Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0996-2018

for

MTCOS Pro 2.5 EAC with PACE / P60D145VB_J (P6022y VB) (BAC)

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-0996-2018 (*)

Security IC with MRTD BAC Application

MTCOS Pro 2.5 EAC with PACE / P60D145VB_J (P6022y VB) (BAC)

from	MaskTech International GmbH
PP Conformance:	Machine Readable Travel Document with "ICAO Application" Basic Access Control, Version 1.10, 25 March 2009, BSI-CC-PP-0055-2009
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_DVS.2

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 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 4.

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.

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

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, 30 April 2018

For the Federal Office for Information Security

Joachim Weber
Head of Branch

L.S.

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

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

This page is intentionally left blank.

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]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.

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 03 March 2005, Bundesgesetzblatt I p. 519

- 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.sogisportal.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: http://www.commoncriteriaportal.org.

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

[4] Proclamation of the Bundesministerium des Innern 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 2.5 EAC with PACE / P60D145VB_J (P6022y VB) (BAC) has undergone the certification procedure at BSI.

The evaluation of the product MTCOS Pro 2.5 EAC with PACE / P60D145VB_J (P6022y VB) (BAC) was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 23 February 2018. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[5] 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 30 April 2018 is valid until 29 April 2023. 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 Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

[5] Information Technology Security Evaluation Facility

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 2.5 EAC with PACE / P60D145VB_J (P6022y VB) (BAC) 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

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 Pro 2.5 EAC with PACE / P60D145VB_J (P6022y VB) (BAC) provided by MaskTech International GmbH and based on the dual interface Smartcard IC P60D145VB_J (P6022y VB) including Libraries for RSA, EC and SHA-2 (NXP Semiconductors). The TOE is the contactless/contact integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) [24] and providing Basic Access Control according to the 'ICAO 9303' [21]. The TOE is based on ISO/IEC 7816 commands and is intended to be used inside a MRTD as storage of the digital data and supports Basic Access Control and Extended Access Control.

It provides following services for MRTDs:

- Storage of the MRTD data, e.g. data groups and signature,
- Organization of the data in a file system as dedicated and elementary files,
- Mutual Authentication and Secure Messaging as specified in TrPKI [23] for Basic Access Control,
- Contactless communication according to ISO/IEC 14443,
- Protection of the privacy of the passport holder with functions like random UID and Basic Access Control.

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" Basic Access Control, Version 1.10, 25 March 2009, BSI-CC-PP-0055-2009 [9].

Please note that in consistency to the claimed protection profile BSI-CC-PP-0055-2009 the security mechanism *Basic Access Control* is in the focus of this evaluation process. The further security mechanisms *Password Authenticated Connection Establishment, Extended Access Control and Active Authentication* are subject of the separate evaluation process BSI-DSZ-CC-0995-2018 [25].

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.

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	Security functions of the hardware (IC) as well as of the cryptographic library
F.Access_Control	Regulates all access by external entities to operations of the TOE which are only executed after this TSF allowed access
F.Identification_Authentication	Provides identification/authentication of user roles
F.Management	Provides management and administrative functionalities

TOE Security Functionality	Addressed issue
F.Crypto	Provides a high-level interface to cryptographic functions
F.Verification	TOE internal functions to ensure correct operation

Table 1: TOE Security Functionalities

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

The assets to be protected by the TOE are defined in the Security Target [6] and [7], 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 [7], chapter 3.

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 Pro 2.5 EAC with PACE / P60D145VB_J (P6022y VB) (BAC)

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/ SW	MTCOS Pro 2.5 EAC with PACE / P60D145VB_J (P6022y VB) (BAC) An initialized module, but without Hardware for the contactless interface, consisting of the following:		
		1. Hardware Platform NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software Crypto Library V3.1.x on P6022y VB: Libraries RSA, EC and SHA-2	Nameplate 9072B, 2016-01-18 CL: v3.1.x	SW implemented in ROM and EEPROM memory, chip initialised and tested. Delivery type: Different module types and sawn wafer
		2. TOE Embedded Software IC Embedded Software (the operating system MTCOS Pro 2.5, implemented in ROM / EEPROM of the IC)	MTCOS Pro Version 2.5	
		3. TOE Embedded Applications IC Embedded Software / Part Application Software (containing the MRTD Application implemented in the EEPROM of the IC with the file system)	MTCOS Pro Version 2.5 EAC with PACE	

No	Type	Identifier	Release	Form of Delivery
2	DOC	MTCOS Pro 2.5 EAC with PACE / P60D145VB_J (P6022y VB) User Guidance, MaskTech International GmbH	Version 0.6, 16.02.2018 [12]	Document in electronic form, delivered via password-protected secure webserver
3	DOC	MTCOS Pro V2.5 on P60D145VB_J (P6022y VB) – Manual, MaskTech GmbH	Version 1.0, 05.10.2017 [13]	Document in electronic form, delivered via password-protected secure webserver
4	DOC	Guidance for Initialization and Pre-personalization MTCOS Pro 2.5 / P60D145VB_J (P6022y VB), MaskTech International GmbH	Version 0.6, 16.02.2018 [14]	Document in electronic form, delivered via password-protected secure webserver

Table 2: Deliverables of the TOE

The TOE is finalized at the end of phase 2 according to the MRTD BAC PP [9]. The delivery is performed from the initialization facility to the personalisation facility respectively the inlay manufacturer as a secured transport to a specific person of contact at the personalization site or inlay manufacturing site. The TOE itself will be delivered as an initialized module but without hardware for the contactless interface to the inlay manufacturer, who securely delivers the inlay containing the pre-personalized MRTD to the personalisation facility. The inlay production including the application of the antenna is not part of the TOE and takes part after the delivery from the initialization facility. Furthermore, the personalizer receives information about the personalization commands and process requirements.

The following delivery methods are used:

- Sensitive electronic documents: There are two ways for delivery of sensitive electronic data, PGP encrypted via email and PGP encrypted download from website.
- Mask production: The developer sends the mask file PGP-authenticated and encrypted.
- Personalization: Chip card hardware is securely shipped to the personalization agent.

The name of the ROM file transferred from MaskTech to NXP is mtcos_sp_v2.5_p60d145vb_j_rom_filled.hex.

To ensure that the personalizer receives this evaluated version, the procedures to start the personalisation process as described in the User's Guide [12] have to be followed.

The personalization agent is able to identify the smart card Embedded Software by:

- the labelling of the pre-personalized chip[7],
- the correct working of the personalization key (EF.PERS),
- the product identifier stored in the file EF.KVC and
- the silicon information retrieved via GET_CHIP_INFORMATION.

[7] If the chip is pre-personalized in MaskTech premises then a unique label is printed after processing of the chips and affixed on the packed chips. This label contains information on the order, product description, version and checksum.

The response values of the command GET_CHIP_INFORMATION can be found in [13], section 10.14 and appendix A. The chip-individual data, e.g. the Chip ID, and possibly the patch information may be different from the manual. A description of silicon information can be found in the IC developer guidance [19].

After personalization the TOE hinders identification using TSFI. The personalisation agent is required to track the TOE version.

3. Security Policy

The Security Policy of the TOE is defined according to the MRTD BAC PP [9] by the Security Objectives and Requirements for the contact-less chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organisation (ICAO). The Security Policy addresses the advanced security methods for authentication and secure communication, which are described in detail in the Security Target [6] and [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-Environment. The following topics are of relevance:

- OE.MRTD_Manufact: Protection of the MRTD Manufacturing
- OE.MRTD_Delivery: Protection of the MRTD delivery
- OE.Personalization: Personalization of logical MRTD
- OE.Pass_Auth_Sign: Authentication of logical MRTD by Signature
- OE.BAC-Keys: Cryptographic quality of Basic Access Control Keys
- OE.Exam_MRTD: Examination of the MRTD passport book
- OE.Passive_Auth_Verif: Verification by Passive Authentication
- OE.Prot_Logical_MRTD: Protection of data of the logical MRTD

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

5. Architectural Information

The TOE is a composite product. It is composed from an Integrated Circuit, IC Dedicated Software, IC Embedded Software and Part Application Software (containing the MRTD Application implemented in the EEPROM of the IC). While the IC Embedded Software contains the operating system MTCOS Pro 2.5, the Part Application Software 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 NXP Secure Smart Card Controller P6022y. For details concerning the CC evaluation of the NXP IC and its cryptographic libraries see the evaluation documentation under the Certification IDs BSI-DSZ-CC-0973-V2 [15] and CC-17-67206 [17].

The security functions of the TOE are:

- F.Access_Control

- F.Identification_Authentication
- F.Management
- F.Crypto
- F.Verification
- F.IC_CL

According to the TOE design these security functions are enforced by the following subsystems:

- Application data (supports the TSF F.Access_Control, F.Identification_Authentication)
- Operation System Kernel (supports the TSF F.Access_Control, F.Identification_Authentication, F.Management, F.Crypto, F.Verification)
- HAL (supports the TSF F.IC_CL, F.Crypto, F.Identification_Authentication, F.Verification)
- Hardware (supports the TSF F.IC_CL)

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

TOE test configuration

The TOE test configuration is defined by the notation: MTCOS Pro 2.5 EAC with PACE / P60D145VB_J (P6022y)VB (BAC).

The TOE has 17 different file system setups due to a total of six layouts, concretely the six layouts (LayoutA-80, LayoutB-80, LayoutC-120, LayoutD-140 and LayoutE-40), each with two Secure Messaging methods with default Chip Authentication file system setup (3DES or AES-128). LayoutA-80 is additionally provided with two methods for Active Authentication (RSA or EC) and a file system setup using PUF. Furthermore, there are two more setups (Layout0-S and Layout0-L), the latter provided with or without PUF. With the exception of Layout0-S and the LayoutD-140 setups, the MRTD layouts are available in combination with one of 14 different SSCD layouts (the PUF option applies either for both applications or for none). This results in a total of 48 combinations.

Please note:

The SSCD application is subject of the separate evaluation process BSI-DSZ-CC-1001-2018 (see [24]).

Testing approach

Each security function is covered by at least one test case. Additionally, test cases exist for all subsystems identified in the TOE design.

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. Hereby not all possible parameters are tested but a sufficiently representative sample including all limit values of the parameter set.

Testing Results

All test cases were executed successfully and ended up with the expected result.

7.2. Evaluator Tests

Independent Testing according to ATE_IND

Test Configuration

The TOE has 17 different file system setups due to a total of six layouts, concretely the six layouts (LayoutA-80, LayoutB-80, LayoutC-120, LayoutD-140 and LayoutE-40), each with two Secure Messaging methods with default Chip Authentication file system setup (3DES or AES-128). LayoutA-80 is additionally provided with two methods for Active Authentication (RSA or EC) and a file system setup using PUF. Furthermore, there are two more setups (Layout0-S and Layout0-L), the latter provided with or without PUF. With the exception of Layout0-S and the LayoutD-140 setups, the MRTD layouts are available in combination with one of 14 different SSCD layouts (the PUF option applies either for both applications or for none). This results in a total of 48 combinations.

Real TOE: Completely installed TOEs in their uniquely defined operational state have been used and are therefore considered to be in a proper and known state.

Emulated TOE: Since these tests use data loaded into an emulator the task of the evaluators here is to determine, whether the initial condition of each test is satisfied. Since the CM system Subversion guarantees that the same initial data is used for the same test every time the state of the emulated card is well defined.

The evaluators conducted the tests with real cards and emulated TOE for a variety of layout combinations.

Testing approach

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.

The developer test suite for non-interactive tests have been conducted by the evaluators using the emulator and real cards. Furthermore, the evaluators performed the two interactive test with the emulator.

Subset size chosen

Based on developer tests (full coverage of all security functionalities of the TOE) the evaluators decided to focus their own independent tests on tests with real cards. For the tests with real cards some test ideas derived from the developer tests under consideration

of the described security functionality were developed by the evaluators. The evaluator additionally performed fuzzing on the known TSFI, e.g. long APDUs of random data.

Security function tested

Test with real cards using the APDU interface, as well as emulator tests concerning the correctness of implementation of TSF code were conducted.

Verdict for the sub-activity

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. The repetition of tests showed the test results are consistent.

Penetration Testing according to AVA_VAN

Overview

The penetration testing (fault injection attacks, power consumption attacks) was performed using the test environment of the evaluation facility of SRC.

The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential enhanced basic was actually successful.

Penetration testing approach

All relevant information as well as evaluation documentation were taken into account for the analysis. Then the important SFRs were analysed and it was shown that all secret keys processed by the TOE have sufficient entropy and are suitably derived for the cryptographic algorithms using them.

In the second part of 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.

Furthermore 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 are analysed.

The next part of the analysis handles the life cycle phases of the TOE.

Afterwards it is analysed on which technical level (hardware, various protocol levels of the external interface) an attacker might try an attack and why no vulnerabilities remain on each level.

Finally the relevant penetration tests are planned, performed and documented.

The evaluation facility has performed side channel analysis and fault injection attacks (laser attacks) on a variety of configurations.

Verdict for the sub-activity

The evaluators have tested the TOE systematically against enhanced basic attack potential during their penetration testing. 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 enhanced basic was actually successful in the TOE's operational environment as defined in the security target [6] and [7].

8. Evaluated Configuration

This certification covers the following configuration of the TOE: MTCOS Pro 2.5 EAC with PACE / P60D145VB_J (P6022y VB) (BAC) consisting of:

- NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software,
- Crypto Library V3.1.x on P6022y VB,
- the IC embedded software,
- a file system in the context of the MRTD application, and
- the associated guidance documentation.

The IC embedded software consists of the operating system MTCOS Pro 2.5 and an application layer, consisting of the MRTD application.

In order to meet customer requirements, the product is provided in various configurations. These differ in the number and size of the data groups, the method used for Active Authentication and the method used for Secure Messaging in the context of Chip Authentication. The configurations are described in table 3.

No	Configuration-ID	Description
1	LayoutA-80-AA_RSA-SM_3DES	80 kbytes memory space for user data, RSA for Active Authentication and 3DES for Secure Messaging
2	LayoutA-80-AA_RSA-SM_3DES-PUF	80 kbytes memory space for user data, RSA for Active Authentication and 3DES for Secure Messaging, as well as physically unclonable function (PUF) functionality available from the hardware platform.
3	LayoutA-80-AA_RSA-SM_AES-128	80 kbytes memory space for user data, RSA for Active Authentication and 128 bit AES for Secure Messaging
4	LayoutA-80-AA_RSA-SM_AES-128-PUF	80 kbytes memory space for user data, RSA for Active Authentication and 128 bit AES for Secure Messaging, as well as physically unclonable function (PUF) functionality available from the hardware platform.
5	LayoutA-80-AA_EC-SM_3DES	80 kbytes memory space for user data, EC for Active Authentication and 3DES for Secure Messaging
6	LayoutA-80-AA_EC-SM_AES-128	80 kbytes memory space for user data, EC for Active Authentication and 128 bit AES for Secure Messaging
7	LayoutB-80-AA_RSA-SM_3DES	80 kbytes memory space for user data, RSA for Active Authentication and 3DES for Secure Messaging
8	LayoutB-80-AA_RSA-SM_AES-128	80 kbytes memory space for user data, RSA for Active Authentication and 128 bit AES for Secure Messaging
9	LayoutC-120-AA_RSA-SM_3DES	120 kbytes memory space for user data, RSA for Active Authentication and 3DES for Secure Messaging
10	LayoutC-120-AA_RSA-SM_AES-128	120 kbytes memory space for user data, RSA Active Authentication and 128 bit AES for Secure Messaging
11	LayoutD-140-AA_RSA-SM_3DES	140 kbytes memory space for user data, RSA for Active Authentication and 3DES for Secure Messaging
12	LayoutD-140-AA_RSA-SM_AES-128	140 kbytes memory space for user data, RSA for Active Authentication and 128 bit AES for Secure Messaging

No	Configuration-ID	Description
13	LayoutE-40-AA_RSA-SM_3DES	40 kbytes memory space for user data, RSA for Active Authentication and 3DES for Secure Messaging
14	LayoutE-40-AA_RSA-SM_AES-128	40 kbytes memory space for user data, RSA for Active Authentication and 128 bit AES for Secure Messaging
15	Layout0-S	80 kbytes memory space for user data, corresponds to LayoutA, no proprietary file EF.ID included
16	Layout0-L	120 kbytes memory space for user data, corresponds to LayoutC, no proprietary file EF.ID included
17	Layout0-L-PUF	120 kbytes memory space for user data, corresponds to LayoutC, no proprietary file EF.ID included (physically unclonable function (PUF) functionality available from the hardware platform)

Table 3: TOE configurations

The configuration identifiers indicate the algorithm (RSA, EC) used for Active Authentication and the algorithm for Secure Messaging with default Chip Authentication (3DES, AES). Additionally, some configurations are available with the hardware functionality physical unclonable function (PUF) enabled. Both variants (PUF enabled / disabled) do not differ neither in their behaviour nor in security relevant aspects and are thus treated as one configuration. The extension '-PUF' is assigned to ensure the correct identification of the TOE.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [8] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components 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) Application of CC to Integrated Circuits,

(ii) Attack Methods for Smartcards and Similar Devices,

(iii) Application of Attack Potential to Smartcards,

(iv) Evaluation Methodology for CC Assurance Classes for EAL5+ and EAL6,

(v) Minimum Requirements for Evaluating Side-Channel Attack Resistance of RSA, DSA and Diffie-Hellman Key Exchange Implementations,

(vi) 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 [15, 16, 17, 18], have been applied in the TOE evaluation.

(see [4], AIS 25, 26, 34, 36, 46).

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

A document ETR for composite evaluation according to AIS 36 has not been provided in the course of this certification procedure.

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 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Machine Readable Travel Document with "ICAO Application" Basic Access Control, Version 1.10, 25 March 2009, BSI-CC-PP-0055-2009 [9]
- 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

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 and therefore relies on the platform certifications of the used IC (certification ID BSI-DSZ-CC-0973-V2) [15,16] and the corresponding Crypto Library (Certification ID CC-17-67206) [17,18].

9.2. Results of cryptographic assessment

The table presented in appendix A of the Security Target [6,7] 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 the these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

The TOE's two key 3DES-implementation shows a reduced remaining security level below 100 bits.

All cryptographic algorithms listed in the table in appendix A of the Security Target [6,7] are implemented by the TOE because of the standards building the TOE application. For that reason, an explicit validity period is not given for this crypto functionality.

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 (if applicable) has to be considered by the user and his system risk management process, too.

For usage of the TOE, the reduced remaining security level below 100 bits of the TOE's two key 3DES-functionality should be taken into account.[8]

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. Definitions

12.1. Acronyms

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
APDU	Application Protocol Data Unit
BAC	Basic Access Control
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
DES	Data Encryption Standard; symmetric block cipher algorithm
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ETR	Evaluation Technical Report
ICAO	International Civil Aviation Organisation

[8] With the exception of the Basic Access Control key, the TOE provides two key 3DES keys only as session keys in the context of Secure Messaging for PACE and Chip Authentication. The usage of these keys can be avoided by configuration during personalisation (PACE) and by chosing a file layout providing AES-128 session keys for Secure Messaging (Chip Authentication), respectively.'

IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MAC	Message Authentication Code
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
PUF	Physical unclonable function
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SM	Secure Messaging
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2. Glossary

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

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.

13. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 4, September 2012, http://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[9] 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

[6] Security Target BSI-DSZ-CC-0996-2018, Version 0.6 29.01.2018, Security Target - MTCOS Pro 2.5 EAC with PACE / P60D145VB_J (P6022y VB) (BAC) Machine Readable Travel Document with “ICAO Application” Basic Access Control, MaskTech International GmbH (confidential document)

[7] Security Target BSI-DSZ-CC-0996-2018, Version 1.1 16.02.2018, Security Target - MTCOS Pro 2.5 EAC with PACE / P60D145VB_J (P6022y VB) (BAC) Machine Readable Travel Document with “ICAO Application” Basic Access Control, MaskTech International GmbH (sanitised public document)

[9] 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 9, 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 38, Version 2, Reuse of evaluation results

[8] Evaluation Technical Report BSI-DSZ-CC-0996-2018, Version 1.6, 23.02.2018, Evaluation Technical Report (ETR) - MTCOS Pro 2.5 EAC with PACE / P60D145VB_J (P6022y VB) (BAC), SRC Security Research & Consulting GmbH (confidential document)

[9] Protection Profile Machine Readable Travel Document with "ICAO Application" Basic Access Control, Version 1.10, 25 March 2009, BSI-CC-PP-0055-2009

[10] Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE (EAC PP), Version 1.3.2, 05.12.2012, BSI-CC-PP-0056-V2-2012-MA-02

[11] Configuration List for MTCOS Pro 2.5 EAC with PACE / P60D145VB_J (P6022y VB), MASKTECH INTERNATIONAL GMBH, Version 0.3, 16.02.2018

[12] MTCOS Pro 2.5 EAC with PACE / P60D145VB_J (P6022y VB) User Guidance, MaskTech International GmbH, Version 0.6, 2018-02-16

[13] MTCOS Pro V2.5 on P60D145VB_J (P6022y VB) – Manual, MaskTech GmbH, 2017-10-05. Version 1.0

[14] Guidance for Initialization and Pre-personalization MTCOS Pro 2.5 / P60D145VB_J (P6022y VB), MaskTech International GmbH, Version 0.6, 2018-02-16

[15] Certification report BSI-DSZ-CC-0973-V2-2016 for NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software, 11.10.2016, Bundesamt für Sicherheit in der Informationstechnik

[16] Evaluation Technical Report for Composite Evaluation P6022y VB, Certification ID BSI-DSZ-CC-0973-V2, version 1, 25.08.2016, TÜV Informationstechnik GmbH (confidential document)

[17] Certification Report Crypto Library V3.1.x on P6022y VB, Report number NSCIB-CC-67206-CR2, 17.11.2017, TÜV Rheinland Nederland B.V. (confidential document)

[18] ETR for Composite Evaluation Crypto Library V3.1.x on P6022y VB EAL6+/5+, Certification ID CC-17-67206, Reference 17-RPT-421, version 3.0, 24.10.2017, Brightsight B.V., (confidential document)

[19] Product data sheet, Secure high-performace smart card controller, SmartMX2 family P6022y VB, rev 3.1, Document ID 292531 NXP Semiconductors, 15.11.2016, filename ds292531 - Product data sheet P6022y VB (3.1) (non-public document of the hardware platform)

[20] TR-SAC, Supplemental Access Control for Machine Readable Travel Documents, ICAO, Version 1.1, 15.04.2014

[21] ICAO Doc 9303, Machine Readable Travel Documents, ICAO, 2015

[22] TR-03110-1, Technical Guideline TR-03110-1: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, BSI, Version 2.20, 26.02.2015

[23] TR-PKI, Technical Report: PKI for Machine Readable Travel Documents offering ICC read-only access, ICAO, V1.1, October 2004

[24] TR-LDS, Technical Report: Development of a Logical Data Structure – LDS - for optional Capacity Expansion Technologies, ICAO, May 2004

[25] Certification Report BSI-DSZ-CC-0995-2018 for MTCOS Pro 2.5 EAC with PACE / P60D145VB_J (P6022y VB) from MaskTech International GmbH, 30.04.2018, Bundesamt für Sicherheit in der Informationstechnik (BSI)

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 10.4
- 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 11
- On the detailled definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 12 to 16
- 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 http://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-0996-2018

Evaluation results regarding development and production environment

The IT product MTCOS Pro 2.5 EAC with PACE / P60D145VB_J (P6022y VB) (BAC), (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 30 April 2018, 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 and ALC_COMP.1) are fulfilled for the development and production sites of the TOE listed below:

a) MaskTech International GmbH, Nordostpark 45, 90411 Nuremberg, Germany (Development)

b) SmarTrac Technology Ltd, 142/121/115 Moo, Hi-Tech Industrial Estate Tambon Ban Laean, Amphor Bang-pa-in 13160 Ayutthaya, Thailand, BSI-DSZ-CC-S-0097-2017, Site Certificate valid until 26.12.2019 (Initialisation)

c) HID Global Ireland, Teoranta Pairc Tionscail na Tullaigh, Baile na hAbhann Galway, Ireland, BSI-DSZ-CC-S-0073-2016, Site Certificate valid until 06.09.2018 (Initialisation)

d) Gemalto AG (former Trüb AG), Hintere Bahnhofstrasse 12, CH-5001 Aarau, Switzerland, BSI-DSZ-CC-S-0064-2016, Site Certificate valid until 05.06.2018 (Initialisation)

e) For development and production sites regarding the platform please refer to the certification reports BSI-DSZ-CC-0973-V2 [15] and NSCIB-CC-15-67206-CR2 [17]

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