Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0916-2015

for

STARCOS 3.6 COS C1

from

Giesecke & Devrient GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0916-2015(*)

STARCOS 3.6 COS C1

from	Giesecke & Devrient GmbH
PP Conformance:	Card Operating System Generation 2 (PP COS G2), Version 1.9, 18 November 2014, BSI-CC-PP-0082-V2-2014
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by AVA_VAN.5, ATE_DPT.2 and ALC_DVS.2

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 4.

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

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.

Common Criteria
Recognition Arrangement
for components up to
EAL 4

Bonn, 7 August 2015

For the Federal Office for Information Security

Bernd Kowalski
Head of Department

L.S.

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

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

This page is intentionally left blank.

Preliminary Remarks

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

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

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

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

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

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

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

Contents

A. Certification

1. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[2]
- BSI Certification and Approval Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1] also published as ISO/IEC 15408
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

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 (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

---

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

3 Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

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 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. This Domain is linked to a conformance claim to one of the related SOGIS Recommended Protection Profiles. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

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

This certificate is recognized under SOGIS-MRA for all assurance components selected.

2.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

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

As the product certified has been accepted into the certification process before 08 September 2014, this certificate is recognized according to the rules of CCRA-2000, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained the components AVA_VAN.5, ATE_DPT.2 and ALC_DVS.2 that are not mutually recognised in accordance with the provisions of the CCRA-2000, for mutual recognition the EAL 4 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 3.6 COS C1 has undergone the certification procedure at BSI.

The evaluation of the product STARCOS 3.6 COS C1 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 31 July 2015. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the 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, as specified in the following report and in the Security Target.

For the meaning of the assurance levels 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 evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 7 August 2015 is valid until 6. August 2020. The validity date can be extended by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report and the Security Target and user guidance documentation mentioned herein to any applicant of the product for the application and usage of the certified product,

[6] Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the product's evaluated life cycle, e.g. related to development and production sites or processes, occur or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the product deliverables according to the Certification Report part B chapter 2 to third parties, permission of the Certification Body at BSI has to be obtained.

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

5. Publication

The product STARCOS 3.6 COS C1 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[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
81677 München
Deutschland

B. Certification Results

The following results represent a summary of

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

1. Executive Summary

The Target of Evaluation (TOE) is the product STARCOS 3.6 COS C1 developed by Giesecke & Devrient GmbH.

The TOE is a smart card product according to the G2-COS specification [23] from gematik and is implemented on the hardware platform Infineon Security Controller M7893 B11 from Infineon Technologies AG [refer to 19, 20, 21].

The TOE is intended to be used as a card operating system platform for different card types and applications of the card generation G2 in the framework of the German health care system.

For this purpose, the TOE serves as secure data storage and secure cryptographic service provider for card applications running on the TOE and supports them for their specific security needs related to storage and cryptographic functionalities. In particular, these storage and cryptographic services are oriented on the different card types eHC (electronic Health Card), HPC (Health Professional Card), SMC-B (Security Module Card Type B), gSMC-K (gerätespezifische Security Module Card Type K for the so-called Konnektor) and gSMC-KT (gerätespezifische Security Module Card Type KT for Terminals) as they are currently specified for card products of the generation G2 within the German health care system. These TOE's storage and cryptographic services that are provided by the TOE and invoked by the human users and components of the German health care system cover the following issues:

- authentication of human user and external devices,
- storage of and access control on user data,
- key management and cryptographic functions,
- management of TSF data including life cycle support,
- export of non-sensitive TSF and user data of the object system if implemented.

The TOE comprises

- the circuitry of the dual-interface chip including all IC Dedicated Software being active in the Smart Card Initialisation Phase, Personalisation Phase and Usage Phase of the TOE (the integrated circuit, IC),
- the IC Embedded Software (STARCOS 3.6 COS C1 Operating System),
- the Wrapper (TOE specific SW tool for interpretation of exported TSF and User data), and
- the associated guidance documentation.

The TOE is ready for the installation and personalisation of object systems (applications) on the TOE that match the G2-COS specification [23], but does not contain itself any object system (applications).

In functional view, the TOE with its IC Embedded Software (STARCOS 3.6 COS C1 Operating System) is implemented according to the G2-COS specification [23] from gematik. Beside the mandatory part of the G2-COS specification [23] with the base functionality of the operating system platform, the TOE implements the following optional functional packages defined in [23]:

- Contactless Interface,
- Logical Channels, and
- Crypto Box.

The STARCOS 3.6 COS C1 Operating System is implemented according to the G2-COS specification [23] from gematik. The TOE provides in addition the commands CREATE and PSO HASH (refer to the user guidances [12], chapter 5.2.1 and 5.2.2 and [15], chapter 2.3) that are outlined as optional in the G2-COS specification [23]. Furthermore, the TOE provides specific initialisation and personalisation commands (refer to the user guidance [15], chapter 2.4).

The TOE's Wrapper is implemented according to the Wrapper specification [24] from gematik, but with the following deviation:

The TOE's Wrapper is *not* able to detect and export key ID and PIN ID duplicates existing within the same folder of an object system (application) that is set up on the TOE. This means that in the case that the object system contains a folder with key ID or PIN ID duplicates the exported lists for <Key_Identifier>, <Password_Identifier> respective persistentPublicKeyList (in the folder's attribute <children>) are not complete.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Card Operating System Generation 2 (PP COS G2), Version 1.9, 18 November 2014, BSI-CC-PP-0082-V2-2014 [8]. The Security Target [6] and [7] comprises beside the mandatory parts of the PP the following optional packages defined in the PP:

- Package Crypto Box ([8], chapter 7),
- Package Logical Channel ([8], chapter 10), and
- Package Contactless ([8], chapter 8).

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C below or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by AVA_VAN.5, ATE_DPT.2 and ALC_DVS.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [7], chapter 6.1, 7.4, 8.4 and 9.4. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

- SF_AccessControl:

  The TOE provides access control mechanisms that allow the restriction of access to only specific users (world, human users, device) based on different security attributes.

- SF_Authentication:

  The TOE supports user and device authentication: PACE, symmetric authentication mechanisms based on 3TDES and AES and asymmetric authentication mechanisms based on RSA and ECC.

- SF_AssetProtection:

  The TOE supports the calculation of block check values for data integrity checking.

The TOE hides information about IC power consumption and command execution time ensuring that no confidential information can be derived from this information.

- SF_TSFProtection:

  The TOE detects and resists physical tampering of the TSF with sensors for operating voltage, clock frequency and temperature.

- SF_KeyManagement:

  The TOE supports onboard generation of cryptographic keys based on the ECDH as well as generation of RSA and ECC key pairs.

- SF_CryptographicFunctions:

  The TOE supports secure messaging for protection of the confidentiality and the integrity of the commands. The TOE supports asymmetric and symmetric cryptographic and hashing algorithms to perform authentication procedures, signature computation and verification, data encryption and decryption. The TOE implements a DRG.4 random number generator.

For more details on the TOE Security Functionality please refer to the Security Target [6] and [7], chapter 6.1, 7.4, 8.4 and 9.4 and 11.

The assets to be protected by the TOE are defined in the Security Target [6] and [7], chapter 3.1, 7.2.1, 8.2.1 and 9.2.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [7], chapter 3.2, 3.3, 3.4, 7.2.2, 7.2.3, 7.2.4, 8.2.2, 8.2.3, 8.2.4, 9.2.2, 9.2.3 and 9.2.4.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

STARCOS 3.6 COS C1

The following table outlines the TOE deliverables:

No.	Type	Identifier	Release	Type / Form of Delivery
1	HW/SW	Infineon Security Controller M7893 B11 including its IC Dedicated Software (Firmware) (refer to the Certification Report BSI-DSZ-CC-0879-2014 ([20]) respective the Maintenance Report BSI-DSZ-CC-0879-2014-MA-01 ([21])	Infineon Security Controller M7893 B11	Dual-interface chip. Delivery as module of type: T-M8.4-8-1. The hardware part of the TOE is delivered to Giesecke & Devrient GmbH for further production of the TOE according to the delivery procedures specified in BSI-DSZ-CC-0879-2014 ([20]) respective BSI-DSZ-CC-0879-2014-MA-01 ([21]).
2	SW	IC Embedded Software (STARCOS 3.6 COS C1 Operating System)	STARCOS 3.6 COS C1 OS Identification: '47 44 00 B6 02 01 00' (refer to Table 2)	Implemented in the flash of the IC. The TOE covering the IC and the IC Embedded Software is delivered without any object system (first production variant) or alternatively with an already installed object system (second production variant). Refer for this to the description of the TOE's life cycle model below under this Table. The TOE respective product is delivered as module or smart card with or without antenna. The delivery of the TOE respective product is performed by Giesecke & Devrient GmbH.
3	DOC	Guidance Documentation STARCOS 3.6 – Main Document [11]	Version 1.7	Document in electronic form (encrypted and signed)
4	DOC	Guidance Documentation for the Usage Phase STARCOS 3.6 COS [12]	Version 2.1	Document in electronic form (encrypted and signed)
5	DOC	Guidance Documentation for the Initialization Phase STARCOS 3.6 COS [13]	Version 2.6	Document in electronic form (encrypted and signed)
6	DOC	Guidance Documentation for the Personalisation Phase STARCOS 3.6 COS [14]	Version 1.9	Document in electronic form (encrypted and signed)
7	DOC	STARCOS 3.6 Functional Specification - Part 1: Interface Specification [15]	Version 1.19	Document in electronic form (encrypted and signed)
8	DOC	STARCOS 3.6 Internal Design Specification [16]	Version 1.3	Document in electronic form (encrypted and signed)
9	DOC	STARCOS 3.6 COS C1/2 Guidance Documentation for Inlay Production [18]	Version 1.1	Document in electronic form (encrypted and signed)

No.	Type	Identifier	Release	Type / Form of Delivery
10	SW	Wrapper	Version 1.6.15	File ZIP-archive: egkwrapper-v1.6.15.rar consisting of the jar files: • wrapper.jar (main file) • gdoffcard.jar (helper library) • gdoffcardstarcos.jar (helper library) (encrypted and signed) The integrity and authenticitiy of the Wrapper is given by the following SHA-256 hash value: 35AE327E5B3A02E3836584418D9A06ACEA10BC27A92B1A11D9244635EA3CCAD7
11	DOC	STARCOS 3.6 COS C1/2 Guidance Documentation for the Wrapper [17]	Version 1.3	Document in electronic form (encrypted and signed)
12	DATA	Cryptographic keys for the TOE's personalisation	--- (customer-specific personalisation keys)	Items in electronic form (encrypted and signed)

Table 1: Deliverables of the TOE

The commercial numbering of the TOE by Infineon Technologies AG is as follows:

- Product Code: M7893-B373-11
- Product Type: Infineon Security Controller M7893 B11
- RMS Version: SLE78V2_M_V19B03

The TOE STARCOS 3.6 COS C1 is as well known under the following product identificator:

Manufacturer: '44 45 47 2B 44' (DEG+D)

Product: '53 33 36 43 4F 53 30 31' (S36COS01)

OS Version Number: '01 00 00' (1.0.0)

According to the Security Target [6] and [7], chapter 1.2.2 the life cycle model of the TOE consists of the following four phases:

Phase 1: Development Phase

Phase 2: Initialisation Phase (loading of the STARCOS 3.6 COS C1 Operating System and installation of an object system)

Phase 3: Personalisation Phase (loading of personalisation data into the installed object system)

Phase 4: Usage Phase

Two different production variants can be distinguished:

In the first production variant, the STARCOS 3.6 COS C1 Operating System is loaded in the framework of the Initialisation Phase (Phase 2) by Giesecke & Devrient GmbH. Hereby, the TOE delivery in the sense of the CC takes place in Phase 2 after loading of the IC Embedded Software by the Initialisation Data Manager (Giesecke & Devrient GmbH). The delivered product is the TOE without any object system installed on the TOE. The TOE is delivered by Giesecke & Devrient GmbH to the Initialiser (Giesecke & Devrient GmbH or third party) for installing an object system on the TOE. In this production variant, loading of an object system is carried out in Phase 2 after TOE respective product delivery by loading a so-called Initialisation Table that is generated by Giesecke & Devrient GmbH and that contains an object system and patches of the Operating System (if applicable for the TOE).

In the second production variant, the STARCOS 3.6 COS C1 Operating System is completely loaded in the framework of the Initialisation Phase (Phase 2) by Giesecke & Devrient GmbH. Furthermore, in the framework of this initialisation in Phase 2 an object system is loaded onto the TOE. Hereby, the TOE delivery in the sense of the CC takes place at the end of Phase 2. The delivered product is the TOE supplemented with an object system installed on the TOE. In this production variant, the product (including the TOE) is delivered by Giesecke & Devrient GmbH directly to the Personalisation Agent (Giesecke & Devrient GmbH or third party) for personalisation.

These production variants may include the antenna respective inlay production step. Hence, the TOE respective product can be delivered as module or smart card with or without antenna.

In order to verify that the user uses a certified TOE, the TOE can be identified using the means described in the user guidance [14], chapter 5.7. The TOE can be identified by using the command GET PROTOCOL DATA. Via the command GET PROTOCOL DATA (CLA = ‘A0’, INS = ‘CA’ with specific P1 and P2 values, see Table 2) the user can read out the chip information and identify the underlying chip as well as the STARCOS 3.6 COS C1 Operating System and its configuration embedded in the chip.

The following identification data can be retrieved within byte strings responded by the command GET PROTOCOL DATA in different command variants:

Command Parameters	Identifier Length	Description
P1 = '9F’ P2 = ’6B’	8 bytes	Chip manufacturer data
P1 = ’9F’ P2 = ’6A’	7 bytes	Identification of the operating system (OS)
P1 = ‘9F’ P2 = ’6F’	7 bytes	Fabkey key material identification

Table 2: TOE Identification via the command GET PROTOCOL DATA

The command GET PROTOCOL DATA with its parameters is described in [14], chp 5.7.

The following table describes the concrete values identifying the TOE:

Data Type	Tag in the ProtocolData DO	Data
Chip manufacturer data	'9F 6B'	'05 78 00 04 00 0D 00 00'
Identification of the operating system (OS)	'9F 6A'	'47 44 00 B6 02 01 00'
Fabkey key material identification	'9F 6F'	Second byte = '12’

Table 3: TOE Identification data retrieved by the command GET PROTOCOL DATA

3. Security Policy

The TOE is a composite smart card product, based on the hardware platform Infineon Security Controller M7893 B11 from Infineon Technologies AG and with IC Embedded Software (STARCOS 3.6 COS C1 Operating System) implemented by Giesecke & Devrient GmbH according to the G2-COS specification [23] from gematik.

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

The TOE is intended to be used as a card operating system platform for different card types and applications of the card generation G2 in the framework of the German health care system. For this purpose, the TOE serves as secure data storage and secure cryptographic service provider for card applications running on the TOE and supports them for their specific security needs related to storage and cryptographic functionalities. In particular, these storage and cryptographic services are oriented on the different card types eHC (electronic Health Card), HPC (Health Professional Card), SMC-B (Security Module Card Type B), gSMC-K (gerätespezifische Security Module Card Type K for the so-called Konnektor) and gSMC-KT (gerätespezifische Security Module Card Type KT for Terminals) as they are currently specified for card products of the generation G2 within the German health care system.

The TOE implements physical and logical security functionality in order to protect user data and TSF data stored and operated on the smart card when used in a hostile environment. Hence the TOE maintains integrity and confidentiality of code and data stored in its memories and the different CPU modes with the related capabilities for configuration and memory access and for integrity, the correct operation and the confidentiality of security functionality provided by the TOE. Therefore the TOE's overall policy is to protect against malfunction, leakage, physical manipulation and probing. Besides, the TOE's life cycle is supported as well as the user Identification whereas the abuse of functionality is prevented. Furthermore, specific cryptographic services including random number generation and key management functionality are being provided to be securely used by the smart card embedded software.

Specific details concerning the above mentioned security policies can be found in the Security Target [6] and [7], chapter 6, 7, 8 and 9.

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:

Security Objectives for the operational environment defined in the Security Target	Description according to the ST
OE.Plat-COS	Usage of COS To ensure that the TOE is used in a secure manner the object system shall be designed such that the requirements from the following

Security Objectives for the operational environment defined in the Security Target	Description according to the ST
	documents are met: (i) user guidance of the COS, (ii) application notes for the COS (iii) other guidance documents, and (iv) findings of the TOE evaluation reports relevant for applications developed for COS as referenced in the certification report.
OE.Resp-ObjS	Treatment of User Data All User Data and TSF Data of the object system are defined as required by the security needs of the specific application context.
OE.Process-Card	Protection of Card during Personalisation Security procedures shall be used after delivery of the TOE during Phase 6 Smartcard personalisation up to the delivery of the smartcard to the end-user to maintain confidentiality and integrity of the TOE and to prevent any theft, unauthorised personalization or unauthorised use.
OE.SecureMessaging	Secure messaging support of external devices The external device communicating with the TOE through a trusted channel supports device authentication with key derivation, secure messaging for received commands and sending responses.
OE.PACE_Terminal	PACE support by contactless terminal The external device communicating trough a contactless interface with the TOE using PACE shall support the terminal part of the PACE protocol.
OE.LogicalChannel	Use of logical channels The operational environment manages logical channels bound to independent subjects for running independent processes at the same time.

Table 4: Security Objectives for the operational environment

Details can be found in the Security Target [6] and [7], chapter 4.2, 7.3, 8.3 and 9.3.

5. Architectural Information

The TOE is set up as a composite product. It is composed of the Integrated Circuit (IC) Infineon Security Controller M7893 B11 from Infineon Technologies AG and the IC Embedded Software with the STARCOS 3.6 COS C1 Operating System developed by Giesecke & Devrient GmbH.

The TOE does not use the cryptographic software libraries of the Infineon hardware platform, but provides its cryptographic services by the cryptographic library developed by Giesecke & Devrient GmbH.

For details concerning the CC evaluation of the underlying IC see the evaluation documentation under the Certification ID BSI-DSZ-CC-0879-2014-MA-01 ([19] to [21]).

According to the TOE design the Security Functions of the TOE as listed in chapter 1 are implemented by the following subsystems:

- System Library: Contains the application framework,
- Chip Card Commands: Pre-processor and processor of all implemented commands,
- Security Management: Manages the security environment, security states and rule analysis,
- Key Management: Search, pre-processing, use and post-processing of keys,
- Secure Messaging: SM handling,
- Crypto Functions: Library with an API to all cryptographic operations,

supported by the Runtime System, File System, Non-Volatile Memory Management, Transport Management and the Wrapper subsystems.

6. Documentation

The evaluated documentation as outlined in Table 1 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 [6] and [7].

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

The developer tested all TOE Security Functions either on real cards or with simulator tests. For all commands and functionality tests, test cases are specified in order to demonstrate its expected behaviour including error cases. Hereby a representative sample including all boundary values of the parameter set, e.g. all command APDUs with valid and invalid inputs are tested and all functions are tested with valid and invalid inputs. Repetition of developer tests was performed during the independent evaluator tests.

Since many Security Functions can be tested by APDU command sequences, the evaluators performed these tests with real cards. This is considered to be a reasonable approach because the developer tests include a full coverage of all security functionality. Furthermore penetration tests were chosen by the evaluators for those Security Functions where internal secrets of the card could maybe be modified or observed during testing. During their independent testing, the evaluators covered

- testing APDU commands related to Key Management and Crypto Functions,
- testing APDU commands related to NVM Management and File System,
- testing APDU commands related to Security Management,
- testing APDU commands related to Secure Messaging,
- testing APDU commands related to Runtime System and System Library,
- penetration testing related to the verification of the reliability of the TOE,
- source code analysis performed by the evaluators,
- side channel analysis for RSA, ECC, AES and SHA (including ECC key generation),
- fault injection attacks (laser attacks),
- testing APDU commands for the initialisation, personalisation and usage phase,

- testing APDU commands for the commands using cryptographic mechanisms,
- fuzzy testing on APDU processing.

The evaluators have tested the TOE systematically against high attack potential during their penetration testing.

The achieved test results correspond to the expected test results.

8. Evaluated Configuration

This certification covers the following configurations of the TOE as outlined in the Security Target [6] and [7]:

STARCOS 3.6 COS C1

There is only one configuration of the TOE. Refer to the information provided in chapter 2 of this Certification Report.

The TOE is installed on a dual-interface chip of type Infineon Security Controller M7893 B11 from Infineon Technologies AG. This IC is certified under the Certification ID BSI-DSZ-CC-0879-2014 respective BSI-DSZ-CC-0879-2014-MA-01 (refer to [20] and [21]).

The TOE does not use the cryptographic software libraries of the Infineon hardware platform, but provides its cryptographic services by the cryptographic library developed by Giesecke & Devrient GmbH.

The TOE covering the IC and the IC Embedded Software is delivered as a module or smart card without any object system (first production variant) or alternatively with an already installed object system (second production variant). Hereby, the module and smart card may be connected to an antenna. For details refer to chapter 2 of this Certification Report.

The user can identify the certified TOE by the TOE response to specific APDU commands, more detailed by using the command GET PROTOCOL DATA in different command variants according to the user guidance [14], chapter 5.7. See chapter 2 of this Certification Report for details.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [9] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL 5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

(i) Composite product evaluation for Smart Cards and similar devices (see AIS 36). According to this concept the relevant guidance documents of the underlying platform (refer to the guidance documents covered by [20] and [21]) and the document ETR for composite evaluation from the platform evaluation ([22]) have

been applied in the TOE evaluation.

(ii) Guidance for Smartcard Evaluation.

(iii) Application of Attack Potential to Smartcards (see AIS 26).

(iv) Functionality classes and evaluation methodology of physical and deterministic random number generators.

For smart card specific methodology the scheme interpretations AIS 25, AIS 26 and AIS 36 (see [4]) were used.

For RNG assessment the scheme interpretation AIS 20 and AIS 31 were used (see [4]).

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

A document ETR for composite evaluation according to AIS 36 has not been provided in the course of this certification procedure. It could be provided by the ITSEF and submitted to the Certification Body for approval subsequently.

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

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report).
- The components AVA_VAN.5, ATE_DPT.2 and ALC_DVS.2 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Common Criteria Protection Profile Card Operating System Generation 2 (PP G2 COS), Version 1.9, 18 November 2014, BSI-CC-PP-0082-V2-2014 [8]
- for the Functionality: PP conformant Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant EAL 4 augmented by AVA_VAN.5, ATE_DPT.2 and ALC_DVS.2

The Security Target [6] and [7] use beside the mandatory parts of the PP the following of its optional packages:

- Package Crypto Box ([8], chapter 7),
- Package Logical Channel ([8], chapter 10), and
- Package Contactless ([8], chapter 8).

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

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
1	Authenticity	RSA signature generation (RSASSA-PSS-SIGN with SHA-256, RSASSA PKCS1-V1_5, RSA ISO9796-2 DS2 with SHA-256)	[26], [27] (RSA) [28] (SHA)	Modulus length = 2048, 3072	[23], chap. 6.6.3.1 [25]	FCS_COP.1.1/COS.RSA.S (PSO COMPUTE DIGITAL SIGNATURE) FCS_COP.1.1/SHA
2		RSA signature verification (RSA ISO9796-2 DS1)	[26], [27] (RSA) [28] (SHA)	Modulus length = 2048	[23], chap. 6.6.4.1 [25]	FCS_COP.1.1/COS.RSA.V (PSO VERIFY CERTIFICATE) FCS_COP.1.1/SHA
3		ECDSA signature generation using SHA-{256, 384, 512}	[29] (ECDSA) [30] [28] (SHA)	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [35] and ansix9p{256, 384}r1 [37]	[23], chap. 6.6.3.2 [25]	FCS_COP.1.1/COS.ECDSA.S (PSO COMPUTE DIGITAL SIGNATURE) FCS_COP.1.1/SHA
4		ECDSA signature verification using SHA-{256, 384, 512}	[29] (ECDSA) [30] [28] (SHA)	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [35] and ansix9p{256, 384}r1 [37]	[23], chap. 6.6.4.2 [25]	FCS_COP.1.1/COS.ECDSA.V (PSO VERIFY CERTIFICATE PSO COMPUTE DIGITAL SIGNATURE) FCS_COP.1.1/SHA
5		SHA-256 based fingerprint	[28]	-	[23], chap. 6.6.1.3	FPT_ITE.1 (FINGERPRINT)
6	Authentication	AES in CBC mode	[33] (AES) [23]	|k|=128, 192, 256 |challenge|=64	[23], chap. 6.7.1.2, 6.7.2.2 [25]	FCS_COP.1.1/COS.AES (MUTUAL AUTHENTICATE EXTERNAL AUTHENTICATE INTERNAL AUTHENTICATE GENERAL AUTHENTICATE)
7		AES in CMAC mode	[25], chap. 3.2.2 [36] [23]	|k|=128, 192, 256 |challenge|=64	[23], chap. 6.6.1, 6.6.2 [25]	FCS_COP.1.1/CB.CMAC (INTERNAL AUTHENTICATE) FCS_COP.1.1/COS.CMAC (MUTUAL AUTHENTICATE EXTERNAL AUTHENTICATE INTERNAL AUTHENTICATE)

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
8		TDES in CBC mode	[31] (TDES)	|k|=168 |challenge|=64	[25], chap. 3.3.1	FCS_COP.1.1/CB.3TDES (MUTUAL AUTHENTICATE EXTERNAL AUTHENTICATE INTERNAL AUTHENTICATE)
9		TDES in Retail MAC	[23]	|k|=168 |challenge|=64	[23], chap. 6.6.1, 6.6.2 [25]	FCS_COP.1/COS.RMAC (MUTUAL AUTHENTICATE EXTERNAL AUTHENTICATE)
10		TDES in Retail MAC	[23]	|k|=168 |challenge|=64	[23], chap. 6.6.1, 6.6.2 [25], chap. 3.2.2	FCS_COP.1/CB.RMAC (INTERNAL AUTHENTICATE)
11		RSA signature generation (RSASSA-PSS-SIGN with SHA-256, RSASSA PKCS1-V1_5, RSA ISO9796-2 DS1 with SHA-256)	[26], [27] (RSA) [28] (SHA)	Modulus length = 2048, 3072	[23], chap. 6.6.3.1 [25]	FCS_COP.1.1/COS.RSA.S (INTERNAL AUTHENTICATE) FCS_COP.1.1/SHA
12		RSA signature verification (RSA ISO9796-2 DS1)	[26], [27] (RSA) [28] (SHA)	Modulus length = 2048	[23], chap. 6.6.4.1 [25]	FCS_COP.1.1/COS.RSA.V (EXTERNAL AUTHENTICATE) FCS_COP.1.1/SHA
13		ECDSA signature generation using SHA-{256, 384, 512}	[29] (ECDSA) [30] [28] (SHA)	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [35] and ansix9p{256, 384}r1 [37]	[23], chap. 6.6.3.2 [25]	FCS_COP.1.1/COS.ECDSA.S (INTERNAL AUTHENTICATE) FCS_COP.1.1/SHA
14		ECDSA signature verification using SHA-{256, 384, 512}	[29] (ECDSA) [30] [28] (SHA)	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [35] and ansix9p{256, 384}r1 [37]	[23], chap. 6.6.4.2 [25]	FCS_COP.1.1/COS.ECDSA.V (EXTERNAL AUTHENTICATE) FCS_COP.1.1/SHA
15		PACEv2	[32] (PACEv2)	Length of |Nonce| = 128 bit	[32] [25]	FIA_UAU.5/PACE.PICC FIA_UAU.6/PACE.PICC FIA_USB.1/PACE.PICC (GENERAL

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
						AUTHENTICATE)
16		Hybrid deterministic RNG DRG.4	[4, AIS 20]	n.a.	[25]	FCS_RNG.1/PACE (GENERAL AUTHENTICATE)
17	Key Agreement	ECDH	[29], chap. 4.3.1 (ECDH)	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [35]	[32]	FCS_CKM.1.1/DH.PACE.PICC (GENERAL AUTHENTICATE) id-PACE-ECDH-GM-AES-CBC-CMAC-128, id-PACE-ECDH-GM-AES-CBC-CMAC-192, id-PACE-ECDH-GM-AES-CBC-CMAC-256
18		Key Derivation Function for TDES based on SHA-1	[30], chap. 5.6.3 [28] (SHA)	|k|= 168	[23], chap. 6.2.1 [25]	FCS_CKM.1.1/3TDES_SM FCS_COP.1.1/SHA
19		Key Derivation Function for AES based on SHA-{1, 256}	[29], chap. 4.4.3 [33] [28] (SHA)	|k|= 128, 192, 256	[23], chap. 6.2.2, 6.2.3, 6.2.4	FCS_CKM.1.1/AES.SM (EXTERNAL AUTHENTICATE GENERAL AUTHENTICATE INTERNAL AUTHENTICATE MUTUAL AUTHENTICATE) FCS_COP.1.1/SHA
20	Confidentiality	AES in CBC mode	[33] (AES)	|k|=128, 192, 256	[32], Part 2 [23], chap. 6.7.1.2, 6.7.2.2	FCS_COP.1.1/PACE.PICC.ENC (Secure messaging for PACE)
21		AES in CBC mode	[33] (AES)	|k|=128, 192, 256	[23], chap. 6.7.1.2, 6.7.2.2 [25], chap. 3.3.1	FCS_COP.1.1/CB.AES (PSO ENCIPHER PSO DECIPHER encryption / decryption for trusted channel PSO ENCIPHER and PSO DECIPHER) FCS_COP.1.1/COS.AES (Secure messaging)
22		TDES in CBC mode	[31] (TDES)	|k|=168	[25], chap. 3.3.1	FCS_COP.1.1/CB.3TDES (PSO ENCIPHER PSO DECIPHER encryption / decryption for trusted channel PSO ENCIPHER and PSO DECIPHER) FCS_COP.1.1/COS.3TDES

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
						(Secure messaging)
23		RSA encryption and decryption (RSAES-PKCS1-v 1.5 RSAES-OAEP) Transcipher RSA to ELC and ELC to RSA	[23] [34], chap. 7.1.1, 7.1.2, 7.2.1, 7.2.2	Modulus length = 2048, 3072 for RSA private key operation and 2048 for RSA public key operation	[23], chap. 6.8.1, 6.8.2 [25]	FCS_COP.1.1/COS.RSA (PSO ENCIPHER PSO DECIPHER PSO TRANSCIPHER) For the ELC part of PSO TRANSCIPHER see FCS_COP.1.1/COS.ELC in row 25.
24		RSA encryption and decryption (RSAES-PKCS1-v 1.5 RSAES-OAEP)	[26] (RSA) [34], chap. 7.1.1, 7.1.2, 7.2.1, 7.2.2	Modulus length = 2048, 3072 for RSA private key operation and 2048 for RSA public key operation	[23], chap. 6.8.1, 6.8.2	FCS_COP.1.1/CB.RSA (PSO ENCIPHER)
25		ELC encryption and decryption Transcipher RSA to ELC and ELC to RSA	[29] [23]	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [35] and ansix9p{256, 384}r1 [37]	[23], chap. 6.8.1, 6.8.2 [25]	FCS_COP.1.1/COS.ELC (PSO ENCIPHER PSO DECIPHER PSO TRANSCIPHER) For the RSA part of PSO TRANSCIPHER see FCS_COP.1.1/COS.RSA in row 23.
26		ELC encryption	[29], chap. 4.3.1, 4.3.3, 5.3.1.2	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [35] and ansix9p{256, 384}r1 [37]	[29], chap. 6.8.2	FCS_COP.1.1/CB.ELC (PSO ENCIPHER)
27	Integrity	AES in CMAC mode	[32], Part 2 [23]	|k|=128, 192, 256	[32] [23], chap. 6.6.1, 6.6.2	FCS_COP.1.1/PACE.PICC .MAC (Secure messaging for PACE)
28		AES in CMAC mode	[25], chap. 3.2.2 [36] [23]	|k|=128, 192, 256 |challenge|=64	[23], chap. 6.6.1, 6.6.2 [25]	FCS_COP.1.1/CB.CMAC (for trusted channel PSO COMPUTE CRYPTOGRAPHIC CHECKSUM PSO VERIFY CRYPTOGRAPHIC CHECKSUM) FCS_COP.1.1/COS.CMAC (Secure messaging)
29		TDES in Retail MAC	[23]	|k|=168 |challenge|=64	[23], chap. 6.6.1, 6.6.2 [25]	FCS_COP.1/CB.RMAC (PSO COMPUTE CRYPTOGRAPHIC CHECKSUM

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
						PSO VERIFY CRYPTOGRAPHIC CHECKSUM trusted channel) FCS_COP.1/COS.RMAC (Secure messaging)
30	Trusted Channel	Secure messaging in MAC-ENC mode using PACE session keys	[32]	-	[32]	FTP_ITC.1/PACE.PICC
31	Cryptographic Primitive	Hybrid deterministic RNG DRG.4	[4, AIS 20]	n.a.	[25]	FCS_RNG.1
32		Physical RNG PTG.2	[4, AIS 31]	n.a.	[25]	FCS_RNG.1/SICP
33		SHA-{1, 256, 384, 512}	[28]	-	[23], chap. 3.2.1	FCS_COP.1.1/SHA
34		SHA-{1, 224, 256, 384, 512}	[28]	-	[23]	FCS_COP.1.1/CB_HASH (PSO HASH)

Table 5: TOE cryptographic functionality

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

According to [23] and [25] the algorithms are suitable for securing integrity, authenticity and confidentiality of the data stored in and processed by the TOE as a card operating system platform that is intended to be used for different card types and applications of the card generation G2 in the framework of the German health care system. The validity period of each algorithm is mentioned in the official catalogue [25].

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in Table 1 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process.

Some security measures are partly implemented in this certified TOE, but require additional configuration or control or measures to be implemented by a product layer on top, e.g. the Application Software using the TOE. For this reason the TOE includes guidance documentation (see Table 1) which contains obligations and guidelines for the

developer of the product layer on top on how to securely use this certified TOE and which measures have to be implemented in order to fulfil the security requirements of the Security Target of the TOE. In the course of the evaluation of the composite product or system it must be examined if the required measures have been correctly and effectively implemented by the product layer on top.

In particular, the following aspects from the TOE user guidance documentation [11] to [18] need to be taken into account when using the TOE and when designing and implementing object systems (applications) intended to be set up on the TOE, especially in view of later TR-conformity testing of card products according to the Technical Guideline BSI TR-03144 ([38]):

- Security requirements and hints for designing and implementing object systems (applications) intended to be set up and running on the TOE.

  This concerns on the one hand the design and generation of Initialisation Tables (production variant 1) respective product flash images (production variant 2) containing such object systems by the Initialisation Data Manager. As well this concerns on the other hand after TOE delivery the application developers and card management e.g. by using the commands LOAD APPLICATION and CREATE.

  For an object system, one has to take care of the choice of the access rules and flag described in chapter 2.5 of [16] for the object system's objects. In particular, this concerns key and PIN objects including their related files for the key and PIN data and assigned security attributes.

  For the choice of the access rules and the flag described in chapter 2.5 of [16] for the object system's objects one has to consider that the TOE's Wrapper is only able to export security attributes and public key data of the object system and its objects if their access rules and these flags are set appropriately for read access. .

  For card products that undergo a later TR-conformity testing according to the Technical Guideline BSI TR-03144 ([38]) it is strongly recommended to care for the appropriate choice of the access rules and the flag described in chapter 2.5 of [16] for all the object system's objects. It shall be possible for the Konsistenz-Prüftool according to the Technical Guideline BSI TR-03143 ([39]) that is used for conformity testing to get a complete picture of the object system installed in the card product for further comparison against the respective object system specification.

  The specific life cycle state concept of the TOE for objects managed and processed by the TOE as the MF, folders, files, key and PIN objects has to be taken into account. Especially, the concept of physical and logical life cycle states and their specific processing by the TOE are of relevance for object systems intended to run on the TOE (refer to [23]).

  Any object system set up on the TOE shall only make use of the TOE's functionality as described in the G2-COS specification [23] and the user guidance [15]. The object system has to be checked for taking this requirement into account by using the TOE's Wrapper and following the requirements outlined in the user guidance [12], chapter 5.1.1.1. Card products with an object system that do not fulfil the requirement run out of the scope of the certified TOE and shall not be delivered respective used.

  Within an object system no key ID or PIN ID duplicates in the same folder shall exist. The object system has to be manually checked for taking this requirement into account by using the TOE's Wrapper and following the requirements outlined in the

user guidance [12], chapter 5.1.1.1. Card products with an object system that do not fulfil the requirement run out of the scope of the certified TOE and shall not be delivered respective used.

An object system running on the TOE shall for its ECC related cryptographic functionality only make use of the elliptic curves brainpoolP{256, 384, 512}r1 [35] and ansix9p{256, 384}r1 [37]. The related curve parameter files in the object system (application) have to be set and filled according to the requirements in the user guidance [16], chapter 2.5.2.4. Card products with an object system that do not fulfil the requirement run out of the scope of the certified TOE.

Refer to the user guidance documentation [12], chapter 5.1.1.1 and 6, [13], chapter 4.2.1 and 4.2.2 and [16], chapter 2.5 and following sub-chapters and 2.5.2.4.

- Restrictions for key usage.

  Refer to the user guidance [12], chapter 5.1.1.2.

- Security requirements and hints for the Initialisation Phase / Phase 2 (concerning the loading and installing of object systems (applications) on the TOE by the Initialiser via Initialisation Tables), for the Personalisation Phase / Phase 3 (concerning the personalisation of installed object systems (applications) by the Personalisation Agent) and for the Usage Phase / Phase 4 of the TOE's life cycle model.

  Refer to the user guidance documentation [11], [12], [13], [14] and [15].

- Security requirements and hints for the inlay respective antenna production.

  Refer to the user guidance [18].

- The TOE's Wrapper and its specifics above the Wrapper specification [24], in particular concerning the exceptions that are thrown by the Wrapper.

  Refer to the user guidance [17].

- The command PSO HASH shall not be used for processing of confidential data.

  Refer to the user guidance [12], chapter 5.2.2.

- For the design and generation of Initialisation Tables (production variant 1) respective product flash images (production variant 2) by the Initialisation Data Manager for card products that undergo a later TR-conformity testing according to the Technical Guideline BSI TR-03144 ([38]) it is strongly recommended to care for that via the TOE's specific personalisation commands initialised security attributes and public key data of the object system and its objects cannot be overwritten (except for where explicitly intended by the object system's intention and design).

For a TR-conformity testing of a card product set up on the TOE according to the Technical Guideline BSI TR-03144 ([38]) the following specific aspects and issues have to be taken into account:

- The card product shall be checked that the export of the security attributes and public key data of the object system and each of its objects via the TOE's Wrapper is possible without any restriction and therefore fulfills the requirements for data export in the Wrapper specification [24]. This means that a check has to be performed to ensure that there is no restriction for read access to all the related files in the object system because of an inappropriate choice of the access rules and the flag described in chapter 2.5 of [16] arises. It shall be possible for the Konsistenz-Prüftool according

to the Technical Guideline BSI TR-03143 ([39]) that is used for conformity testing to get a complete picture of the object system installed in the card product for further comparison against the respective object system specification. Refer to the user guidance [16], chapter 2.5 and following sub-chapters.

Note: If such export property cannot be checked in the card product or if read access for the export of the security attributes and public key data of the object system and each of its objects via the TOE's Wrapper is not given the card product will be rejected for a TR-certificate according to the Technical Guideline BSI TR-03144 ([38]).

- Any object system set up on the TOE shall only make use of the TOE's functionality as described in the G2-COS specification [23] and the user guidance [15].

  The card product's object system has to be manually checked for taking this requirement into account by using the TOE's Wrapper and following the requirements outlined in the user guidance [12], chapter 5.1.1.1.

  Note: If there is any object found for which the TOE's Wrapper throws an exception the card product will be rejected for a TR-certificate according to the Technical Guideline BSI TR-03144 ([38]).

- The TOE's Wrapper is *not* able to detect and export key ID and PIN ID duplicates existing within the same folder of an object system (application) that is set up on the TOE. This means that in the case that the object system contains a folder with key ID or PIN ID duplicates the exported lists for <Key_Identifier>, <Password_Identifier> respective persistentPublicKeyList (in the folder's attribute <children>) are not complete.

  As a workaround each folder in the card product's object system has to be manually checked whether key ID or PIN ID duplicates within this folder are existing. This check shall be done by using the TOE's Wrapper and following the requirements outlined in the user guidance [12], chapter 5.1.1.1.

  Note: If this manual check cannot be carried out (e.g. because of a denied read access) or if there is any folder with key ID or PIN ID duplicates found, the card product will be rejected for a TR-certificate according to the Technical Guideline BSI TR-03144 ([38]).

- The card product's object system (application) running on the TOE shall for its ECC related cryptographic functionality only make use of the elliptic curves brainpoolP{256, 384, 512}r1 [35] and ansix9p{256, 384}r1 [37]. All related curve parameter files contained in the object system have therefore to be manually checked that only the elliptic curves as mentioned above are used and that the curve parameters are correctly set according to the requirements in the user guidance [16], chapter 2.5.2.4.

  Note: If a curve parameter file cannot be read out, if elliptic curves beyond those mentioned above are used in the card product's object system or if a curve is incorrectly coded in the related curve parameter files the card product will be rejected for a TR-certificate according to the Technical Guideline BSI TR-03144 ([38]).

- For the card product, it has to be checked that via the TOE's specific personalisation commands initialised security attributes and public key data of the object system and its objects cannot be overwritten (except for where explicitly intended by the object system's intention and design).

  Note: If overwriting of initialised security attributes and public key data of the object

system and its objects via the TOE's specific personalisation commands is possible and not technically suppressed (except for data where overwriting is explicitly intended by the object system's intention and design) the card product will be rejected for a TR-certificate according to the Technical Guideline BSI TR-03144 ([38]).

- If in the framework of the TR-conformity testing of a card product according to the Technical Guideline BSI TR-03144 ([38]) the Konsistenz-Prüftool according to the Technical Guideline BSI TR-03143 ([39]) depicts in its test report within an access rule of an object a wild card or an APDU header lying outside the G2-COS specification [23] or the user guidance [15] this has to be manually examined and valuated.
- The TOE implements for the file management commands ACTIVATE, DEACTIVATE, DELETE, TERMINATE and TERMINATE DF the additional command variant with selection of the file in the command itself. If such command variant is indicated in an access rule of an object in the card product this can be considered as security uncritical and does not undermine the object system's design and security aspects.

11. Security Target

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

12. Definitions

12.1. Acronyms

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
APDU	Application Protocol Data Unit
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
CPU	Central Processing Unit
DEMA	Differential Electromagnetic Analysis
DES	Data Encryption Standard
3TDES	Three Key DES
DFA	Differential Fault Analysis / Attack
DPA	Differential Power Analysis
DRNG	Deterministic Random Number Generator

EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
EEPROM	Electrically Erasable Programmable Read-Only Memory
eHC	electronic Health Card
ETR	Evaluation Technical Report
gSMC-K	gerätespezifische Security Module Card Type K (Konnektor)
gSMC-KT	gerätespezifische Security Module Card Type KT (Kartenterminal)
HPC	Health Professional Card
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
NVM	Non-Volatile Memory
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
PRNG	Physical Random Number Generator
RFU	Reserved for Future Use
RNG	Random Number Generator
RSA	Rivest Shamir Adleman Algorithm
SAR	Security Assurance Requirement
SEMA	Simple Electromagnetic Analysis
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SM	Secure Messaging
SMC-B	Security Module Card Type B
SPA	Single Power Analysis
ST	Security Target
TOE	Target of Evaluation
TR	Technische Richtlinie (Technical Guideline)
TSF	TOE Security Functionality

12.2. Glossary

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

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

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

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

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - Named set of either security functional or security assurance requirements.

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

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

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

13. Bibliography

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

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012

[3] BSI certification: Technical information on the IT security certification of products, protection profiles and sites (CC-Produkte) and Requirements regarding the Evaluation Facility for the Evaluation of Products, Protection Profiles and Sites under the CC and ITSEC (CC-Prüfstellen)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8]

[8] specifically

- AIS 1, Version 13, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 8, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 23, Version 3, Zusammentragen von Nachweisen der Entwickler
- AIS 25, Version 8, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document

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

[6] Security Target BSI-DSZ-CC-0916, Security Target STARCOS 3.6 COS C1, Version 1.0.87, 31 July 2015, Giesecke & Devrient GmbH (confidential document)

[7] Security Target Lite BSI-DSZ-CC-0916, Security Target Lite STARCOS 3.6 COS C1, Version 1.5, 31 July 2015, Giesecke & Devrient GmbH (sanitised public document)

[8] Common Criteria Protection Profile Card Operating System Generation 2 (PP COS G2), Version 1.9, 18 November 2014, BSI-CC-PP-0082-V2-2014, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[9] ETR BSI-DSZ-CC-0916, Evaluation Technical Report (ETR) – Summary for STARCOS 3.6 COS C1, Version 1.6, 31 July 2015, SRC Security Research & Consulting GmbH (confidential document)

[10] Configuration List BSI-DSZ-CC-0916, Configuration List STARCOS 3.6 COS C1, Version 1.4, 30 July 2015, Giesecke & Devrient GmbH (confidential document)

[11] Guidance Documentation STARCOS 3.6 – Main Document, Version 1.7, 25 July 2015, Giesecke & Devrient GmbH

[12] Guidance Documentation for the Usage Phase STARCOS 3.6 COS, Version 2.1, 31 July 2015, Giesecke & Devrient GmbH

[13] Guidance Documentation for the Initialization Phase STARCOS 3.6 COS, Version 2.6, 31 July 2015, Giesecke & Devrient GmbH

[14] Guidance Documentation for the Personalisation Phase STARCOS 3.6 COS, Version 1.9, 29 July 2015, Giesecke & Devrient GmbH

[15] STARCOS 3.6 Functional Specification - Part 1: Interface Specification, Version 1.19, 31 July 2015, Giesecke & Devrient GmbH

[16] STARCOS 3.6 Internal Design Specification, Version 1.3, 31 July 2015, Giesecke & Devrient GmbH

[17] STARCOS 3.6 COS C1/2 Guidance Documentation for the Wrapper, Version 1.3, 29 July 2015, Giesecke & Devrient GmbH

[18] STARCOS 3.6 COS C1/2 Guidance Documentation for Inlay Production, Version 1.1, 13 July 2015, Giesecke & Devrient GmbH

[19] Security Target of the underlying hardware platform, Security Target M7893 B11, Version 1.5, 01 December 2014, Infineon Technologies AG, BSI-DSZ-CC-0879-2014-MA-01

- AIS 26, Version 9, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 36, Version 4, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.9, Reuse of evaluation results

[20] Certification Report of the underlying hardware platform Infineon Security Controller M7893 B11 with optional RSA2048/4096 v1.03.006, EC v1.03.006,SHA-2 v1.01 libraries and Toolbox v1.03.006 and with specific IC dedicated software (firmware) from Infineon Technologies AG, BSI-DSZ-CC-0879-2014, March 2014, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[21] Maintenance Report of the underlying hardware platform Infineon Security Controller M7893 B11 with optional RSA2048/4096 v1.03.006, EC v1.03.006,SHA-2 v1.01 libraries and Toolbox v1.03.006 and with specific IC dedicated software (firmware) from Infineon Technologies AG, BSI-DSZ-CC-0879-2014-MA-01, December 2014, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[22] ETR for Composite Evaluation of the underlying hardware platform Infineon Security Controller M7893 B11 from certification procedure BSI-DSZ-CC-0879-2014, Version 1, 20 December 2013, TÜV Informationstechnik GmbH (confidential document)

[23] Einführung der Gesundheitskarte, Spezifikation des Card Operating System (COS), Elektrische Schnittstelle, Version 3.7.0 vom 26.08.2014, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Errata zu Release 1.4.0, Kartenspezifikationen und Konnektor, Version 1.0.0 vom 02.10.2014, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

2. Errata zu Release 1.4.0, Spezifikation des Card Operating System und Spezifikation Wrapper, Version 1.0.0 vom 06.10.2014, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Errata zu Release 1.4.2, Störungsampel, Zertifikate, Testkarten und COS-Wrapper, Version 1.0.1 vom 08.12.2014, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[24] Einführung der Gesundheitskarte, Spezifikation Wrapper, Version 1.6.0, 26.08.2014, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[25] Technische Richtlinie BSI TR-03116-1 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 1 – Telematikinfrastruktur, Version 3.18, 30.01.2014, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[26] PKCS #1 v2.2: RSA Cryptography Standard, 27 October 2012, RSA Laboratories

[27] ISO/IEC 9796-2:2010 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms, 2010-12, ISO

[28] Federal Information Processing Standards Publication FIPS PUB 180-4, Specifications for the Secure Hash Standard (SHS), March 2012, U.S. Department of Commerce/National Institute of Standards and Technology

[29] Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.0, 2013-03, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[30] American National Standard X9.63-2001, Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography, 16 November 2005

[31] Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST Special Publication 800-67, Revised January 2012, 2012-01, National Institute of Standards and Technology

[32] Technische Richtlinie BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.10, 20.03.2012, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[33] Federal Information Processing Standards Publication FIPS PUB 197, Advanced Encryption Standard (AES), 2001-11-26, U.S. Department of Commerce/National Institute of Standards and Technology

[34] Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, RFC 3447, 2003-02, J. Jonsson, B. Kaliski, IETF

[35] Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, 2010-03, M. Lochter, J. Merkle, IETF

[36] ISO 15946 Information technology – Security techniques – Cryptographic techniques – Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, May 2005, National Institute of Standards and Technology

[37] Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013, U.S. Department of Commerce/National Institute of Standards and Technology

[38] Technische Richtlinie BSI TR-03144 eHealth – Konformitätsnachweis für Karten-Produkte der Kartengeneration G2, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[39] Technische Richtlinie BSI TR-03143 eHealth G2-COS Konsistenz-Prüftool, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[40] Certification Report for Giesecke & Devrient GmbH Development Centre Germany (DCG), BSI-DSZ-CC-S-0017-2014, August 2014, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[41] Certification Report for Giesecke & Devrient GmbH Dienstleistungscenter (DLC, Production Site), BSI-DSZ-CC-S-0029-2014, September 2014, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[42] Certification Report for Giesecke & Devrient GmbH Slovakia s.r.o. (GDSK), BSI-DSZ-CC-S-0031-2014, April 2014, Bundesamt für Sicherheit in der Informationstechnik (BSI)

C. Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model

Assurance Class	Assurance Components
	ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“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 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

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

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC 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 augmented with extended assurance requirements.

Evaluation assurance level 1 (EAL 1) - functionally tested (chapter 8.3)

“Objectives

EAL 1 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.

EAL 1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL 1 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 EAL 1 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.”

Evaluation assurance level 2 (EAL 2) - structurally tested (chapter 8.4)

“Objectives

EAL 2 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 practise. As such it should not require a substantially increased investment of cost or time.

EAL 2 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 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 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 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL 4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 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 (EAL 5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL 5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 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 (EAL 6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL 6 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.

EAL 6 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 (EAL 7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL 7 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 EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

D. Annexes

List of annexes of this certification report

Annex A: Security Target [6] provided within a separate document.

Annex B: Evaluation results regarding development and production environment.

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0916-2015

Evaluation results regarding development and production environment

The IT product STARCOS 3.6 COS C1 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 7 August 2015, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1)

are fulfilled for the development and production sites of the TOE listed below:

a) Giesecke & Devrient GmbH Development Centre Germany (DCG), Zamdorfer Strasse 88, 81677 München, Germany (Development / Testing). Refer to the Certification Report BSI-DSZ-CC-S-0017-2014 ([40]).

b) Giesecke & Devrient GmbH Dienstleistungscenter (DLC, Production Site), Prinzregentenstrasse 159, 81677 München, Germany (Production / Initialisation). Refer to the Certification Report BSI-DSZ-CC-S-0029-2014 ([41]).

c) Giesecke & Devrient GmbH Development Slovakia s.r.o. (GDSK), Dolné Hony 11, SK - 949 01 Nitra, Slovakia (Initialisation / Inlay Embedding). Refer to the Certification Report BSI-DSZ-CC-S-0031-2014 ([42]).

d) For development and production sites regarding the platform please refer to the Certification Report BSI-DSZ-CC-0879 ([20]) and the Maintenance Report BSI-DSZ-CC-0879-MA-01 ([21]).

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6] and [7]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and [7]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.