Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0362-2006

for

TCOS Passport Version 1.0 Release 2 / P5CD072V0Q and TCOS Passport Version 1.0 Release 2 / SLE66CLX641P/m1522-a12

from

T-Systems Enterprise Services GmbH SSC Testfactory & Security

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 228 9582-0, Fax +49 228 9582-455, Infoline +49 228 9582-111

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0362-2006

Security IC with MRTD BAC Application

TCOS Passport Version 1.0 Release 2 / P5CD072V0Q and TCOS Passport Version 1.0 Release 2 / SLE66CLX641P/m1522-a12

from

T-Systems Enterprise Services GmbH SSC Testfactory & Security

Common Criteria Arrangement for components up to EAL4

The IT products identified in this certificate have been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Part 1 Version 0.6*, *Part 2 Version 1.0* extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)* and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

Evaluation Results:

PP Conformance:	**Machine Readable Travel Document with „ICAO Application", Basic Access Control, version 1.0 (BSI-PP-0017-2005)**
Functionality:	**BSI-PP-0017-2005 conformant** **Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL4 augmented by:** ADV_IMP.2 (Implementation of the TSF) and ALC_DVS.2 (Sufficiency of security measures)

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.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 31. March 2006

The President of the Federal Office
for Information Security

IT Security Certified

Dr. Helmbrecht L.S. SOGIS - MRA

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-455 - Infoline +49 228 9582-111

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 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.

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 setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), Version 2.1[5]
- Common Methodology for IT Security Evaluation (CEM)
- Part 1, Version 0.6
- Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

The use of Common Criteria Version 2.1, Common Methodology, part 2, Version 1.0 and final interpretations as part of AIS 32 results in compliance of the certification results with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2 as endorsed by the Common Criteria recognition arrangement committees.

---

2 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 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 22 September 2000 in the Bundesanzeiger p. 19445

2 Recognition Agreements

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

2.1 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

2.2 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland, France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003, the Czech Republic in September 2004, the Republic of Singapore in March 2005, India in April 2005.

This evaluation contains the components ADV_IMP.2 (Implementation of the TSF) and ALC_DVS.2 (Sufficiency of security measures) 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 products TCOS Passport Version 1.0 Release 2 / P5CD072V0Q and TCOS Passport Version 1.0 Release 2 / SLE66CLX641P/m1522-a12 have undergone the certification procedure at BSI.

The evaluation of the products TCOS Passport Version 1.0 Release 2 / P5CD072V0Q and TCOS Passport Version 1.0 Release 2 / SLE66CLX641P/m1522-a12 was conducted by TÜV Informationstechnik GmbH, Evaluation Body for IT-Security. The TÜV Informationstechnik GmbH,

Evaluation Body for IT-Security is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is:

T-Systems Enterprise Services GmbH
SSC Testfactory & Security
Untere Industriestr. 20
57250 Netphen

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 31. March 2006.

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.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

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.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-22 and D1 to D-4.

The products TCOS Passport Version 1.0 Release 2 / P5CD072V0Q and TCOS Passport Version 1.0 Release 2 / SLE66CLX641P/m1522-a12 have been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer and sponsor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] T-Systems Enterprise Services GmbH
SSC Testfactory & Security
Untere Industriestr. 20
57250 Netphen

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.

Contents of the certification results

1 Executive Summary

Target of Evaluation (TOE) and subject of the Security Target (ST) [6] is the Security IC with a Machine Readable Travel Document, Basic Access Control Application TCOS Passport Version 1.0 Release 2 / P5CD072V0Q and TCOS Passport Version 1.0 Release 2 / SLE66CLX641P/m1522-a12.

The Security Target is based on the Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control [8].

The TOE is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) [9] and providing the Basic Access Control according to ICAO document [10]. It will be embedded as an inlay chip module into a passport booklet.

The TOE comprises

- the circuitry of the MRTD's chip (the integrated circuit, IC) with hardware for the contactless interface, e.g. antennae, capacitors
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software
- the IC Embedded Software (operating system TCOS)
- the MRTD application (dedicated file for the ICAO application in a file system on the chip and
- the associated guidance documentation.

The TOE is a Smart Device with an operating system (TCOS) and a dedicated file-system, that contains all data relevant for the ICAO application.

For details on the MRTD chip and IC Dedicated Software see certification reports BSI-DSZ-CC-0349-2006 [12] for the Philips chip P5CD072V0Q and BSI-DSZ-CC-0338-2005-MA-01 [13] for the Infineon chip SLE66CLX641P.

Following the protection profile PP0002 [11, Fig. 15] the life cycle phases of a TCOS Passport device can be divided into the following seven phases:

- Phase 1: Development of operating system software by the operating system manufacturer
- Phase 2: Development of the smart card controller by the semiconductor manufacturer
- Phase 3: Fabrication of the smart card controller (integrated circuit) by the semiconductor manufacturer
- Phase 4: Installation of the chip in an inlay with an antenna
- Phase 5: Completion of the smart card operating system
- Phase 6: Initialisation and personalization of the MRTD

- Phase 7: Operational phase of the MRTD

According to the MRTD BAC PP [8] the TOE life cycle is described in terms of the four life cycle phases.

- Life cycle phase 1 “Development”: Development of Hardware and Software. This life cycle phase 1 covers Phase 1 and Phase 2 of PP0002 [11] [8].
- Life cycle phase 2 “Manufacturing”: IC Production, Initialisation and Pre-Personalization of the MRTD Application. This life cycle phase 2 corresponds to Phase 3 and Phase 4 of PP0002 [11] and may include for flexibility reasons Phase 5 and some production processes from Phase 6 as well. [9]
- Life cycle phase 3 “Personalization of the MRTD”: This life cycle phase corresponds to the remaining initialisation and personalization processes not covered yet from Phase 6 of the PP0002 [11].
- Life cycle phase 4 “Operational Use”. This life cycle phase corresponds to the Phase 7 of the PP0002 [11].

The TOE is finished after initialisation, testing the OS and creation of the dedicated file system with security attributes and ready made for the import of LDS. This corresponds to the end of life cycle phase 2 of the Protection Profile MRTD BAC PP [8]. A more detailed description of the production processes in Phases 5 and 6 of PP0002 resp. Phase 3 of the MRTD BAC PP is given in the Administrator Guidance document [14].

The IT product TCOS Passport Version 1.0 Release 2 / P5CD072V0Q and TCOS Passport Version 1.0 Release 2 / SLE66CLX641P/m1522-a12 was evaluated by TÜV Informationstechnik GmbH, Evaluation Body for IT-Security. The evaluation was completed on 23.03.2006. The TÜV Informationstechnik GmbH, Evaluation Body for IT-Security is an evaluation facility (ITSEF)[10] recognised by BSI.

The developer and sponsor is

T-Systems Enterprise Services GmbH
SSC Testfactory & Security
Untere Industriestr. 20
57250 Netphen

---

[8] Software development at T-Systems, Netphen; for hardware development sites refer to [12] resp. [13]

[9] Completion and inlay module initialisation at Bundesdruckerei (Berlin), SPSL (Chadderton) and Sokymat GmbH (Erfurt).
The personalization process at SPSL and the Bundesdruckerei was not part of the evaluation. For hardware manufacturing sites refer to [12] resp. [13];

[10] Information Technology Security Evaluation Facility

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL4+ (Evaluation Assurance Level 4 augmented). The following table shows the augmented assurance components.

Requirement	Identifier
EAL4	TOE evaluation: methodically designed, tested, and reviewed
+: ADV_IMP.2	Development – Implementation of the TSF
+: ALC_DVS.2	Life cycle support – Sufficiency of security measures

Table 1: Assurance components and EAL-augmentation

1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 extended as shown in the following tables.

The following SFRs are taken from CC part 2:

Security Functional Requirement	Identifier and addressed issue
FCS	**Cryptographic support**
FCS_CKM.1/BAC_MRTD	Cryptographic key generation – Generation of Document Basic Access Keys by the TOE
FCS_CKM.4	Cryptographic key destruction - MRTD
FCS_COP.1/SHA_MRTD	Cryptographic operation – Hash for Key Derivation by MRTD
FCS_COP.1/TDES_MRTD	Cryptographic operation – Encryption / Decryption Triple-DES
FCS_COP.1/MAC_MRTD	Cryptographic operation – Retail MAC
FDP	**User data protection**
FDP_ACC.1 (PRIM)	Subset access control – Primary Access Control
FDP_ACC.1 (BASIC)	Subset access control – Basic Access control
FDP_ACF.1 (PRIM)	Security attribute based access control – Primary Access Control
FDP_ACF.1 (Basic)	Security attribute based access control – Basic Access Control
FDP_UCT.1/MRTD	Basic data exchange confidentiality - MRTD
FDP_UIT.1/MRTD	Data exchange integrity - MRTD

Security Functional Requirement	Identifier and addressed issue
FIA	**Identification and authentication**
FIA_UID.1	Timing of identification
FIA_UAU.1	Timing of authentication
FIA_UAU.4/MRTD	Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.6/MRTD	Re-authenticating – Re-authenticating of Terminal by the TOE
FMT	**Security Management**
FMT_MOF.1	Management of functions in TSF
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FMT_MTD.1/INI_ENA	Management of TSF data – Writing of Initialization Data and Pre-personalization Data
FMT_MTD.1/INI_DIS	Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data
FMT_MTD.1/KEY_WRITE	Management of TSF data – Key Write
FMT_MTD.1/KEY_READ	Management of TSF data – Key Read
FPT	**Protection of the TOE Security Functions**
FPT_FLS.1	Failure with preservation of secure state
FPT_TST.1	TSF testing
FPT_PHP.3	Resistance to physical attack
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation

Table 2: SFRs for the TOE taken from CC Part 2

The following CC part 2 extended SFRs are defined:

Security Functional Requirement	Identifier and addressed issue
FAU	**Security Audit**
FAU_SAS.1	Audit storage
FCS	**Cryptographic support**
FCS_RND.1/MRTD	Quality metric for random numbers
FMT	**Security management**
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability

Security Functional Requirement	Identifier and addressed issue
FPT	**Protection of the TOE Security Functions**
FPT_EMSEC.1	TOE Emanation

Table 3: SFRs for the TOE, CC part 2 extended

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST [6] chapter 5.1.

The following Security Functional Requirements are defined for the IT-Environment of the TOE:

Security Functional Requirement	Identifier and addressed issue
FCS	**Cryptographic support**
FCS_CKM.1/BAC_BT	Cryptographic key generation – Generation of Document Basic Access Keys by the Basic Terminal
FCS_CKM.4/BT	Cryptographic key destruction – BT
FCS_COP.1/SHA_BT	Cryptographic operation – Hash Function by the Basic Terminal
FCS_COP.1/ENC_BT	Cryptographic operation – Secure Messaging Encryption / Decryption by the Basic Terminal
FCS_COP.1/MAC_BT	Cryptographic operation – Secure messaging Message Authentication Code by the Basic Terminal
FCS_RND.1/BT	Quality metric for random numbers - Basic Terminal
FDP	**User data protection**
FDP_DAU.1/DS	Basic data authentication – Passive Authentication
FDP_UCT.1/BT	Basic data exchange confidentiality - Basic Terminal
FDP_UIT.1/BT	Data exchange integrity - Basic Terminal
FIA	**Identification and authentication**
FIA_UAU.4/BT	Single-use authentication mechanisms – Basic Terminal
FIA_UAU.6/BT	Re-authentication - Basic Terminal
FIA_API.1/SYM_PT	Authentication Proof of Identity - Personalization Terminal Authentication with Symmetric Key

Table 4: SFRs for the IT-Environment

Note: Only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST [6] chapter 5.3.

These Security Functional Requirements are implemented by the TOE Security Functions:

- Identification and Authentication based on Challenge-Response
- Data exchange under secure messaging
- Access Control of stored data objects
- Reliability

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

1.3 Strength of Function

The TOE's strength of functions is claimed high (SOF-High) for the following security functions Identification and Authentication based on Challenge-Response and Data exchange under secure messaging.

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.

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The ST defines the following assets taken from the MRTD BAC PP [8]:

Logical MRTD Data consisting of the data groups DG1 to DG16 and the Document security object according to LDS [10].

Authenticity of the MRTD's chip

Assets have to be protected in terms of confidentiality and/or integrity.

The ST considers the following subjects taken from the MRTD BAC PP [8]: Manufacturer, MRTD Holder, Traveller, Personalization Agent, Inspection System (split into Primary Inspection System (PIS), Basic Inspection System (BIS), and Extended Inspection System (EIS)), the Terminal and the Attacker. For details refer to the Security Target chapter 3.2.

The following list of considered threats for the TOE is defined in the Security Target. They are taken from the MRTD BAC PP [8].

T.Chip_ID Identification of MRTD's chip

An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening a communication through the contactless communication interface. The attacker can not read and does not know in advance the MRZ data printed on the MRTD data page.

T.Skimming Skimming the logical MRTD

An attacker imitates the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE. The attacker can not read and does not know in advance the MRZ data printed on the MRTD data page.

T.Eavesdropping Eavesdropping to the communication between TOE and inspection system

An attacker is listening to the communication between the MRTD's chip and an inspection system to gain the logical MRTD or parts of it. The inspection system uses the MRZ data printed on the MRTD data page but the attacker does not know this data in advance.

T.Forgery Forgery of data on MRTD's chip

An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to impose on an inspection system by means of the changed MRTD holder's identity or biometric reference data. This threat comprises several attack scenarios of MRTD forgery.

T.Abuse-Func Abuse of Functionality

An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data. This threat addresses the misuse of the functions for the initialisation and the personalization in the operational state after delivery to MRTD holder.

T.Information_Leakage Information Leakage from MRTD's chip

An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage may be inherent in the normal operation or caused by the attacker.

T.Phys-Tamper Physical Tampering

An attacker may perform physical probing of the MRTD's chip in order to disclose TSF Data to disclose/reconstruct the MRTD's chip Embedded Software. An attacker may physically modify the MRTD's chip in order to (i) modify security features or functions of the MRTD's chip, (ii) modify security functions of the MRTD's chip Embedded Software, (iii) to modify User Data or (iv) to modify TSF data.

T.Malfunction Malfunction due to Environmental Stress

An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent or deactivate or modify security functions of the MRTD's chip Embedded Software.

For more details refer to the Security Target chapter 3.3.

The TOE shall comply to the following organisation security policies as security rules, procedures, practices, or guidelines imposed by an organisation upon its operations:

P.Manufact Manufacturing of the MRTD's chip

The IC Manufacturer and MRTD Manufacturer ensure the quality and the security of the manufacturing process and control the MRTD's material in the Phase 2 Manufacturing. The Initialisation Data are written by the IC Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

P.Personalization Personalization of the MRTD by issuing State or Organisation only

The issuing State or Organisation guarantees the correctness of the biographical data, the printed portrait and the digitised portrait, the biometric reference data and other data of the logical MRTD with respect to the MRTD holder. The personalization of the MRTD for the holder is performed by authorised agents of the issuing State or Organisation only.

P.Personal_Data Personal data protection policy

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (DG1), the printed portrait and the digitised portrait (DG2), the biometric reference data of finger(s) (DG3), the biometric reference data of iris image(s) (DG4) and data according to LDS (DG5 to DG14, DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys as defined in [9].

1.5 Special configuration requirements

The issuing State or Organisation decides (i) to enable the Basic Access Control for the protection of the MRTD holder personal data or (ii) to disable the Basic Access Control to allow Primary Inspection Systems of the receiving States and all other terminals to read the logical MRTD. This configuration is performed during the personalization phase 3 of the TOE life cycle.

1.6 Assumptions about the operating environment

The assumptions are describe the security aspects of the environment in which the TOE will be used or is intended to be used. The ST defines the following assumptions taken from the MRTD BAC PP [8]:

A.Pers_Agent Personalization of the MRTD's chip

The Personalization Agent ensures the correctness of (i) the logical MRTD with respect to the MRTD holder, (ii) the Document Basic Access Keys, (iii) the Active Authentication Public Key Info (DG15) if stored on the MRTD's chip, and (iv) the Document Signer Public Key Certificate (if stored on the MRTD's chip) on the MRTD's chip. (Note: Because the Active Authentication Public Key Info (DG15) is not stored on the TOE, this assumption from the MRTD BAC PP [8] is not relevant.) The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

A.Insp_Sys Inspection Systems for global interoperability

The Inspection System is used by the border control officer of the receiving State (i) examining an MRTD presented by the traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder. The Primary Inspection System for global interoperability contains the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organisation [9]. The Primary Inspection System performs the Passive Authentication to verify the logical MRTD if the logical MRTD is not protected by Basic Access Control. The Basic Inspection System in addition to the Primary Inspection System implements the terminal part of the Basic Access Control and reads the logical MRTD being under Basic access Control.

1.7 Disclaimers

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:

TCOS Passport Version 1.0 Release 2 / P5CD072V0Q and TCOS Passport Version 1.0 Release 2 / SLE66CLX641P/m1522-a12

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1a	HW / SW	TCOS Passport operating system and file-system for the ICAO application with Philips chip P5CD072V0Q[11]	Version 1 Release 2 / P5CD072V0Q, mask ICAO10R1 Philips	SW completely contained in ROM and EEPROM memory, chip mounted into an inlay package (OM9500/1) initialised and tested
1b	HW / SW	TCOS Passport operating system and file-system for the ICAO application with Infineon chip SLE66CLX641P[12]	Version 1 Release 2 / SLE66CLX641P/m1522a12, mask ICAO10R1 Infineon	SW completely contained in ROM and EEPROM memory, chip mounted into an inlay package initialised and tested
2	DOC	Administrator manuals TCOS Passport Version 1.02 [14] and [15]	Version 1.02 10.March 2006	Document in paper / electronic form as pdf file
3	DOC	User Manual TCOS Passport Version 1.02 [16]	Version 1.02 10.March 2006	Document in paper / electronic form as pdf file

Table 5: Deliverables of the TOE

The TOE is finalized at the end of phase 2 according to the MRTD BAC PP. Delivery is performed from the Initialization facility to the personalisation facility by 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 administrator manual for personalisation [15] have to be followed.

3 Security Policy

The security policy of the TOE is defined according to the MRTD BAC PP [8] 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 Basic Access Control in the Technical reports of the ICAO New Technology Working Group.

4 Assumptions and Clarification of Scope

The assumptions on Personalization of the MRTD's chip and on Inspection Systems for global interoperability as outlined above are of relevance.

---

[11] For details on the MRTD chip and IC Dedicated Software see certification report BSI-DSZ-CC-0349-2006 [12] for the Philips chip P5CD072V0Q.

[12] For details on the MRTD chip and IC Dedicated Software see certification report BSI-DSZ-CC-0338-2005-MA-01 [13] for the Infineon chip SLE66CLX641P.

The state or organisation issues the MRTD to be used by the holder for international travel. The traveller presents a MRTD to the inspection system to prove his or her identity. The authentication of the traveller is based on (i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and (ii) biometrics using the reference data stored in the MRTD. The issuing State or Organisation ensure the authenticity of the data of genuine MRTD's. The receiving State trust a genuine MRTD of a issuing State or Organisation.

5 Architectural Information

The TOE consists of hardware and software. Hardware is either the Infineon Chip SLE66CX641P or the Philips Chip P5CD072V0Q.

The TOE software is the chip card operation system TCOS and the specific ICAO file-system specified by specific initialisation data. The software is grouped as follows:

The kernel subsystem controls the communication between all other subsystems. It checks the used memory areas, allocates resources and controls the order of operation.

The administrative subsystem contains all administrative functionality of the TOE. It provides functionality for generation and deletion of files and directories and for reading and writing of files. This subsystem is also responsible for access control.

The crypto subsystem contains the cryptographic functionality and guarantees controlled access to keys.

The IO subsystem is responsible for all communication to the external world. It implements the protocol T=CL and checks syntax of APDUs.

The ROM TCOS-Type Task includes the ISO specific parts of the code. It analysis the APDUs and enforces calls to other subsystems.

The User-Type Task of TCOS including application specific code but is not used within the TOE.

The TSF of the software uses the hardware via evaluated hardware interfaces. External interface of the composite TOE used in the MRTD application is a specific set of commands operating on a defined file-system of the application. This interface is available to the inspection system via the contactless chip interface.

6 Documentation

The administrator manual for personalisation [14] is provided for the Personalization Agent of the TOE who needs information about security procedures and how the TOE supports the personalisation process.

The administrator manual for initialisation [15] includes information about the initialisation process which is done before TOE delivery.

The user manual [16] is provided for the developer of an inspection system who needs information how the TOE interacts with the inspection system.

7 IT Product Testing

Developer tests, independent evaluator tests and penetration tests were performed using MRTD chips TCOS Passport Version 1.02/P5CD072 (Philips Chip) and TCOS Passport Version 1.02/SLE66CLX641P (Infineon Chip) composed of the hardware chip, its dedicated software, the operating system TCOS and a file-system for the ICAO application. TOEs in the configuration LDS (Logical Data Structure) and BAC (Basic Access Control) were tested.

The developer performed functional tests with a TOE in the personalization phase and in the operational phase. All security functions were tested including their sub-functions. The test coverage analysis and the test depth analysis gave evidence that the TOE was systematically tested on the level of the functional specification and on subsystem level.

The test cases defined based on the security functionality specified in the functional specification showed the conformance to the expected behaviour of the TOE in the personalization and operational phase. The tests were performed using a smart card simulator and real chips with the TOE software and the ICAO file-system.

The evaluator repeated developer tests by sampling. The sample covered all security functions and was performed by using real chips and an emulator. The TOE operated as specified.

Independent evaluator tests were performed in phase 5 (completion of the smart card operating system), phase 6 (initialisation and personalization of the MRTD) and in phase 7 (Operational phase of the MRTD) of the TOE. The tests confirmed the expected behaviour as specified.

The evaluators penetration tests confirmed the effectiveness of all security functions of the TOE. During these tests the different life cycle phases were considered. The penetration tests were performed based on the developers vulnerability analysis and based on the independent vulnerability analysis of the evaluator. Potential vulnerabilities were assessed upon their exploitability by analysis and tests. Analysis results and tests results showed that potential vulnerabilities are not exploitable in the intended operational environment of the TOE and that the TOE is resistant against low attack potential AVA_VLA.2 as specified.

8 Evaluated Configuration

The TOE is delivered at the end of phase 6.1 in form of initialised and tested inlay module. This corresponds to the end of life cycle phase 2 of the Protection Profile MRTD BAC PP [8].

All procedures for personalisation and configuration for the end-user necessary after delivery are described in the Administrator Guidance document [14].

9 Results of the Evaluation

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.

As the evaluation of the TOE was conducted as a composition evaluation, the ETR [7] includes also the evaluation results of the composite evaluation activities in accordance with CC Supporting Document, ETR-lite for Composition: Annex A Composite smart card evaluation [4, AIS 36]. The ETR [7] builds up on the *ETR-lite for Composition* document of the evaluation of the underlying Philips chip P5CD072V0Q (see BSI-DSZ-CC-0349-2006 [12]) and the Infineon chip SLE66CLX641P (BSI-DSZ-CC-0338-2005-MA-01 [13]).

The evaluation methodology CEM [2] was used for those components identical with EAL4. For components beyond EAL4 the methodology was defined in coordination with the Certification Body [4, AIS 34]). For smart card specific methodology the scheme interpretations AIS 25, AIS 26 and AIS 36 (see [4]) were used.

The verdicts for the CC, Part 3 assurance components (according to EAL4 augmented and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components		**Verdict**
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Partial CM automation	ACM_AUT.1	PASS

Assurance classes and components		Verdict
Generation support and acceptance procedures	ACM_CAP.4	PASS
Problem tracking CM coverage	ACM_SCP.2	PASS
Delivery and operation	CC Class ADO	PASS
Detection of modification	ADO_DEL.2	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Fully defined external interfaces	ADV_FSP.2	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Implementation of the TSF	ADV_IMP.2	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Informal TOE security policy model	ADV_SPM.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Sufficiency of security measures	ALC_DVS.2	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Well-defined development tools	ALC_TAT.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Validation of analysis	AVA_MSU.2	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Independent vulnerability analysis	AVA_VLA.2	PASS

Table 6: Verdicts for the assurance components

The evaluation has shown that:

- the TOE is conformant to the PP Machine Readable Travel Document with „ICAO Application", Basic Access Control, version 1.0 (BSI-PP-0017-2005) [8]
- Security Functional Requirements specified for the TOE are PP conformant and Common Criteria Part 2 extended

- the assurance of the TOE is Common Criteria Part 3 conformant, EAL4 augmented by ADV_IMP.2 (Implementation of the TSF) and ALC_DVS.2 (Sufficiency of security measures).

The following TOE Security Functions fulfil the claimed Strength of Function SOF-high:

- Identification and Authentication based on Challenge-Response
- Data exchange under secure messaging.

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 Triple-DES functionality.

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

The results of the evaluation are only applicable to the TCOS Passport Version 1.0 Release 2 / P5CD072V0Q and TCOS Passport Version 1.0 Release 2 / SLE66CLX641P/m1522-a12. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The operational documents [14], [15] and [16] contain necessary information about the usage of the TOE and all security hints therein have to be considered.

The TOEs implemented security functions meet the claimed strength of function SOF-high from design and construction point of view. The strength of function available in a specific system context where the TOE is used depends on the selection of the data used to set up the communication to the TOE. Therefore the issuing state or organisation is responsible for the strength of function that can be achieved in a specific system context. This has to be assessed in the specific system context. Then, the administrator (personalizer) is in collaboration with the issuing state or organisation responsible to provide keys with sufficient entropy, as required by the specific system context.

Only chips from the production sites (waferfabs, module and inlay production sites) as outlined in the certification reports for the Philips chip P5CD072V0Q (BSI-DSZ-CC-0349-2006 [12]) and for the Infineon chip SLE66CLX641P (BSI-DSZ-CC-0338-2005-MA-01 [13]) shall be used.

The Personalization Agent has to verify that they got the correct version of the TOE.

Defect chips and invalid passports including a chip must be destroyed in a way that the chip itself is destructed.

11 Annexes

Annex A: Evaluation results regarding the development and production environment (see part D of this report).

12 Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 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
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
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

13.2 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.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

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

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

- AIS 25, Version 2, 29 July 2002 for: CC Supporting Document, - The Application of CC to Integrated Circuits, Version 1.2, July 2002
- AIS 26, Version 2, 6 August 2002 for: CC Supporting Document, - Application of Attack Potential to Smartcards, Version 1.1, July 2002
- AIS 32, Version 1, 02 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungs-schema.
- AIS 34, Version 1.00, 1 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 36, Version 1, 29 July 2002 for:
  CC Supporting Document, ETR-lite for Composition, Version 1.1, July 2002 and CC Supporting Document, ETR-lite for Composition: Annex A Composite smartcard evaluation, Version 1.2 March 2002

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

[6] T-Systems, Specification of the Security Target TCOS Passport Version 1.0 Release 2, 16.01.2006, Version: 1.02, BSI-DSZ-CC-0362-2006

[7] Technischer Evaluierungsbericht (ETR), Version: 2, 23.03.2006 for TCOS Passport Version 1 Revision 2 / P5CD072 and TCOS Passport Version 1.0 Revision 2 / SLE66CLX641P, TÜVIT

[8] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-PP-0017, Version 1.0, 18. August 2005, BSI

[9] 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

[10] 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

[11] 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

[12] Certification Report BSI-DSZ-CC-0349-2006 for Philips Secure Smart Card Controller P5CT072V0Q, P5CD072V0Q and P5CD036V0Q with specific IC Dedicated Software, 28. March 2006, BSI

[13] Certification Report BSI-DSZ-CC-0338-2005-MA-01 for Infineon Smart Card IC (Security Controller) SLE66CLX640P/m1523-a12 and SLE66CLX641P/m1522-a12 both with RSA2048 V1.3 and specific IC Dedicated Software, 15. December 2005, BSI

[14] Administratorhandbuch zur Initialisierung TCOS Passport Version 1.0 Release 2, T-Systems, Version 1.02, 10. March 2006

[15] Administratorhandbuch zur Personalisierung TCOS Passport Version 1.0 Release 2, Version 1.02, 10. March 2006

[16] Benutzerhandbuch TCOS Passport Version 1.0 Release 2, T-Systems, Version 1.02, 10. March 2006

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (chapter 5.4) / **Final Interpretation 008**

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 Part 2 (functional requirements), 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:

Part 2 conformant - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2

plus one of the following:

Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in 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:

Assurance categorisation (chapter 2.5)

"The assurance classes, families, and the abbreviation for each family are shown in Table 2.1.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class 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
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 2.1. -Assurance family breakdown and mapping“

Evaluation assurance levels (chapter 6)

"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 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 6.1)

“Table 6.1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

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

These EALs consist of an appropriate combination of assurance components as described in chapter 2 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 CC 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 6.1 - Evaluation assurance level summary“

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 6.2.1)

"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 6.2.2)

"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 6.2.3)

"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 6.2.4)

"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 6.2.5)

"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 6.2.6)

"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 6.2.7)

"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 14.3)

AVA_SOF Strength of TOE security functions

"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 14.4)

AVA_VLA Vulnerability analysis

"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), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential.“

D Annexes

List of annexes of this certification report

This page is intentionally left blank.

Annex A of Certification Report BSI-DSZ-CC-0362-2006

Evaluation results regarding development and production environment

The IT products TCOS Passport Version 1.0 Release 2 / P5CD072V0Q and TCOS Passport Version 1.0 Release 2 / SLE66CLX641P/m1522-a12 (Target of Evaluation, TOE) have been evaluated at an accredited and licensed/ approved evaluation facility using the Common Methodology for IT Security Evaluation, Part 1 Version 0.6, Part 2 Version 1.0, extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance, for conformance to the Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC15408: 1999) and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

As a result of the TOE certification, dated 31. March 2006, the following results regarding the development and production environment apply. The Common Criteria 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 sites of the TOE listed below:

- T-Systems Enterprise Services GmbH, SSC Testfactory & Security, Untere Industriestr. 20, 57250 Netphen, Germany (embedded software development).
- Bundesdruckerei, Oranienstrass 91, 10958 Berlin, Germany (TOE Completion, Initialisation and Pass Production).
- Security Printing And System Limited (SPSL), Gorse Street, Chadderton, Oldham OL9 9QH, United Kingdom (TOE Completion, Initialisation and Pass Production).

  Note: The personalisation process at SPSL and the Bundesdruckerei was not part of the evaluation.
- Sokymat GmbH, In den Weiden 4 B, 99099 Erfurt, Germany (TOE Completion and Initialisation).

For development and productions sites regarding the Philips chip P5CD072V0Q refer to the certification report BSI-DSZ-CC-0349-2006 and regarding the

Infineon chip SLE66CLX641P refer to the certification report BSI-DSZ-CC-0338-2005-MA-01.

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target (T-Systems, Specification of the Security Target TCOS Passport Version 1.0 Release 2, 16.01.2006, Version: 1.02, BSI-DSZ-CC-0362-2006 [6]). The evaluators verified, that the requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6]) are fulfilled by the procedures of these sites.