph Card Applications, the TOE provides different file system setups due to four different card types, concretely the card types driver card (DC), workshop card (WC), company card (CC) and control card (PC), each with six cipher suites (based on BrainpoolP256r1, NIST P-256, BrainpoolP384r1, NIST P-384, BrainpoolP512r1 and NIST P-521, refer to [18] and [19]). However, the TOE is delivered in exactly one configuration as driver card. It is up to the Personalization Agent to select one of the other card types (if necessary) and to select the cipher suite to be used.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [9] 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:

(i) Composite product evaluation for Smart Cards and similar devices according to AIS 36 (see [4]). On base of this concept the relevant guidance documents of the underlying IC platform (refer to the guidance documents covered by [13]) and the document ETR for composite evaluation from the IC's evaluation ([14]) have been applied in the TOE evaluation. Concerning AIS 36 the updated version of the JIL document 'Composite product evaluation for Smart Cards and similar devices', version 1.5.1, May 2018 was taken into account.

(ii) Guidance for Smartcard Evaluation (AIS 37, see [4]).

(iii) Attack Methods for Smartcards and Similar Devices (AIS 26, see [4]).

(iv) Application of Attack Potential to Smartcards (AIS 26, see [4]).

(v) Application of CC to Integrated Circuits (AIS 25, see [4]).

(vi) Security Architecture requirements (ADV_ARC) for smart cards and similar devices (AIS 25, see [4]).

(vii) Evaluation Methodology for CC Assurance Classes for EAL5+ and EAL6 (AIS 34, see [4]).

(viii) Functionality classes and evaluation methodology of physical and deterministic random number generators (AIS 20 and AIS 31, see [4]).

(ix) Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren (AIS 46, see [4]).

For smart card specific methodology the scheme interpretations AIS 25, AIS 26, AIS 34, AIS 36, AIS 37 and AIS 46 (see [4]) were used. For RNG assessment the scheme interpretations AIS 20 and AIS 31 were used (see [4]).

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 ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 augmented for this TOE evaluation.

The evaluation has confirmed:

● PP Conformance:	Digital Tachograph - Tachograph Card (TC PP) Version 1.0, 19 May 2017, BSI-CC-PP-0091-2017 [8]
● for the Functionality:	PP conformant Common Criteria Part 2 extended
● for the Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_DVS.2, 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 table presented in Annex B of the Security Target [6] and [7] gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines the standard of application where its specific appropriateness is stated.

The strength of these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

According to the Digital Tachograph System specification given by COMMISSION IMPLEMENTING REGULATION (EU) 2016/799 [15], Annex 1C, Appendix 11, Part A and B the cryptographic algorithms of the TOE as a Tachograph Card are suitable for authentication and key agreement and for supporting integrity, authenticity and confidentiality of the data stored in and processed by the TOE. The suitability of the cryptographic algorithms used in the framework of personalization processes is given analogously. An explicit validity period is therefore not given here.

The cryptographic algorithms and protocols as outlined in the table of Annex B in the Security Target [6] and [7] are implemented in the card operating system and hereby make use of the IC SLE78CFX4000P and its related Crypto Libraries provided by Infineon

Technologies AG. In particular, the core routines for RSA (encryption, decryption, signature generation, signature verification), ECC (ECDSA signature generation, ECDSA signature verification, ECDH), DES and AES in CBC mode are taken from the IC with its Crypto Libraries. For random number generation the TOE uses the PTG.2 provided by the IC (and supplements a PTG.3 related cryptographic post-processing). The security evaluation of these cryptographic algorithms was performed in the framework of the certification of the IC with its related Crypto Libraries (refer to the Certification Report [13] and the corresponding Security Target [12]). The TOE relies on the correct (i.e. standard-conform) and secure implementation of these cryptographic algorithms. The remaining cryptographic implementation is part of the TOE's operating system and was analysed in the framework of the present composite evaluation of the TOE.

10. Obligations and Notes for the Usage of the TOE

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

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

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

11. Security Target

For the purpose of publishing, the Security Target [7] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12. Tachograph Regulation-specific Aspects

The IT product identified in this certificate fulfils the certified

- Common Criteria Protection Profile Digital Tachograph - Tachograph Card (TC PP) Version 1.0, 19 May 2017, BSI-CC-PP-0091-2017 [8]

and complies with the requirements for Tachograph Cards outlined in the

- COMMISSION IMPLEMENTING REGULATION (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components, European Commission, 2016 (consolidated version of 2020-02-26) [15], and
- COMMISSION IMPLEMENTING REGULATION (EU) 2021/1228 of 16 July 2021 amending Implementing Regulation (EU) 2016/799 as regards the requirements for the construction, testing, installation, operation and repair of smart tachographs and their components, European Commission, 2021 [17].

Therefore, the IT product certified is technically suitable to be a compliant Tachograph Card according to COMMISSION IMPLEMENTING REGULATION (EU) 2016/799 [15], Annex 1C, Appendix 10 provided that the following operational conditions are followed:

- The obligations and notes for the usage of the TOE have to be followed as outlined in chapter 10 of this report.
- The Tachograph Card issuer has to follow the operational requirements from the regulation as relevant for a compliant Tachograph Card as well as to follow all related obligations from any Digital Tachograph System related supervisory body.
- The Tachograph Card issuer shall consider the results of the certification and the operational conditions listed above within the system risk management process for the product usage. Specifically, the evolution of limitations of cryptographic algorithms and parameters as well as the evolution of attack methods related to the product or to the type of product has to be considered e.g. by a regular re-assessment of the TOE assurance.

13. Definitions

13.1. Acronyms

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CBC	Cipher Block Chaining mode
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CC	Company Card
CEM	Common Methodology for Information Technology Security Evaluation
CL	Crypto Library
cPP	Collaborative Protection Profile
DC	Driver Card
DES	Data Encryption Standard
DF	Dedicated File
DO	Data Object
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EF	Elementary File
ETR	Evaluation Technical Report

FW	Firmware
GNSS	Global Navigation Satellite System
HW	Hardware
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PC	Control Card
PP	Protection Profile
PTG	Physical True Random Number Generator
RNG	Random Number Generator
RSA	Rivest Shamir Adleman Algorithm
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
SW	Software
TOE	Target of Evaluation
TSF	TOE Security Functionality
WC	Workshop Card

13.2. Glossary

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

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

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

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

Informal - Expressed in natural language.

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

Package - Named set of either security functional or security assurance requirements.

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

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

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 5, April 2017
https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen)
https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7]
https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website
https://www.bsi.bund.de/zertifizierungsreporte

[7] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document (but with usage of updated JIL document 'Composite product evaluation for Smart Cards and similar devices', version 1.5.1, May 2018)
- AIS 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluierungen
- AIS 38, Version 2.9, Reuse of evaluation results
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[6] Security Target BSI-DSZ-CC-1088-2022, Security Target – MTCOS Smart Tachograph V2 / SLE78CFX4000P, Digital Tachograph – Tachograph Card, Version 1.0, 10 March 2022, MaskTech International GmbH (confidential document)

[7] Security Target Lite BSI-DSZ-CC-1088-2022, Security Target lite – MTCOS Smart Tachograph V2 / SLE78CFX4000P, Digital Tachograph – Tachograph Card, Version 1.2, 06 April 2022, MaskTech International GmbH (sanitised public document)

[8] Common Criteria Protection Profile Digital Tachograph – Tachograph Card (TC PP), Version 1.0, 19 May 2017, BSI-CC-PP-0091

[9] Evaluation Technical Report BSI-DSZ-CC-1088-2022, Evaluation Technical Report (ETR) – MTCOS Smart Tachograph V2 / SLE78CFX4000P, Version 1.5, 12 May 2022, SRC Security Research & Consulting GmbH (confidential document)

[10] Configuration List BSI-DSZ-CC-1088-2022, Configuration List – MTCOS Smart Tachograph V2 / SLE78CFX4000P, Version 0.6, 10 May 2022, MaskTech International GmbH (confidential document)

[11] User Guidance BSI-DSZ-CC-1088-2022, User Guidance – MTCOS Smart Tachograph V2 / SLE78CFX4000P, Version 1.3, 06 April 2022, MaskTech International GmbH

[12] Security Target BSI-DSZ-CC-0782-V5, Confidential Security Target M7892 B11 Recertification Common Criteria CCv3.1 EAL6 augmented (EAL6+), Version 4.1, 21 October 2020, Infineon Technologies AG (confidential document)

Security Target Lite BSI-DSZ-CC-0782-V5, Security Target Lite M7892 B11 Recertification Common Criteria CCv3.1 EAL6 augmented (EAL6+), Version 4.1, 21 October 2020, Infineon Technologies AG (sanitised public document)

[13] Certification Report BSI-DSZ-CC-0782-V5 for Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013 or v2.07.003, EC v1.02.013 or v2.07.003, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013 or v2.07.003, and Toolbox v1.02.013 or v2.07.003 libraries and with specific IC dedicated software (firmware) from Infineon Technologies AG, 26 November 2020, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[14] Evaluation Technical Report for Composite Evaluation (ETR COMP), BSI-DSZ-CC-0782-V5, Version 5, TÜV Informationstechnik GmbH (confidential document)

[15] COMMISSION IMPLEMENTING REGULATION (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components, European Commission, 2016 (consolidated version of 2020-02-26)

[16] COMMISSION IMPLEMENTING REGULATION (EU) 2018/502 of 28 February 2018 amending Implementing Regulation (EU) 2016/799 laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components, European Commission, 2018

[17] COMMISSION IMPLEMENTING REGULATION (EU) 2021/1228 of 16 July 2021 amending Implementing Regulation (EU) 2016/799 as regards the requirements for the construction, testing, installation, operation and repair of smart tachographs and their components, European Commission, 2021

[18] RFC 5480, Elliptic Curve Cryptography Subject Public Key Information, S. Turner, D. Brown, K. Yiu, R. Housley, and T. Polk, 2009

[19] RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, M. Lochter and J. Merkle, 2010

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC Part 1 chapter 10.5.
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1.
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8.
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12.
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17.
- The table in CC Part 3, Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/.

D. Annexes

List of annexes of this certification report

Annex A:	Security Target Lite [7] provided within a separate document
Annex B:	Evaluation results regarding development and production environment

Annex B of Certification Report BSI-DSZ-CC-1088-2022

Evaluation results regarding development and production environment

The IT product MTCOS Smart Tachograph V2 / SLE78CFX4000P (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 3 June 2022, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1)

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

a) MaskTech International GmbH, Nordostpark 45, 90411 Nürnberg (Germany) for Development and Testing.

b) For development and production sites regarding the underlying IC platform please refer to the Certification Report BSI-DSZ-CC-0782-V5 ([13]).

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6] and [7]. 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] and [7]) are fulfilled by the procedures of these sites.

Note: End of report