Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1098-2020

for

IDEMIA_HC_Germany_NEO_G2.1_COS, V1

from

IDEMIA Germany 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-1098-2020 (*)

IDEMIA_HC_Germany_NEO_G2.1_COS, V1

from	IDEMIA Germany 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, 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 and by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

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

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

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2

Bonn, 30 July 2020

For the Federal Office for Information Security

Matthias Intemann
Head of Branch

L.S.

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

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

This page is intentionally left blank.

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]
- BSI Schedule of 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 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 3 March 2005, Bundesgesetzblatt I, p. 519

- 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 IDEMIA_HC_Germany_NEO_G2.1_COS, V1 has undergone the certification procedure at BSI.

The evaluation of the product IDEMIA_HC_Germany_NEO_G2.1_COS, V1 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 17 July 2020. 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: IDEMIA Germany GmbH.

The product was developed by: IDEMIA Germany GmbHIDEMIA Germany 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 30 July 2020 is valid until 29 July 2025. 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 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,

[5] Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the 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 IDEMIA_HC_Germany_NEO_G2.1_COS, V1 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] IDEMIA Germany GmbH
Konrad-Zuse-Ring 1
24220 Flintbek

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 IDEMIA_HC_Germany_NEO_G2.1_COS, V1 developed by IDEMIA Germany GmbH.

The TOE is a smart card product according to the G2-COS specification [17] from gematik and is implemented on the hardware platform Infineon Security Controller IFX_CCI_000005h from Infineon Technologies AG (refer to [14], [15]).

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) and SMC-B (Security Module Card Type B) as currently specified for card products of the generation G2 within the German health care system. These TOE's storage and cryptographic services that are provided by the TOE and invoked by the human users and components of the German health care system cover the following issues:

- authentication of human 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 of

- 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 Smart Card Embedded Software (IDEMIA_HC_Germany_NEO_G2.1_COS, V1 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 [17], but does not contain itself any object systems (applications).

In functional view, the TOE with its Smart Card Embedded Software (IDEMIA_HC_Germany_NEO_G2.1_COS, V1 Operating System) is implemented according to the G2-COS specification [17] from gematik. Hereby, the TOE implements the mandatory part of the G2-COS specification [17] with the base functionality of the operating system platform. Concerning [17], the TOE implements in addition the options Contactless (“Option_kontaktlose_Schnittstelle”), Logical Channel (“Option_logische_-Kanäle“) and RSA Key Generation (“Option_RSA_KeyGeneration”) as defined in the G2-

COS specification [17]. None of the further options Crypto Box (“Option_Kryptobox”), PACE for Proximity Coupling Device (“Option_PACE_PCD”), USB (“Option_USB_-Schnittstelle”) and RSA CVC (“Option_RSA_CVC”) specified in the G2-COS specification [17] is implemented in the TOE.

Furthermore, the TOE implements some optional commands from the G2-COS specification [17] and some additional commands and command variants beyond the G2-COS specification [17] for the usage phase. Refer to the user guidance [12], chapter 3.2 and 7.

For support of the TOE’s OS Personalisation consisting of the Product PrePersonalisation (loading of an object system) and Product Personalisation (personalisation of a loaded object system) in the TOE’s life-cycle model (refer to chapter 2), the TOE provides developer-specific (pre-)personalisation commands. Refer to the user guidance [11], chapter 8.6.

The TOE's Wrapper is implemented according to the Wrapper specification [18] 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 [8]. The Security Target [6] and [7] uses the mandatory parts of the PP and the optional packages Contactless, Logical Channel and RSA Key Generation defined in the PP. None of the PP’s further optional packages Crypto Box, 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, AVA_VAN.5.

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

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

TOE Security Functionality	Addressed issue
User Authentication	The authentication of users is supported by the following security services: The product implements a classical PIN-based user authentication. It is possible to flexibly instantiate the service, e.g. by a minimum required password length, or varying user or retry counter values. The system allows for unblocking of a blocked PIN using a PIN unblocking code and to user roles which have the right to unblock the PIN. For convenience purposes, the product implements multi-reference PINs which share the same personal identification number and other attributes. This way it is possible that a user keeps several different PINs in synchronisation with each other. A role with the required rights is allowed to activate or deactivate the verification requirement. This is also a convenience function which leverages the requirement to enter PINs.

TOE Security Functionality	Addressed issue
Internal and External Device Authentication	The product is capable to authenticate an external role. After a successful role authentication, the product grants additional access and usage rights to the external entity. The product also implements internal authentication services, which proof the authenticity of the card to an external entity. These services can either be used as one step of a mutual authentication protocol or to use the product as an authentication token in a larger eco-system. Mutual Authentication protocols with the establishment of secure sessions between the card and a trusted external entity are also a major security service provided by the product. Via the secured channels it is possible to import and export data protecting the data integrity and confidentiality.
Security State Model	The product effectively models, stores and manages the security states acquired by external entities via user or device authentication. The proper modelling of security states is a prerequisite for controlling the access to the object system and the usage of cryptographic services.
Cryptographic Services	The product implements several cryptographic services. The card is capable to verify and import digital certificates. This way it is possible to load key material of a public key infrastructure onto the card for further processing. The generation and verification of digital signatures are additional security services which enable the card holder to effectively sign electronic data and verify such signed data. Various enciphering, deciphering, and transciphering services support cryptographic use cases in collaboration with the background system and other cards. As an additional service, the product implements the generation of a fingerprint over the effective code-base which allows for precisely identifying a specific product release.
Secure Access-Controlled Object System	The object system that acts as storage for PINs, cryptographic keys, and user data provides strict access control mechanisms. It is possible to model access rules in a fine-grained manner based on the effective command currently executed, the life-cycle state of the affected object and the product, the security environment the product operates in and the current IO state, i.e. the IO interface used or the status of a secure session. It is also possible to extend the object system by the loading of new application dedicated files containing additional data and key material in the field. This feature is also subject to the access control enforced by the object system. The object system provides additional means to initialize users which allow for initializing the content of the object system. This feature is used in the approval process of object systems to ensure that a specific instantiation of an object system adheres to a given specification.

TOE Security Functionality	Addressed issue
Elementary Cryptographic Functions	The elementary cryptographic functions of the product form the basis for the different authentication protocols and cryptographic services. The product supports the AES symmetric ciphers with up to 256 bits as well as additional modes of operation like cipher-block-chaining, or CMAC computations. Both the RSA and ECC crypto operations support asymmetric crypto services and authentication protocols. Additionally, the product supports on-card key generation. Several hash-functions like SHA1 and SHA2 support cryptographic operations like the generation of digital signatures or the derivation of session keys for secure initialization. A high-quality random number generator is used internally e.g. for the generation of cryptographic key material of high quality and also supports the implementation of many cryptographic protocols. For the implementation of the elementary cryptographic functions the embedded software uses the cryptographic features of the underlying high-secure IC and its dedicated crypto library.
High Attack Resistance	The product is a secure element which exhibits a high attack resistance even if an attacker has physical access to the product. This attack resistance is achieved by strong self-protection mechanisms and a security design which prevents the bypassing of security features. Furthermore, the start-up phase (after Reset or Power On) of the product is secured to ensure that the product properly initializes from a down-state to a secure mode of operation. The domain separation is secured by memory access control based on different privilege levels. The security features implemented by the product closely collaborate with the protection mechanisms of the underlying security IC.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [7], chapter 6.1, 7.4, 8.4, 9.4 and 10.

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

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

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

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

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

IDEMIA_HC_Germany_NEO_G2.1_COS, V1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release / Version	Form of Delivery
1	HW / SW	Infineon Security Controller IFX_CCI_000005h with Crypto Libraries ACL v2.08.007, SCL v02.04.002 and Hardware Support Library (HSL) v03.12.8812 provided by Infineon Technologies AG (refer to the Certification Report BSI-DSZ-CC-1110-V3-2020 ([15]))	IFX_CCI_000005h with ACL v2.08.007, SCL v02.04.002, HSL v03.12.8812	Delivery procedures of the IC according to the delivery procedures specified in BSI-DSZ-CC-1110-V3-2020 ([15]). Delivery of not-OS pre-personalised / OS pre-personalised smart cards containing the IC and the OS loaded in the flash memory (dual-interface, with or without activated contactless interface). The TOE is delivered without any object system installed. However, the delivery of the TOE is in general combined with the delivery of a so-called PrePersonalisation Sequence that contains an object system intended to be installed on the TOE.
2	SW	Smart Card Embedded Software comprising the IDEMIA_HC_Germany_NEO_G2.1_COS, V1 Operating System (designed as flash implementation)	OS Revision/Release: 2.2.4 Variant: 10‘ (Deferred Production Variant) or ‚11‘ (Integrated Production Variant) (see information on the GET DATA command below)	
3	SW	Wrapper The 7z-archive of the Wrapper consists of: • Wrapper.jar • iwrapper.jar • jdom-2.0.5.jar • bcprov-ext-jdk15on-150.jar	Version 2.2.6	Delivery as electronic file (7z-archive). SHA256 checksum of the 7z-archive: A1BC338E1B4F40E2F0334DBB2643160020505B929E23C1F391FA47E69202E5C6 (see [13], chapter 1.1)
4	SW	OS PrePersonalisation Sequence Signed command sequence used by the OS PrePersonalizer for configuration of the Operating System (import of key material) and prepared by IDEMIA Germany GmbH.	n/a	Delivery as electronic file
5	DOC	IDEMIA_HC_Germany_NEO_G2.1_COS, V1 Preparative Guidance [11]	Version 1.10	Document in paper / electronic form
6	DOC	IDEMIA_HC_Germany_NEO_G2.1_COS, V1 Operational User Guidance [12]	Version 2.1	Document in paper / electronic form
7	DOC	IDEMIA_HC_Germany_NEO_G2.1_COS, V1 Wrapper Guidance [13]	Version 1.7	Document in paper / electronic form

No	Type	Identifier	Release / Version	Form of Delivery
8	DOC	IDEMIA_HC_Germany_NEO_G2.1_COS, V1 Data Sheet	n/a	Document in paper / electronic form
9	KEY	K_MORPHO_AUT Public part of the authentication key pair used for the authenticity of the TOE.	n/a	Document in paper / electronic form (key included in the Data Sheet)
10	KEY	K_OBJ_PERS Personalisation key relevant for the product personalisation of the TOE.	n/a	Document in paper / electronic form
11	KEY	K_OBJ_VERIFICATION Object system signature key used for calculation of the signature over an object system.	n/a	Document in paper / electronic form
12	KEY	K_OS_PREPERS_MK OS PrePersonaliser Master Key used for derivation of card individual authentication keys.	n/a	Document in paper / electronic form
13	KEY	K_OPE_DEC Key used for encryption of secrets in Load Application sequences in the operational phase.	n/a	Document in paper / electronic form
14	KEY	K_OPE_VERIFICATION Key used for calculation of a signature over Load Application se-quences in the operational phase.	n/a	Document in paper / electronic form

Table 2: Deliverables of the TOE

The commercial numbering of the TOE IDEMIA_HC_Germany_NEO_G2.1_COS, V1 by Infineon Technologies AG is as follows:

H13 chip family

Product Type: SLC32GDA

By executing the GET DATA command (refer to the user guidance documentation [11], [12]), the following product identification data of the foundry are set:

IC Manufacturer: 81 00

IC Type: 13 2A

OS Version: 02 02

Mask Date: 00 62

OS Subversion: 04 00

The TOE IDEMIA_HC_Germany_NEO_G2.1_COS, V1 is as well known under the following product identificator:

Manufacturer: ‘44 45 49 44 4D' (DEIDM)

Product: ‘4D 48 43 47 5F 47 32 32' (MHCG_G22)

OS Version Number: '02 02 04' (2.2.4)

Hereby, the TOE is related to Release R3.1.1-1 and Product Type Version (PTV) 4.5.0-0 as defined by gematik.

According to the Security Target [6] and [7], chapter 1.3.4.1 the life-cycle model of the TOE consists of the following phases:

Phase 1: Smart Card Embedded Software Development

Phase 2: IC Development

Phase 3: IC Manufacturing

Phase 4: IC Packaging (combined with Phase 3 to IC Manufacturing)

Phase 5: OS Loading

Phase 6: OS Personalisation, consisting of Product PrePersonalisation and Product Personalisation

Phase 7: Operational Use

For TOE production, two different production variants can be distinguished: In the Integrated Production Variant loading of the Operating System takes place at the IC manufacturer whereas in the Deferred Production Variant loading of the Operating System is carried by IDEMIA Germany GmbH. There is a further intermediate phase called OS PrePersonalisation between Phase 5 and Phase 6, which is either coupled to Phase 5 (in the Deferred Production Variant) or coupled to Phase 6 (Integrated Production Variant).

TOE delivery in the sense of the CC takes place at the end of Phase 5, more detailed after the OS PrePersonalisation in the Deferred Production Variant has been carried out, or alternatively in the Integrated Production Variant without having the OS PrePersonalisation performed. In the latter case, the OS PrePersonalisation lies in the hands of the Product PrePersonaliser.

The TOE or product respectively is delivered as smart card (dual-interface, with or without activated contactless interface) with already loaded Operating System and, depending on the production variant (see above), with or without finished OS PrePersonalisation.

The user is provided with guidance for TOE identification in [12], chapter 3.1.2. For TOE identification the COS version as well as the product variant has to be checked. The variant can either be a test configuration (Test Card) or an operational configuration (Real Card). The Test Configuration is not considered as part of the TOE.

For identification of the product during its different life-cycle states the GET DATA command (CLA=80, INS=CA) can be used.

With the parameters P1=’DF’ and P2=’99’ the Card Configuration Data as described in [11], chapter 8.6.5, 8.7.6 can be retrieved whereby the COS version can be identified. The following response is expected:

Response
DF 99 0C XX XX **02 02** 00 62 **04 00** 81 00 13 2A 90 00

Table 3: Response to GET DATA command (P1=’DF’ and P2=’99’)

The following table describes the evaluated COS version:

Product information	#Byte of Response APDU	Expected value
Mask Identifier (OS Identifier)	6-7	‘02 02’
Mask Identifier (OS Release Level)	10-11	‘04 00’

Table 4: TOE Identification (COS version) with GET DATA command (P1=’DF’ and P2=’99’)

With the parameters P1=’9F’ and P2=’7F’ the CPLC information as described in [11], chapter 8.6.5, 8.7.2 and in [12], chapter 3.2.4, 7.7.7, 7.7.7.1.2 can be retrieved whereby the COS version and the variant can be identified. The following response is expected:

Response
9F 7F 2A XX XX XX XX **02 02** 00 62 **04 00** XX XX XX XX XX XX XX XX **1Y** XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX 90 00

Table 5: Response to GET DATA command (P1=’9F’ and P2=’7F’)

Hereby, XX stands for any byte value, and with Y=‘0’ or ‘1’ the variant can be identified (see below).

The following table describes the evaluated COS version and variant:

Product information	#Byte of Response APDU	Value according to [12], chapter 3.1.2.2
OS Identifier	8-9	‘02 02’
OS Release Level	12-13	‘04 00’
Product Configuration	22	Real Card: ‘10’ (Deferred Production Variant) ‘11’ (Integrated Production Variant) Test Card: ‘01’ or ‘00’

Table 6: TOE Identification (COS version and variant) with GET DATA command (P1=’9F’ and P2=’7F’)

The COS version can as well be identified by using the FINGERPRINT command with prefix “00…00” (128 bytes with value zero). This command is available after TOE Flashing.

Response
88AD4B53F4EA19ED939D5507C8D0F5C3FFC5C88FE109F1F5318DE46A51496DF29000

Table 7: Response to FINGERPRINT command with prefix “00…00”

The Identification of the TOE's Wrapper is described in [13], chapter 1.1. Refer as well to Table 2, row no. 3 in this Certification Report.

3. Security Policy

The TOE is a composite smart card product, based on the hardware platform Infineon Security Controller IFX_CCI_000005h from Infineon Technologies AG and with Smart Card Embedded Software IDEMIA_HC_Germany_NEO_G2.1_COS, V1 Operating System implemented by IDEMIA Germany GmbH according to the G2-COS specification [17] from gematik.

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

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

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

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

Security Objectives for the operational environment defined in the Security Target	Description according to the ST
	ments are met: (i) TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the user guidance, including TOE related application notes, usage requirements, recommendations and restrictions, and (ii) certification report including TOE related usage requirements, recommendations, restrictions and findings resulting from the TOE's evaluation and certification.
OE.Resp-ObjS	Treatment of User Data and TSF Data by the Object System All User Data and TSF Data of the object system are defined as required by the security needs of the specific application context.
OE.Process-Card	Protection during Personalisation Security procedures shall be used after delivery of the TOE during Phase 6 'Personalisation' up to the delivery of the smart card to the end-user in order to maintain confidentiality and integrity of the TOE and to prevent any theft, unauthorised personalisation or unauthorised use.
OE.PACE_Terminal	PACE support by contactless terminal The external device communicating through a contactless interface with the TOE using PACE shall support the terminal part of the PACE protocol.
OE.LogicalChannel	Support of more than one logical channel The TOE supports more than one logical channel each bound to an independent subject.

Table 8: Security Objectives for the operational environment

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

5. Architectural Information

The TOE is set up as a composite product. It is composed of the Infineon Security Controller IFX_CCI_000005h from Infineon Technologies AG and the Smart Card Embedded Software with the IDEMIA_HC_Germany_NEO_G2.1_COS, V1 Operating System developed by IDEMIA Germany GmbH.

For the implementation of the cryptographic functionality the Smart Card Embedded Software uses the cryptographic features of the underlying high-secure IC and (partially) its dedicated cryptographic library.

For details concerning the CC evaluation of the underlying IC see the evaluation documentation under the Certification ID BSI-DSZ-CC-1110-V3-2020 ([14], [15]).

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

- Application Layer (APP)
- Hardware Abstraction Layer (HAL)
- System Layer (SYS)

- Shared System/Standard Services (SSS)
- Wrapper

6. Documentation

The evaluated documentation as outlined in Table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target [6] and [7].

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

7. IT Product Testing

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

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

- testing APDU commands related to authentication
- testing APDU commands related to access control,
- testing APDU commands related to general protection of User data and TSF data
- testing APDU commands related to cryptographic functions,
- testing APDU commands related to key management,
- testing APDU commands related to protection of communication,
- testing APDU commands related to security relevant attributes,
- testing the LOAD APPLICATION commands,
- penetration testing related to the verification of the reliability of the TOE,
- source code analysis performed by the evaluators,
- side channel analysis for hash,
- fault injection attacks (laser 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] and [7]:

IDEMIA_HC_Germany_NEO_G2.1_COS, V1

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-V3-2020 (refer to [15]).

For the implementation of the cryptographic functionality the Smart Card Embedded Software uses the cryptographic features of the underlying high-secure IC and (partially) its dedicated cryptographic library.

The TOE covering the IC and the Smart Card Embedded Software (IDEMIA_HC_Germany_NEO_G2.1_COS, V1 Operating System) is delivered as a smart card (dual-interface with or without activated contactless interface) without any object system installed. The configuration as Test Card is explicitly not in scope of this evaluation as it is not considered as part of the TOE. 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 DATA in different command variants according to the user guidance documentation [11], chapter 8.6.5, 8.7.2 and 8.7.6, and [12], chapter 3.2.4, 7.7.7 and 777.1.2. See chapter 2 of this Certification Report for details.

9. Results of the Evaluation

9.1. CC specific results

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

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

The following guidance specific for the technology was used:

(i) Composite product evaluation for Smart Cards and similar devices according to AIS 36 (see [4]). On base of this concept the relevant guidance documents of the underlying IC platform (refer to the guidance documents covered by [15]) and the document ETR for composite evaluation from the IC's evaluation ([16]) 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, AVA_VAN.5 augmented for this TOE evaluation.

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, AVA_VAN.5

The Security Target [6] and [7] uses the mandatory parts of the PP and the optional packages Contactless, Logical Channel and RSA Key Generation defined in the PP. None of the PP's further optional packages Crypto Box, 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 [17] and the Technical Guideline BSI TR-03116-1 [21] 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. The validity period of each algorithm is mentioned in the official catalogue [21].

The cryptographic algorithms and protocols as outlined in Table 9 in annex C of part D of this report are implemented in the card operating system and hereby make use of the IFX_CCI_000005h secure dual-interface controller and its related Crypto Libraries ACL v2.08.007 and SCL v02.04.002 provided by Infineon Technologies AG that are part of the TOE. In particular, the core routines for RSA (encryption, decryption, signature generation, signature verification and key generation) and ECC (ECDSA signature generation and verification, ECDH, key generation), the AES CBC mode and the SHA hash calculation are taken from the Crypto Libraries, for random number generation the TOE uses the PTG.3 provided by the IC. The security evaluation of these cryptographic algorithms was performed in the framework of the certification of the IC with its related Crypto Libraries (refer to the Certification Report [15] and the corresponding Security Target [14]). The TOE relies on the correct (i.e. standard-conform) and secure implementation of these cryptographic algorithms. The remaining cryptographic implementation was analysed in the framework of the present composite evaluation of the TOE.

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in Table 2 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 2) which contains obligations and guidelines for the developer of the product layer on top on how to securely use this certified TOE and which measures have to be implemented in order to fulfil the security requirements of the Security Target of the TOE. In the course of the evaluation of the composite product or

system it must be examined if the required measures have been correctly and effectively implemented by the product layer on top.

In particular, the following aspects from the TOE user guidance documentation [11] to [13] 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 ([19]):

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

  This concerns the design and implementation of object systems of card products including application development prior to and after card product delivery as well as card management e.g. by using the command LOAD APPLICATION.

  For an object system, one has to take care of the choice of the access rules, flags and other security attributes for the object system and its objects. In particular, this concerns key objects, PIN objects and TOE specific system objects including their assigned security attributes.

  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 [17]).

  Any object system set up on the TOE shall only make use of the TOE's certified functionality. Card products with an object system that do not fulfil this requirement run out of the scope of the certified TOE and shall not be delivered respective used. It has to be considered that the TOE implements the functionality of the G2-COS specification [17] that is defined as mandatory as well as the chosen optional packages Contactless, Logical Channel and RSA Key Generation in [17], but none of the further optional packages Crypto Box, PACE for Proximity Coupling Device and RSA CVC (and USB) specified in [17]. Optional commands from the G2-COS specification [17] and additional commands and command variants beyond the G2-COS specification [17] for the usage phase provided by the TOE are outlined in the user guidance [12], chapter 3.2 and 7. Developer-specific (pre-)personalisation commands are described in the user guidance [11], chapter 8.6.

  Within an object system no key ID or PIN ID duplicates in the same folder shall exist. The object system has to be checked for taking this requirement into account by using the TOE's Wrapper according to the user guidance [13], chapter 2.3.6. 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 to the user guidance documentation [11], [12] and [13], chapter 2.3.

- Key usage and handling:

  Refer to the user guidance [12], chapter 8.4, 13.1 and 13.3.

- PIN / PUK Handling:

  Refer to the user guidance [12], chapter 6, 8.3, 13.2, 13.3.1 and 13.3.2.

- Security requirements and hints for Phase 6 of the TOE's life-cycle model described in the ST ([6], [7]), more detailed for the OS Personalisation Phase consisting of the Product PrePersonalisation (covering the loading of a pre-configured object system onto the card) and the Product Personalisation (covering the personalisation of the previously loaded object system with individual data and secrets):

  In particular, the TOE's specific load concept and functionality for loading a pre-configured object system onto the card in the Product PrePersonalisation and for the personalisation of such installed object system in the Product Personalisation has to be taken into account.

  Refer to the user guidance [11].

- Security requirements and hints for Phase 7 of the TOE's life-cycle model described in the ST ([6], [7]), more detailed for the operational use of the card:

  Refer to the user guidance documentation [12].

- The TOE's Wrapper and its specifics beyond the Wrapper specification [18]:

  Refer to the user guidance [13].

- Overwriting security attributes of objects in card products:

  For the design and implementation of a card product running on the TOE that undergoes a later TR-conformity testing according to the Technical Guideline BSI TR-03144 ([19]) it is strongly recommended to care for that via the TOE's specific personalisation commands as well as via the TOE's regular commands available in Phase 7 of the TOE's life-cycle model 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). This addresses the appropriate setting of access rules and flags for the object system's objects.

  Refer to the user guidance documentation [11] and [12].

For a TR-conformity testing of a card product set up on the TOE according to the Technical Guideline BSI TR-03144 ([19]) the following specific aspects and issues have to be taken into account:

- For the usage of the TOE's Wrapper in the framework of the TR-conformity testing of a card product according to the Technical Guideline BSI TR-03144 ([19]) refer in particular to its specifics beyond the Wrapper specification [18] as these are outlined in the user guidance [13].
- For the TR-conformity testing of a card product according to the Technical Guideline BSI TR-03144 ([19]), the TOE’s Wrapper shall not be used together with the configuration file CFG_THROW_WARNING. Refer to the user guidance [13], chapter 2.4.
- Specific requirements for the TR-conformity testing of a card product according to the Technical Guideline BSI TR-03144 ([19]) are specified in the user guidance [13], chapter 2.3 including subchapters. Each requirement for a card product addressed there has to be fulfilled by the card product undergoing a TR-conformity testing according to the Technical Guideline BSI TR-03144 ([19]), and a corresponding check for fulfilment of these requirements within the card product has to be performed in the framework of the TR-conformity testing.

Note: If for a card product such check for fulfilment of the requirements addressed in [13], chapter 2.3 is not possible or if the card product does not fulfil the requirements addressed in [13], chapter 2.3 this card product will be rejected for a TR-certificate according to the Technical Guideline BSI TR-03144 ([19]).

- The implementation of the TOE's Wrapper provides the functionality to handle and export Key-/PIN-objects (including corresponding public security attributes) with duplicated key-/PIN-Identifiers within the same folder of an object system (application) that is set up on the TOE.

  Each folder in the card product's object system has to be checked whether key ID or PIN ID duplicates within this folder are existing. This check shall be done by using the TOE's Wrapper according to the user guidance [13], chapter 2.3.6.

  Note: If there is any folder with key ID or PIN ID duplicates found the card product will be rejected for a TR-certificate according to the Technical Guideline BSI TR-03144 ([19]).

- For the card product, it has to be checked that via the TOE's specific personalisation commands as well as via the TOE's regular commands available in Phase 7 of the TOE's life-cycle model initialised security attributes and public key data of the object system and its objects cannot be overwritten (except for where explicitly intended by the object system's intention and design).

  Note: If overwriting of initialised security attributes and public key data of the object system and its objects via the TOE's specific personalisation commands or via the TOE's regular commands available in Phase 7 of the TOE's life-cycle model 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 ([19]).

- Any object system set up on the TOE shall only make use of the TOE's certified functionality. The card product's object system has to be checked for taking this requirement into account.

  It has to be considered that the TOE implements the functionality of the G2-COS specification [17] that is defined as mandatory as well as the chosen optional packages Contactless, Logical Channel and RSA Key Generation in [17], but none of the further optional packages Crypto Box, PACE for Proximity Coupling Device and RSA CVC (and USB) specified in [17]. Optional commands from the G2-COS specification [17] and additional commands and command variants beyond the G2-COS specification [17] for the usage phase provided by the TOE are outlined in the user guidance [12], chapter 3.2 and 7. Developer-specific (pre-)personalisation commands are described in the user guidance [11], chapter 8.6.

  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 ([20]) indicates the use of uncertified COS functionality the card product will be rejected for a TR-certificate according to the Technical Guideline BSI TR-03144 ([19]).

- If in the framework of the TR-conformity testing of a card product according to the Technical Guideline BSI TR-03144 ([19]) the Konsistenz-Prüftool according to the Technical Guideline BSI TR-03143 ([20]) 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 [17] or the user guidance [12] this has to be manually examined and valuated.

- For a card product that undergoes a TR-conformity testing according to the Technical Guideline BSI TR-03144 ([19]), the identification data of the underlying platform (TOE) shall be checked for correctness, that is consistency related to the identification data depicted in chapter 2 of this Certification Report.
- For a card product that undergoes a TR-conformity testing according to the Technical Guideline BSI TR-03144 ([19]) with using the Konsistenz-Prüftool according to the Technical Guideline BSI TR-03143 ([20]) it has to be taken into account that for an initialised, not yet personalised card product the functionality of the command READ BINARY (in particular for reading out a file as e.g. EF.ATR) is not available.

  In the case that the Konsistenz-Prüftool according to the Technical Guideline BSI TR-03143 ([20]) expects for its conformity test run read access to a file (as e.g. the EF.ATR) via the command READ BINARY, for conformity testing of the initialised, not yet personalised card product an appropriate workaround has to be set up by the TR-evaluation body. This workaround has to satisfy the overall intention of the TR-conformity testing according to the Technical Guideline BSI TR-03144 ([19]) that in the end a complete picture of the object system installed in the initialised, not yet personalised card product is obtained and a comparison against the respective object system specification is carried out.

11. Security Target

For the purpose of publishing, the Security Target [9] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12. Regulation specific aspects (eIDAS, QES)

None.

13. Definitions

13.1. Acronyms

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
APDU	Application Protocol Data Unit
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CBC	Cipher Block Chaining
CC	Common Criteria for IT Security Evaluation
CCRA	Common Criteria Recognition Arrangement
CEM	Common Methodology for Information Technology Security Evaluation

CMAC	Cipher-based Message Authentication Code
CPLC	Card Production Life Cycle
cPP	Collaborative Protection Profile
CPU	Central Processing Unit
DEMA	Differential Electromagnetic Analysis
DFA	Differential Fault Analysis / Attack
DGI	Data Grouping Identifier
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 Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
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
MAC	Message Authentication Code
NVM	Non-Volatile Memory
PACE	Password Authenticated Connection Establishment
PIN	Personal Identification Number
PP	Protection Profile
PRNG	Physical Random Number Generator
PTV	Product Type Version
PUK	Personal Unblocking Key
QES	Qualified Electronic Signature
RFU	Reserved for Future Use

RNG	Random Number Generator
RSA	Rivest Shamir Adleman Algorithm
SAR	Security Assurance Requirement
SEMA	Simple Electromagnetic Analysis
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SM	Secure Messaging
SMC-B	Security Module Card Type B
SPA	Simple Power Analysis
ST	Security Target
SW	Software
TOE	Target of Evaluation
TR	Technische Richtlinie (Technical Guideline)
TSF	TOE Security Functionality

13.2. Glossary

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

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

14. Bibliography

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

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

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

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

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

[7] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) 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, Reuse of evaluation resultsAIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers

[6] Security Target BSI-DSZ-CC-1098-2020, Security Target IDEMIA_HC_Germany_NEO_G2.1_COS, V1, Version 1.18, 3 July 2020, IDEMIA Germany GmbH (confidential document)

[7] Security Target Lite BSI-DSZ-CC-1098-2020, Security Target Lite IDEMIA_HC_Germany_NEO_G2.1_COS, V1, Version 1.05, 2 July 2020, IDEMIA Germany GmbH (sanitised public document)

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

[9] ETR BSI-DSZ-CC-1098-2020, Evaluation Technical Report (ETR) – Summary for IDEMIA_HC_Germany_NEO_G2.1_COS, V1, Version 1.1, 17 July 2020, SRC Security Research & Consulting GmbH (confidential document)

[10] Configuration List BSI-DSZ-CC-1098-2020, Configuration List IDEMIA_HC_Germany_NEO_G2.1_COS, V1, Version 3.20, 16 July 2020, IDEMIA Germany GmbH (confidential document)

[11] IDEMIA_HC_Germany_NEO_G2.1_COS, V1 – Preparative Guidance, Version 1.10, 3 July 2020, IDEMIA Germany GmbH

[12] IDEMIA_HC_Germany_NEO_G2.1_COS, V1 – Operational User Guidance, Version 2.1, 16 July 2020, IDEMIA Germany GmbH

[13] IDEMIA_HC_Germany_NEO_G2.1_COS, V1 – Wrapper Guidance, Version 1.7, 3 July 2020, IDEMIA Germany GmbH

[14] Security Target of the underlying hardware platform, Common Criteria Confidential Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h, H13, Revision 3.3, 22 April 2020, Infineon Technologies AG, BSI-DSZ-CC-1110-V3-2020 (confidential document)

Security Target Lite of the underlying hardware platform, Common Criteria Public Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h H13, Revision 1.8, 22 April 2020, Infineon Technologies AG, BSI-DSZ-CC-1110-V3-2020 (sanitised public document)

[15] Certification Report BSI-DSZ-CC-1110-V3-2020 for Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions from Infineon Technologies AG, 13 May 2020, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[16] ETR for Composite Evaluation of the underlying hardware platform Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h, H13 from certification procedure BSI-DSZ-CC-1110-V3-2020, Version 1, 23 April 2020, TÜV Informationstechnik GmbH (confidential document)

[17] Einführung der Gesundheitskarte, Spezifikation des Card Operating System (COS), Elektrische Schnittstelle, Version 3.12.0, 15.05.2019, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Errata zu Release 3.1.1 Online-Produktivbetrieb (Stufe 3), Version 1.0.0, 27.08.2019, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

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

[19] 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)

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

[21] 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)

[22] Technical Guideline BSI TR-03111: Elliptic Curve Cryptography, Version 2.10, 01.06.2018, Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

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

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

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

[27] 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)

[28] 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)

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

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

[31] 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

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

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

[34] 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)

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 Lite [7] 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-1098-2020

Evaluation results regarding development and production environment

The IT product IDEMIA_HC_Germany_NEO_G2.1_COS, V1 (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 and 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 30 July 2020, 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) Achelos GmbH, Vattmannstraße 1, 33100 Paderborn, Germany (Development)

b) IDEMIA Courbevoie, 2 Place Samuel de Champlain, 92 400 Courbevoie, France (Development)

c) IDEMIA Germany GmbH, Konrad-Zuse-Ring 1, 24220 Flintbek, Germany (OS Flash Loading, OS PrePersonalisation)

d) NedCard Shanghai Microelectronics Co. Ltd., Standardized Plant Building #8, No. 789 Puxing Road, Caohejing Hi-Tech Park, EPZ, 201114 Shanghai, China (Module Production)

e) IDEMIA Noida, Idemia Tower Plot No 1-A, Sec 73 Noida Uttar Pradesh, India (Card Embedding)

f) IDEMIA Ostrava, CZECH s.r.o. Jelínkova 1174/3a, 72100 Ostrava, Czechia (Card Embedding)

g) IDEMIA Shenzhen, 6/F, Great Wall Technology Building 2# No.3 Kefa Road, Science & Technology Park, Nanshan District Shenzhen 518057, China (Card Embedding, Module Production)

h) PAV Lütjensee, Hamburger Straße 6, 22952 Lütjensee, Germany (Card Embedding)

i) GNC TCS TECHNOLOGIE, CARDS & SERVICES GMBH (TCS Neu-Isenburg), Odenwaldstraße 19, 63263 Neu-Isenburg, Germany (Card Embedding)

j) TCS CARDS & SERVICES GMBH (TCS Bamberg), Kronacher Straße 61, 96052 Bamberg, Germany (Card Embedding)

k) For development and production sites regarding the underlying IC platform please refer to the Certification Report BSI-DSZ-CC-1110-V3-2020 ([15]).

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

Annex C of Certification Report BSI-DSZ-CC-1098-2020

Overview and rating of cryptographic functionalities implemented in the TOE

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
1	Authenticity	RSA signature generation (RSASSA-PSS-SIGN with SHA-256, RSASSA PKCS1-V1_5, RSA ISO9796-2 DS2 with SHA-256)	[24], [25] (RSA) [26] (SHA]	Modulus length = 2048, 3072	[17], chap. 6.6.3.1 [21]	FCS_COP.1/COS.RSA.S, FCS_COP.1/SHA • PSO COMPUTE DIGITAL SIGNATURE FCS_COP.1/RSA-1_SICP • RSA by ACL-1 used
2		ECDSA signature generation	[22], [23] (ECDSA)	Key sizes according to the used elliptic curve: ansix9p256r1, ansix9p384r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1 [32], [33]	[17], chap. 6.6.3.2 [21]	FCS_COP.1/COS.ECDSA.S • PSO COMPUTE DIGITAL SIGNATURE FCS_COP.1/ECDSA-1_SICP • ECDSA by ACL-1 used Note: the hash value (SHA-256, -384, -512) is given within the command data of PSO COMPUTE DIGITAL SIGNATURE
3		ECDSA signature verification using SHA-256, SHA-384, SHA-512	[22], [23] (ECDSA) [26] (SHA)	Key sizes according to the used elliptic curve: ansix9p256r1, ansix9p384r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1 [32], [33]	[17], chap. 6.6.4.2 [21]	FCS_COP.1/COS.ECDSA.V, FCS_COP.1/SHA • PSO VERIFY CERTIFICATE • PSO VERIFY DIGITAL SIGNATURE • LOAD APPLICATION FCS_COP.1/ECDSA-1_SICP • ECDSA by ACL-1 used 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	[26] (SHA)	-	[17], chap. 6.1.2, 14.9.2	FPT_ITE.1 • FINGERPRINT
5	Authentication	AES in CBC mode	[27] (AES) [29] (CBC) [17]	|k| = 128, 192, 256	[17], chap. 6.7.1.2, 6.7.2.2 [21]	FCS_COP.1/COS.AES • MUTUAL AUTHENTICATE • GENERAL

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
						AUTHENTICATE, mode asynchronous symmetric card administration FCS_COP.1/AES-SCL-1_SICP • AES-CBC by SCL-1 used
6		AES in CMAC mode (incl. generation of sub-keys)	[27] (AES) [28] (CMAC) [17]	|k| = 128, 192, 256	[17], chap. 6.6.1, 6.6.2 [21], chap. 3.6.2]	FCS_COP.1/COS.CMAC • MUTUAL AUTHENTICATE • GENERAL AUTHENTICATE, mode asynchronous symmetric card administration FCS_COP.1/AES-SCL-1_SICP • AES-CBC by SCL-1 used, last block of AES in CBC mode used as CMAC
7		RSA signature generation (RSASSA-PSS-SIGN with SHA-256, RSASSA PKCS1-V1_5)	[24] (RSA) [26] (SHA)	Modulus length = 2048, 3072	[17], chap. 6.6.3.1 [21]	FCS_COP.1/COS.RSA.S, FCS_COP.1/SHA • INTERNAL AUTHENTICATE FCS_COP.1/RSA-1_SICP • RSA by ACL-1 used
8		ECDSA signature generation	[22], [23] (ECDSA)	Key sizes according to the used elliptic curve: ansix9p256r1, ansix9p384r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1 [32], [33]	[17], chap. 6.6.3.2 [21]	FCS_COP.1/COS.ECDSA.S • INTERNAL AUTHENTICATE FCS_COP.1/ECDSA-1_SICP • ECDSA by ACL-1 used Note: the hash value (SHA-256, -384, -512) is given within the command data of INTERNAL AUTHENTICATE
9		ECDSA signature verification using SHA-256, SHA-384, SHA-512	[22], [23] (ECDSA) [26] (SHA)	Key sizes according to the used elliptic curve: ansix9p256r1, ansix9p384r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1 [32], [33]	[17], chap. 6.6.4.2 [21]	FCS_COP.1/COS.ECDSA.V, FCS_COP.1/SHA • EXTERNAL AUTHENTICATE • GENERAL AUTHENTICATE, mode asynchronous asymmetric card administration FCS_COP.1/ECDSA-1_SICP • ECDSA by ACL-1 used Note: there is no hash computation by the TOE in case of EXTERNAL

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
						AUTHENTICATE as the hash value is given within the command data
10	Authenticated Key Agreement	ECDH Diffie-Hellman-Protocol by PACE	[34], part 3, chap. A.2.3 [22], chap. 4.4	Key sizes according to the used protocol ids and elliptic curves: id-PACE-ECDH-GM-AES-CBC-CMAC-128 with brainpoolP256r1, id-PACE-ECDH-GM-AES-CBC-CMAC-192 with brainpoolP384r1, id-PACE-ECDH-GM-AES-CBC-CMAC-256 with brainpoolP512r1 |k| = 128, 192, 256 [32], [33]	[17], chap. 14.7.2.1 [34] [22]	FCS_CKM.1/DH.PACE.PICC • GENERAL AUTHENTICATE, mode PACE for end user cards FCS_COP.1/ECDH-1_SICP • ECDH by ACL-1 used
11	Key Derivation	Key Derivation for AES using SHA-1, SHA-256	[22], chap. 4.3.3.2 [27] (AES) [26] (SHA)	|k| = 128, 192, 256	[17], chap. 6.2.2, 6.2.3, 6.2.4, 6.2.5	FCS_CKM.1/AES.SM, FCS_COP.1/SHA • MUTUAL AUTHENTICATE • GENERAL AUTHENTICATE, mode mutual authenticate with ELC keys with secure messaging establishment • GENERAL AUTHENTICATE, mode PACE for end user cards
12		Key Derivation of OS PrePersonaliser Authentication Key	[27] (AES) [29] (CBC)	|k| = 256	n/a	IDEMIA proprietary Key Derivation mechanism. FCS_COP.1/COS.AES • MUTUAL AUTHENTICATE (OS PrePersonalisation phase) FCS_COP.1/AES-SCL-1_SICP • AES-CBC by SCL-1 used
13	Confidentiality	AES in CBC mode	[27] (AES) [29] (CBC) [34] (PACE SM)	|k| = 128, 192, 256	[17], chap. 6.7.1.2, 6.7.2.2 [21] [34]	FCS_COP.1/COS.AES • secure messaging FCS_COP.1/ PACE.PICC.ENC • PACE secure

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
						messaging FCS_COP.1/AES-SCL-1_SICP • AES-CBC by SCL-1 used
14		RSA encryption and decryption (RSA-OAEP) Transcipher RSA to ELC and ELC to RSA	[17] [24], chap. 7.1.1, 7.1.2	Modulus length = 2048, 3072 for RSA private key operation and 2048 for RSA public key operation	[17], chap. 6.8.1.2, 6.8.2.2 [21]	FCS_COP.1/COS.RSA • PSO ENCIPHER • PSO DECIPHER • PSO TRANSCIPHER (in case of transcription from or to an ELC key: in combination with ELC encryption and decryption in row 15) FCS_COP.1/RSA-1_SICP • RSA by ACL-1 used
15		ELC encryption and decryption Transcipher RSA to ELC and ELC to RSA	[17] [22]	Key sizes according to the used elliptic curve: ansix9p256r1, ansix9p384r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1 [32], [33]	[17], chap. 6.8.1.4, 6.8.2.3 [21]	FCS_COP.1/COS.ELC • PSO ENCIPHER • PSO DECIPHER • PSO TRANSCIPHER (in case of transcription from or to an RSA key: in combination with RSA encryption and decryption in row 14) • GENERAL AUTHENTICATE, mode asynchronous asymmetric card administration FCS_COP.1/ECDH-1 • ECDH by ACL-1 used FCS_RNG.1/HPRG_SICP • HPRG of platform used FCS_COP.1/AES-SCL-1_SICP • AES-CBC by SCL-1 used
16	Integrity	AES in CMAC mode (incl. generation of sub-keys)	[27] (AES) [28] (CMAC) [34] (PACE SM)	|k| = 128, 192, 256	[17], chap. 6.6.1, 6.6.2 [21], chap. 3.6.2 [34]	FCS_COP.1/COS.CMAC • secure messaging FCS_COP.1/PACE.PICC.MAC • PACE secure messaging FCS_COP.1/AES-SCL-1_SICP

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
						• AES-CBC by SCL-1 used, last block of AES in CBC mode used as CMAC
17	Trusted Channel	Secure Messaging based on asymmetric authentication	[22], [23] (ECDSA) [26] (SHA)	|k| = 128, 192, 256	[17], chap. 14.7.2.2, 14.7.2.5, 13.1	FTP_ITC.1/TC • GENERAL AUTHENTICATE, mode mutual authenticate with ELC keys with secure messaging establishment, ECDH key agreement according row 26 is used, Key Derivation for AES according row 11 is used for the derivation of session keys • GENERAL AUTHENTICATE, mode asynchronous asymmetric card administration, ECDSA signature verification using SHA-256, SHA-384, SHA-512 according row 9 is used, ELC decryption according row 15 is used FCS_COP.1/COS.AES, FCS_COP.1/COS.CMAC • secure messaging according rows 13, 16
18		Secure Messaging based on symmetric authentication	[27] (AES) [29] (CBC) [28] (CMAC)	|k| = 128, 192, 256	[17], chap. 14.7.1.2, 14.7.2.3, 13.1	FTP_ITC.1/TC • MUTUAL AUTHENTICATE, symmetric authentication according rows 5 and 6 is used, Key Derivation for AES according row 11 is used for the derivation of session keys • GENERAL AUTHENTICATE, mode asynchronous symmetric card administration, symmetric authentication according rows 5

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
						and 6 is used FCS_COP.1/COS.AES, FCS_COP.1/COS.CMAC • secure messaging according rows 13, 16
19		Secure Messaging in ENC/MAC mode established during PACE	[34], part 2	|k| = 128, 192, 256	[17], chap. 14.7.2.1, 13.1	FTP_ITC.1/PACE.PICC • GENERAL AUTHENTICATE, mode PACE for end user cards, ECDH Diffie-Hellman-Protocol by PACE according row 10 is used, Key Derivation for AES according row 11 is used for the derivation of session keys FCS_COP.1/ PACE.PICC.MAC, FCS_COP.1/PACE.PICC.ENC • PACE secure messaging according rows 13, 16
20	Key Generation	RSA key generation	Infineon/ Idemia-proprietary algorithm, generated keys are in conformance with [24], chap. 3.1, 3.2 [21]	Modulus length = 2048, 3072	[17], chap. 14.9.3.13 and (N002.100)	FCS_CKM.1/RSA • PSO GENERATE ASYMMETRIC KEY PAIR FCS_CKM.1/RSA-1_SICP • RSA by ACL-1 used
21		ECC key generation	Infineon/ Idemia-proprietary algorithm, generated keys are in conformance with [23], chap. A.4.3 [22], chap. 4.1.3	Key sizes according to the used elliptic curve: ansix9p256r1, ansix9p384r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1 [32], [33]	[17], chap. 14.9.3.13 and (N002.500)	FCS_CKM.1/ELC • PSO GENERATE ASYMMETRIC KEY PAIR FCS_CKM.1/EC-1_SICP • EC by ACL-1 used
22	Cryptographic Primitive	Hybrid physical RNG PTG.3	AIS20/AIS31, refer to BSI-DSZ-CC-1110-V3 [15]	n/a	[17] [21]	FCS_RNG.1 • GET CHALLENGE • authentication protocols (EXTERNAL AUTHENTICATE, MUTUAL AUTHENTICATE,

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
						GENERAL AUTHENTICATE) • key agreement for secure messaging FCS_RNG.1/PACE • PACE protocol FCS_RNG.1/GR • GET RANDOM FCS_RNG.1/HPRG_SICP • HPRG of platform used in any cases
23		SHA-1, SHA-256, SHA-384, SHA-512	[26]	n/a	[17], chap. 6.1 [21]	FCS_COP.1/SHA
24		RSA signature generation	[24]	Modulus length = 2048, 3072	[17], chap. 6.4 [21]	FCS_COP.1/RSA-1_SICP • RSA by ACL-1
25		ECDSA signature generation and verification	[22], [23]	Key sizes according to the used elliptic curve: ansix9p256r1, ansix9p384r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1 [32], [33]	[17], chap. 6.6.3.2, 6.6.4.2 [21]	FCS_COP.1/ECDSA-1_SICP • ECDSA by ACL-1
26		ECDH key agreement	[34], part 3, chap. A.2.3 [22], chap. 4.4	Key sizes according to the used elliptic curve: ansix9p256r1, ansix9p384r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1 [32], [33]	[17], chap. 6.8.1.3 [21]	FCS_COP.1/ECDH-1 • ECDH by ACL-1
27		RSA encryption	[24]	Modulus length = 2048	[17], chap. 6.4 [21]	FCS_COP.1/RSA-1_SICP • RSA by ACL-1
28		RSA decryption	[24]	Modulus length = 2048, 3072	[17], chap. 6.4 [21]	FCS_COP.1/RSA-1_SICP • RSA by ACL-1
29		AES in CBC mode	[27] (AES) [29] (CBC)	|k| = 128, 192, 256	[17], chap. 6.7.1.2, 6.7.2.2	FCS_COP.1/AES-SCL-1_SICP • AES-CBC by SCL-1
30		AES in CMAC mode	[27] (AES) [28] (CMAC)	|k| = 128, 192, 256	[17], chap. 6.6.1, 6.6.2	FCS_COP.1/AES-SCL-1_SICP • AES-CBC by SCL-1 used, last block of

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
						AES in CBC mode used as CMAC

Table 9: TOE cryptographic functionality

Note: End of report