

# Certification Report

**BSI-DSZ-CC-1147-V3-2023**

for

**MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121)**

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

erteilt vom



IT-Sicherheitszertifikat

Bundesamt für Sicherheit in der Informationstechnik

**BSI-DSZ-CC-1147-V3-2023 (\*)**

Security IC with MRTD EAC/PACE Application

**MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121)**

from MaskTech International GmbH

PP Conformance: Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE, Version 1.3.2, 5 December 2012, BSI-CC-PP-0056-V2-2012-MA-02

Functionality: PP conformant plus product specific extensions  
Common Criteria Part 2 extended

Assurance: Common Criteria Part 3 conformant  
EAL 5 augmented by ALC\_DVS.2 and AVA\_VAN.5

valid until: 26 October 2028



SOGIS  
Recognition Agreement



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



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 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(\*) 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.

Bonn, 27 October 2023

For the Federal Office for Information Security

Sandro Amendola  
Director-General

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.

## Contents

A. Certification.....	6
1. Preliminary Remarks.....	6
2. Specifications of the Certification Procedure.....	6
3. Recognition Agreements.....	7
4. Performance of Evaluation and Certification.....	8
5. Validity of the Certification Result.....	8
6. Publication.....	9
B. Certification Results.....	10
1. Executive Summary.....	11
2. Identification of the TOE.....	12
3. Security Policy.....	14
4. Assumptions and Clarification of Scope.....	14
5. Architectural Information.....	15
6. Documentation.....	16
7. IT Product Testing.....	17
8. Evaluated Configuration.....	18
9. Results of the Evaluation.....	19
10. Obligations and Notes for the Usage of the TOE.....	21
11. Security Target.....	21
12. Regulation specific aspects (eIDAS, QES).....	21
13. Definitions.....	21
14. Bibliography.....	23
C. Excerpts from the Criteria.....	26
D. Annexes.....	27

## A. Certification

### 1. Preliminary Remarks

Under the BSIG<sup>1</sup> 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<sup>1</sup>
- BSI Certification and Approval Ordinance<sup>2</sup>
- BSI Schedule of Costs<sup>3</sup>
- Special decrees issued by the Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community)
- 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]
- Common Criteria for IT Security Evaluation (CC), Version 3.1<sup>4</sup> [1] also published as ISO/IEC 15408

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

<sup>2</sup> 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

<sup>3</sup> BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- 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.

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

<sup>4</sup> Proclamation of the Bundesministerium des Innern und für Heimat of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

## 4. Performance of Evaluation and Certification

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

The product MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121) has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1147-V2-2023. Specific results from the evaluation process BSI-DSZ-CC-1147-V2-2023 were re-used.

The evaluation of the product MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121) was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 20 October 2023. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)<sup>5</sup> recognised by the certification body of BSI.

For this certification procedure the 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 27 October 2023 is valid until 26 October 2028. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security

<sup>5</sup> Information Technology Security Evaluation Facility



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 Pro 2.6 EAC with PACE / P71D352 (N7121) 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<sup>6</sup> of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

<sup>6</sup> MaskTech International GmbH  
Nordostpark 45  
90411 Nürnberg

## **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

Target of evaluation (TOE) is the product MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121) provided by MaskTech International GmbH. The TOE is a fully interoperable multi-application smart card operating system compliant to [15] with a contact and contactless interface. It contains an MRTD application which is programmed according to ICAO Technical Report "Supplemental Access Control" [13] and additionally providing the Extended Access Control according to the 'ICAO 9303' [14] and [16], respectively. The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE) according to "Electronic Passport using Standard Inspection Procedure with PACE", BSI-CCPP-0068-V2-2011-MA01 [10]. Additionally, Active Authentication according to [14] is provided.

The main security features of the TOE are:

- PACE function (mutual authentication and Secure Messaging);
- Active Authentication support function (prevention of copying the IC chip);
- Extended Access Control (chip authentication and terminal authentication protocol)
- Write protection function (protection against writing data after issuing a passport);
- Protection function in transport (protection against attacks during transport before issuing the TOE); and
- Tamper resistance (protection against confidential information leak due to physical attacks).

The TOE MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121), which is realized by a smartcard, comprises of:

Hardware Platform:

- P71D352 (N7121) secure dual-interface controller of NXP Semiconductors Germany GmbH release packages R1, R2 and R3 (BSI-DSZ-CC-1136-V3-2022 [21]). Chip including cryptographic library are certified according to CC EAL6 augmented with ALC\_FLR.1 and ASE\_TSS.2 compliant to the Protection Profile BSI-CC-PP-0084-2014 [11]).

Software:

- IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software
- IC Embedded Software (Operating System MTCOS Pro 2.6)
- MRTD application

Documentation:

- User Guidance -- MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121) [17]
- MTCOS MANUAL - MTCOS 2.6 on P71D352 (N7121) [18]

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE, Version 1.3.2, 5 December 2012, BSI-CC-PP-0056-V2-2012-MA-02 [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 5 augmented by ALC\_DVS.2 and AVA\_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], 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 TSF regulates all access by external entities to operations of the TOE which are only executed after this TSF allowed access.
F.Identification_Authentication	This function provides identification/authentication of user roles
F.Management	Provides management and administrative functionalities.
F.Crypto	This function provides a high-level interface to cryptographic functions.
F.Verification	TOE internal functions ensure correct operation by implementing internal hardware test routines.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [9], chapter 7.1.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 3.1. 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 [9], chapter 3.2 to 3.4.

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

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 Pro 2.6 EAC with PACE / P71D352 (N7121)**

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/SW	MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121) An IC module including the necessary basic software (OS) and ePassport application (file system)		SW is implemented in NVM memory; chip is initialized and tested before delivery to  Personalization Agent. Delivery type: The OS and application software flashed on the IC Platform
		1. Hardware Platform P71D352 (N7121) secure dual-interface controller of NXP Semiconductors Germany GmbH release packages R1, R2 and R3 (BSI-DSZ-CC-1136-V3-2022 [21]). Chip including cryptographic library are certified according to CC EAL6 augmented with ALC_FLR.1 and ASE_TSS.2 compliant to the Protection Profile BSI-CC-PP-0084-2014 [11]).	P71D352 (N7121) FW: 9.2.3 CL: 0.7.6	
		2. TOE Embedded Software IC Embedded Software (the operating system MTCOS Pro 2.6, implemented in NVM of the IC)	MTCOS Pro Version 2.6 Build date: Basic: 2022-08-11 Plus: 2022-10-14	
		3. TOE Embedded Applications IC Embedded Software / Part Application Software (containing the MRTD Application implemented in the NVM of the IC with the file system)	MTCOS Pro 2.6 EAC with PACE	
2	DOC	1. User Guidance – MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121), Machine Readable Travel Document with “ICAO Application, MaskTech International GmbH	[17] Version 1.2, 24.08.2023	Password protected Secure Webserver
		2. MTCOS MANUAL – MTCOS 2.6 on P71D352 (N7121)	[18] Version 1.0, 07.08.2023	

Table 2: Deliverables of the TOE

## 2.1. Delivery items and associated delivery methods

Sensitive electronic documents: Delivery of sensitive electronic data is performed PGP encrypted via email. The guidance documentation can be obtained by password-protected download from the MaskTech International GmbH website (<http://www.masktech.com>).

Flash image production: The developer sends the flash image (HEX file) securely to NXP Semiconductors Germany GmbH via email.

TOE for Personalization: Chip card hardware is securely shipped to the Personalization Agent.

## 2.2. Identification of the TOE by User

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

Further checks can be done using the GET CHIP ID or GET CHIP INFORMATION command. They return the chip identifier respectively additional information about the platform, the operating system and the patch level. Whether the chip contains the correct

file system layout can be verified by checking the product identifier stored in the file EF.PROJID (see section 3.4 of [17]).

An example for possible response values of the command GET CHIP INFORMATION can be found in [17], Annex D. The chip-individual data, e.g. batch number, wafer number and coordinates may vary from the manual.

### **3. Security Policy**

The security policy enforced is defined by the selected set of Security Functional Requirements and implemented by the TOE. It covers the following issues: The TOE implements physical and logical security functionality in order to protect user data stored and operated on the smartcard when used in a hostile environment. Due to the nature of its intended application, i.e. the TOE may be issued to users and may not be directly under the control of trained and dedicated administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect. The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives. Specific details concerning the above mentioned security policies can be found in [6], sec. 6.3.

### **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:

Security Objectives for the operational environment defined in Security Target	Description according to ST	Reference to Guidance
OE.Auth_Key_Travel_Document	Travel document Authentication Key	[17] sec. 3.5.11
OE.Authoriz_Sens_Data	Authorization for Use of Sensitive Biometric Reference Data	[17] sec. 3.5.11
OE.Active_Auth_Key_Travel_Document	Travel document Active Authentication Key	[17] sec. 3.5.11
OE.Exam_Travel_Document	Examination of the physical part of the travel document	[17] sec. 3.6.3
OE.Prot_Logical_Travel_Document	Protection of data from the logical travel document	[17] sec. 3.6.3
OE.Ext_Insp_Systems	Authorization of Extended Inspection Systems	[17] sec. 3.6.3
OE.Legislative_Compliance	Issuing of the travel document	[17] sec. 3.5.11
OE.Passive_Auth_Sign	Authentication of travel document by Signature	[17] sec. 3.5.11
OE.Personalization	Personalization of travel document	[17] sec. 3.5.11
OE.Terminal	Terminal operating	[17] sec. 3.6.3
OE.Travel_Document_Holder	Travel document holder Obligations	[17] sec. 3.6.3

Table 3: Security Objectives for the Operational Environment

Details can be found in the Security Target [6] and [9], chapter 4.2 as well as in the Protection Profile.

## 5. Architectural Information

The TOE is a composite product. It is composed of an Integrated Circuit P71D352 (N7121), IC Dedicated Software including Test and Support Software, IC Embedded Software (Operating System) and the MRTD Application. While the IC Embedded software contains the operating system MTCOS Pro 2.6, the NVM contains the MRTD application. As all these parts of software are running inside the IC, the external interface of the TOE to its environment can be defined as the external interface of this IC, the P71D352 (N7121) secure dual-interface controller of NXP Semiconductors Germany GmbH release packages R1, R2 and R3 (BSI-DSZ-CC-1136-V3-2022 [21]). Chip including cryptographic library are certified according to CC EAL6 augmented with ALC\_FLR.1 and ASE\_TSS.2 compliant to the Protection Profile BSI-CC-PP-0084-2014 [CC\_PP-0084]). For details concerning the CC evaluation of the NXP IC and its cryptographic libraries see the evaluation documentation under the Certification ID BSI-DSZ-CC-1136-V3-2022 (see also sec. 1.4.1). This chapter gives an overview of the TOE's Embedded Software and the corresponding TSFs which were objects of this evaluation.

The security functions of the TOE are enforced by the following subsystems:

Subsystem	TSF supported
Application data	SP.Access_Control, SP.Identification_Authentication
Operation System Kernel	SP.Access_Control, SP.Crypto, SP.Identification_Authentication, SP.Management, SP.Verification
HAL	SP.IC_CL, SP.Crypto, SP.Identification_Authentication, SP.Verification
Hardware	SP.IC_CL

Table 4: Subsystems enforcing TSF

## 6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.



## 7. IT Product Testing

### 7.1. Developer Test concept

#### Test Configuration

Suitable samples were chosen from the described configurations (chapter 8) to test all security functions.

#### Testing approach

Each security function is covered by at least one test case. The tests performed can be categorized into two groups: tests with the real card and tests with the emulator. The latter are used for situations that cannot be achieved in a real card's life.

#### Amount of developer testing performed

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 resp. Functionality, test cases are specified in order to demonstrate the expected behaviour including error cases.

#### Testing results

All test cases were executed successfully and produced the expected result.

### 7.2. Evaluator Tests

#### Independent Testing according to ATE\_IND

#### Test Configuration

Suitable samples were chosen from the described configurations (chapter 8) to test all security functions.

#### Testing approach

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 resp. Functionality, 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 setups was chosen for evaluator testing. The conducted tests can be categorized into two groups: tests with the real card 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 setups the evaluators conducted all test cases of the developer's test suite for non-interactive tests using the test equipment provided by the developer. 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. Furthermore, the evaluators used fuzzy testing to determine the correct implementation of the TOE.

#### Testing Results

All test cases developed by the evaluators were executed successfully and ended up with the expected result. All test cases have been conducted successfully and all the actual test results (resulting from evaluator's repetition of the tests) were as the expected ones (as

gained by the developer). For the test results of the emulator tests the evaluator repeated the emulator tests executed by the developer during the base evaluation. The repetition of tests showed the test results are consistent. Fuzz testing did not reveal any flaws in the TOE's implementation. In the course of the fuzzy testing no results indicating a wrong implementation could be found.

## **Penetration Testing according to AVA\_VAN**

### **Penetration testing approach**

The penetration testing was performed using the test environment of the evaluation facility. All relevant information as well as evaluation documentation was 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 evaluator used the potential vulnerabilities from the JIL document as the lead for further investigations. All possible attack methods against an authentic operational TOE were analysed. Thereby the results and experience of the ISCI working group were taken into account.

### **Testing Results**

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential High was actually successful in the TOE's operational environment as defined in [6] provided that all measures required by the developer are applied. Potential vulnerabilities cannot be exploited during the phases development, manufacturing and personalization.

## **8. Evaluated Configuration**

This certification covers the following configurations of the TOE: MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121) consisting of:

- Operating system and a file system in the context of the ePassport application with the NXP Semiconductors Germany GmbH P71D352 (N7121) Chip; software completely contained in NVM
- File system layout (included in [17])
- User guidance [17]
- Product Manual [18].

The IC embedded software consists of the operating system MTCOS Pro 2.6 and an application layer, consisting of the MRTD application.

### **8.1. TOE configurations**

In order to meet customer requirements, the product is provided in different configurations. These differ in the amount of memory space for user data and the combination of data groups. The TOE has the following main MRTD configurations:

- LayoutA
- LayoutFlex

For data group files sizes please refer to [17], sec. 3.3. The key files to be used for asymmetric cryptography can be configured by the Personalization Agent with the configurations as listed in [17], sec. 3.5.6.

## 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:

- (i) *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 [19, 20] have been applied in the TOE evaluation.*
- (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) *Security Architecture requirements (ADV\_ARC) for smart cards and similar devices (AIS 25, see [4])*
- (vi) *Evaluation Methodology for CC Assurance Classes for EAL5+ and EAL6 (AIS 34, see [4])*
- (vii) *Functionality classes and evaluation methodology of physical and deterministic random number generators (AIS 20 and AIS 31, see [4])*
- (viii) *Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren (AIS 46, see [4])*

For RNG assessment the scheme interpretations AIS 20 and AIS 31 were used (see [4]).

A document ETR for composite evaluation according to AIS 36 has not been provided in the course of this certification procedure. It could be provided by the ITSEF and submitted to the certification body for approval subsequently.

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

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

- All components of the EAL 5 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC\_DVS.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-1147-V2-2023, re-use of specific

evaluation tasks was possible. Subject to the re-evaluation are changes to the certified product with respect to current development and findings:

- While the base certification was provided as an ePassport application only, the TOE now includes a multi-application product, containing an SSCD certified in another procedure under the certification ID BSI-DSZ-CC-1211-2023.
- The TOE now includes both interfaces: contact and contactless.
- Flexible file sizes can be set during personalization.
- There is an updated HW certificate for P71D352 (N7121) by NXP Semiconductors Germany GmbH (certification-ID: BSI-DSZ-CC-1136-V3-2022 [19])
- The history of the TOE and the changes are detailed in [22].

The evaluation has confirmed:

- PP Conformance: Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE, Version 1.3.2, 5 December 2012, BSI-CC-PP-0056-V2-2012-MA-02 [8]
- for the Functionality: PP conformant plus product specific extensions Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant EAL 5 augmented by ALC\_DVS.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.

The evaluation was performed as a composite evaluation according to AIS 36 (see [4]) and therefore relies on the platform certification of the used IC including its cryptographic libraries. Refer to certification ID BSI-DSZ-CC-1136-V3-2022 and subsequent BSI-DSZ-CC-1136-V3-2022-MA-01 ([19], [23], [20]).

## 9.2. Results of cryptographic assessment

The Table A.1 presented in the Security Target [6], chapter A gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy. The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

For the TOE's cryptographic functionalities, Table A.1 in the Security Target outlines the standard of application where their specific appropriateness is stated. According to the referenced standards these algorithms are suitable for authentication, key agreement, authenticity, integrity, confidentiality and trusted channel. An explicit validity period is not given at this point.

Cryptographic functionalities with a security level of lower than 120 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related cryptographic operations are appropriate for the intended system. Further hints and guidelines on the respective security level and validity period of the cryptographic algorithms can be derived from the document 'Technische Richtlinie BSI TR-02102-1' (refer to <https://www.bsi.bund.de>) and as well from the SOG-IS crypto catalogue [24].

The cryptographic algorithms and protocols as outlined in Table A.1 of the Security Target are implemented in the card operating system and hereby make use of the P71D352 (N7121) secure dual-interface controller and its related cryptographic libraries (V0.7.6) from NXP Semiconductors Germany GmbH certified under ID BSI-DSZ-CC-1136-V3-2022 and subsequent BSI-DSZ-CC-1136-V3-2022-MA-01. In particular, the core routines for RSA (signature generation, RSA DH), ECC (ECDSA signature generation and verification, ECDH), the SHA hash calculation, the symmetric cryptographic algorithms AES and 3DES encryption and decryption in CBC mode and the PTG.3 random number generation are taken from the cryptographic libraries. The security evaluation of these cryptographic algorithms was performed in the framework of the certification of the IC with its related cryptographic libraries (refer to [19], [23]). The TOE relies on the correct (i.e. standard-conform) and secure implementation of these cryptographic algorithms. The remaining cryptographic implementation 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 [6] not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product, in particular the card issuing organisation and the national organisation responsible for the risk management, 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 [9] 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. Regulation specific aspects (eIDAS, QES)

None

## 13. Definitions

### 13.1. Acronyms

<b>AA</b>	Active Authentication
<b>AES</b>	Advanced Encryption Standard
<b>AIS</b>	Application Notes and Interpretations of the Scheme
<b>BAC</b>	Basic Access Control

<b>BSI</b>	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
<b>BSIG</b>	BSI-Gesetz / Act on the Federal Office for Information Security
<b>CCRA</b>	Common Criteria Recognition Arrangement
<b>CC</b>	Common Criteria for IT Security Evaluation
<b>CEM</b>	Common Methodology for Information Technology Security Evaluation
<b>cPP</b>	Collaborative Protection Profile
<b>DES</b>	Data Encryption Standard
<b>DOC</b>	Documentation
<b>EAC</b>	Extended Access Control
<b>EAL</b>	Evaluation Assurance Level
<b>ECC</b>	Elliptic Curve Cryptography
<b>ECDH</b>	Elliptic Curve Diffie-Hellman
<b>ETR</b>	Evaluation Technical Report
<b>HW</b>	Hardware
<b>IC</b>	Integrated Circuit
<b>ICAO</b>	International Civil Aviation Organisation
<b>IT</b>	Information Technology
<b>ITSEF</b>	Information Technology Security Evaluation Facility
<b>MRTD</b>	Machine Readable Travel Document
<b>MRZ</b>	Machine Readable Zone
<b>NVM</b>	Non Volatile Memory
<b>OS</b>	Operating System
<b>PACE</b>	Password Authenticated Connection Establishment
<b>PP</b>	Protection Profile
<b>SAR</b>	Security Assurance Requirement
<b>SFP</b>	Security Function Policy
<b>SFR</b>	Security Functional Requirement
<b>SSCD</b>	Secure Signature Creation Device
<b>ST</b>	Security Target
<b>SW</b>	Software
<b>TOE</b>	Target of Evaluation
<b>TSF</b>	TOE Security Functionality

## 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, Rev. 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<sup>7</sup>  
<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/zertifizierungsberichte>
- [6] Security Target BSI-DSZ-CC-1147-V3-2023, Version 0.5, 13 September 2023, Security Target – Machine Readable Travel Document with “ICAO Application”, MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121), MaskTech International GmbH (confidential document)
- [7] Evaluation Technical Report, Version 1.4, 20 October 2023, Evaluation Technical Report BSI-DSZ-CC-1147-V3, MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121), SRC Security Research & Consulting GmbH, (confidential document)
- [8] Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE, Version 1.3.2, 5 December 2012, BSI-CC-PP-0056-V2-2012-MA-02
- [9] Security Target BSI-DSZ-CC-1147-V3-2023, Version 1.2, 24 August 2023, Security Target– Machine Readable Travel Document with “ICAO Application”, MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121), MaskTech International GmbH (sanitised public document)
- [10] Common Criteria Protection Profile - Electronic Passport using Standard Inspection Procedure with PACE (ePass PACE PP), Version 1.01, 13 January 2014, Certification-ID: BSI-CC-PP-0068-V2-2011-MA01
- [11] Common Criteria Protection Profile - Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13 January 2014, Certification-ID: BSI-CC-PP-0084-2014

<sup>7</sup>specifically

- 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
- AIS 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluierungen
- AIS 38, Version 2, Reuse of evaluation results
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren
- AIS 47, Version 1.1, Regelungen zu Site Certification



- [12] Configuration list for the TOE, Version 0.5, 13 October 2023, Configuration List – MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121), MaskTech International GmbH (confidential document)
- [13] ICAO. Technical Report: Supplemental Access Control for Machine Readable Travel Documents. V1.01. International Civil Aviation Organization, 15 April 2014
- [14] ICAO, Machine Readable Travel Documents, Part 1 - Machine Readable Passports. International Civil Aviation Organization, 2021 ICAO, Machine Readable Travel Documents, Part 3 - Machine Readable Official Travel Documents. International Civil Aviation Organization, 2021
- [15] ISO/IEC 7816:2008, Information technology – Identification cards – Integrated circuit cards – Multipart Standard, ISO/IEC, 2008
- [16] Technical Guideline TR-03110-1: Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, BSI, 2015
- [17] User Guidance – MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121), Machine Readable Travel Document with “ICAO Application, Version 1.2, 24 August 2023, MaskTech International GmbH
- [18] MTCOS 2.6 on P71D352 (N7121) – Manual, Version 1.0, 07 August 2023, MaskTech International GmbH
- [19] Certification Report, BSI-DSZ-CC-1136-V3-2022 for NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library from NXP Semiconductors Germany GmbH, 07 September 2022
- [20] ETR for Composition NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (N7121) – EAL6+ according to AIS36, TÜV Informationstechnik GmbH, BSI-DSZ-CC-1136-V3-2022, Version 2, 25 August 2022
- [21] NXP Semiconductors, Security Target Lite 'NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library', BSI-DSZ-CC-1136-V3-2022, Rev. 2.6, 13 June 2022
- [22] CHANGES AND IMPACT ANALYSIS, MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121), Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE, Version 1.0, 09 September 2022 (confidential document)
- [23] Assurance Continuity Maintenance Report - BSI-DSZ-CC-1136-V3-2022-MA-01 NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) from NXP Semiconductors Germany GmbH, 17 May 2023
- [24] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.3, February 2023

## 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 provided within a separate document.

Annex B: Evaluation results regarding development and production environment

## Annex B of Certification Report BSI-DSZ-CC-1147-V3-2023

### Evaluation results regarding development and production environment



The IT product MTCOS Pro 2.6 EAC with PACE / P71D352 (N7121) (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 27 October 2023, 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.5, ALC\_DEL.1, ALC\_DVS.2, ALC\_LCD.1, ALC\_TAT.2, ALC\_COMP.1)

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

- a) MaskTech International GmbH, Nordostpark 45, 90411 Nuernberg, Germany, Re-use of complete Site Audit of BSI-DSZ-CC-1064-2020-MA-01, Site certificate valid until 15.01.2024 (Software Development)
- b) Linxens (Thailand) Co Ltd., 142 Moo, Hi-Tech Industrial Estate, Tambon Ban Laean, Amphor Bang-pa-in, 13160 Ayutthaya, Thailand, BSI-DSZ-CC-S-0207-2021, Site Certificate valid until 01.11.2023 (Initialization/Pre-Personalization)
- c) HID Global Ireland Teoranta, Pairc Tionscail na Tullaigh, Baile na hAbhann, Co. Galway, Ireland, BSI-DSZ-CC-S-0232-2023, Site Certificate valid until 22.09.2025 (Initialization/Pre-personalization)
- d) HID Global Sdn. Bhd. No. 2, Jalan i-Park 1/1, Kawasan Perindustrian i-Park, Bandar Indahpura, 81000 Kulai, Johor, Malaysia, BSI-DSZ-CC-S-0233-2023, Site certificate valid until 10.07.2025 (Initialization/Pre-personalization)
- e) NXP Semiconductors GmbH, Business Unit security and connectivity (BU S&C) Troplowitzstraße 20, 22529 Hamburg, Germany, BSI-DSZ-CC-1136-V3-2022, Site certificate valid until 06.09.2027<sup>8</sup> (Initialization/Pre-personalization, Manufacturer)
- f) Linxens Germany GmbH, Manfred-von-Ardenne-Ring 12, 01099 Dresden, BSI-DSZ-CC-S-0214-2022, Site certificate valid until 22.09.2024 (Initialization/Pre-Personalization)

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] and [9]) are fulfilled by the procedures of these sites.

<sup>8</sup> Expiration date of the IC certificate. The NXP site in Hamburg is also equipped with a site certificate with certification ID BSI-DSZ-CC-S-0181-2022. This site certificate is valid until 29.02.2024.

Note: End of report