Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0467-2008

for

STARCOS 3.01 PE
Version 1.2

from

Giesecke & Devrient GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0467-2008

Security IC with MRTD BAC Application

STARCOS 3.01 PE
Version 1.2

from	Giesecke & Devrient GmbH
PP Conformance:	Machine Readable Travel Document with "ICAO Application", Basic Access Control, BSI-PP-0017-2005
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ADV_IMP.2 and ALC_DVS.2

Common Criteria Arrangement for components up to EAL 4

Common Criteria

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 extended by advice of the Certification Body for* components beyond EAL 4 and smart card specific guidance for conformance to the *Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)*.

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

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

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

Bonn, 31 January 2008
For the Federal Office for Information Security

IT Security Certified
SOGIS - MRA

Bernd Kowalski
Head of Department

L.S.

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

This page is intentionally left blank.

Preliminary Remarks

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

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

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

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

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

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

[1] Act 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 2.3 (ISO/IEC 15408:2005)[5]
- Common Methodology for IT Security Evaluation, 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 Recognition Agreements

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

---

2 Act 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

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 03 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). The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

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

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria 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

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

This evaluation contains the components ADV_IMP.2 (Implementation of the TSF) 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, Version 1.2 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0429-2007. Specific results from the evaluation process based on BSI-DSZ-CC-0429-2007 were re-used.

The evaluation of the product STARCOS 3.01 PE, Version 1.2 was conducted by TÜV Informationstechnik GmbH . The evaluation was completed on

24 January 2008. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Giesecke & Devrient GmbH.

The product was developed by: Giesecke & Devrient GmbH.

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

4 Validity of the certification result

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

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

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

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

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

5 Publication

The following Certification Results contain pages B-1 to B-14 and D1 to D-4.

The product STARCOS 3.01 PE, Version 1.2 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.

---

[6] Information Technology Security Evaluation Facility

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

[7] Giesecke & Devrient GmbH
Prinzregentenstr. 159
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

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 STARCOS 3.01 PE Version 1.2.

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 Version 1.2 is a re-certification based on BSI-DSZ-CC-0429-2007 (Starcos 3.01 PE V1.1) with some changes at the level of life cycle.

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 security assurance requirements of the TOE are based entirely on the assurance components defined in part 3 of the Common Criteria (see part C or [1], part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ADV_IMP.2 and ALC_DVS.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] resp. [7], chapter 5.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC part 2 extended.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6] resp. [7], chapter 5.3.

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

TOE Security Function	Addressed issue
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

TOE Security Function	Addressed issue
	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

Table 1: TOE Security Funktions

For more details please refer to the Security Target [6] resp. [7], chapter 6.1.

The claimed TOE's strength of functions 'high (SOF-high) for specific functions as indicated in the Security Target [6] resp. [7], chapter 6.1 is confirmed. The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security Target [6] resp. [7], chapter 3.1.1 . Based on these assets the security environment is defined in terms of assumptions, threats and policies. This is outlined in the Security Target [6] resp. [7], chapter 3.2.

This certification covers the following configurations of the TOE:

- 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 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, Version 1.2

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 V1.2 - 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 V1.2 [14]	Version 2.3, 27. June 2007	Document in electronic form (encrypted / signed)
3	DOC	User guidance STARCOS 3.01 PE V1.2 [15]	Version 1.2, 27. June 2007	Document in electronic form (encrypted / signed)
4	DOC	Correspondence between initialisation table and Common Criteria Certification [16]	Version 1.6, 27. June 2007	Document in electronic form (encrypted / signed)
5	DOC	Installation, generation and start up STARCOS 3.01 PE V1.2[17]	Version 1.2, 07. January 2008	Document in electronic form (encrypted / signed)

Table 2: Deliverables of the TOE

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].

Delivery is performed from Giesecke & Devrient GmbH in Munich 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 defined in the Security Target and some aspects of threats and organisational security policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- Personalization of the MRTD’s chip and
- Inspection Systems for global interoperability.

Details can be found in the Security Target [6] resp. [7], chapter 3.2.

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

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

7 IT Product Testing

Developer tests, independent evaluator tests and penetration tests were performed using MRTD chips STARCOS 3.01 PE, Version 1.2 on NXP (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 at the level of the functional specification and at 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 Access 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 Version 1.2.

The certification body shall be advised of any modifications made to this configuration and of modifications to the initialisation table of the TOE. 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

9.1 CC specific results

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

For components beyond EAL4 the evaluation methodology applied was defined in co-ordination with the Certification Body [4] (AIS 34).

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

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

- All components of the class ASE
- All components of the EAL 4 package as defined in the CC (see also part C of this report)
- The components
  ADV_IMP.2 – Implementation of the TSF
  ALC_DVS.2 – Sufficiency of security measures
  augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0429-2007, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the change at the level of the life cycle of the TOE.

The evaluation has confirmed:

- for PP Conformance Machine Readable Travel Document with “ICAO Application”, Basic Access Control, BSI-PP-0017-2005 [8]
- for the functionality: PP conformant
  Common Criteria Part 2 extended
- for the assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by
  ADV_IMP.2 and ALC_DVS.2

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

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

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

9.2 Results of cryptographic assessment

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This holds for

- SF.AUTH Authentication of the authorized TOE user and
- SF.CRYPTO Cryptographic Support.

10 Obligations and notes for the usage of the TOE

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

11 Security Target

For the purpose of publishing, the security target [7] of the target of evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete security target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12 Definitions

12.1 Acronyms

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
LDS	Logical Data Structure
MRTD	Machine Readable Travel Document
PP	Protection Profile
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function

ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
TSS	TOE Summary Specification

12.2 Glossary

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

13 Bibliography

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

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

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

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

- AIS 25, Version 3, 6 August 2007 for: CC Supporting Document, - The Application of CC to Integrated Circuits, Version 2.0, CCDB-2006-04-003, April 2006
- AIS 26, Version 3, 6 August 2007 for: CC Supporting Document, - Application of Attack Potential to Smartcards, Version 2.3, CCDB-2007-04-001, April 2007
- 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

- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

[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 Version 1.2, BSI-DSZ-CC-0467-2008, Version 3.8, 09 July 2007, Giesecke & Devrient GmbH (confidential document)

[7] Security Target Lite STARCOS 3.01 PE V1.2, BSI-DSZ-CC-0467-2008, Version 1.0, 25 January 2008, Giesecke & Devrient GmbH (sanitized public document)

[8] Evaluation Technical Report, Version 3, 23 January 2008, CC Evaluation of STARCOS 3.01 PE Version 1.2 , 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, 07 October 2005, BSI

[14] Administrator Guidance STARCOS 3.01 PE V1.2, Giesecke & Devrient GmbH, Version 2.3, 27 June 2007

[15] User guidance STARCOS 3.01 PE V1.2, Giesecke & Devrient GmbH, Version 1.2, 27 June 2007

[16] Correspondence between initialisation table and Common Criteria Certification, V1.6, 27 June 2007

[17] Installation, generation and start up STARCOS 3.01 PE V1.2, Version 1.2, 07 January 2008

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:

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

plus one of the following:

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

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

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

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

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

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

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

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

Table 3 - Protection Profile families - CC extended requirements ”

Security Target criteria overview (Chapter 8.3)

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

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

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

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

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

Table 1: Assurance family breakdown and mapping"

Evaluation assurance levels (chapter 11)

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

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

Evaluation assurance level (EAL) overview (chapter 11.1)

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

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

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

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

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

Table 6: Evaluation assurance level summary”

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

“Objectives

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

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

“Objectives

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

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

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

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

"Application notes

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

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

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment D-3

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0467-2008

Evaluation results regarding development and production environment

The IT product STARCOS 3.01 PE, Version 1.2 (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* extended by advice of the Certification Body for components beyond EAL 4 and smart card specific guidance for conformance to the *Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)*.

As a result of the TOE certification, dated 31 January 2008, 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 Munich, Germany (Development Center)

b) Giesecke & Devrient GmbH, Dienstleistungscenter DLC, Prinzregentenstr. 159, 81677 Munich, Germany (Initialisation)

c) Smartrac Technology, 142 Moo 1 Hi-Tech industrial Estate, Ban Laean,Bang, Pa-In Phra nakorn Si Ayatthaya, 13160 Thailand (TOE Completion)

For development and productions sites regarding the NXP (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 Version 1.2, BSI-DSZ-CC-0467-2008, Version 3.8, 09 July 2007, Giesecke & Devrient GmbH [6] resp. [7]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] resp. [7]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.