Federal Office
for Information Security

Certification Report

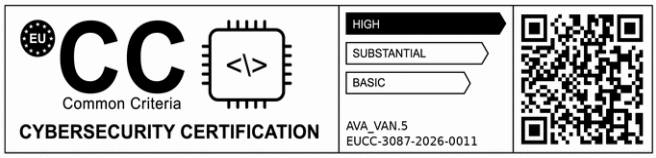
EUCC-3087-2026-0011
Administration ID
BSI-DSZ-CC-0976-V5-2026

for

STARCOS 3.7 COS HBA-SMC

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 9582-11

Contents

A. Certification....4
1. Preliminary Remarks....4
2. Specifications of the Certification Procedure....4
3. Recognition Agreements....5
4. Performance of Evaluation and Certification....5
5. Publication....7
B. Certification Results....8
1. Executive Summary....9
2. Identification of the TOE....11
3. Security Policy....14
4. Assumptions and Clarification of Scope....14
5. Architectural Information....15
6. Supplementary Cybersecurity Information....16
7. IT Product Testing....16
8. Evaluated Configuration....17
9. Results of the Evaluation....18
10. Obligations and Notes for the Usage of the TOE....19
11. Security Target....23
12. Regulation specific aspects (eIDAS, QES)....23
13. Definitions....23
14. Bibliography....25
C. Annexes....31

A. Certification

1. Preliminary Remarks

The Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 [EUCC-VO] establishes a Union-wide cybersecurity certification scheme for TOEs and Protection Profiles for conformity assessments using the requirements of Common Criteria.

By implementing the Cybersecurity Act[1], certification activities at assurance level 'high' and in duly justified cases at assurance level 'substantial' are reserved to the National Cybersecurity Certification Agency of a Member State.

In accordance to BSIG[2] Act, the Federal Office for Information Security (BSI) issues certificates for information technology products.

Certification of a product is carried out at the request of a developer, vendor or a distributor, hereinafter called the applicant.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria referenced in the above mentioned Implementing Regulation (EU) 2024/482 as well as relevant application notes and interpretations published by the certification body of the BSI.

Evaluation facilities notified by the German National Cybersecurity Certification Authority carry out the evaluation.

This Certification Report is the result of the certification activities carried out by the certification body of the BSI in conclusion of the technical evaluation. 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 carries out its activities according to the criteria laid down in the following:

- Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) [EUCC-VO]
- EUCC state-of-the-art documents of relevance to the TOE [EUCC_SOTA]
- Act on the Federal Office for Information Security[2]

[1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[2] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 2 December 2025, BGBl. 2025 Nr. 301, S. 2

- BSI Certification and Approval Ordinance[3]
- BMI Regulations on Ex-parte Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior and Community)
- ISO/IEC 15408 (Common Criteria for IT Security Evaluation (CC), Version CC:2022 R1) [CC]
- ISO/IEC 18045 (Common Methodology for IT Security Evaluation (CEM), Version CEM:2022 R1) [CEM]
- DIN EN ISO/IEC 17065 standard
- EUCC programme: Scheme documentation describing the certification process (EUCC) [EUCC_PROG]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [AIS]

3. Recognition Agreements

In order to avoid multiple certifications 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. 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 5 EAL 2 and ALC_FLR components.

4. Performance of Evaluation and Certification

- The certification body monitors each individual evaluation to ensure a uniform application and interpretation of the criteria as well as uniform ratings.

[3] Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung – BSIZertV) of 02 December 2025, Bundesgesetzblatt 2025, no. 301

[4] 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

- The TOE STARCOS 3.7 COS HBA-SMC has been previously certified by the certification body of the Federal Office for Information Security (BSI) based on administration ID BSI-DSZ-CC-0976-V4-2021 (including subsequent maintenance procedures). Specific results from the corresponding evaluation process were re-used.
- The present evaluation of the product STARCOS 3.7 COS HBA-SMC was carried out by SRC Security Research & Consulting GmbH, located at Emil-Nolde-Straße 7, 53113 Bonn, Germany.
- The evaluation was completed on 27 May 2026. SRC Security Research & Consulting GmbH is a notified evaluation facility (ITSEF).
- This certification was applied for: Giesecke+Devrient ePayments GmbH.
- The assessed TOE was developed by: Giesecke+Devrient ePayments GmbH.
- The certification activities are concluded with the comparability check and the production of this Certification Report. This work was completed by the certification body of the BSI.

This Certification Report applies only to the version of the TOE as identified in this document. The confirmed assurance package is valid on the condition that

- all statements and indications regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in an environment 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 [CC] itself.

The issued Certificate confirms the assurance of the product claimed in the Security Target [ST] on certificate’s issuance day. 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 holder of the Certificate should involve the assurance continuity program of the EUCC Certification Scheme (e.g. by a re-assessment or re-certification) in its obligations to monitor the certified product. Specifically, if certification results should be 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 prevent an indefinite certificate usage where evolving attack methods justify a recent re-assessment of the product’s resistance, the maximum validity period of the certificate is limited. The certificate issued on 17 June 2026 is valid until 16 June 2031 and its validity can be renewed by certifying the TOE again.

The holder of this certificate is obliged:

- to meet the obligations from the Implementing Regulation (EU) 2024/482, in particular but not exclusively to respect the rules for certificate usage, to monitor the conformity of the certified TOE, to inform the certification body about subsequently detected vulnerabilities or irregularities with relevance to the security of the TOE and to maintain vulnerability management and disclosure procedures.

Should changes be introduced into the certified version of the TOE, the validity period of its related certificate can be extended in order to cover the changed TOE, provided the holder of the certificate applies for measures under EUCC scheme’s assurance continuity (i.e. re-certification or maintenance) and the changed TOE then meets the assurance requirements.

5. Publication

The TOE STARCOS 3.7 COS HBA-SMC has been notified to ENISA for publication on the website on European cybersecurity certification schemes and has also been included in BSI's list of certified products, which is published regularly (see [EUCC_CERT]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

This holder of the certificate[5] has to publish on its website this Certification Report and supplementary information. The Certification Report may also be obtained in electronic form at the internet address stated above.

[5] Giesecke+Devrient ePayments GmbH
Prinzregentenstraße 161
81677 München
Germany

B. Certification Results

The following chapters summarise the assessment results of

- the applicant’s Security Target specified for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes, statements and indications from the certification body.

1. Executive Summary

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

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

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_000005h),
- the IC Embedded Software (STARCOS 3.7 COS HBA-SMC 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 [Spec G2 COS], 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 HBA-SMC Operating System) is implemented according to the G2-COS specification [Spec G2 COS] from gematik. Hereby, the TOE implements the mandatory part of the G2-COS specification [Spec G2 COS] 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 [Spec G2 COS]. 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 [Spec G2 COS] is implemented in the TOE.

Furthermore, the TOE provides the commands CREATE and PSO HASH (refer to the user guidances [Guide Usage], chapter 5.2.1 and 5.2.2 and [Guide FS 1], chapter 2.3.1 and 2.3.2) that are outlined as optional in the G2-COS specification [Spec G2 COS]. In addition, the TOE provides developer-specific initialisation and personalisation commands (refer to the user guidance [Guide FS 1], chapter 2.4) for support of the Initialisation Phase and Personalisation Phase of the TOE’s life cycle model (refer to chapter 2).

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

The product STARCOS 3.7 COS HBA-SMC has been certified under the EUCC scheme in accordance to the provisions of the Implementing Regulation (EU) 2024/482. This is a certification based on BSI administration ID BSI-DSZ-CC-0976-V4-2021 (including subsequent maintenance procedures). Specific results from the evaluation process BSI-DSZ-CC-0976-V4-2021 and subsequent maintenance procedures were re-used. The TOE deliverables are listed in table 1.

The evaluation of the product STARCOS 3.7 COS HBA-SMC was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 27 May 2026. SRC Security Research & Consulting GmbH is a notified evaluation facility (ITSEF).

The Evaluation Technical Report (ETR) [ETR] was provided by the ITSEF according to the Common Criteria [CC], the Methodology [CEM], the requirements of the Scheme [EUCC-VO] and [EUCC_PROG].

The evaluation has confirmed:

- CC Version and Release: see [CC] and [CEM]
- PP Conformance: Card Operating System Generation 2 (PP COS G2), Version 2.1, 10 July 2019, BSI-CC-PP-0082-V4-2019 [PP]
- Assurance Level: EUCC High with component AVA_VAN.5
- Assurance Package: EAL 4
- Augmentation: ALC_DVS.2, ATE_DPT.2, AVA_VAN.5 and ALC_FLR.1

The Security Target [ST] 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 [PP]. The Security Target [ST] 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.

A detailed description of the security functionality, addressed threats, organisational security policies and the operational environment can be found in the Security Target [ST].

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

The vulnerability assessment results stated in this certificate do not express an appraisal of the strength and suitability of the cryptographic algorithms implemented in the TOE (see BSIG Section 52, Para. 4, Clause 2).

The certification results apply only to the version of the product indicated in the certificate and on the condition that all the statements and indications are kept as detailed in this Certification Report. Neither the BSI nor any other organisation that recognises or gives effect to this certificate implicitly or explicitly guarantee or endorse the certified TOE.

2. Identification of the TOE

The Information and communications technology (ICT) product is identified as follows:

STARCOS 3.7 COS HBA-SMC

Holder of the certificate: Giesecke+Devrient ePayments GmbH
Prinzregentenstraße 161
81677 München
Germany
https://www.gi-de.com/en/cybersecurity-information

The following table outlines the TOE deliverables:

No.	Type	Identifier	Release	Type / Form of Delivery
1	HW/SW	Infineon Security Controller IFX_CCI_000005h including its IC Dedicated Software (Firmware) (refer to the Certification Report BSI-DSZ-CC-1110-V8-2025 ([CertRep IC]))	Infineon Security Controller IFX_CCI_000005h (with Firmware version 80.100.17.3)	Dual-interface chip (contact-based and contactless chip). Delivery as chip to the module production sites according to the delivery procedures specified in BSI-DSZ-CC-1110-V8-2025 ([CertRep IC]).
2	SW	IC Embedded Software: STARCOS 3.7 COS HBA-SMC Operating System	STARCOS 3.7 COS HBA-SMC OS Identification: ‘47 44 00 B7 04 01 01’ (refer to table 2)	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 HBA-SMC – Main Document [Guide Main]	Version 1.6	Document in electronic form (encrypted and signed)
4	DOC	Guidance Documentation for the Usage Phase STARCOS 3.7 COS HBA-SMC [Guide Usage]	Version 1.9	Document in electronic form (encrypted and signed)

No.	Type	Identifier	Release	Type / Form of Delivery
5	DOC	Guidance Documentation for the Initialization Phase STARCOS 3.7 COS HBA-SMC [Guide Init]	Version 2.3	Document in electronic form (encrypted and signed)
6	DOC	Guidance Documentation for the Personalisation Phase STARCOS 3.7 COS HBA-SMC [Guide Perso]	Version 2.2	Document in electronic form (encrypted and signed)
7	DOC	STARCOS 3.7 COS HBA-SMC Functional Specification - Part 1: Interface Specification [Guide FS 1]	Version 1.6	Document in electronic form (encrypted and signed)
8	DOC	STARCOS 3.7 Internal Design Specification [Guide IDS]	Version 1.0	Document in electronic form (encrypted and signed)
9	SW	Wrapper	Version 1.8.6	File rar-archive: egkwrapper-v1.8.6.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: D277B7E7E239E2EC1157465794A48625272AF86373D22C1B307FA2F1635590FF
10	DOC	STARCOS 3.7 COS Guidance Documentation for the Wrapper [Guide Wrap]	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 HBA-SMC is as well known under the following product identificator:

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

Product: '53 33 37 4F 53 48 42 41' (S37OSHBA)

OS Version Number: '01 00 01 (1.0.1)

According to the Security Target [ST], 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 HBA-SMC 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 HBA-SMC 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 [Guide Init], chapter 4.6, [Guide Perso], chapter 5.7 and [Guide Usage], 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 HBA-SMC 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)

Table 2: TOE Identification via the command GET PROTOCOL DATA

The command GET PROTOCOL DATA with its parameters is described in the user guidances [Guide Init], chapter 4.6, [Guide Perso], chapter 5.7 and [Guide Usage], 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 04 01 01'

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

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers 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 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 [ST], chapter 6, 7, 8, 9 and 10.

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 uncovered aspects need to be provided by specific security objectives that have to be met 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 [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

Security Objectives for the operational environment defined in the Security Target	Description according to the ST [ST]
	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.
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 4: Security Objectives for the operational environment

Details can be found in the Security Target [ST], chapter 4.2, 7.3, 8.3, 9.3 and 10.3.

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 HBA-SMC 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-V8-2025 ([ST IC], [CertRep IC]).

According to the TOE design the Security Functions of the TOE 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
- Wrapper: Export of non-sensitive TSF and user data

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

6. Supplementary Cybersecurity Information

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 [ST].

The developer's website as stated in chapter 2 provides the following supplementary information:

- the period during which support is offered (esp. security related updates)
- contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers
- a reference to online repositories listing publicly disclosed vulnerabilities related to the TOE/ICT, ICT service or ICT process and to any relevant cybersecurity advisories

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

All tests have been carried out by the ITSEF

SRC Security Research & Consulting GmbH
Emil-Nolde-Straße 7
D-53113 Bonn

under the responsibility of the certification body

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87
Postfach 20 03 63
D-53175 Bonn

Please refer to chapter 1 of this report for details on assurance levels or packages involved into testing.

For the state-of-the-art documents and supporting documents applied please refer to chapter 9.1 of this report.

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 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 Runtime System and System Library,
- penetration testing related to the verification of the reliability of the TOE,
- source code analysis performed by the evaluators,
- side channel analysis for SHA, RSA and ECC, including RSA and ECC key generation,
- fault injection attacks (laser and EM 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.

Please refer to chapter 8 for complete and precise information on settings and configuration of the TOE during the evaluation, including relevant operational notes and observations.

8. Evaluated Configuration

This certification covers the following configuration of the TOE as outlined in the Security Target [ST]:

STARCOS 3.7 COS HBA-SMC

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-V8-2025 (refer to [CertRep IC]).

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 HBA-SMC 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 [Guide Init], chapter 4.6, [Guide Perso], chapter 5.7 and [Guide Usage], chapter 4.1.1. See chapter 2 of this Certification Report for details.

9. Results of the Evaluation

9.1. CC specific results

The ITSEF produced and provided the Evaluation Technical Report (ETR) [ETR] according to the requirements of the Scheme [EUCC-VO], [EUCC_PROG], the Common Criteria [CC], the Common Evaluation Methodology [CEM], and all relevant interpretations and guidelines of the Scheme (AIS) [AIS].

For the evaluation the following state-of-the-art documents and supporting documents specific for the technology were applied:

- EUCC Scheme State-of-the-Art document - Composite product evaluation and certification for CC:2022, Version 1, February 2025, ENISA
- EUCC Scheme State-of-the-Art document - Security Architecture requirements (ADV_ARC) for smart cards and similar devices extended to Secure Sub Systems in SoCs, Version 1.1, October 2023, ENISA
- EUCC Scheme State-of-the-Art document - Application of Attack Potential to smartcards and similar devices, Version 2, February 2025, ENISA
- Attack Methods for Smartcards and Similar Devices, Version 2.5, 2022-05, Joint Interpretation Working Group (confidential)
- EUCC Scheme State-of-the-Art document - Application of CC to integrated circuits, Version 2, December 2024, ENISA
- EUCC Scheme State-of-the-Art document - Minimum Site Security Requirements, Version 2, February 2025, ENISA
- EUCC Scheme State-of-the-Art document - STAR methodology, Version 1, February 2025, ENISA
- EUCC Scheme State-of-the-Art document - Minimum ITSEF requirements for security evaluations of smart cards and similar devices, Version 1.1, October 2023, ENISA
- Functionality classes and evaluation methodology of physical and deterministic random number generators (AIS 20 and AIS 31, see [AIS])
- Guidance for smartcard evaluation (AIS 37, see [AIS])

- Information on cryptographic evaluation (AIS 46, see [AIS])
- Reuse of evaluation results (AIS 38, see [AIS])
- Site audits (AIS 1, see [AIS])
- Test validity (AIS 25, see [AIS])
- CC and CEM interpretations (AIS 32, see [AIS])
- Transition Policy to CC:2022 and CEM:2022, 20 April 2023, Common Criteria Recognition Arrangement Management Committee, CCMC-2023-04-001

A document ETR for composite evaluation according to the State-of-the-Art document 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 Protection Profile [PP] were followed in the course of the evaluation of the TOE.

As a result of the evaluation, the verdict PASS is confirmed for the assurance components that are identified in chapter 1 of this report and claimed by the Security Target [ST] for the corresponding TOE identified in chapter 1 and 2 of this report.

The certificate

- is uniquely identified by: EUCC-3087-2026-0011, administration ID BSI-DSZ-CC-0976-V5-2026
- was issued on: 17 June 2026
- is valid until: xx June 2031 (Datum der Ausstellung plus x Jahre - 1Tag)

The results of the evaluation are only applicable to the TOE as defined in chapter 1 and 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The table in annex C of part C 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 52, Para. 4, Clause 2).

According to the specification [Spec G2 COS] and the Technical Guideline BSI TR-03116-1 [TR-03116-1] 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), 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)) in the framework of the German health care system. An explicit validity period of each algorithm is not provided here.

10. Obligations and Notes for the Usage of the TOE

Table 1 outlines the documents that contain necessary information on the intended use of the TOE including all security related information, conditions and instructions to be taken into account by the user. In addition, all aspects of Assumptions, Threats and OSPs as

outlined in the Security Target and not covered by the TOE itself need to be met by the operational environment of the TOE.

The customer or user of the TOE shall take the statements of this certificate into account in its system risk management process. The user should define measures in its risk management that respond to emerging and new attack methods and techniques to the TOE until the TOE has been re-assessed.

The user also has to consider in its risk management the limited validity for the usage of cryptographic algorithms as outlined in chapter 9.

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 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 ([TR-03144]):

- 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 [Guide IDS] 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 [Guide IDS] 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 ([TR-03144]) it is strongly recommended to care for the appropriate choice of the access rules and the flag described in chapter 2.5 of [Guide IDS] for all object system's objects. It shall be possible for the Konsistenz-Prüftool according to the Technical Guideline BSI TR-03143 ([TR-03143]) 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 [Spec G2 COS]).

Any object system set up on the TOE shall only make use of the TOE's functionality as described in the G2-COS specification [Spec G2 COS] and the user guidance [Guide FS 1]. 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 [Guide Usage], chapter 5.1.1.1 and [Guide Init], chapter 3.2.1 and 3.2.3 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 [RFC 5639] and ansix9p{256, 384}r1 [ANSI X9.62]. Refer to the user guidances [Guide Usage], chapter 6 and [Guide Perso], 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 [Guide IDS], 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 [Guide Usage], chapter 5.1.1.1 and 6, [Guide Init], chapter 3.2.1 and 3.2.3, [Guide Perso], chapter 6, [Guide FS 1] and [Guide IDS], 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 [Guide Main], [Guide Usage], [Guide Init], [Guide Perso] and [Guide FS 1].

- The TOE's Wrapper and its specifics beyond the Wrapper specification [Spec Wrapper], in particular concerning the exceptions that are thrown by the Wrapper:

  Refer to the user guidance [Guide Wrap].

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

  Refer to the user guidance [Guide Usage], chapter 5.2.2.

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

  [Guide Usage], chapter 5.1.1 and 5.1.2 including subchapters, [Guide Init], chapter 3.2 including subchapters and 4.7.1 and [Guide Perso], chapter 5.8.1 and 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 ([TR-03144]) it is strongly recommended to care for that via the TOE's specific personalisation commands initialised security attributes and public key data of the object system and its objects cannot be overwritten (except for where explicitly intended by the object system's intention and design).

For a TR-conformity testing of a card product set up on the TOE according to the Technical Guideline BSI TR-03144 ([TR-03144]) 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 [Spec Wrapper]. 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 [Guide IDS]. It shall be possible for the Konsistenz-Prüftool according to the Technical Guideline BSI TR-03143 ([TR-03143]) 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 [Guide Usage], chapter 5.1.1.1, [Guide Init], chapter 3.2.1 and 3.2.3 and [Guide IDS], 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 ([TR-03144]).

- Any object system set up on the TOE shall only make use of the TOE's functionality as described in the G2-COS specification [Spec G2 COS] and the user guidance [Guide FS 1].

  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 [Guide Usage], chapter 5.1.1.1 and [Guide Init], chapter 3.2.1. Refer to the user guidance [Guide Init], chapter 3.2.3.

  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 ([TR-03143]) 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 ([TR-03144]).

- 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 [RFC 5639] and ansix9p{256, 384}r1 [ANSI X9.62]. Refer to the user guidance [Guide Usage], chapter 6 and [Guide Perso], 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 [Guide IDS], chapter 2.5.2.4. Refer to the user guidance [Guide Init], chapter 3.2.3.

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 ([TR-03144]).

- 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 [Guide Init], chapter 3.2.3.

  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 ([TR-03144]).
- If in the framework of the TR-conformity testing of a card product according to the Technical Guideline BSI TR-03144 ([TR-03144]) the Konsistenz-Prüftool according to the Technical Guideline BSI TR-03143 ([TR-03143]) 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 [Spec G2 COS] or the user guidance [Guide FS 1] this has to be manually examined and valuated. Refer to the user guidance [Guide Init], chapter 3.2.3.
- For card products that undergo a TR-conformity testing according to the Technical Guideline BSI TR-03144 ([TR-03144]), 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 [ST] of the TOE / Information and communications technology (ICT) product 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
ICT	Information and communications 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

[EUCC-VO] Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)

and

Implementation Regulation (EU) 2025/2462 of 8 December 2025 amending Implementing Regulation (EU) 2024/482 as regards definitions, ICT product series certification, assurance continuity and state-of-the-art document

[CC] ISO 15408:2022, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirements

https://www.iso.org/standard/72891.html
https://www.iso.org/standard/72892.html
https://www.iso.org/standard/72906.html
https://www.iso.org/standard/72913.html
https://www.iso.org/standard/72917.html

as mirrored by CCRA's edition:

CC:2022 R1, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirements

https://www.commoncriteriaportal.org

amended by:

CCMB Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2, 15 October 2025, CCRA

https://www.commoncriteriaportal.org

[CEM] ISO 18045:2022: Evaluation criteria for IT security – Methodology for IT security evaluation

https://www.iso.org/standard/72889.html

as mirrored by CCRA's edition:

CEM:2022 R1, Common Methodology for Information Technology Security Evaluation – Evaluation methodology

https://www.commoncriteriaportal.org

amended by:

CCMB Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2, 15 October 2025, CCRA

https://www.commoncriteriaportal.org

[EUCC_SOTA]	EUCC state-of-the-art documents: https://certification.enisa.europa.eu/publications/eucc-state-art-documents_en
[EUCC_PROG]	EUCC program of the BSI: Scheme documentation describing the certification process (EUCC) https://www.bsi.bund.de/zertifizierung
[EUCC_CERT]	EUCC Certificates, periodically updated list published on ENISA's website on European cybersecurity certification schemes (https://certification.enisa.europa.eu/), but also on BSI's website (https://www.bsi.bund.de/zertifizierungsreporte)
[AIS]	Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[6] https://www.bsi.bund.de/AIS
[ST]	Security Target BSI-DSZ-CC-0976-V5-2026, Security Target STARCOS 3.7 COS HBA-SMC, Version 2.2, 23 April 2026, Giesecke+Devrient ePayments GmbH
[PP]	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)
[ETR]	ETR BSI-DSZ-CC-0976-V5-2026, Evaluation Technical Report (ETR) – Summary for STARCOS 3.7 COS HBA-SMC, Version 3.2, 24 May 2026, SRC Security Research & Consulting GmbH (confidential document)
[ConfList]	Configuration List BSI-DSZ-CC-0976-V5-2026, Configuration List STARCOS 3.7 COS HBA-SMC, Version 1.0, 21 May 2026, Giesecke+Devrient ePayments GmbH (confidential document)

[6]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 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 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluierungen
- AIS 38, Version 2.9, Reuse of evaluation results
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[Guide Main] Guidance Documentation STARCOS 3.7 COS HBA-SMC – Main Document, Version 1.6, 23 March 2021, Giesecke+Devrient ePayments GmbH

[Guide Usage] Guidance Documentation for the Usage Phase STARCOS 3.7 COS HBA-SMC, Version 1.9, 19 May 2025, Giesecke+Devrient ePayments GmbH

[Guide Init] Guidance Documentation for the Initialization Phase STARCOS 3.7 COS HBA-SMC, Version 2.3, 29 April 2021, Giesecke+Devrient ePayments GmbH

[Guide Perso] Guidance Documentation for the Personalisation Phase STARCOS 3.7 COS HBA-SMC, Version 2.2, 6 April 2021, Giesecke+Devrient ePayments GmbH

[Guide FS 1] STARCOS 3.7 COS HBA-SMC Functional Specification - Part 1: Interface Specification, Version 1.6, 3 March 2021, Giesecke+Devrient ePayments GmbH

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

[Guide Wrap] STARCOS 3.7 COS Guidance Documentation for the Wrapper, Version 1.3, 10 February 2021, Giesecke+Devrient ePayments GmbH

[ST IC] Security Target of the underlying hardware platform, 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 design step H13, Version 6.2, 26 June 2025, Infineon Technologies AG, BSI-DSZ-CC-1110-V8-2025 (confidential document)

Security Target Lite of the underlying hardware platform, 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 design step H13, Version 6.2, 26 June 2025, Infineon Technologies AG, BSI-DSZ-CC-1110-V8-2025 (sanitised public document)

[CertRep IC] Certification Report BSI-DSZ-CC-1110-V8-2025 for Infineon Security Controller 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 in the design step H13 and including optional software libraries and dedicated firmware in several versions from Infineon Technologies AG, 5 August 2025, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[ETRfComp IC] ETR for Composite Evaluation of the underlying hardware platform Infineon Security Controller 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 design step

H13 from certification procedure BSI-DSZ-CC-1110-V8-2025, Version 2, 25 July 2025, TÜV Informationstechnik GmbH (confidential document)

[Spec 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

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

[TR-03144] 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)

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

[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)

[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

[CertRep DCG] Certification Report for Giesecke+Devrient Development Center Germany (DCG) of Giesecke+Devrient ePayments GmbH, BSI-DSZ-CC-S-0347-2026, 28 April 2026, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[CertRep DCS] Certification Report CCN-CC/2024-24/INF-4575 for Giesecke+Devrient Development Center Spain (DCS), related to CCN-CC-21/2025, 22 May 2025 (Certificate date), National Cryptologic Centre (CCN)

[CertRep LINX S] Certification Report CCN-CC/2025-19/INF-4714 for Linxens Singapore Changi Site, related to CCN-CC-50/2025, 22 December 2025 (Certificate date), National Cryptologic Centre (CCN)

[CertRep LINX T] Certification Report CCN-CC/2023-35/INF-4423 for Linxens Tianjin Site, related to CCN-CC-24/2024, 21 October 2024 (Certificate date), National Cryptologic Centre (CCN)

[CertRep INESA] Certification Report SiteCC-2500140-01-CR for INESA Shanghai, INESA Intelligent Electronics Co. Ltd., related to SiteCC-2500140-01, 13 January 2026, TrustCB B.V.

[CertRep UTAC] Certification Report ANSSI-CC-SITE-2025/05 for PT UTAC Manufacturing Services Indonesia, 12 August 2025, ANSSI

[CertRep HS] Certification Report ANSSI-CC-SITE-2025/03 for Giesecke+Devrient (China) Technologies Co. Ltd., Huangshi Branch (GDCHINA HS), 27 May 2025, ANSSI

[CertRep GDIMS] Certification Report CCN-CC/2024-08/INF-4392 for Giesecke+Devrient ePayments Iberia S.A. (GDIMS), related to CCN-CC-18/2024, 6 September 2024 (Certificate date), National Cryptologic Centre (CCN)

C. 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-0976-V5-2026

Evaluation results regarding development and production environment

The IT product STARCOS 3.7 COS HBA-SMC (Target of Evaluation, TOE, also named as ICT product) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM) [CEM].

As a result of the TOE certification, dated 17 June 2026, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support as claimed by the ST [ST] and that are stated in chapter 1 of this report 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-0347-2026 [CertRep DCG].

b) Giesecke+Devrient Development Center Spain (DCS) for Development. Refer to the Certification Report CCN-CC/2024-24/INF-4575 [CertRep DCS].

c) Linxens Singapore Changi Site for Module Production. Refer to the Certification Report CCN-CC/2025-19/INF-4714 [CertRep LINX S].

d) Linxens Tianjin Site for Module Production. Refer to the Certification Report CCN-CC/2023-35/INF-4423 [CertRep LINX T].

e) INESA Shanghai, INESA Intelligent Electronics Co. Ltd. for Module Production. Refer to the Certification Report SiteCC-2500140-01-CR [CertRep INESA].

f) PT UTAC Manufacturing Services Indonesia for Module Production. Refer to the Certification Report ANSSI-CC-SITE-2025/05 [CertRep UTAC].

g) Giesecke+Devrient (China) Technologies Co. Ltd., Huangshi Branch (GDCHINA HS) for Production (in particular Inlay Embedding) and Initialisation. Refer to the Certification Report ANSSI-CC-SITE-2025/03 [CertRep HS].

h) Giesecke+Devrient ePayments Iberia S.A. (GDIMS) for Production (in particular Inlay Embedding) and Initialisation. Refer to the Certification Report CCN-CC/2024-08/INF-4392 [CertRep GDIMS].

i) For development and production sites regarding the underlying IC platform please refer to the Certification Report BSI-DSZ-CC-1110-V8 [CertRep IC].

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

Annex C of Certification Report BSI-DSZ-CC-0976-V5-2026

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] (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] (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		SHA-256 based fingerprint	[FIPS 180-4] (SHA)	-	[G2 COS], chap. 6.1.2, 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] (AES) [SP800-38A]	|k| = 128, 192, 256 |challenge| = 64	[G2 COS], chap. 6.7.1.2, 6.7.2.2	*package Crypto Box:* FCS_COP.1/CB.AES (EXTERNAL

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
			(CBC) [G2 COS], chap. 6.7.1.2, 6.7.2.2		[TR-03116-1]	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] (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.
11		ECDSA signature verification using SHA-{256, 384, 512}	[TR-03111] (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.

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
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
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)

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
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)
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)

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
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
26	Cryptographic Primitive	Hybrid deterministic RNG DRG.3	[ISO 18031], Appendix C.3.2 with developer specific enhancements [AIS 20]	n.a.	[TR-03116-1]	FCS_RNG.1 (GET CHALLENGE)
27		Hybrid deterministic RNG DRG.4	[ISO 18031], Appendix C.3.2 with developer specific enhancements [AIS 20]	n.a.	[TR-03116-1]	FCS_RNG.1/PACE (GENERAL AUTHENTICATE)
28		Physical RNG PTG.2	[AIS 31]	n.a.	[TR-03116-1]	FCS_RNG.1/SICP FCS_RNG.1/GR (GET RANDOM)
29		SHA-{1, 256, 384, 512}	[FIPS 180-4]	-	[G2 COS], chap. 6.1 [TR-03116-1]	FCS_COP.1/SHA

#	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
30		SHA-{1, 224, 256, 384, 512}	[FIPS 180-4]	-	[G2 COS], chap. 6.1 [TR-03116-1]	FCS_COP.1/CB_HASH (PSO HASH)
31	Key Generation	RSA key generation	[TR-02102-1] with G+D 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-03111] with G+D 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 5: TOE cryptographic functionality

Bibliography for Table 5

[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 2026-01, 23.01.2026, 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

[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)

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

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

Note: End of report