Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0429-2007

for

Starcos 3.01 PE V1.1

from

Giesecke & Devrient GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 9582-111

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0429-2007

Security IC with MRTD BAC Application

Starcos 3.01 PE V1.1

from

Giesecke & Devrient GmbH

Common Criteria Arrangement
for components up to EAL4

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, version 2.3* (ISO/IEC 15408:2005) 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 2.3 (ISO/IEC 15408:2005)*.

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, 18. July 2007

The President of the Federal Office
for Information Security

IT Security Certified

SOGIS - MRA

Dr. Helmbrecht 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)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 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

Part A: Certification
Part B: Certification Results
Part C: Excerpts from the Criteria
Part D: Annexes

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 2.3[5]
- Common Methodology for IT Security Evaluation (CEM), version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

---

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 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 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 European Recognition of ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective in March 1998. This agreement has been 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). The German Federal Office for Information Security (BSI) recognizes certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

2.2 International Recognition of 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 has been signed in May 2000 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC. As of February 2007 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, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America.

The current list of signatory nations resp. approved certification schemes can be seen on the web site: http:\\www.commoncriteriaportal.org

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 product Starcos 3.01 PE V1.1 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0313-2006.

The evaluation of the product Starcos 3.01 PE V1.1 was conducted by TÜV Informationstechnik GmbH, Prüfstelle IT-Sicherheit. The TÜV Informationstechnik GmbH, Prüfstelle IT-Sicherheit is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is

Giesecke & Devrient GmbH
Prinzregentenstraße 159
Postfach 80 07 29
81607 München

The certification is concluded with

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

This work was completed by the BSI on 18. July 2007.

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 product Starcos 3.01 PE V1.1 has 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 vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] Giesecke & Devrient GmbH
Prinzregentenstraße 159
Postfach 80 07 29
81607 München

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	3
2	Identification of the TOE	12
3	Security Policy	13
4	Assumptions and Clarification of Scope	13
5	Architectural Information	13
6	Documentation	14
7	IT Product Testing	14
8	Evaluated Configuration	15
9	Results of the Evaluation	15
10	Comments/Recommendations	18
11	Annexes	18
12	Security Target	18
14	Bibliography	20

1 Executive Summary

Target of Evaluation (TOE) and subject of the Security Target (ST) [7] is the Security IC with a Machine Readable Travel Document, Basic Access Control Application Starcos 3.01 PE V1.1.

The Security Target is based on the Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control [9].

The certification of Starcos 3.01 PE V1.1 is a re-certification based on BSI-DSZ-CC-0313-2006 (Starcos 3.01 PE V1.0) with some changes at the level of implementation and the integration of a new initialisation facility.

The TOE is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) [10] and providing the Basic Access Control according to ICAO document [11]. 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 STARCOS)
- 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 (Starcos) 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 the certification report BSI-DSZ-CC-0312-2006 [13] for the Philips chip P5CT072V0N.

Following the protection profile PP0002 for SmarCard IC platforms [12, Fig. 15] the life cycle phases of a 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 [9] 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 [12][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 [12] 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 [12].
- Life cycle phase 4 “Operational Use”. This life cycle phase corresponds to the Phase 7 of the PP0002 [12].

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 [9]. A more detailed description of the production processes in Phases 5 and 6 of PP0002 resp. Phase 2 and 3 of the MRTD BAC PP is given in the Administrator Guidance document [14].

The IT product Starcos 3.01 PE V1.1 was evaluated by TÜV Informationstechnik GmbH, Prüfstelle IT-Sicherheit. The evaluation was completed on 27.06.2007. The TÜV Informationstechnik GmbH, Prüfstelle IT-Sicherheit is an evaluation facility (ITSEF)[10] recognised by BSI.

The sponsor, vendor and distributor is

Giesecke & Devrient GmbH
Prinzregentenstraße 159
Postfach 80 07 29
81607 München

---

8 Software development at G&D, Munich; for hardware development sites refer to [13]

9 Completion, Initialisation and Pass Production at Bundesdruckerei (Berlin).
The personalization process at the Bundesdruckerei was not part of the evaluation.
For hardware manufacturing sites refer to [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 augmented (Evaluation Assurance Level 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 1: 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 2: 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 [7] 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 3: 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 [7] chapter 5.3.

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

- SF.ACCESS (Access Control)
  Before the TSF performs an operation requested by a user, this Security function checks if the operation specific requirements on user authorisation and protection of communication data are fulfilled.
- SF.ADMIN (Administration of the TOE)
  The administration of the TOE is managed by this Security Function. The TOE administration is mainly done in the initialisation and personalisation phase.
- SF.AUTH (Authentication of the authorized TOE user)
  The authentication of the Signatory is managed by this Security Function. This Security function is only active during the usage phase.
- SF.CRYPTO (Cryptographic Support)
  This Security Function provides the cryptographic support for the other Security Functions.
- SF.PROTECTION (Protection of TSC)
  This Security Function protects the TSF functionality, TSF data and user data. If BAC is enabled, no unencrypted data transmission between TOE and the outside of the TOE is allowed.
- SF.IC (Security Functions of the IC)
  This Security Function covers the Security Functions of the IC.

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

1.3 Strength of Function

The TOE's strength of functions is claimed high (SOF-High) for the security functions SF.ADMIN, SF.AUTH, SF.CRYPTO, SF.IC.

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 [9]:

- Logical MRTD Data consisting of the data groups DG1 to DG16 and the Document security object according to LDS [10] and
- 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 [9]:

- 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 [7] chapter 3.1.

The following list of considered threats for the TOE is defined in the Security Target. They are taken from the MRTD BAC PP [9].

- 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[11]

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.

[11] Logical MRTD: Data of the MRTD holder stored on the contactless integrated circuit according to the Logical Data Structure [10].

- 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 the 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 the 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 [10].

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 [9]:

- 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:

Starcos 3.01 PE V1.1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW / SW	Chip modules with Philips P5CT072V0N including STARCOS 3.01 PE V1.1 - ROM mask of the TOE already Implemented: "P5CT072EV4/T0N49360" (MOB4).	CPAZ0SCSR30-01Au_V200 dated 08.06.2004	SW completely contained in ROM and EEPROM memory, chip mounted into an inlay package initialised and tested
		- EEPROM part of the TOE loaded before TOE delivery: Initialisation Table ID: 02 41 01 00 EA 64 C5 24 96 43 2C 7D	CPAZ0SCSR301-01Cu_V100 dated 14.12.2006	
2	DOC	Administrator Guidance STARCOS 3.01 PE V1.1 [14]	Version 2.2, 9. February 2007	Document in electronic form (encrypted / signed)
3	DOC	User guidance STARCOS 3.01 PE V1.1 [15]	Version 1.1, 18. April 2007	Document in electronic form (encrypted / signed)
4	DOC	Correspondence between initialisation table and Common Criteria Certification [16]	Version 1.4, 6. February 2007	Document in electronic form (encrypted / signed)
5	DOC	Installation, generation and start up STARCOS 3.01 PE V1.1[17]	Version 1.0, 9. February 2007	Document in electronic form (encrypted / signed)

Table 4: 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. Any delivery of the initialised inlays is done via a security transport of the MRTD Manufacturer (G&D) or a security transport maintained by the Personalization Agent. This delivery process has therefore to be regarded as 'personal pickup'. In addition, the correct inlay modules for the TOE are secured by cryptographic means. 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 [14] have to be followed.

3 Security Policy

The security policy of the TOE is defined according to the MRTD BAC PP [9] by the security objectives and requirements for the 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.

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 embedded software which can be separated into the following subsystems: Access Control, Setup, Commands, Application Data and Basic Functions, Crypto Functions, Secure Messaging, Hardware.

At the subsystem ‘Setup’ the startup of the TOE is initiated. This subsystem calls ‘Access control’ for the initialisation of security states. Then ‘Setup’ gives the control to ‘Commands’ which receives command messages via the corresponding interfaces of ‘Hardware’, calls ‘Access control’ for verification of access conditions, calls ‘Secure Messaging’ for verification and unwrapping of the incoming message if BAC is required, performs the command execution, calls ‘Secure Messaging’ for wrapping of the outgoing message, calls

'Hardware' for transmitting the outgoing message and then starts this process again. 'Crypto functions' and 'Application Data and basic functions' are general support subsystems which are called for cryptographic support or access to application data, respectively.

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 guidance document [14] describes the tasks of an administrator to install and configure the TOE in a secure manner. This administrator guidance is addressed to all persons who are responsible for configuring, maintaining and administering the TOE e.g. for personalisation the Personalization Agent of the TOE who needs information about security procedures and how the TOE supports the personalisation process.

Information for initialisation is also included in [14] although this process is performed before TOE delivery.

The user guidance document [15] is provided for the developer of an inspection system who needs information how the TOE interacts with the inspection system and includes requirements for the issuer and MRTD holder.

The document "Correspondence between initialisation table and Common Criteria Certification" [16] defines the initialisation table relevant for the TOE.

7 IT Product Testing

Developer tests, independent evaluator tests and penetration tests were performed using MRTD chips Starcos 3.01 PE V1.1 on Philips P5CT072V0N composed of the hardware chip, its dedicated software, the operating system and a file-system for the ICAO application. Both the Passive Authentication and BAC (Basic Access Control) configurations were tested. The Tests have been conducted via the contactless interface. The composite smartcard TOE was tested by using specific tools.

All TSF and related sub-functions and subsystems are tested in order to assure complete coverage of all SFR. The Test suites were implemented in accordance with functional specification and high level design in order to verify the TOE's compliance with its expected behaviour. All test cases in each test suite were run successfully on this TOE version. The developer performed functional tests with a TOE in the personalization phase and in the operational phase. 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 tests were performed using a smart card simulator and real chips with the TOE software and the ICAO file-system.

During independent testing the evaluator has verified the developer's test by performing the whole developer's test campaign covering all security functions. During the evaluator's TSF testing the TOE operated as specified.

Independent evaluator tests were performed in various life cycle phases of the TOE using real chips and an emulator. 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 test 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 in form of initialised and tested inlay modules. This corresponds to the end of life cycle phase 2 of the Protection Profile MRTD BAC PP [9].

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

The TOE only features two fixed configurations which cannot be altered by the end user. One configuration is Passive Authentication and the other is Basic Authentication Control (BAC). The personalizer sets the TOE to one of the above configurations. Both configurations have the same version number. The TOE was tested in both configurations. The evaluation and subsequent certification are only valid for Starcos 3.01 PE V1.1

The certification body shall be advised of any modifications made to this configuration and of modifications to the initialisation tables listed in Table 5 by the developer. The certification body will then check if the certification results are still valid and initiate further steps concerning a re-evaluation and re-certification, if necessary.

9 Results of the Evaluation

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

As the evaluation of the TOE was conducted as a composition evaluation, the ETR [8] 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 [8] builds up on the *ETR-lite for Composition* document of the evaluation of the underlying Philips chip P5CT072V0N (see BSI-DSZ-CC-0312-2006 [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
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

Assurance classes and components		Verdict
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 5: 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) [9]
- 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: SF.ADMIN, SF.AUTH, SF.CRYPTO, SF.IC. 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 Starcos 3.01 PE V1.1. 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] and [15] 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.

Furthermore an appropriate protection after the initialization must be ensured up to delivery to the end-user to prevent any possible copy, modification, retention, theft, or unauthorized use of the TOE and of its manufacturing and test data (refer to the assumption A.Process-Card from the ST of the hardware platform).

Only chips from the production sites (waferfabs, module production sites) as outlined in the certification reports for the Philips chip P5CT072V0N (BSI-DSZ-CC-0312-2005 [13]) shall be used.

The Personalization Agent has to verify that the correct version of the TOE was delivered.

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 [7] of the target of evaluation (TOE) is provided within a separate document. It is a sanitized version of the complete security target [6] used for the evaluation performed.

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
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
LDS	Logical Data Structure
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

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.

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.

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

[6] Securtity Target STARCOS 3.01 PE V1.1, BSI-DSZ-CC-0429-2007, Version 3.7, 9 February 2007, Giesecke & Devrient GmbH (confidential document)

[7] Security Target Lite STARCOS 3.01 PE V1.1, BSI-DSZ-CC-0429-2007, Version 1.0, 10.07.2007, Giesecke & Devrient GmbH (sanitized public document)

[8] Evaluation Technical Report, Version 1, 4 June 2007, CC Evaluation of STARCOS 3.01 PE Version 1.1 , TÜVIT (confidential document)

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

[10] 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, 18 May 2004

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

[12] 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

[13] Certification Report BSI-DSZ-CC-0312-2005 for Philips Secure Smart Card Controller P5CT072V0N including OM9500/1 and OM9501/2, P5CD072V0N and P5CD036V0N with specific IC Dedicated Software, 7 October 2005, BSI

[14] Administrator Guidance STARCOS 3.01 PE V1.1, Giesecke & Devrient GmbH, Version 2.2, 9 February 2007

[15] User guidance STARCOS 3.01 PE V1.1, Giesecke & Devrient GmbH, Version 1.1, 18 April 2007

[16] Correspondence between initialisation table and Common Criteria Certification, V1.4, 6 February 2007

[17] Installation, generation and start up STARCOS 3.01 PE V1.1, Version 1.0, 9 February 2007

This page is intentionally left blank.

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:

a) **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.

b) **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:

a) **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.

b) **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:

a) **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.

b) **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:

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

CC Part 3:

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: Evaluation results regarding development and production environment D-3

This page is intentionally left blank.

Annex A of Certification Report BSI-DSZ-CC-0429-2007

Evaluation results regarding development and production environment

The IT product Starcos 3.01 PE V1.1 (Target of Evaluation, TOE) has been evaluated at an accredited and licensed/ approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 (ISO/IEC 15408:2005) 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 2.3 (ISO/IEC 15408:2005).

As a result of the TOE certification, dated 18. July 2007, 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:

a) Giesecke & Devrient GmbH, Prinzregentenstrasse 159, 81677 München, Germany (Development Center)

b) Bundesdruckerei, Oranienstrasse 91, 10958 Berlin, Germany (TOE Completion, Initialisation and Pass Production).

c) For development and productions sites regarding the Philips chip P5CT072V0N refer to the certification report BSI-DSZ-CC-0312-2005.

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target (Securtity Target STARCOS 3.01 PE V1.1, BSI-DSZ-CC-0429-2007, Version 3.7, 9 February 2007, Giesecke & Devrient GmbH [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.

This page is intentionally left blank.