Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1243-2024

for

STARCOS 3.7 COS GKV C2

from

Giesecke+Devrient ePayments 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-1243-2024 (*)

STARCOS 3.7 COS GKV C2

from	Giesecke+Devrient ePayments GmbH
PP Conformance:	Card Operating System Generation 2 (PP COS G2), Version 2.1, 10 July 2019, BSI-CC-PP-0082-V4-2019
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5
valid until:	21 August 2029

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 Scheme Interpretations and 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 5.

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
recognition for components
up to EAL 2 only

Bonn, 22 August 2024

For the Federal Office for Information Security

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

Sandro Amendola L.S.
Director-General

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.

Contents

A. Certification

1. 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.

2. 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[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs [3]
- Special decrees issued by the Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community)
- 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[4] [1] also published as ISO/IEC 15408

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

[2] 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

[3] BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- 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]

3. 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.

3.1. European Recognition of 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.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. 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. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

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

3.2. 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), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://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 related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2 and ALC_FLR components.

[4] Proclamation of the Bundesministerium des Innern und für Heimat of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

4. 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 3.7 COS GKV C2 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0976-V3-2019 including subsequent maintenance procedures BSI-DSZ-CC-0976-V3-2019-MA-01 and BSI-DSZ-CC-0976-V3-2019-MA-02. Specific results from the evaluation process BSI-DSZ-CC-0976-V3-2019 and related maintenance procedures were re-used.

The evaluation of the product STARCOS 3.7 COS GKV C2 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 2 August 2024. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

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

The product was developed by: Giesecke+Devrient ePayments GmbH.

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

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is 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 components and assurance levels please refer to CC itself. Detailed references are listed in part C of this 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-assessment or 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 would 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 22 August 2024 is valid until 21 August 2029. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

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, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
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 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 where the certification of the product has assumed this confidentiality being maintained, 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 deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

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.

6. Publication

The product STARCOS 3.7 COS GKV C2 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[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Giesecke+Devrient ePayments GmbH
Prinzregentenstraße 161
81677 München

B. Certification Results

The following results represent a summary of

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

1. Executive Summary

The Target of Evaluation (TOE) is the product STARCOS 3.7 COS GKV C2 developed by Giesecke+Devrient ePayments GmbH.

The TOE is a smart card product according to the G2-COS specification [21] from gematik and is implemented on the hardware platform Infineon Security Controller IFX_CCI_000005h from Infineon Technologies AG (refer to [18], [19]).

The TOE is intended to be used as a card operating system platform for cards of the card generation G2 (in particular of type eHC (electronic Health Card)) 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 card type eHC (electronic Health Card) as currently specified for a card product 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 users 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 (i.e. contact-based and contactless 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 Infineon IFX_CCI_000005h),
- the IC Embedded Software (STARCOS 3.7 COS GKV C2 Operating System),
- the so-called Wrapper (TOE specific SW tool for re-coding and 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 [21], but does not contain itself any object systems (applications). However, the delivered product comprises beside the TOE also an object system already installed on the TOE.

In functional view, the TOE with its IC Embedded Software (STARCOS 3.7 COS GKV C2 Operating System) is implemented according to the G2-COS specification [21] from gematik. Hereby, the TOE implements the mandatory part of the G2-COS specification [21] with the base functionality of the operating system platform. In addition, the TOE implements the option RSA Key Generation (“Option_RSA_KeyGeneration”) and the option Contactless (“Option_kontaktlose_Schnittstelle”) as defined in the G2-COS specification [21]. None of the further options Crypto Box (“Option_Kryptobox”), Logical

Channel (“Option_logische_Kanäle“), PACE for Proximity Coupling Device (“Option_-PACE_PCD”), USB (“Option_USB_Schnittstelle”) and RSA CVC (“Option_RSA_CVC”) defined in the G2-COS specification [21] is implemented in the TOE.

Furthermore, the TOE provides the commands CREATE and PSO HASH (refer to the user guidances [12], chapter 5.2.1 and 5.2.2 and [15], chapter 2.3.1 and 2.3.2) that are outlined as optional in the G2-COS specification [21]. In addition, the TOE provides developer-specific initialisation and personalisation commands (refer to the user guidance [15], chapter 2.4) for support of the Initialisation Phase and Personalisation Phase of the TOE’s life cycle model. Refer to chapter 2 of this report.

The TOE's Wrapper is implemented according to the Wrapper specification [22] from gematik GmbH with some minor deviations. The requirements towards an object system and the conformity testing according to [37] handling this deviation can be found in the TOE user guidance documentation [13], chapter 4.2.1, [14], chapter 5.8.2 and [12], chapter 5.1.1.1. Refer as well to chapter 10 of this report.

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 2.1, 10 July 2019, BSI-CC-PP-0082-V4-2019 [8]. The Security Target [6] and [7] uses the mandatory parts of the PP and the optional packages RSA Key Generation and Contactless defined in the PP. None of the PP’s further optional packages Crypto Box, Logical Channel, PACE for Proximity Coupling Device and RSA CVC is used.

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

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [7], chapter 6.1, 7.4 and 8.4. 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: symmetric authentication mechanisms based on AES and asymmetric authentication mechanisms based on ECC and RSA.

- SF_AssetProtection:

  The TOE provides mechanisms for supporting data integrity for User Data and TSF Data. The TOE hides information about IC power consumption and command execution time ensuring that no confidential information about User Data and TSF Data 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 ECDH as well as generation of RSA and ECC key pairs. Moreover, it supports the generation of session keys in authentication mechanisms (based on symmetric and asymmetric cryptography, in particular PACE) which includes session key negotiation.

- 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 and a PTG.2 random number generator.

For more details please refer to the Security Target [6] chapter 6.1, 7.4, 8.4 and 10 and [7], chapter 6.1, 7.4 and 8.4.

The assets to be protected by the TOE are defined in the Security Target [6] and [7], chapter 3.1, 7.2.1 and 8.2.1. 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 and 8.2.4.

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 3.7 COS GKV C2

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/ SW	Infineon Security Controller IFX_CCI_000005h including its IC Dedicated Software (Firmware) (refer to the Certification Report	Infineon Security Controller IFX_CCI_000005h (with Firmware version	Dual-interface chip (contact-based and contactless chip). Delivery as chip to the module production site NedCard according to the delivery procedures specified

No	Type	Identifier	Release	Form of Delivery
		BSI-DSZ-CC-1110-V6-2023 ([19]))	80.100.17.3)	in BSI-DSZ-CC-1110-V6-2023 ([19]).
2	SW	IC Embedded Software: STARCOS 3.7 COS GKV C2 Operating System	STARCOS 3.7 COS GKV C2 OS Identification: ‘47 44 00 B7 03 01 00’ (refer to Table 3)	Implemented in the flash of the IC (refer to row no. 1). The TOE itself covers the IC and the IC Embedded Software and is delivered as product together with an already installed object system. The TOE or product respectively (i.e. the TOE plus an already installed object system) is delivered as initialised module or smart card. The delivery is performed by the TOE developer Giesecke+Devrient ePayments GmbH. Refer to the description of the TOE's life cycle model and related production processes below this Table.
3	DOC	Guidance Documentation STARCOS 3.7 COS GKV C2 – Main Document [11]	Version 1.5	Document in electronic form (encrypted and signed)
4	DOC	Guidance Documentation for the Usage Phase STARCOS 3.7 COS GKV C2 [12]	Version 1.7	Document in electronic form (encrypted and signed)
5	DOC	Guidance Documentation for the Initialization Phase STARCOS 3.7 COS GKV C2 [13]	Version 1.8	Document in electronic form (encrypted and signed)
6	DOC	Guidance Documentation for the Personalisation Phase STARCOS 3.7 COS GKV C2 [14]	Version 1.9	Document in electronic form (encrypted and signed)
7	DOC	STARCOS 3.7 Functional Specification - Part 1: Interface Specification [15]	Version 1.3	Document in electronic form (encrypted and signed)
8	DOC	STARCOS 3.7 Internal Design Specification [16]	Version 1.0	Document in electronic form (encrypted and signed)
9	SW	Wrapper	Version 1.8.4	File rar-archive: egkwrapper-v1.8.4.rar consisting of the jar files: • wrapper.jar (main file) • gdoffcard.jar (helper library) • gdoffcardstarcos.jar (helper library) (encrypted and signed) The integrity and authenticity of the Wrapper is given by the following SHA-256 hash value: 0ED4C08CC5E1F33127E9F6347D08760998A07B0A9B516F7349AEEFE5B2ACB930

No	Type	Identifier	Release	Form of Delivery
10	DOC	STARCOS 3.7 COS Guidance Documentation for the Wrapper [17]	Version 1.3	Document in electronic form (encrypted and signed)
11	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 TOE STARCOS 3.7 COS GKV C2 is as well known under the following product identificator:

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

Product: ‘53 33 37 4F 53 47 4B 32’ (S37OSGK2)

OS Version Number: '01 00 03' (1.0.3)

The TOE corresponds to the gematik product type version (PTV) 4.5.2-0.

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 3.7 COS GKV C2 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

The STARCOS 3.7 COS GKV C2 Operating System is completely loaded in the framework of the Initialisation Phase (Phase 2) by Giesecke+Devrient ePayments GmbH. Furthermore, in the framework of this initialisation process 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. The product (including the TOE) is delivered by Giesecke+Devrient ePayments GmbH to the Personalisation Agent (Giesecke+Devrient ePayments GmbH or third party) for personalisation.

The TOE or product respectively (i.e. TOE plus an already installed object system) is delivered as initialised module or smart card.

In order to verify that the user uses a certified TOE, the TOE can be identified using the means described in the user guidances [13], chapter 5.6, [14], chapter 5.7 and [12], chapter 4.1.1. 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 3.7 COS GKV C2 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 version)
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 the user guidances [13], chapter 5.6, [14], chapter 5.7 and [12], chapter 4.1.1.

The following table describes the concrete values identifying the TOE:

Data Type	Tag in the ProtocolData DO	Data
Chip manufacturer data	'9F 6B'	‘05 16 00 13 00 02 00 00'
Identification of the operating system (OS version)	'9F 6A'	'47 44 00 B7 03 01 00'
Fabkey key material identification	'9F 6F'	Second byte = '17’

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 IFX_CCI_000005h from Infineon Technologies AG and with IC Embedded Software STARCOS 3.7 COS GKV C2 Operating System implemented by Giesecke+Devrient ePayments GmbH according to the G2-COS specification [21] 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 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 card type eHC (electronic Health Card) as currently specified for a card product 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 and 7.

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 documents are met: (i) TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the user guidance, including TOE related application notes, usage requirements, recommendations and restrictions, and (ii) certification report including TOE related usage requirements, recommendations, restrictions and findings resulting from the TOE’s evaluation and certification.
OE.Resp-ObjS	Treatment of User Data and TSF Data by the Object System 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 during Personalisation Security procedures shall be used after delivery of the TOE during Phase 6 ‘Personalisation’ up to the delivery of the smart card to the end-user in order to maintain confidentiality and integrity of the TOE and to prevent any theft, unauthorised personalisation or unauthorised use.
OE.PACE_Terminal	PACE support by contactless terminal The external device communicating through a contactless interface with the TOE using PACE shall support the terminal part of the PACE protocol.

Table 4: Security Objectives for the operational environment

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

5. Architectural Information

The TOE is set up as a composite product. It is composed of the Infineon Security Controller IFX_CCI_000005h from Infineon Technologies AG and the IC Embedded Software with the STARCOS 3.7 COS GKV C2 Operating System developed by Giesecke+Devrient ePayments 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 ePayments GmbH.

For details concerning the CC evaluation of the underlying IC see the evaluation documentation under the Certification ID BSI-DSZ-CC-1110-V6-2023 ([18], [19]).

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

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

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 including analysis by machine learning methods for SHA, AES, RSA and ECC, including RSA and 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 configuration of the TOE as outlined in the Security Target [6] and [7]:

STARCOS 3.7 COS GKV C2

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 (contact-based and contactless chip) of type Infineon Security Controller IFX_CCI_000005h from Infineon Technologies AG. This IC is certified under the Certification ID BSI-DSZ-CC-1110-V6-2023 (refer to [19]).

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 ePayments GmbH.

The TOE covering the IC and the IC Embedded Software (STARCOS 3.7 COS GKV C2 Operating System) is delivered as a module or smart card together with an already installed object system. 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 guidances [13], chapter 5.6, [14], chapter 5.7 and [12], chapter 4.1.1. 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 according to AIS 36 (see [4]). On base of this concept the relevant guidance documents of the underlying IC platform (refer to [22]) and the document ETR for composite evaluation from the IC's evaluation (refer to [23]) have been applied in the TOE evaluation. Related to AIS 36 the updated version of the JIL document 'Composite product evaluation for Smart Cards and similar devices', Version 1.5.1, May 2018 was taken into account.

(ii) Guidance for Smartcard Evaluation (AIS 37, see [4]).

(iii) Attack Methods for Smartcards and Similar Devices (AIS 26, see [4]).

(iv) Application of Attack Potential to Smartcards (AIS 26, see [4]).

(v) Application of CC to Integrated Circuits (AIS 25, see [4]).

(vi) Security Architecture requirements (ADV_ARC) for smart cards and similar devices (AIS 25, see [4]).

(vii) Evaluation Methodology for CC Assurance Classes for EAL 5+ and EAL 6 (AIS 34, see [4]).

(viii) Functionality classes and evaluation methodology of physical and deterministic random number generators (AIS 20 and AIS 31, see [4]).

(ix) Informationen zur Evaluierung von kryptographischen Algorithmen (AIS 46, see [4]).

For smart card specific methodology the scheme interpretations AIS 25, AIS 26, AIS 34, AIS 36, AIS 37 and AIS 46 (see [4]) were used. For RNG assessment the scheme interpretations AIS 20 and AIS 31 were used (see [4]).

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.

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

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 ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0976-V3-2019 including subsequent maintenance procedures BSI-DSZ-CC-0976-V3-2019-MA-01 and BSI-DSZ-CC-0976-V3-2019-MA-02, re-use of specific evaluation tasks was possible. The TOE and its implementation itself did not change. The focus of this re-evaluation was on the change of the TOE's life-cycle model regards production sites including renewal of corresponding site certificates, the update of the underlying HW certificate, and the renewal of the TOE's

vulnerability analysis and assessment including penetration testing of the TOE's (crypto) implementation.

The evaluation has confirmed:

- PP Conformance: Card Operating System Generation 2 (PP COS G2), Version 2.1, 10 July 2019, BSI-CC-PP-0082-V4-2019 [8]
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5

The Security Target [6] and [7] uses the mandatory parts of the PP and the optional packages RSA Key Generation and Contactless defined in the PP. None of the PP's further optional packages Crypto Box, Logical Channel, PACE for Proximity Coupling Device and RSA CVC is used.

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 table in annex C of part D of this report gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines the standard of application where its specific appropriateness is stated.

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

According to the specification [21] and the Technical Guideline BSI TR-03116-1 [23] the algorithms are suitable for authentication and key agreement and for supporting 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 cards of the card generation G2 (in particular of type eHC (electronic Health Card)) in the framework of the German health care system. The validity period of each algorithm is mentioned in the official catalogue [23].

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, too.

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 composed 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 [17] 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 ([37]):

- 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 product flash images containing such object system 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 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 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 ([37]) 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 object system's objects. It shall be possible for the Konsistenz-Prüftool according to the Technical Guideline BSI TR-03143 ([38]) 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 [21]).

  Any object system set up on the TOE shall only make use of the TOE's functionality as described in the G2-COS specification [21] 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 carrying out further manual checks in order to get information about functionality that lies beyond the certified TOE scope, but is used in the card product. The requirements outlined in the user guidances [12], chapter 5.1.1.1 and [13], chapter 4.2.1 and 4.2.2 shall be followed, i.e. looking for

exceptions thrown by the Wrapper and looking for information provided via the Wrapper that indicates the use of proprietary (uncertified) COS functionality in the card product. 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 [30] and ansix9p{256, 384}r1 [33]. Refer to the user guidance [12], chapter 6. 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, [15] and [16], chapter 2.5 (in particular 2.5.2.4) and following subchapters.

- Security requirements and hints for the Development Phase / Phase 1 (concerning the design and implementation of object systems (applications) and the generation of the related product flash images by the Initialisation Data Manager), for the Initialisation Phase / Phase 2 (concerning the load and install processes for the product flash images to be performed by the Initialiser), 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].

- The TOE's Wrapper and its specifics beyond the Wrapper specification [22], 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.

- In particular, the following aspects need to be taken into account when using the TOE and its cryptographic functionality:

  [12], chapter 5.1.1 and 5.1.2 including subchapters, [13], chapter 4.1, 4.2 and 5.7.1 including subchapters and [14], chapter 5.8.1 and 5.8.2.

  For usage of the PACE protocol and achieving resistance of the TOE against high attack potential, please refer specifically to [13], chapter 4.2.1 and related references by [12], chapter 5.1.1.1 and [14], chapter 5.8.2.

- For the design and generation of product flash images containing an object system for card products that undergo a later TR-conformity testing according to the Technical Guideline BSI TR-03144 ([37]) 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 card products that undergo a TR-conformity testing according to the Technical Guideline BSI TR-03144 ([37]) the OS Version Number '01 00 03' (1.0.3) shall be inserted in the EF.ATR, even if the OS version number that is retrieved by the

command GET PROTOCOL DATA (refer to chapter 2 of this certification report) differs from this entry.

For a TR-conformity testing of a card product set up on the TOE according to the Technical Guideline BSI TR-03144 ([37]) 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 fulfils the requirements for data export in the Wrapper specification [22]. This means that it has to be ensured 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]. It shall be possible for the Konsistenz-Prüftool according to the Technical Guideline BSI TR-03143 ([38]) 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 guidances [12], chapter 5.1.1.1, [13], chapter 4.2.1 and 4.2.2 and [16], chapter 2.5 and following subchapters.

  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 ([37]).

- Any object system set up on the TOE shall only make use of the TOE's functionality as described in the G2-COS specification [21] 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 guidances [12], chapter 5.1.1.1 and [13], chapter 4.2.1. Refer to the user guidance [13], chapter 4.2.2.

  Note: If there is any object found for which the TOE's Wrapper throws an exception or where the Wrapper or Konsistenz-Prüftool according to the Technical Guideline BSI TR-03143 ([38]) indicates the use of proprietary (uncertified) COS functionality the card product will be rejected for a TR-certificate according to the Technical Guideline BSI TR-03144 ([37]).

- 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 [30] and ansix9p{256, 384}r1 [33]. Refer to the user guidance [12], chapter 6. 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. Refer to the user guidance [13], chapter 4.2.2.

  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 ([37]).

- 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). Refer to the user guidance [13], chapter 4.2.2.

  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 ([37]).
- If in the framework of the TR-conformity testing of a card product according to the Technical Guideline BSI TR-03144 ([37]) the Konsistenz-Prüftool according to the Technical Guideline BSI TR-03143 ([38]) 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 [21] or the user guidance [15] this has to be manually examined and valuated. Refer to the user guidance [13], chapter 4.2.2.
- For card products that undergo a TR-conformity testing according to the Technical Guideline BSI TR-03144 ([37]), it shall be checked that the OS Version Number inserted in the EF.ATR equals '01 00 03' (1.0.3). Furthermore, the OS version number retrieved via the command GET PROTOCOL DATA shall be checked for correctness related to the identification data described in chapter 2 of this certification report.

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. Regulation specific aspects (eIDAS, QES)

None.

13. Definitions

13.1. 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
DFA	Differential Fault Analysis / Attack
DO	Data Object
DPA	Differential Power Analysis
DRNG	Deterministic Random Number Generator
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
EEPROM	Electrically Erasable Programmable Read-Only Memory
eHC	electronic Health Card
eIDAS	electronic IDentification, Authentication and trust Services
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
HW	Hardware
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
PTV	Product Type Version
QES	Qualified Electronic Signature
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	Simple Power Analysis
ST	Security Target
SW	Software
TOE	Target of Evaluation
TR	Technische Richtlinie (Technical Guideline)
TSF	TOE Security Functionality

13.2. 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.

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 5, April 2017
https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen)
https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7]
https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website
https://www.bsi.bund.de/zertifizierungsreporte

[7] specifically

- AIS 1, Version 14, 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 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 10, 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 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document (but with usage of updated JIL document ‘Composite product evaluation for Smart Cards and similar devices’, Version 1.5.1, May 2018)
- AIS 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluierungen
- AIS 38, Version 2, Reuse of evaluation results
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[6] Security Target BSI-DSZ-CC-1243, Security Target STARCOS 3.7 COS GKV C2, Version 1.6, 10 June 2024, Giesecke+Devrient ePayments GmbH (confidential document)

[7] Security Target Lite BSI-DSZ-CC-1243, Security Target Lite STARCOS 3.7 COS GKV C2, Version 1.6, 10 June 2024, Giesecke+Devrient ePayments GmbH (sanitised public document)

[8] Common Criteria Protection Profile Card Operating System Generation 2 (PP COS G2), Version 2.1, 10 July 2019, BSI-CC-PP-0082-V4-2019, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[9] ETR BSI-DSZ-CC-1243, Evaluation Technical Report (ETR) – Summary for STARCOS 3.7 COS GKV C2, Version 1.1, 1 August 2024, SRC Security Research & Consulting GmbH (confidential document)

[10] Configuration List BSI-DSZ-CC-1243, Configuration List STARCOS 3.7 COS GKV C2, Version 1.2, 22 July 2024, Giesecke+Devrient ePayments GmbH (confidential document)

[11] Guidance Documentation STARCOS 3.7 COS GKV C2 – Main Document, Version 1.5, 5 June 2024, Giesecke+Devrient ePayments GmbH

[12] Guidance Documentation for the Usage Phase STARCOS 3.7 COS GKV C2, Version 1.7, 5 June 2024, Giesecke+Devrient ePayments GmbH

[13] Guidance Documentation for the Initialization Phase STARCOS 3.7 COS GKV C2, Version 1.8, 19 June 2024, Giesecke+Devrient ePayments GmbH

[14] Guidance Documentation for the Personalisation Phase STARCOS 3.7 COS GKV C2, Version 1.9, 5 June 2024, Giesecke+Devrient ePayments GmbH

[15] STARCOS 3.7 Functional Specification - Part 1: Interface Specification, Version 1.3, 30 August 2019, Giesecke+Devrient ePayments GmbH

[16] STARCOS 3.7 Internal Design Specification, Version 1.0, 4 April 2018, Giesecke+Devrient ePayments GmbH

[17] STARCOS 3.7 COS Guidance Documentation for the Wrapper, Version 1.3, 5 April 2024, Giesecke+Devrient ePayments GmbH

[18] Security Target of the underlying hardware platform, Common Criteria Confidential Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h, H13, Revision 4.4, 30 November 2023, Infineon Technologies AG, BSI-DSZ-CC-1110-V6-2023 (confidential document)

Security Target Lite of the underlying hardware platform, Common Criteria Public Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h H13, Revision 4.4, 30 November 2023, Infineon Technologies AG, BSI-DSZ-CC-1110-V6-2023 (sanitised public document)

[19] Certification Report BSI-DSZ-CC-1110-V6-2023 for Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions from Infineon

Technologies AG, 07 December 2023, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[20] ETR for Composite Evaluation of the underlying hardware platform Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h, H13 from certification procedure BSI-DSZ-CC-1110-V6-2023, Version 3, 01 December 2023, TÜV Informationstechnik GmbH (confidential document)

[21] Einführung der Gesundheitskarte, Spezifikation des Card Operating System (COS), Elektrische Schnittstelle, Version 3.14.0, 16 May 2022, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[22] Einführung der Gesundheitskarte, Spezifikation Wrapper, Version 1.8.0, 24 August 2016, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[23] Technische Richtlinie BSI TR-03116-1: Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1 – Telematikinfrastruktur, Version 3.20, 21 September 2018, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[24] PKCS #1: RSA Cryptography Standard, Version 2.2, October 2012, RSA Laboratories

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

[26] Federal Information Processing Standards Publication 180-4 (FIPS PUB 180-4), Secure Hash Standard (SHS), August 2015, U.S. Department of Commerce/National Institute of Standards and Technology (NIST)

[27] Technical Guideline BSI TR-03111: Elliptic Curve Cryptography, Version 2.10, 1 June 2018, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[28] American National Standard X9.63 (R2017), Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography, December 2011 (reaffirmed 10 February 2017), ANSI

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

[30] Elliptic Curve Cryptography (ECC), Brainpool Standard Curves and Curve Generation, RFC 5639, March 2010, IETF

[31] Recommendation for Block Cipher Modes of Operation: Methods and techniques, NIST Special Publication 800-38A, 2001, National Institute of Standards and Technology (NIST)

[32] Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, 2005, National Institute of Standards and Technology (NIST)

[33] American National Standard X9.62, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), November 2005, ANSI

[34] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised 1 November 1993, RSA Laboratories

[35] Technical Guideline BSI TR-03110:

Technical Guideline BSI TR-03110-1: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 1: eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, 26 February 2015, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Technical Guideline BSI TR-03110-2: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2: Protocols for electronic IDentification, Authentication and trust Services (eIDAS), Version 2.21, 21 December 2016, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Technical Guideline BSI TR-03110-3: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3: Common Specifications, Version 2.21, 21 December 2016, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[36] ISO/IEC 18031:2005, Information technology – Security techniques – Random bit generation, 2005, ISO

[37] Technische Richtlinie BSI TR-03144 eHealth – Konformitätsnachweis für Karten-Produkte der Kartengeneration G2, Version 1.2, 27 July 2017, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[38] Technische Richtlinie BSI TR-03143 eHealth – G2-COS Konsistenz-Prüftool, Version 1.1, 18 May 2017, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[39] Certification Report for Giesecke+Devrient Development Center Germany (DCG) of Giesecke+Devrient ePayments GmbH, BSI-DSZ-CC-S-0260-2023, 20 December 2023, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[40] Certification Report CCN-CC/2022-53/INF-4095 and maintenance report CCN-CC/2023-21/INF-4149 for Giesecke+Devrient Development Center Spain (DCS), related to CCN-CC-15/2023, 17 May 2023 (Certificate´date), National Cryptologic Centre (CCN)

[41] Certification Report CCN-CC/2023-01/INF-4274 for Linxens Singapore Changi Site, related to CCN-CC-2/2024, 29 February 2024 (Certificate date), National Cryptologic Centre (CCN)

[42] Certification Report NSCIB-SS-2300084-01 for INESA Shanghai, INESA Intelligent Electronics Co. Ltd., related to NSCIB-SS-2300084-01, 14 August 2023, Netherlands Scheme for Certification in the Area of IT Security (NSCIB)

[43] Certification Report CCN-CC/2022-01/INF-3825 for Giesecke+Devrient Mobile Security Iberia (GDIMS), related to CCN-CC-23/2022, 26 May 2022 (Certificate date), National Cryptologic Centre (CCN)

[44] Certification Report CCN-CC/2022-46/INF-4163 for Giesecke+Devrient (China) Technologies Co. Ltd., Huangshi Branch (GDCHINA HS), related to CCN-CC-31/2023, 18 August 2023 (Certificate date), National Cryptologic Centre (CCN)

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC Part 1 chapter 10.5.
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1.
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8.
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12.
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17.
- The table in CC Part 3, Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/.

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document

Annex B: Evaluation results regarding development and production environment

Annex C: Overview and rating of cryptographic functionalities implemented in the TOE

Annex B of Certification Report BSI-DSZ-CC-1243-2024

Evaluation results regarding development and production environment

The IT product STARCOS 3.7 COS GKV C2 (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 Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 22 August 2024, 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 Development Center Germany (DCG) for Development and Testing. Refer to the Certification Report BSI-DSZ-CC-S-0260-2023 ([39]).

b) Giesecke+Devrient Development Center Spain (DCS) for Development. Refer to the Certification Report CCN-CC/2022-53/INF-4095 and maintenance report CCN-CC/2023-21/INF-4149 ([40]).

c) Linxens Singapore Changi Site for Module Production. Refer to the Certification Report CCN-CC/2023-01/INF-4274 ([41]).

d) INESA Shanghai, INESA Intelligent Electronics Co. Ltd. for Module Production. Refer to the Certification Report NSCIB-SS-2300084-01 ([42]).

e) Giesecke+Devrient Mobile Security Iberia (GDIMS) for Production (in particular Inlay Embedding) and Initialisation. Refer to the Certification Report CCN-CC/2022-01/INF-3825 ([43]).

f) Giesecke+Devrient (China) Technologies Co. Ltd., Huangshi Branch (GDCHINA HS) for Production (in particular Inlay Embedding) and Initialisation. Refer to the Certification Report CCN-CC/2022-46/INF-4163 ([44]).

g) For development and production sites regarding the underlying IC platform please refer to the Certification Report BSI-DSZ-CC-1110-V6-2023 ([19]).

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.

Annex C of Certification Report BSI-DSZ-CC-1243-2024

Overview and rating of cryptographic functionalities implemented in the TOE

No.	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)	[24], [25] (RSA) [26] (SHA)	Modulus length = 2048, 3072	[21], chap. 6.6.3.1 [23]	FCS_COP.1/ COS.RSA.S (PSO COMPUTE DIGITAL SIGNATURE) FCS_COP.1/SHA
2		ECDSA signature generation using SHA-{256, 384, 512}	[27], [33](ECDSA) [26] (SHA)	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [30] and ansix9p{256, 384}r1 [33]	[21], chap. 6.6.3.2 [23]	FCS_COP.1/ COS.ECDSA.S (PSO COMPUTE DIGITAL SIGNATURE) FCS_COP.1/SHA
3		ECDSA signature verification using SHA-{256, 384, 512}	[27], [33] (ECDSA) [26] (SHA)	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [30] and ansix9p{256, 384}r1 [33]	[21], chap. 6.6.4.2 [23]	FCS_COP.1/ COS.ECDSA.V (PSO VERIFY CERTIFICATE PSO VERIFY DIGITAL SIGNATURE) FCS_COP.1/SHA
4		SHA-256 based fingerprint	[26]	-	[21], chap. 6.6.1.3	FPT_ITE.1 (FINGERPRINT)
5	Authentication	AES in CBC mode	[29] (AES) [31] (CBC) [21]	|k| = 128, 192, 256 |challenge| = 64	[21], chap. 6.7.1.2, 6.7.2.2 [23]	FCS_COP.1/ COS.AES (MUTUAL AUTHENTICATE GENERAL AUTHENTICATE)
6		AES in CMAC mode	[29] (AES) [32], [23], chap. 3.6.2 (CMAC) [21]	|k| = 128, 192, 256 |challenge| = 64	[21], chap. 6.6.1, 6.6.2 [23], chap. 3.6.2	FCS_COP.1/ COS.CMAC (MUTUAL AUTHENTICATE)
7		RSA signature generation (RSASSA-PSS-SIGN with SHA-256, RSASSA PKCS1-V1_5)	[24] (RSA) [26] (SHA)	Modulus length = 2048, 3072	[21], chap. 6.6.3.1 [23]	FCS_COP.1/ COS.RSA.S (INTERNAL AUTHENTICATE) FCS_COP.1/SHA

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
8		ECDSA signature generation using SHA-{256, 384, 512}	[27], [33] (ECDSA) [26] (SHA)	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [30] and ansix9p{256, 384}r1 [33]	[21], chap. 6.6.3.2 [23]	FCS_COP.1/ COS.ECDSA.S (INTERNAL AUTHENTICATE) FCS_COP.1/SHA
9		ECDSA signature verification using SHA-{256, 384, 512}	[27], [33] (ECDSA) [26] (SHA)	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [30] and ansix9p{256, 384}r1 [33]	[21], chap. 6.6.4.2 [23]	FCS_COP.1/ COS.ECDSA.V (EXTERNAL AUTHENTICATE) FCS_COP.1/SHA
10		PACEv2	[35] (PACEv2)	Length of nonce: 128	[21] [35] [23]	Package Contactless FIA_UAU.5/ PACE.PICC FIA_UAU.6/ PACE.PICC FIA_USB.1/ PACE.PICC (GENERAL AUTHENTICATE)
11	Key Agreement	Key Derivation Function for AES based on SHA-{1, 256}	[27], chap. 4.3.3 [29] (AES) [26] (SHA)	|k| = 128, 192, 256	[21], chap. 6.2.2, 6.2.3, 6.2.4	FCS_CKM.1/ AES.SM (within authentication) FCS_COP.1/SHA
12		ECDH	[27], chap. 4.3.1, [34] (ECDH)	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [30]	[21] [27]	Package Contactless FCS_CKM.1/ DH.PACE.PICC id-PACE-ECDH-GM-AES-CBC-CMAC-128 id-PACE-ECDH-GM-AES-CBC-CMAC-192 id-PACE-ECDH-GM-AES-CBC-CMAC-256
13	Confidentiality	AES in CBC mode	[29] (AES) [31] (CBC) [21]	|k| = 128, 192, 256	[21], chap. 6.7.1.2, 6.7.2.2 [23], chap. 3.3.1	FCS_COP.1/ COS.AES (Secure messaging)
14		AES in CBC mode	[29] (AES) [31] (CBC) [21]	|k| = 128, 192, 256	[35], Part 2 [21], chap. 6.7.1.2, 6.7.2.2	Package Contactless FCS_COP.1/ PACE.PICC.ENC

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
					[23], chap. 3.3.1	(Secure messaging for PACE)
15		RSA encryption and decryption (RSA-OAEP) Transcipher RSA to ELC and ELC to RSA	[21] [24], chap. 7.1.1, 7.1.2	Modulus length = 2048, 3072 for RSA private key operation and 2048 for RSA public key operation	[21], chap. 6.8.1, 6.8.2 [23]	FCS_COP.1/ COS.RSA (PSO ENCIPHER PSO DECIPHER PSO TRANSCIPHER) For the ELC part of PSO TRANSCIPHER see FCS_COP.1/COS. ELC in row 16.
16		ELC encryption and decryption Transcipher RSA to ELC and ELC to RSA	[21] [27]	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [30] and ansix9p{256, 384}r1 [33]	[21], chap. 6.8.1, 6.8.2 [23]	FCS_COP.1/ COS.ELC (PSO ENCIPHER PSO DECIPHER PSO TRANSCIPHER) For the RSA part of PSO TRANSCIPHER see FCS_COP.1/COS. RSA in row 15.
17	Integrity	AES in CMAC mode	[29] (AES) [32], [23], chap. 3.6.2 (CMAC) [21]	|k| = 128, 192, 256	[21], chap. 6.6.1, 6.6.2 [23], chap. 3.6.2	FCS_COP.1/ COS.CMAC (Secure messaging)
18		AES in CMAC mode	[29] (AES) [32], [23], chap. 3.6.2 (CMAC) [21]	|k| = 128, 192, 256	[21], chap. 6.6.1, 6.6.2 [23], chap. 3.6.2	Package Contactless FCS_COP.1/ PACE.PICC.MAC (Secure messaging for PACE)
19	Cryptographic Primitive	Hybrid deterministic RNG DRG.4	[36] with developer specific enhancements [4, AIS 20]	n.a.	[23]	FCS_RNG.1
20		Hybrid deterministic RNG DRG.4	[36] with developer specific enhancements [4, AIS 20]	n.a.	[23]	Package Contactless FCS_RNG.1/ PACE (GENERAL AUTHENTICATE)
21		Physical RNG PTG.2	[4, AIS 31]	n.a.	[23]	FCS_RNG.1/SICP FCS_RNG.1/GR

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
22		SHA-{1, 256, 384, 512}	[26]	-	[21], chap. 3.2.1 [23]	FCS_COP.1/SHA
23		SHA-{1, 224, 256, 384, 512}	[26]	-	[21] [23]	FCS_COP.1/ CB_HASH (PSO HASH)
24	Key Generation	RSA key generation	n.a.	Modulus length = 2048, 3072	[21]	Package RSA Key Generation FCS_CKM.1/RSA (PSO GENERATE ASYMMETRIC KEY PAIR)
25		ECC key generation	n.a.	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [30] and ansix9p{256, 384}r1 [33]	[21]	FCS_CKM.1/ELC (PSO GENERATE ASYMMETRIC KEY PAIR)

Table 5: TOE cryptographic functionality

Note: End of report