Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0904-V2-2021

for

TCOS FlexCert Version 2.0 Release 2/SLC52

from

Deutsche Telekom Security 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-0904-V2-2021 (*)

eHealth: Smart Cards

TCOS FlexCert Version 2.0 Release 2/SLC52

from	Deutsche Telekom Security 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

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, 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, 24 June 2021

For the Federal Office for Information Security

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

Sandro Amendola
Head of Division

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 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 (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[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+ ALC_FLR components.

[4] Proclamation of the Bundesministerium des Innern 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 TCOS FlexCert Version 2.0 Release 2/SLC52 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0904-2015. Specific results from the evaluation process BSI-DSZ-CC-0904-2015 (including subsequent maintenance procedures BSI-DSZ-CC-0904-2015-MA-01 and BSI-DSZ-CC-0904-2015-MA-02) were re-used.

The evaluation of the product TCOS FlexCert Version 2.0 Release 2/SLC52 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 2 June 2021. 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: Deutsche Telekom Security GmbH.

The product was developed by: Deutsche Telekom Security 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 24 June 2021 is valid until 23 June 2026. Validity can be re-newed 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

[5] Information Technology Security Evaluation Facility

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 TCOS FlexCert Version 2.0 Release 2/SLC52 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] Deutsche Telekom Security GmbH
Bonner Talweg 100
53113 Bonn
Germany

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 TCOS FlexCert Version 2.0 Release 2/SLC52 developed by Deutsche Telekom Security GmbH.

The TOE is a smart card product according to the G2-COS specification [18] from gematik and is implemented on the hardware platform Infineon Security Controller IFX_CCI_000010h (SLC52GDA600A8 / SLC52GDA600A9) from Infineon Technologies AG (refer to [15], [16]).

The TOE is intended to be used as a card operating system platform for cards 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 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_000010h (SLC52GDA600A8 / SLC52GDA600A9)),
- the IC Embedded Software (TCOS FlexCert Version 2.0 Release 2/SLC52 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 [18], 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 (TCOS FlexCert Version 2.0 Release 2/SLC52 Operating System) is implemented according to the G2-COS specification [18] from gematik. Hereby, the TOE implements the mandatory part of the

G2-COS specification [18] with the base functionality of the operating system platform. In addition, the TOE implements the option RSA Key Generation (“Option_RSA_-KeyGeneration”), the option Contactless (“Option_kontaktlose_Schnittstelle”), the option Crypto Box (“Option_Kryptobox”) and the option Logical Channel (“Option_logische_-Kanäle“) as defined in the G2-COS specification [18]. None of the further options PACE for Proximity Coupling Device (“Option_PACE_PCD”), USB (“Option_USB_Schnittstelle”) and RSA CVC (“Option_RSA_CVC”) defined in the G2-COS specification [18] is implemented in the TOE.

Furthermore, the TOE provides developer-specific administration commands for support of the TOE’s life cycle model (refer to the user guidance [10], chapter 6 and [12], chapter 4).

The TOE's Wrapper is implemented according to the Wrapper specification [19] from gematik.

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 [7]. The Security Target [6] uses the mandatory parts of the PP and the optional packages RSA Key Generation, Contactless, Crypto Box and Logical Channel defined in the PP. None of the PP’s further optional packages 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], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

- General Protection of User Data and TSF Data:

  The access to user data is restricted by defined rules laid down in the respective object system. The TOE enforces these access rules, but there is no a priori protection of a said object. The access rights may be provided by certificates. The TOE is able to interpret these certificates accordingly.

  The TOE provides export functionality for non-sensitive but important user data and TSF data. The export using the wrapper tool allows checking the access rules and other security attributes of an implemented object system and its objects. The fingerprint command allows the integrity and authenticity check of the TOE implementation.

  The TOE runs self-tests during initial start-up to ensure the correct function of the TSF.

  Residual information of sensitive data in previously used resources will not be available after its usage. Session keys and message authentication keys will be destroyed after reset or termination of the secure messaging channel. The TOE hides the correlation of power or timing variations and the command execution accessing sensitive user data as different keys and passwords. In case of a malfunction, operating errors or integrity check failures the TOE enters a secure

state. This is supported by the functional services of the hardware.

The TOE executes self-tests to demonstrate the correct operation of the TSF and its confidentiality protection capabilities. In case of failures, the preservation of a secure state is guaranteed.

- Identification and Authentication:

  The protocols for identification and authentication of users and devices are described in the G2-COS specification [18].

  The security and the reliability of the identification and authentication are supported by the correct key agreement and the quality of random numbers. This concerns also the authentication via the contactless interface. As the authentication state is left, the session keys cannot be used anymore.

  The user is authenticated by means of PINs and PUCs, which are bounded to corresponding failure or usage counters. The device is authenticated by using a correct key which is derived from the provided certificate and the authentication context.

  Before a user or device is identified only dedicated commands can be executed.

  The TOE maintains security attributes according to the G2-COS specification [18] beside the identity of user and device.

  The authentication commands are implemented as required by the G2-COS specification [18].

- Access Control:

  The access to user data is restricted. The access to the TOE security functions and the TSF data is controlled by several functionalities.

  The management of the authentication data and corresponding security attributes is implemented in accordance with the G2-COS specification [18]. The TOE does not allow the export of session and authentication keys, passwords and other sensitive user and TSF data specified as such in the object system. Note that the TOE enforces the access rights of elements of the object system, i.e. data specified as unprotected will be exposed by the TOE.

- Cryptographic Functions:

  The TOE provides a hybrid deterministic random number generator of class DRG.4. It is based on a random number generator of class PTG.2 provided by the hardware. Note that a generator of class PTG.2 is unpredictable but may have a small bias. The random numbers returned in the GET RANDOM command are based on a PTG.3, where additionally to the PTG.2 an extra post-processing algorithm is applied, which does not reduce the entropy of the input but removes any bias. The random numbers used in the PACE protocol and by the GET CHALLENGE command are generated by the implemented random number generator of class DRG.4.

  The TOE implements cryptographic checksum functions, including hash functions used for signature verification and key derivation and message authentication codes (MACs).

  The TOE provides the symmetric encryption algorithm AES with standardized key

lengths of 128, 192 and 256 bits.

The TOE implements asymmetric crypto algorithms used for encryption/decryption, key agreement and digital signatures based on RSA and elliptic curves. The selection of the curve used for ECC based algorithms might be a security issue. The TOE supports only the curves defined in [23] and [24], that are required by the G2-COS specification [18].

Cryptographic keys are explicitly deleted by overwriting the memory data with zeros or random numbers, e.g. the new key.

- Protection of Communication:

  The secure data exchange in a trusted channel is required. This is supported by cryptographic operations. The TOE enforces a protected communication over the contactless interface by means of the PACE protocol.

  The randomness of the parameters of the PACE protocol is guaranteed by the RNG class DRG.4.

  The strength of algorithms for ensuring confidentiality and integrity is supplied.

- Accuracy of the TOE security functionality / Self-protection:

  The operating system of the TOE protects the security functionality of the TOE as soon as it installed and completed (before TOE delivery). The TOE will not emit physical or logical data information on security user data outside the secure channels controlled by the operating system. User data and TSF data are protected by the TOE if processed or transferred within different parts of the TOE according to the TOE Data Processing Policy.

  The TOE will resist physical manipulation and probing and enter a secure state in case of a failure. This functionality is supported also by the hardware, which was approved in a separate evaluation process.

  To protect the TOE against malfunction the operating conditions must be in the tolerated ranges.

  Dedicated test software is no more available after the TOE is finished. These functions are disabled for the TOE.

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

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. 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], chapter 3.2, 3.3 and 3.4.

This certification covers the configuration 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:

TCOS FlexCert Version 2.0 Release 2/SLC52

The following table outlines the TOE deliverables:

No.	Type	Identifier	Release	Type / Form of Delivery
1	HW/SW	IFX Secure Smart Card Controller SLC52 (design step G12) including its IC Dedicated Support Software (refer to the Certification Report BSI-DSZ-CC-1079-V2-2020 [16])	IFX_CCI_000010h (SLC52GDA600A8 / SLC52GDA600A9) ROM Masks: TCOS30_SLC52_ROM_And_NVM_GDA600A8.hex / TCOS30_SLC52_ROM_And_NVM_GDA600A9.hex	Smart card or module (type: M8.8 / COM10.8) Two module types are used for the TOE, they only differ in their antenna capacitance. For each module type a separate flash image exists, however the fingerprint is the same for both images. The hardware part of the TOE is delivered in an insured parcel to the Installation Agent. The TOE is protected in Phase 6 of the TOE's life cycle model by an authentication procedure.
2	SW	IC Embedded Software: TCOS FlexCert Version 2.0 Release 2/SLC52 Operating System including completion data	OS Version: '01 B8' Completion Code Version: '00' (refer to Table 2)	Implemented in ROM/EEPROM of the IC
3	DOC	TCOS FlexCert Version 2.0 Release 2, Administrator's Guidance, Guidance Documentation of TCOS FlexCert Version 2.0 Release 2 [10]	Version 1.0	Document in electronic form (encrypted and signed)
4	DOC	TCOS FlexCert Version 2.0 Release 2, Operational Guidance – Part 1, Guidance Documentation of TCOS FlexCert Version 2.0 Release 2 [11]	Version 1.0	Document in electronic form (encrypted and signed)
5	DOC	TCOS FlexCert Version 2.0 Release 2, Operational Guidance – Part 2, Guidance Documentation of TCOS FlexCert Version 2.0 Release 2 [12]	Version 1.0	Document in electronic form (encrypted and signed)
6	DOC	Anforderungen an den Antennenfertiger/Einbetter	Version 0.4	Document in electronic form

No.	Type	Identifier	Release	Type / Form of Delivery
		von Modulen mit TCOS FlexCert [14]		(encrypted and signed)
7	SW	Wrapper	TCOSeHealthWrapperLib.jar lib\ jdom-2.0.4.jar in ZIP-Archive TCOSeHealthWrapperLib.zip	File (encrypted and signed) The integrity and authenticitiy of the Wrapper is given by the following SHA-256 hash value: CA2FC637967EF9C8BF0DF111C96FBEF71BB540DEB9907C128D81EF80D4840185
8	DOC	TCOS FlexCert Version 2.0 Release 2, Guidance, Guidance Documentation of the Wrapper to TCOS FlexCert Version 2.0 Release 2 [13]	Version 1.0	Document in electronic form (encrypted and signed)
9	DATA	Text files with FORMAT-command APDUs (for opening of Phases 6 and 7 of the TOE's life cycle model)	---	Text files in electronic form (encrypted and signed)
10	DATA	Authentication Key	--- (customer-specific key)	Text file in electronic form (encrypted and signed)

Table 1: Deliverables of the TOE

The TOE TCOS FlexCert Version 2.0 Release 2/SLC52 is as well known under the following product identificator:

Manufacturer: '54 53 59 53 49 ' (TSYSI)

Product: "54 43 4F 53 46 43 32 30' (TCOSFC20)

OS Version Number: '02 02 03' (2.2.3)

According to the Security Target [6], chapter 1.4.4 the life cycle model of the TOE consists of the following 7 phases:

Phase 1: Smartcard embedded software development

Phase 2: IC Development

Phase 3: IC manufacturing and testing

Phase 4: IC packaging and testing

Phase 5: Smartcard product finishing process

Phase 6: Smartcard personalization (including object system installation and personalisation)

Phase 7: Smartcard end-usage

The finalised TOE is a chip with completed IC Embedded Software and may be of type module or smart card depending on the chosen production variant. Hereby, the TOE delivery in the sense of the CC takes place at the end of Phase 5 after completion of the IC Embedded Software by the COS-Installation Agent so that the evaluation process is

limited to Phases 1 to 5 up to the finalisation of the completion process in Phase 5. Independent of the different production variants and TOE form factor the TOE is delivered by Deutsche Telekom Security GmbH at the end of Phase 5 to the OS-Initialization Agent (acting in Phase 6) as already embedded 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 guidance [10], chapter 6.1.1.1 and [12], chapter 7.7. The TOE can be identified by using the command FORMAT (only in Phase 6 of the TOE's life cycle model) respective the command GET CARD INFO (in Phases 6 and 7 of the TOE's life cycle model). Via the command FORMAT (CLA = ‘B0’, INS = ‘50’ with P1 = '00' and P2 = '00') respective the command GET CARD INFO (CLA = '80', INS = 'AA' with P1 = '06' and P2 = '00') the user can read out the chip information and identify the underlying chip as well as the TCOS FlexCert Version 2.0 Release 2/SLC52 Operating System (including completion data) installed in the chip. In order to open the Personalization Phase for object system installation and personalisation of the installed object system (Phase 6 of the TOE's life cycle model) a mutual authentication via the command FORMAT as described in the user guidances [10], chapter 6.1.1.4 and [12], chapter 4.1.4 is necessary, therefore the authenticity of the TOE is verified before further usage of the TOE.

The following identification data can be retrieved within a 16 Byte string responded by the commands FORMAT respective GET CARD INFO:

Byte	Product information	Value
1	Indicator of the chip manufacturer according to ISO 7816-6	'05'
2	Chip Type (Type ID of the chip manufacturer)	'22'
3 - 8	Unique identification number for the chip	chip dependent
9	Card type	'06'
10-11	Operating system version (ROM mask version)	'01 B8'
12	Version of the pre-completion code / completion code for finalizing the operating system	'00'
13	'00' (RFU: File system version)	'00'
14	'00' (RFU)	'00'
15	'00' (RFU)	'00'
16	Authentication key identifier	key dependent

Table 2: TOE Identification via the commands FORMAT respective GET CARD INFO

The command FORMAT with its parameters is described in [10], chapter 6.1.1.1. Information on the command GET CARD INFO and its parameters can be found in [12], chapter 7.7.

Note that Bytes 3 – 8 (Unique identification number for the chip) are chip specific data which differ for each chip used in the TOE. Byte 16 (Authentication key identifier) is customer specific data and differs for each different authentication key. The authentication key can also be changed by the installation or personalisation agent, which results in changing the authentication key identifier as well. Therefore, the unique identification number for the chip and the authentication key identifier are not specified in the table above.

3. Security Policy

The TOE is a composite smart card product, based on the hardware platform Infineon Security Controller IFX_CCI_000010h (SLC52GDA600A8 / SLC52GDA600A9) from Infineon Technologies AG and with IC Embedded Software TCOS FlexCert Version 2.0 Release 2/SLC52 Operating System implemented by Deutsche Telekom Security GmbH according to the G2-COS specification [18] 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 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 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], chapter 6.

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,

Security Objectives for the operational environment defined in the Security Target	Description according to the ST
	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.
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.LogicalChannel	Use of logical channels The operational environment manages logical channels bound to independent subjects for running independent processes at the same time.

Table 3: Security Objectives for the operational environment

Details can be found in the Security Target [6], chapter 4.2.

5. Architectural Information

The TOE is set up as a composite product. It is composed of the Infineon Security Controller IFX_CCI_000010h (SLC52GDA600A8 / SLC52GDA600A9) from Infineon Technologies AG and the IC Embedded Software with the TCOS FlexCert Version 2.0 Release 2/SLC52 Operating System developed by Deutsche Telekom Security 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 Deutsche Telekom Security GmbH.

For details concerning the CC evaluation of the underlying IC see the evaluation documentation under the Certification ID BSI-DSZ-CC-1079-V2-2020 ([15], [16]).

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

- Hardware: Underlying IC including its IC Dedicated Support Software.
- Kernel: Management of the interfaces between all components.
- Crypto Component: Processing the cryptographic functions.
- Admin Component: Processing administrative base functions.
- IO Component: Controlling the input and output.
- ROM TCOS-Type Task: APDU processing (system, applications).
- Wrapper: Export and re-coding of non-confidential TSF and user data.

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].

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 of possible parameters including all boundary values of the parameter set was tested, e.g. all command APDUs with valid and invalid inputs were tested and all functions were 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 the PACE-protocol,
- penetration testing related to the verification of the reliability of the TOE,
- source code analysis performed by the evaluators,
- side channel analysis including machine learning methods for SHA, RSA and ECC, including RSA and ECC key generation,
- fault injection attacks (laser and EM attacks),

- testing APDU commands for the object system installation / 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]:

TCOS FlexCert Version 2.0 Release 2/SLC52

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_000010h (SLC52GDA600A8 / SLC52GDA600A9) from Infineon Technologies AG. This IC is certified under the Certification ID BSI-DSZ-CC-1079-V2-2020 (refer to [16]).

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 Deutsche Telekom Security GmbH.

The TOE covering the IC and the IC Embedded Software (TCOS FlexCert Version 2.0 Release 2/SLC52 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 FORMAT (only in Phase 6 of the TOE's life cycle model) and the command GET CARD INFO (in Phases 6 and 7 of the TOE's life cycle model) according to the user guidance [10], chapter 6.1.1.1 and [12], chapter 7.7. See chapter 2 of this Certification Report for details.

9. Results of the Evaluation

9.1. CC specific results

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

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 the guidance documents covered by [16]) and the document ETR for composite evaluation from the IC's evaluation ([17]) 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 EAL5+ and EAL6 (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-0904-2015 (including subsequent maintenance procedures BSI-DSZ-CC-0904-2015-MA-01 and BSI-DSZ-CC-0904-2015-MA-02), re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the change of the underlying IC platform, on functional and security-related changes in the TOE's (crypto) implementation as well as on changes of the TOE life cycle model. In particular, the TOE's (crypto) implementation was re-evaluated and re-assessed.

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] uses the mandatory parts of the PP and the optional packages RSA Key Generation, Contactless, Crypto Box and Logical Channel defined in the PP. None of the PP's further optional packages 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 [18] and the Technical Guideline BSI TR-03116-1 [22] 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 the framework of the German health care system. In particular, the card operating system platform is intended for use by 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 currently specified by gematik. The validity period of each algorithm is mentioned in the official catalogue [22].

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 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 [10] to [14] 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 ([20]):

- 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 production files containing such object system by the developer. As well this concerns on the other hand after TOE delivery the application developers and card management e.g. by using the command LOAD APPLICATION.

  The TOE implements a specific access rule concept, in particular concerning the default settings for access rules by the TOE itself and the flexibility to define customer-specific access rules. Refer to the user guidances [12], Annex A and [13], chapter 2.2.

  For an object system, one has to take care of the choice of the access rules 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 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 are set appropriately for read access.

  For card products that undergo a later TR-conformity testing according to the Technical Guideline BSI TR-03144 ([20]) it is strongly recommended to care for the appropriate choice of the access rules for all object system's objects. It shall be possible for the Konsistenz-Prüftool according to the Technical Guideline BSI TR-03143 ([21]) 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, their specific processing by the TOE and their handling in combination with the TOE's specific access rule concept (see above) are of relevance for object systems intended to run on the TOE.

  Any object system set up on the TOE shall only make use of the TOE's functionality as described in the G2-COS specification [18] and the user guidance [10], [11] and [12]. 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. In particular, this means looking for exceptions thrown by the Wrapper as well as 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. Refer in particular to the user guidance [12], chapter 10.5.

- Security requirements and hints for Phase 5 (concerning the antenna production), Phase 6 (concerning the installation and personalisation of object systems on the TOE by the OS-Initialization Agent respective Personalisation Agent) and for Phase 7 (for end-usage) of the TOE's life cycle model:

  Refer to the user guidances [14], [10], in particular chapter 5 and 7, [12], chapter 10.5.

- The TOE's Wrapper and its specifics beyond the Wrapper specification [19], in particular concerning manufacturer specific attributes exported by the Wrapper:

  Refer to the user guidance [13].

- For security instructions related to the secure use of the TOE:

  Refer to the user guidance [12], chapter 10. In particular, the following aspects need to be taken into account:

  Restrictions for key usage. Refer to the user guidance [12], chapter 10.5.

  Uniqueness of key identifier. Refer to the user guidance [13], chapter 2.1.

- For the design and generation of production files containing an object system for card products that undergo a later TR-conformity testing according to the Technical Guideline BSI TR-03144 ([21]) it is strongly recommended to care for that via the card product's personalisation 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 ([20]) 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 [19]. 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. It shall be possible for the Konsistenz-Prüftool according to the Technical Guideline BSI TR-03143 ([21]) 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 10.5 and Annex A, [13], chapter 2.2.

  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 ([20]).

- Any object system set up on the TOE shall only make use of the TOE's functionality as described in the G2-COS specification [18] and the user guidances [10], [11] and [12].

The card product's object system has to be manually 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. In particular, this means looking for exceptions thrown by the Wrapper as well as looking for information provided via the Wrapper that indicates the use of proprietary (uncertified) COS functionality in the card product.

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 ([21]) 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 ([20]).

- For the card product, it has to be checked that via the card product's personalisation 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 card product's personalisation 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 ([20]).
- If in the framework of the TR-conformity testing of a card product according to the Technical Guideline BSI TR-03144 ([20]) the Konsistenz-Prüftool according to the Technical Guideline BSI TR-03143 ([21]) 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 [18] or the user guidances [10], [11] and [12] this has to be manually examined and valuated.
- For card products that undergo a TR-conformity testing according to the Technical Guideline BSI TR-03144 ([21]), the OS identification data retrieved via the command FORMAT or GET CARD INFO 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 [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

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
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

[6] Security Target BSI-DSZ-CC-0904-V2-2021, Specification of the Security Target TCOS FlexCert Version 2.0 Release 2/SLC52, Version 2.0.2, 25 May 2021, Deutsche Telekom Security GmbH

[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) und ITSEC
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 23, Version 4, Zusammentragen von Nachweisen der Entwickler
- 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 38, Version 2.9, Reuse of evaluation results

[7] 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)

[8] ETR BSI-DSZ-CC-0904-V2-2021, Evaluation Technical Report (ETR) – Summary for TCOS FlexCert Version 2.0 Release 2/SLC52, Version 1.1, 2 June 2021, SRC Security Research & Consulting GmbH (confidential document)

[9] Configuration List BSI-DSZ-CC-0904-V2-2021, Konfigurationsliste von TCOS FlexCert Version 2.0 Release 2/SLC52, Version 0.92, 26 May 2021, Deutsche Telekom Security GmbH (confidential document)

[10] TCOS FlexCert Version 2.0 Release 2, Administrator's Guidance, Guidance Documentation of TCOS FlexCert Version 2.0 Release 2, Version 1.0, 26 May 2021, Deutsche Telekom Security GmbH

[11] TCOS FlexCert Version 2.0 Release 2, Operational Guidance – Part 1, Guidance Documentation of TCOS FlexCert Version 2.0 Release 2, Version 1.0, 26 May 2021, Deutsche Telekom Security GmbH

[12] TCOS FlexCert Version 2.0 Release 2, Operational Guidance – Part 2, Guidance Documentation of TCOS FlexCert Version 2.0 Release 2, Version 1.0, 26 May 2021, Deutsche Telekom Security GmbH

[13] TCOS FlexCert Version 2.0 Release 2, Guidance, Guidance Documentation of the Wrapper to TCOS FlexCert Version 2.0 Release 2, Version 1.0, 26 May 2021, Deutsche Telekom Security GmbH

[14] Anforderungen an den Antennenfertiger/Einbetter von Modulen mit TCOS FlexCert, Version 0.4, 5 June 2015, T-Systems International GmbH

[15] Security Target of the underlying hardware platform, Confidential Security Target Common Criteria v3.1 – EAL6 augmented / EAL6+, IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch G12, Revision 1.3, 3 April 2020, Infineon Technologies AG, BSI-DSZ-CC-1079-V2-2020 (confidential document)

Security Target Lite of the underlying hardware platform, Public Security Target Common Criteria v3.1 – EAL6 augmented / EAL6+, IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch G12, Revision 0.8, 3 April 2020, Infineon Technologies AG, BSI-DSZ-CC-1079-V2-2020 (sanitised public document)

[16] Certification Report BSI-DSZ-CC-1079-V2-2020 for Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 and including optional software libraries and dedicated firmware, BSI-DSZ-CC-1079-V2-2020, 16 June 2020, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[17] ETR for Composite Evaluation of the underlying hardware platform Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 and including optional software libraries and dedicated firmware from certification procedure BSI-

DSZ-CC-1079-V2-2020, Version 2, 15 May 2020, TÜV Informationstechnik GmbH (confidential document)

[18] Einführung der Gesundheitskarte, Spezifikation des Card Operating System (COS), Elektrische Schnittstelle, Version 3.13.1, 01.11.2019, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[19] Einführung der Gesundheitskarte, Spezifikation Wrapper, Version 1.8.0, 24.08.2016, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[20] Technische Richtlinie BSI TR-03144 eHealth – Konformitätsnachweis für Karten-Produkte der Kartengeneration G2, Version 1.2, 27.07.2017, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[21] Technische Richtlinie BSI TR-03143 eHealth – G2-COS Konsistenz-Prüftool, Version 1.1, 18.05.2017, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[22] Technische Richtlinie BSI TR-03116-1: Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1 – Telematikinfrastruktur, Version 3.20, 21.09.2018, Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

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

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 detailled 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 [6] 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-0904-V2-2021

Evaluation results regarding development and production environment

The IT product TCOS FlexCert Version 2.0 Release 2/SLC52 (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 24 June 2021, 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) Deutsche Telekom Security GmbH, Untere Industriestraße 20, D-57250 Netphen-Dreis-Tiefenbach (Development and Production)

b) exceet Card AG Niederlassung Unterschleißheim, Edisonstraße 3, D-85716 Unterschleißheim (Card Embedding)

c) For development and production sites regarding the underlying IC platform please refer to the Certification Report BSI-DSZ-CC-1079-V2-2020 ([16]).

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. 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]) are fulfilled by the procedures of these sites.

Annex C of Certification Report BSI-DSZ-CC-0904-V2-2021

Overview and rating of cryptographic functionalities implemented in the TOE

#	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-SIGN, RSA ISO9796-2 DS2 SIGN with SHA-256)	[PKCS#1], chap. 8.1.1, 8.2.1, 9.1.1, 9.2, [ISO 9796-2] (RSA) [FIPS 180-4] (SHA)	Modulus length = 2048, 3072	[G2 COS], chap. 6.6.3.1 [TR-03116-1]	FCS_COP.1/COS.RSA.S (PSO COMPUTE DIGITAL SIGNATURE) FCS_COP.1/SHA
2		ECDSA signature generation using SHA-{256, 384, 512}	[TR-03111], [ANSI X9.63] (ECDSA)	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [RFC 5639] and ansix9p{256, 384}r1 [ANSI X9.62]	[G2 COS], chap. 6.6.3.2 [TR-03116-1]	FCS_COP.1/ COS.ECDSA.S (PSO COMPUTE DIGITAL SIGNATURE) Note: The hash value is given within the command data of PSO COMPUTE DIGITAL SIGNATURE.
3		ECDSA signature verification using SHA-{256, 384, 512}	[TR-03111], [ANSI X9.63] (ECDSA) [FIPS 180-4] (SHA)	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [RFC 5639] and ansix9p{256, 384}r1 [ANSI X9.62]	[G2 COS], chap. 6.6.4.2 [TR-03116-1]	FCS_COP.1/ COS.ECDSA.V (PSO VERIFY CERTIFICATE PSO VERIFY DIGITAL SIGNATURE) FCS_COP.1/SHA Note: There is no hash computation by the TOE in case of PSO VERIFY DIGITAL SIGNATURE as the hash value is given within the command data.
4		AES CMAC based fingerprint	[FIPS 197] (AES) [SP800-38B] (CMAC)	|k| = 128	[G2 COS], chap. 6.6.1.3, 14.9.2	FPT_ITE.1 (FINGERPRINT)
5	Authentication	AES in CBC mode	[FIPS 197] (AES) [SP800-38A] (CBC) [G2 COS], chap. 6.7.1.2, 6.7.2.2	|k| = 128, 192, 256 |challenge| = 64	[G2 COS], chap. 6.7.1.2, 6.7.2.2 [TR-03116-1]	FCS_COP.1/COS.AES (MUTUAL AUTHENTICATE GENERAL AUTHENTICATE)
6		AES in CBC mode	[FIPS 197]	|k| = 128, 192,	[G2 COS],	*package Crypto Box:*

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
			(AES) [SP800-38A] (CBC) [G2 COS], chap. 6.7.1.2, 6.7.2.2	256 |challenge| = 64	chap. 6.7.1.2, 6.7.2.2 [TR-03116-1]	FCS_COP.1/CB.AES (EXTERNAL AUTHENTICATE INTERNAL AUTHENTICATE)
7		AES in CMAC mode	[FIPS 197] (AES) [SP800-38B], [TR-03116-1], chap. 3.6.2 (CMAC) [G2 COS], chap. 6.6.1, 6.6.2	|k| = 128, 192, 256 |challenge| = 64	[G2 COS], chap. 6.6.1, 6.6.2 [TR-03116-1], chap. 3.6.2	FCS_COP.1/COS.CMAC (MUTUAL AUTHENTICATE GENERAL AUTHENTICATE)
8		AES in CMAC mode	[FIPS 197] (AES) [SP800-38B], [TR-03116-1], chap. 3.6.2 (CMAC) [G2 COS], chap. 6.6.1, 6.6.2	|k| = 128, 192, 256 |challenge| = 64	[G2 COS], chap. 6.6.1, 6.6.2 [TR-03116-1], chap. 3.6.2	*package Crypto Box:* FCS_COP.1/CB.CMAC (EXTERNAL AUTHENTICATE INTERNAL AUTHENTICATE)
9		RSA signature generation (RSASSA-PSS-SIGN with SHA-256, RSASSA-PKCS1-V1_5-SIGN)	[PKCS#1], chap. 8.1.1, 8.2.1, 9.1.1, 9.2 (RSA) [FIPS 180-4] (SHA)	Modulus length = 2048, 3072	[G2 COS], chap. 6.6.3.1 [TR-03116-1]	FCS_COP.1/COS.RSA.S (INTERNAL AUTHENTICATE) FCS_COP.1/SHA
10		ECDSA signature generation using SHA-{256, 384, 512}	[TR-03111], [ANSI X9.63] (ECDSA)	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [RFC 5639] and ansix9p{256, 384}r1 [ANSI X9.62]	[G2 COS], chap. 6.6.3.2 [TR-03116-1]	FCS_COP.1/ COS.ECDSA.S (INTERNAL AUTHENTICATE) Note: The hash value is given within the command data of INTERNAL AUTHENTICATE.

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
11		ECDSA signature verification using SHA-{256, 384, 512}	[TR-03111], [ANSI X9.63] (ECDSA) [FIPS 180-4] (SHA)	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [RFC 5639] and ansix9p{256, 384}r1 [ANSI X9.62]	[G2 COS], chap. 6.6.4.2 [TR-03116-1]	FCS_COP.1/ COS.ECDSA.V (EXTERNAL AUTHENTICATE GENERAL AUTHENTICATE) FCS_COP.1/SHA Note: There is no hash computation by the TOE in case of EXTERNAL AUTHENTICATE as the hash value is given within the command data.
12		PACEv2	[TR-03110], Part 1 (PACEv2)	Length of nonce: 128 Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [RFC 5639]	[G2 COS] [TR-03110], Part 3 [TR-03116-1]	*package Contactless:* FIA_UAU.5/PACE.PICC FIA_UAU.6/PACE.PICC FIA_USB.1/PACE.PICC (GENERAL AUTHENTICATE)
13	Key Agreement	Key Derivation Function for AES based on SHA-{1, 256}	[TR-03111], chap. 4.3.3, 4.4.3 [FIPS 180-4] (SHA) [FIPS 197] (AES)	|k| = 128, 192, 256	[G2 COS], chap. 6.2.2, 6.2.3, 6.2.4, 6.2.5 [TR-03116-1] [TR-03110], Part 3	FCS_CKM.1/AES.SM (within authentication: MUTUAL AUTHENTICATE GENERAL AUTHENTICATE *package Crypto Box:* EXTERNAL AUTHENTICATE INTERNAL AUTHENTICATE *package Contactless:* GENERAL AUTHENTICATE (PACE)) FCS_COP.1/SHA
14		ECDH	[TR-03111], chap. 4.3.1 (ECDH)	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [RFC 5639]	[G2 COS], chap. 14.7.2.1, 14.7.2.7 [TR-03111]	*package Contactless:* FCS_CKM.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

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
15	Confidentiality	AES encryption and decryption in CBC mode	[FIPS 197] (AES) [SP800-38A] (CBC) [G2 COS], chap. 6.7.1.2, 6.7.2.2	|k| = 128, 192, 256	[G2 COS], chap. 6.7.1.2, 6.7.2.2 [TR-03116-1], chap. 3.3.1	FCS_COP.1/COS.AES (secure messaging)
16		AES encryption and decryption in CBC mode	[FIPS 197] (AES) [SP800-38A] (CBC) [G2 COS], chap. 6.7.1.2, 6.7.2.2	|k| = 128, 192, 256	[TR-03110], Part 2 [G2 COS], chap. 6.7.1.2, 6.7.2.2 [TR-03116-1], chap. 3.3.1	*package Contactless:* FCS_COP.1/ PACE.PICC.ENC (secure messaging for PACE)
17		AES encryption and decryption in CBC mode	[FIPS 197] (AES) [SP800-38A] (CBC) [G2 COS], chap. 6.7.1.2, 6.7.2.2	|k| = 128, 192, 256	[G2 COS], chap. 6.7.1.2, 6.7.2.2 [TR-03116-1], chap. 3.3.1	*package Crypto Box:* FCS_COP.1/CB.AES (PSO ENCIPHER PSO DECIPHER) (for trusted channel)
18		RSA encryption and decryption (RSA-OAEP) Transcipher RSA to ELC and ELC to RSA	[PKCS#1], chap. 7.1.1, 7.1.2 [G2 COS], chap. 6.8.1.2, 6.8.2.2	Modulus length = 2048, 3072 for RSA private key operation and 2048 for RSA public key operation	[G2 COS], chap. 6.8.1.2, 6.8.2.2 [TR-03116-1]	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 19.
19		ELC encryption and decryption Transcipher RSA to ELC and ELC to RSA	[TR-03111] [G2 COS], chap. 6.8.1.3, 6.8.2.3	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [RFC 5639] and ansix9p{256, 384}r1 [ANSI X9.62]	[G2 COS], chap. 6.8.1.3, 6.8.2.3 [TR-03116-1]	FCS_COP.1/COS.ELC (PSO ENCIPHER PSO DECIPHER PSO TRANSCIPHER GENERAL AUTHENTICATE) For the RSA part of PSO TRANSCIPHER see FCS_COP.1/COS.RSA in row 18.
20		RSA encryption (RSA-OAEP)	[PKCS#1], chap. 7.1.1 [G2 COS], chap. 6.8.1.2	Modulus length = 2048	[G2 COS], chap. 6.8.1.2 [TR-03116-1]	*package Crypto Box:* FCS_COP.1/CB.RSA (PSO ENCIPHER)

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
21		ELC encryption	[TR-03111], chap. 4.3.1, 4.3.3, 5.3.1.2 [G2 COS], chap. 6.8.1.3	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [RFC 5639] and ansix9p{256, 384}r1 [ANSI X9.62]	[G2 COS], chap. 6.8.1.3 [TR-03116-1]	*package Crypto Box:* FCS_COP.1/CB.ELC (PSO ENCIPHER)
22	Integrity	AES in CMAC mode	[FIPS 197] (AES) [SP800-38B], [TR-03116-1], chap. 3.6.2 (CMAC) [G2 COS], chap. 6.6.1, 6.6.2	|k| = 128, 192, 256	[G2 COS], chap. 6.6.1, 6.6.2 [TR-03116-1], chap. 3.6.2	FCS_COP.1/COS.CMAC (secure messaging)
23		AES in CMAC mode	[FIPS 197] (AES) [SP800-38B], [TR-03116-1], chap. 3.6.2 (CMAC) [G2 COS], chap. 6.6.1, 6.6.2	|k| = 128, 192, 256	[TR-03110], Part 2 [G2 COS], chap. 6.6.1, 6.6.2 [TR-03116-1], chap. 3.6.2	*package Contactless:* FCS_COP.1/ PACE.PICC.MAC (secure messaging for PACE)
24		AES in CMAC mode	[FIPS 197] (AES) [SP800-38B], [TR-03116-1], chap. 3.6.2 (CMAC) [G2 COS], chap. 6.6.1, 6.6.2	|k| = 128, 192, 256	[G2 COS], chap. 6.6.1, 6.6.2 [TR-03116-1], chap. 3.6.2	*package Crypto Box:* FCS_COP.1/CB.CMAC (PSO COMPUTE CRYPTOGRAPHIC CHECKSUM PSO VERIFY CRYPTOGRAPHIC CHECKSUM) (for trusted channel)
25	Trusted channel	Secure messaging in MAC-ENC mode	[G2 COS], chap. 13 [TR-03110]	n.a.	[G2 COS], chap. 13 [TR-03110]	based on symmetric, asymmetric or PACE authentication mechanisms, see rows for authentication, key derivation, AES based encryption / decryption / MAC generation / MAC verification FTP_ITC.1/TC *package contactless:* FTP_ITC.1/PACE.PICC

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
26	Cryptographic Primitive	Hybrid deterministic RNG DRG.4	[AIS31] / [AIS20] [TCOS RNG], sec. 3.1-3.3 [ISO 18031]	n.a.	[TR-03116-1]	FCS_RNG.1/SICP from IC evaluation BSI-DSZ-CC-1079-V2 (PTG 2 for seeding) FCS_RNG.1 (GET CHALLENGE)
27		Hybrid deterministic RNG DRG.4	[AIS31] / [AIS20] [TCOS RNG], sec. 3.1-3.3 [ISO 18031]	n.a.	[TR-03116-1]	*package Contactless:* FCS_RNG.1/SICP from IC evaluation BSI-DSZ-CC-1079-V2 (PTG 2 for seeding) FCS_RNG.1/PACE (GENERAL AUTHENTICATE)
28		Physical RNG PTG.2	[AIS 31]	n.a.	[TR-03116-1]	FCS_RNG.1/SICP from IC evaluation BSI-DSZ-CC-1079-V2
29		Physical RNG PTG.3	[AIS 31]	n.a.	[TR-03116-1]	FCS_RNG.1/HPRG from IC evaluation BSI-DSZ-CC-1079-V2 FCS_RNG.1/GR (GET RANDOM)
30		SHA-{1, 256, 384, 512}	[FIPS 180-4]	-	[G2 COS], chap. 6.1 [TR-03116-1]	FCS_COP.1/SHA
31	Key Generation	RSA key generation	[TR-02102-1] with Deutsche Telekom Security GmbH specific modification	Modulus length = 2048, 3072	[G2 COS]	*package RSA Key Generation:* FCS_CKM.1/RSA (PSO GENERATE ASYMMETRIC KEY PAIR)
32		ECC key generation	[TR-02102-1] with Deutsche Telekom Security GmbH specific modification	Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [RFC 5639] and ansix9p{256, 384}r1 [ANSI X9.62]	[G2 COS]	FCS_CKM.1/ELC (PSO GENERATE ASYMMETRIC KEY PAIR)

Table 4: TOE cryptographic functionality

Bibliography for Table 4

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

[ISO 9796-2]	ISO/IEC 9796-2:2010 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms, December 2010, ISO
[FIPS 180-4]	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)
[TR-03111]	Technical Guideline BSI TR-03111: Elliptic Curve Cryptography, Version 2.10, 01.06.2018, Bundesamt für Sicherheit in der Informationstechnik (BSI)
[FIPS 197]	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)
[SP800-38A]	Recommendation for Block Cipher Modes of Operation: Methods and techniques, NIST Special Publication 800-38A, 2001, National Institute of Standards and Technology (NIST)
[SP800-38B]	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)
[TR-03110]	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)
[ISO 18031]	ISO/IEC 18031:2005, Information technology – Security techniques – Random bit generation, 2005, ISO
[TR-02102-1]	BSI – Technische Richtlinie BSI TR-02102-1: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2021-01, 24.03.2021, Bundesamt für Sicherheit in der Informationstechnik (BSI)
[RFC 5639]	Elliptic Curve Cryptography (ECC), Brainpool Standard Curves and Curve Generation, RFC 5639, March 2010, IETF
[ANSI X9.62]	American National Standard X9.62, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), November 2005, ANSI

[ANSI X9.63] 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

[G2 COS] Einführung der Gesundheitskarte, Spezifikation des Card Operating System (COS), Elektrische Schnittstelle, Version 3.13.1, 01.11.2019, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[TR-03116-1] Technische Richtlinie BSI TR-03116-1: Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1 – Telematikinfrastruktur, Version 3.20, 21.09.2018, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[TCOS RNG] Zufallszahlengenerierung in TCOS, Version 0.7, 3 November 2020, T-Systems International GmbH (confidential document)

[AIS 20] see chapter 14, [4] of this report

[AIS 31] see chapter 14, [4] of this report

Note: End of report