Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0575-2009

for

MTCOS Pro 2.1 EAC / P5CD080 / CZ

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-0575-2009

MTCOS Pro 2.1 EAC / P5CD080 / CZ

from	MaskTech International GmbH
PP Conformance:	none
Functionality:	Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4

Common Criteria
Recognition
Arrangement
for components up to
EAL 4

Common Criteria

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

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

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

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

Bonn, 30 September 2009

For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Bernd Kowalski
Head of Department

L.S.

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

This page is intentionally left blank.

Preliminary Remarks

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

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

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

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

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

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

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

Contents

A Certification....7

1 Specifications of the Certification Procedure....7
2 Recognition Agreements....7
2.1 European Recognition of ITSEC/CC - Certificates....8
2.2 International Recognition of CC - Certificates....8
3 Performance of Evaluation and Certification....8
4 Validity of the certification result....9
5 Publication....9

B Certification Results....11

1 Executive Summary....12
2 Identification of the TOE....13
3 Security Policy....14
4 Assumptions and Clarification of Scope....14
5 Architectural Information....14
6 Documentation....15
7 IT Product Testing....15
7.1 Description of the Test Configuration....15
7.2 Developer Tests according to ATE_FUN....15
7.3 Evaluator Tests according to ATE_IND....16
7.4 Penetration Testing according to AVA_VLA....16
7.4.1 Developer Vulnerability Analysis....16
7.4.2 Evaluator Vulnerability Analysis....17
8 Evaluated Configuration....17
9 Results of the Evaluation....18
9.1 CC specific results....18
9.2 Results of cryptographic assessment....18
10 Obligations and notes for the usage of the TOE....19
11 Security Target....20
12 Definitions....20
12.1 Acronyms....20
12.2 Glossary....21
13 Bibliography....23

C Excerpts from the Criteria....25

D Annexes....33

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5] [1]
- Common Methodology for IT Security Evaluation, Version 2.3 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

2 Recognition Agreements

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

---

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

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

5 Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became initially effective in March 1998.

This agreement on the mutual recognition of IT security certificates was extended in April 1999 to include certificates based on the Common Criteria for the Evaluation Assurance Levels (EAL 1 – EAL 7). This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and United Kingdom, and from The Netherlands since January 2009 within the terms of this agreement.

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

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of January 2009 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the web site: 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.

This evaluation contains the components ADV_IMP.2 (Implementation of the TSF), ALC_DVS.2 (Sufficiency of Security Measures), AVA_VLA.4 (Highly Resistant) and AVA_MSU.3 (Analysis and Testing for insecure States) that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4-components of these assurance families are relevant.

3 Performance of Evaluation and Certification

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

The product MTCOS Pro 2.1 EAC / P5CD080 / CZ has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0479-2008. Specific results from the evaluation process BSI-DSZ-CC-0479-2008 were re-used.

The evaluation of the product MTCOS Pro 2.1 EAC / P5CD080 / CZ was conducted by SRC - Security Research & Consulting GmbH. The evaluation was completed on 20 August 2009. The SRC - Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

[6] Information Technology Security Evaluation Facility

For this certification procedure the sponsor and applicant is:

MaskTech International GmbH

The product was developed by:

MaskTech International GmbH

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

4 Validity of the certification result

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

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

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular basis.

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

5 Publication

The product MTCOS Pro 2.1 EAC / P5CD080 / CZ has been included in the BSI list of the certified products, which is published regularly (see also Internet: https://www.bsi.bund.de) and [5]. Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[7] MaskTech International GmbH
Nordostpark 16
90411 Nürnberg

This page is intentionally left blank.

B Certification Results

The following results represent a summary of

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

1 Executive Summary

Target of Evaluation (TOE) and subject of the Security Target (ST) [6] resp. [9] is the Security IC with a Machine Readable Travel Document, Extended Access Control Application.

The Security Target [6] resp. [9] is the basis for this certification. It does not claim conformance to a Protection Profile but it fulfills the certified Protection Profile Common Criteria Protection Machine Readable Travel Document with “ICAO Application", Extended Access Control, Version 1.2, 19.11.2006, Certification ID: BSI-PP-0026-2006 [10] except a specific filesystem requirement because the TOE does not contain the file EF.DG4 (to be used for the biometric reference data of iris image(s) of the MRTD holder).

The TOE is the contactless integrated circuit chip of machine readable travel documents (MRTD’s chip) programmed according to the Logical Data Structure (LDS) [12]. It provides the Basic Access Control, the Extended Access Control as well as the Active Authentication mechanism according to the ICAO document [11] and the Chip Authentication mechanism described in the Technical Report [13]. It will be embedded as an inlay chip module into a passport booklet.

The TOE security assurance requirements 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 ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] resp. [9], chapter 5.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC part 2 extended.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6] resp. [9], chapter 5.3.

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

TOE Security Function	Addressed issue
F.Access_Control	This Security Function regulates all access by external entities to operations of the TOE which are only executed after this TSF allowed access.
F.Identification_Authentication	This Security Function provides identification/ authentication of the user roles
F.Management	This Security Function is performed by the pre-personalization agent in phases 2b (initialization) and 2c (pre-personalization)
F.Crypto	This Security Function provides a high level interface to the DES functionality and implements the used hash algorithms of the TOE
F.Verification	This Security Function ensures correct operation of the TOE
F.IC_CL	This Security Function covers the security functions of the hardware (IC) as well as of the cryptolibrary

Table 1: TOE Security Functions

For more details please refer to the Security Target [6] resp. [9], chapter 5.1.

The claimed TOE's Strength of Functions 'high' (SOF-high) for specific functions as indicated in the Security Target [6] resp. [9], chapter 5.1 is confirmed. The rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security Target [6] resp. [9], chapter 3.1. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] resp. [9], chapter 3.2, 3.3 and 3.4.

This certification covers the following configurations of the TOE:

MTCOS Pro 2.1 EAC / P5CD080 / CZ consisting of

- the NXP Chip P5CD080V0B,
- the embedded software, and
- a file system in the context of the ICAO application.

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 2.1 EAC / P5CD080 / CZ

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/ SW	MTCOS Passport operating system and a file-system in the context of the ICAO application with the contactless NXP Chip P5CD080V0B[8]	MTCOS Pro 2.1, Rom Mask: 156 A B012	SW completely contained in ROM and EEPROM memory, chip mounted into an inlay package (type MOB4 module), initialised and tested
2	DOC	MTCOS Pro 2.1 EAC / P5CD080 / CZ User guidance	Version 1.2, 04.12.2008 [22]	Document in electronic form
3	DOC	MTCOS Standard & Pro V2.1: Part 1 - File system and security architecture	Version 1.0, 07.04.2008 [18]	Document in electronic form
4	DOC	MTCOS Standard & Pro V2.1: Part 2 - Basic Access Control and Secure Messaging	Version 1.0, 08.04.2008 [19]	Document in electronic form
5	DOC	MTCOS Standard & Pro V2.1: Part 3 - Digital Signature	Version 1.0, 02.04.2008 [20]	Document in electronic form

[8] For details on the MRTD chip and the IC Dedicated Software see Certification Report BSI-DSZ-CC-0410-2007 [23].

No	Type	Identifier	Release	Form of Delivery
6	DOC	MTCOS Standard & Pro V2.1: Part 5 - Advanced Security Mechanisms Extended Access Control (EAC)	Version 1.01, 20.06.2008 [21]	Document in electronic form

Table 2: Deliverables of the TOE

The TOE is finalized at the end of phase 2 according to the MRTD EAC PP [10]. Delivery is performed from the Initialization facility to the personalisation facility as a secured transport to a specific person of contact at the personalization site. Furthermore, the personalizer receives information about the personalisation commands and process requirements. To ensure that the personalizer receives this evaluated version, the procedures to start the personalisation process as described in the User's Guide [22] have to be followed.

3 Security Policy

The security policy of the TOE is defined according to the MRTD EAC PP [10] by the security objectives and requirements for the contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organisation (ICAO). It addresses the advanced security methods Extended Access Control in the Technical reports of the ICAO New Technology Working Group.

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: Personalization of the MRTD’s chip, Inspection Systems for global interoperability, PKI for Passive Authentication and PKI for Inspection Systems. Details can be found in the Security Target [6] resp. [9], chapter 3.2.

5 Architectural Information

The TOE is a composite product. It is composed from an Integrated Circuit, IC Embedded Software and Part Application Software. While the IC Embedded software contains the operating system MTCOS Pro 2.1, 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 the IC, the NXP P5CD080V0B Security Controller. For details concerning the CC evaluation of the NXP IC see the evaluation documentation under the Certification ID BSI-DSZ-CC-0410-2007.

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 high-level design of the TOE these Security Functions are enforced by the following subsystems:

- Application data (supports the TSF F.Access_Control, F.Identification_Authentication)
- Kernel (supports the TSF F.Access_Control, F.Identification_Authentication, F.Management, F.Crypto, F.Verification)
- HAL (supports the TSF 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 Description of the Test Configuration

The tests were performed with the composite smartcard product MaskTech MTCOS Pro 2.1 / P5CD080 / CZ consisting of the NXP Security/PKI Controller P5CD080V0B, the operating system MTCOS Pro 2.1 and a file system (called MRTD application) in the context of the ICAO application.

7.2 Developer Tests according to ATE_FUN

In the following the developer's testing effort is summarised:

TOE test configuration

For the description of the test configuration refer to chapter 7.1 of this report.

Developer's testing approach

- The developer performed functional tests in the Lifecycle Phases 2, 3 and 4 (for details see [6] resp. [9]) of the TOE and covered all the TSF and related subfunctions.
- Test suites were implemented in accordance with the functional specification of the TOE in order to verify the TOE's compliance with its expected behaviour.
- The tests were performed on a smartcard emulator and on the test samples with the MRTD Application.

Amount of developer testing performed

The developer has tested the 6 TSF of the TOE with a total of approx. 600 test cases. As demonstrated by the documentation of the test coverage the developer has tested the TOE systematically at the level of TSF functionalities as given in the functional specification. As demonstrated by the documentation of the test depth the developer has tested the TOE systematically at the level of the subsystems as given in the high level design of the TOE.

Overall developer testing results

All test of the TSF in the Lifecycle Phases 2, 3 and 4 of the TOE passed all test cases so that all TSF have been successfully tested against the functional specification and the high level design of the TOE.

7.3 Evaluator Tests according to ATE_IND

In the following the evaluator's independent testing effort is summarised:

TOE test configuration

The tests were performed in the Lifecycle Phases 2, 3 and 4. For the description of the test configuration refer to chapter 7.1 of this report.

Evaluator's testing approach

The evaluator's independent tests covered the security functionality of the TOE in the Lifecycle Phases 2, 3 and 4.

Subset size chosen

The evaluators have tested all 6 TSF.

TSF subset selection criteria

The evaluators have chosen a subset of developer tests so that all TSF could be covered by at least one test case in order to confirm that the TOE operates as specified. The valid cases as well as invalid cases were considered. For the simulator tests all tests were reproduced by the evaluators.

Security functions tested

The evaluators have covered all 6 TSF within the independent testing.

Developer tests performed

The evaluators have selected and tested a sample of approx. 100 test cases from the developer TSF tests. The evaluator's sample of developer tests covers all TSF and was performed on a smartcard emulator as well as on the test samples with the MRTD Application.

Verdict for the activity

During the evaluator's TSF subset testing the TOE operated as specified. The evaluators have verified the developer's test results by executing a sample of tests in the developer's test documentation.

7.4 Penetration Testing according to AVA_VLA

7.4.1 Developer Vulnerability Analysis

In the following the evaluator's penetration testing effort based on developer vulnerability analysis is summarised:

Testing approach

Examination of developer's vulnerability analysis in the intended environment of the TOE.

TOE test configuration

For the description of the test configuration refer to chapter 7.1 of this report.

Security functions penetration tested

The evaluators have covered all the TSF within the penetration testing.

Verdict for the sub-activity

The evaluator has performed penetration testing based on the developer vulnerability analysis. During the evaluator's penetration testing the TOE operated as specified. The vulnerabilities are not exploitable in the intended environment for the TOE. The TOE is resistant to attackers with high attack potential.

7.4.2 Evaluator Vulnerability Analysis

In the following the evaluator's penetration testing effort based on his independent vulnerability analysis is summarised:

Testing approach

Examination of evaluator's vulnerability analysis in the intended environment of the TOE.

TOE test configuration

For the description of the test configuration refer to chapter 7.1 of this report.

Security functions penetration tested

The evaluators have covered all the TSF within the penetration testing.

Verdict for the sub-activity

The evaluator has performed penetration testing based on his independent vulnerability analysis. During the evaluator's penetration testing the TOE operated as specified. The vulnerabilities are not exploitable in the intended environment for the TOE. The TOE is resistant to attackers with high attack potential.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

MTCOS Pro 2.1 / P5CD080 / CZ consisting of

- the NXP Chip P5CD080V0B,
- the embedded software, and
- a file system in the context of the ICAO application.

The IC embedded software consists of the operating system MTCOS 2.1 Pro EAC, including a cryptographic library which supports T-DES, RSA and ECDH (Elliptic Curve Diffie-Hellman) and an application layer, consisting of the ICAO application.

The customer specific ROM mask is labelled by NXP as 156 A B012. The name of the ROM file transferred from MaskTech to NXP is *rom_mtcos_sp_v2.1_p5cd080_b1-071012.hex*.

Since an MRTD may have different file structures here the certified configuration of the TOE is addressed. The certified configuration of the TOE consists of the hardware applied with the initialisation as well as pre-personalisation file STC-patch1v7-FSP-initscript-v2.txt. All files are maintained using the configuration management system Subversion. The certified version number of the above mentioned script is 3488.

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.

For components beyond EAL 4 the evaluation methodology applied was defined in co-ordination with the Certification Body [4] (AIS 34).

The evaluation methodology CEM [2] was used for those components used up to EAL 4 extended by advice of the Certification Body for components beyond EAL 4 and smart card specific guidance.

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

- All components of the class ASE
- All components of the EAL 4 package as defined in the CC (see also part C of this report)
- The components
  ADV_IMP.2 – Implementation of the TSF
  ALC_DVS.2 – Sufficiency of security measures
  AVA_MSU.3 – Analysis and testing for insecure states
  AVA_VLA.4 – Highly resistant
  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-0479-2008, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the integration additional production sites, some changes at the filesystem and some changes at the level of implementation.

The evaluation has confirmed:

- for the Functionality: Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by
  ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4

The TOE Security Functions fulfil the claimed Strength of Function 'high'.

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

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

9.2 Results of cryptographic assessment

The rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This holds for the following TOE Security Functions:

- F.Identification_Authentication Identification/ authentication of the user roles

- F.Crypto — Interface to the DES functionality and implementation of the used hash algorithms
- F.IC_CL — Security Functions of the hardware (IC) as well as of the cryptolibrary

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

- Hash functions:

  SHA-1, SHA-224 and SHA-256 according to FIPS 180-2
- Algorithms for the encryption and decryption:

  Triple-DES in CBC mode with cryptographic key size of 112 bits according to FIPS 46-3
- Algorithms for the message authentication:

  Retail MAC with cryptographic key size of 112 bits according to ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)
- Algorithms for the signature verification:

  ECDSA with SHA-1, SHA-224 or SHA-256 and cryptographic key sizes of 224, 256 and 320 bits according to FIPS 186-2
- Algorithms for the signature creation:

  RSA with SHA-1 and cryptographic key sizes of 1024 - 2048 bits according to ISO/IEC 9796-2:2002
- Algorithms for key agreement:

  ECDH with key size of 112 bits for the generated session keys according to TR-03110

This holds for the following security functions:

- F.Identification_Authentication — Identification/ authentication of the user roles
- F.Crypto — Interface to the DES functionality and implementation of the used hash algorithms
- F.IC_CL — Security Functions of the hardware (IC) as well as of the cryptolibrary

The strength of the cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 4, Para. 3, Clause 2). According to Technical Guideline BSI-TR-03110, Version 1.11 [13], the algorithms are suitable for securing originality and confidentiality of the stored data for machine readable travel documents (MRTDs). A validity period of each algorithm is not mentioned in BSI-TR-03110 [13].

10 Obligations and notes for the usage of the TOE

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

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 Definitions

12.1 Acronyms

APDU Application Protocol Data Unit

BAC Basic Access Control

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

CC Common Criteria for IT Security Evaluation

CEM Common Methodology for IT Security Evaluation

DES Data Encryption Standard; symmetric block cipher algorithm

DOC Document

EAC Extended Access Control

EAL Evaluation Assurance Level

EEPROM Electronically Erasable Programmable Read Only Memory

ES Embedded Software

ETR Evaluation Technical Report

IC Integrated Circuit

ICAO International Civil Aviation Organisation

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

LDS Logical Data Structure

MRTD Machine Readable Travel Document

PP Protection Profile

RAM Random Access Memory

RNG Random Number Generator

ROM Read Only Memory

SF Security Function

SFP Security Function Policy

SOF Strength of Function

ST Security Target

TOE Target of Evaluation

Triple-DES Symmetric block cipher algorithm based on the DES

TSC TSF Scope of Control

TSF TOE Security Functions

TSP TOE Security Policy

TSS TOE Summary Specification

12.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

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

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

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

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

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

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

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

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

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

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

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

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

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

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

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

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

13 Bibliography

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

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

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.[9]

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Website

[6] Security Target – Machine Readable Travel Document with "ICAO Application", Extended Access Control, MTCOS Pro 2.1 EAC / P5CD080 / CZ, Version 1.8, 28.05.2009, MaskTech International GmbH

[7] Evaluation Technical Report, Version 1.3, 18.08.2009, MaskTech MTCOS Pro 2.1 / P5CD080 / CZ, SRC Security Research & Consulting GmbH (confidential document)

[8] Configuration list of MTCOS Pro 2.1 EAC / P5CD080 / CZ, Version 1.20, 28.05.2009, MaskTech International GmbH (confidential document)

[9] Security Target BSI-DSZ-CC-0575-2009, Version 1.0, 25.09.2009, Security Target lite – Machine Readable Travel Document with „ICAO Application", Extended Access Control MTCOS Pro 2.1 EAC / P5CD080 / CZ, MaskTech International GmbH (sanitised public document)

[10] Machine Readable Travel Document with „ICAO Application", Extended Access Control, BSI-PP-0026 , Version 1.2, 19.11.2007, BSI

[11] Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Version - 1.1, Date - October 01, 2004, published by authority of the secretary general, International Civil Aviation Organisation

---

[9] specifically

- AIS 25, Version 3, 6 August 2007, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 3, 6 August 2007, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 34, Version 1.00, 1 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 2, 12 November 2007, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

[12] Machine Readable Travel Documents Technical Report, Development of a Logical Data Structure – LDS, For Optional Capacity Expansion Technologies, Revision 1.7, published by authority of the secretary general, International Civil Aviation Organisation, LDS 1.7, 2004-05-18

[13] Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), TR-03110, Version 1.11, 21.02.2008, BSI

[14] Smartcard IC Platform Protection Profile, Version 1.0, July 2001, BSI registration ID: BSI-PP-0002-2001, developed by Atmel Smart Card ICs, Hitachi Ltd., Infineon Technologies AG, Philips Semiconductors

[15] ETR for composition - Secured Crypto Library on the NXP P5CD080V0B according to AIS36, BSI-DSZ-CC-0417, Version 4.0, 04.04.2008, Brightsight

[16] Security Target Lite BSI-DSZ-CC-0417-2008, Version 1.3, 11.08.2008, Secured Crypto Library on the P5CD080V0B - Security Target Lite, NXP Semiconductors

[17] Certification Report BSI-DSZ-CC-0417-2008 for NXP Smart Card Controller P5CD080V0B with IC dedicated software: Secured Crypto Library Release 2.0 from NXP Semiconductors Germany GmbH, 13 Juni 2008, BSI

[18] MTCOS Standard & Pro V2.1: Part 1 - File System and Security Architecture, Version 1.0, 07.04.2008, MaskTech GmbH

[19] MTCOS Standard & Pro V2.1: Part 2 - Basic Access Control and Secure Messaging, Version 1.0, 08.04.2008, MaskTech GmbH

[20] MTCOS Standard & Pro V2.1: Part 3 - Digital Signature, Version 1.0, 02.04.2008, MaskTech GmbH

[21] MTCOS Standard & Pro V2.1: Part 5 - Advanced Security Mechanisms Extended Access Control (EAC), Version 1.01, 20.06.2008, MaskTech GmbH

[22] MTCOS Pro 2.1 EAC / P5CD080 / CZ User guidance, Version 1.2, 04.12.2008, MaskTech GmbH

[23] Certification Report for NXP Secure Smart Card Controller P5CD080V0B, P5CN080V0B and P5CC080V0B each with specific IC Dedicated Software, BSI-DSZ-CC-410-2007, 05.07.2007, BSI

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

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

The conformance result consists of one of the following:

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

plus one of the following:

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

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

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

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

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

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

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

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

Table 3 - Protection Profile families - CC extended requirements”

Security Target criteria overview (Chapter 8.3)

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

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

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

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

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

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 11.1)

“Table 6 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 7 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

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

Table 6: Evaluation assurance level summary”

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

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.”

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

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 11.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 11.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 11.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

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

“Objectives

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

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

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

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

"Application notes

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

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

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment 35

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0575-2009

Evaluation results regarding development and production environment

The IT product MTCOS Pro 2.1 EAC / P5CD080 / CZ (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005) .

As a result of the TOE certification, dated 30 September 2009, the following results regarding the development and production environment apply. The Common Criteria Security Assurance Requirements

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

are fulfilled for the development and production site of the TOE named below:

(a) MaskTech International GmbH, Nordostpark 16, 90411 Nuremberg, Germany (Development)

(b) TRÜB AG, Hintere Bahnhofstrasse 12, CH-5001 Aarau, Switzerland (Initialisation)

(c) Cardag Deutschland GmbH, An der Allee 6, 99848 Wutha-Farnroda, Germany (TOE Completion)

(d) Smartrac Technology Ltd., 142 Moo 1 Hi-Tech industrial Estate, Tambon Ban Laean, Amphor Bang-pa-in, 13160 Phra Nakhon Si Ayutthaya, Thailand (TOE Completion)

(e) TRÜB Cards AG (once Cardag CH), Suhrenmattstrasse 23, 5035 Unterentfelden, Switzerland (Pre-Personalisation)

For development and production sites regarding the NXP chip P5CD080V0B refer to the certification report BSI-DSZ-CC-0410-2007.

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.

This page is intentionally left blank.