Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0956-2016

for

Health Insurance Card G2 1.0.0

from

Gemalto 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-0956-2016 (*)

Health Insurance Card G2 1.0.0

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

SOGIS
Recognition Agreement

Common Criteria

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

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

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

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

Common Criteria
Recognition Arrangement
for components up to
EAL 4

Bonn, 28 October 2016

For the Federal Office for Information Security

Joachim Weber
Head of Division

L.S.

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

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

This page is intentionally left blank.

Preliminary Remarks

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

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

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

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

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

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

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

Contents

A. Certification

1. Specifications of the Certification Procedure

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

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

2. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1. European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

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

---

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

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

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

5 Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

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

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. 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.sogisportal.eu.

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

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

2.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), 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 CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

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

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

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

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

3. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Health Insurance Card G2 1.0.0 has undergone the certification procedure at BSI.

The evaluation of the product Health Insurance Card G2 1.0.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 29.09.2016. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Gemalto GmbH.

The product was developed by: Gemalto GmbH.

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

4. Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report or in the CC itself.

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

In order to avoid an indefinite usage of the certificate when evolved attack methods require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 28 October 2016 is valid until 27 October 2021. 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,

[6] Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the 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.

5. Publication

The product Health Insurance Card G2 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Gemalto GmbH
Werinherstr. 81
81541 München

B. Certification Results

The following results represent a summary of

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

1. Executive Summary

The Target of Evaluation (TOE) is the product Health Insurance Card G2 1.0.0 developed by Gemalto GmbH.

The TOE is a smart card product according to the G2-COS specification [20] from gematik and is implemented on the hardware platform Infineon Security Controller M7892 B11 from Infineon Technologies AG ([refer to [17], [18]).

The TOE is intended to be used as a card operating system platform within the framework of the German health care system.

For this purpose, the TOE implements a classical PIN-based user authentication. The product is capable to authenticate an external role and internal authentication services. Mutual authentication protocols allow for the establishment of secure sessions between the card and a trusted external entity. Its security state model is a prerequisite for controlling the access to the object system and the usage of cryptographic services. The object system stores PINs and cryptographic keys securely by access control mechanisms. Elementary cryptographic functions of the product form the basis for the different authentication protocols and cryptographic services. The following issues are covered:

- user authentication
- internal and external device authentication
- secure state model
- access-controlled cryptographic services
- secure access controlled object system
- elementary cryptographic functions

The TOE comprises:

- the circuitry of the contact-based chip including all IC Dedicated Software being active in the Smart Card Initialisation Phase, Personalisation Phase and Usage Phase of the TOE (the integrated circuit, IC)
- the IC Embedded Software (Health Insurance Card G2 Operating System)
- the Wrapper (TOE specific software tool for interpretation of exported TSF and User data)
- 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 [20], but does not contain itself any object system (applications). However, the delivered product can comprise beside the TOE also an object system already installed on the TOE.

In functional view, the TOE with its IC Embedded Software (Health Insurance Card G2 Operating System) is implemented according to the G2-COS specification [20] from gematik. Hereby, the TOE implements the mandatory part of the G2-COS specification [20] with the base functionality of the operating system platform. None of the optional packages defined in the G2-COS specification [20] as Crypto Box, Contactless, Logical Channels, PACE for Proximity Coupling Device and USB are implemented in the TOE.

The TOE supports none of the commands that are outlined as optional in the G2-COS specification [20]. Furthermore, the TOE provides specific initialisation and personalisation commands.

The Health Insurance Card G2 1.0.0 Operating System is implemented according to the G2-COS specification [20] from gematik, but with the following deviation: The implementation of the command MUTUAL AUTHENTICATE slightly differs concerning the internal handling of the challenge. However, this deviation is not externally visible at command level and does not affect security aspects.

The TOE provides further commands and command variants for the initialisation, personalisation and operational use as those are outlined in the user guidance [11], chapter 5 and 6.

The TOE's Wrapper is implemented according to the Wrapper specification [21] from gematik, but with the following deviation: The TOE's Wrapper implementation differs concerning the export of algorithm IDs. Refer to the user guidance [13], chapter 3.5.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Card Operating System Generation 2 (PP COS G2), Version 1.9, 18 November 2014, BSI-CC-PP-0082-V2-2014 [8]. The Security Target [6] and [7] uses the mandatory parts of the PP, but none of the PP's optional packages.

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 AVA_VAN.5, ATE_DPT.2 and ALC_DVS.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [7], chapter 8.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
Card Life Cycle State Machine	The Embedded Software incorporates a state machine to reflect the TOE life cycle phases. It ensures the secure evolution of the TOE from the IC manufacturing phase to the usage phase.
Production Commands	The production of the TOE is accomplished via a dedicated set of production commands according to the Specification for Chip card Personalization for German Health Card eGK Generation 2.
TOE Identification	The TOE provides functionality for identification of the wrapper, the chip, the platform and the image. Further the TOE provides the FINGERPRINT functionality according to the Gematik Specification.
Object System Management	The TOE provides a hierarchical file system according to ISO 7816 with formatted and transparent elementary files, life cycle states for objects and files and data export functionality in accordance with the wrapper.
Random Numbers	The TOE provides random numbers for cryptographic computations and authentication protocols.
Cryptographic Computations	The Embedded Software contains a cryptographic library to implement the cryptographic procedures made available via the respective APDU commands.

TOE Security Functionality	Addressed issue
PIN Authentication and PIN Object Management	The TOE provides functionality for PIN authentication and PIN management.
Asymmetric Device Authentication	The TOE accepts asymmetric authentication used by external devices to prove their authenticity to the card and optionally to secure the subsequent communication.
Symmetric Device Authentication	The TOE functionality is used for authentication of external devices by a symmetric one-time challenge-response protocol.
Access Management in Productive Phases	Access check in the productive phase is hard wired within the production commands and determines the life-cycle state, additionally secured by authentication or authentication and secure messaging.
Access Management in Usage Phase	Access is only granted according to defined access rules for each file and object.
Secure Messaging	The TOE provides the functionality to ensure protection of the data exchanged via APDUs by authenticity, integrity, and confidentiality using 3TDES or AES cryptography.
TSF Protection	The Embedded Software is designed to protect the TOE against fraudulent attacks.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [7], chapter 8.

The assets to be protected by the TOE are defined in the Security Target [6] and [7], chapter 4.1.1. 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 4.2, 4.3 and 4.4.

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:

Health Insurance Card G2 1.0.0

The following table outlines the TOE deliverables:

No.	Type	Identifier	Release	Form of Delivery
1.	HW/SW	Modules	Infineon Security Controller M7892 B11	Delivery of the contact based IF Modules with its IC dedicated software is done according to the delivery procedures specified in BSI-DSZ-CC-0782-V2-2015 [18]
2.	KEY	(Transport) Keys MK_ICC and KMC	-	Data exchange with ZMK encryption or by secure channel between KMSs.
3.	DOC	Specification for Chip card Personalization for German Health Card eGK Generation 2 (GeGKOS C1 on M7892) [11]	Version 1.12	Signed and encrypted delivery by email
4.	DOC	Software Requirements Specification For GeGKOS Generation 2 [12]	Version B12	Signed and encrypted delivery by email
5.	DOC	User guidance for Wrapper, Health Insurance Card G2 [13]	Version 1.8	Signed and encrypted delivery by email
6.	DOC	Card Initialization Specification, GeGKOS C1, Infineon M7892 B11 [14]	Version A05	Signed and encrypted delivery by email
7.	DOC	Operational User guidance ES, Electronic Health Card [15]	Version 1.23	Signed and encrypted delivery by email
8.	DOC	Preparative Procedures, Electronic Health Card - GeGKOS C1 [16]	Version 1.16	Signed and encrypted delivery by email
9.	SW	Wrapper	Version 1.31	Delivery in signed and encrypted email. Further a checksum of the wrapper jar-file “iwrapper.jar” is used to ensure integrity. The SHA-256 checksum is: 0x4D5CC0A619FBF2047F1DC55E1B93481E8DBEF39AB0A94DCFF7F5E859E154CD00
10.	SW	IC Embedded Software (the OS GeGKOS C1)	Version 1.00 Platform identifier: 0x05010D00C1010000 (refer to Table 5)	Implemented in the flash of the IC. The TOE covering the IC and the IC Embedded Software is delivered without any object system as module or smart card.

Table 2: Deliverables of the TOE

The Keys Kicc, K_Verify and personalization keys (Kenc, Kmac and Kdec) are included in the Software part of the TOE as on-card key containers. The key values are out of TOE scope. Outside the card, the keys MK_ICC and KMC are delivered in sense of CC.

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

- Product Code: M7892-B508-11
- Product Type: Infineon Security Controller M7892 B11
- RMS Version: IFX_SLE78V2_M_v15b14_78.015.14.0

The TOE Health Insurance Card G2 is as well known under the following product identificator:

Manufacturer: GEMAL (Gemalto)

Product: COS-G2 (GeGKOS C1)

OS Version Number: 1.0.0

According to the Security Target [6] and [7], chapter 2.1.7 the life cycle model of the TOE consists of the following eight phases:

Phase 1: IC Manufacturing (Infineon)

Phase 2: Software Development (Gemalto)

Phase 3: Loader File Generation (Gemalto)

Phase 4: Module Manufacturing (Gemalto)

Phase 5: Flashing of Loader File (Gemalto)

Phase 6: Initialization (Gemalto)

Phase 7: Personalization (Gemalto)

Phase 8: Usage

The delivery in the sense of CC comprises the delivery from the card manufacturer to the initializer as mentioned in the Table 2 above. The modules are delivered between the Gemalto sites by dedicated transport vehicles. Further are the transport keys delivered between the Gemalto sites by data exchange with ZMK encryption or by secure channel between both KMSs. Further the Product Image Data is transferred between the Gemalto sites by usage of the PDM or encrypted by mail. The Product Image file contains a Message Authentication Code to ensure the authenticity of the image. The wrapper is delivered signed and encrypted. The integrity of the wrapper could be ensured by checking the checksum over the jar-file according to the guidance [13].

Identification of the TOE can be done in each life cycle stage by retrieving the administrative data objects ‘DF70’ up to ‘DF76’ with the GET DATA command. For further information regarding the parametrization of the APDU and the expected response values according to the TOE life-cycle phase, please refer to [15] chapter 14. The following command APDU parametrization can be used to identify the TOE according to the guidance:

Field	Description - Value
CLA	00h in APPLICATIVE state, 80h else
INS	CAh
P1	DFh
P2	70h to 76h
Lc	-
Data	Not present
Le	00h – Response data expected

Table 3: Parametrization for GET DATA APDU for retrieving identification data

The Card Life Cycle State can be retrieved by GET DATA on OSDATA Tag ('DF74'). Life Cycle object is byte 2 of the response to GET DATA ('DF74'). Please find the meaning of the life cycle bytes in the following table:

State	Description	Life Cycle Byte in DO DF74
VIRGIN	Chip after manufacturing	40h
MODULE	Chip after module handler process	41h
GENERATE	Chip at the embedding process (optional)	42h
PERSO	Chip after the embedding process	43h
APPLICATIVE	Finished card production	14h

Table 4: Definition of life-cycle byte regarding GET DATA (DF74) response

The TOE is identified by its Platform Identifier. The Platform Identifier is an 8 byte sequence retrieved with GET DATA ('DF71'). For this TOE it must read:

Byte No.	Description	Value
1	IC Fabricator	05
2	IC Type (1)	01
3	IC Type (2)	0D
4	IC Type (3)	00
5	Product Type	C1
6	COS Version (1)	01
7	COS Version (2)	00
8	COS Version (3)	00

Table 5:Platform Identifier retrieved by GET DATA (DF71)

3. Security Policy

The TOE is a composite smart card product, based on the hardware platform Infineon Security Controller M7892 B11 from Infineon Technologies AG and with IC Embedded Software (Health Insurance Card G2 Operating System) implemented by Gemalto GmbH according to the G2-COS specification [20] from gematik.

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

- User Data Protection
- Protection of the TSF
- Identification and Authentication
- Security Management
- Cryptographic Support
- Trusted Path/Channels
- Security Audit
- Resource Utilisation

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment.

The following topics are of relevance:

Security Objectives for the operational environment defined in the Security Target	Description according to the ST
OE.Plat-COS	Usage of COS To ensure that the TOE is used in a secure manner the object system shall be designed such that the requirements from the following documents are met: (i) user guidance of the COS, (ii) application notes for the COS (iii) other guidance documents, and (iv) findings of the TOE evaluation reports relevant for applications developed for COS as referenced in the certification report.
OE.Resp-ObjS	Treatment of User Data All User Data and TSF Data of the object system are defined as required by the security needs of the specific application context.
OE.Process-Card	Protection of Smartcard during Initialization and Personalisation Security procedures shall be used after delivery of the TOE during Phase 6 Smartcard initialization and phase 7 personalisation up to the delivery of the smartcard to the end-user in order to maintain confidentiality and integrity of the TOE and to prevent any theft, unauthorised personalization or unauthorised use.

Table 6: Security Objectives for the operational environment

Details can be found in the Security Target [6] and [7], chapter 5.3.

5. Architectural Information

The TOE is set up as a composite product. It is composed of the Integrated Circuit (IC) Infineon Security Controller M7892 B11 from Infineon Technologies AG and the IC Embedded Software with the Health Insurance Card G2 1.0.0 Operating System developed by Gemalto GmbH.

A cryptographic library internally developed by Gemalto GmbH supplies the basic cryptographic functionalities needed for these OS components, utilizing the chip's cryptographic co-processors.

For details concerning the CC evaluation of the underlying IC see the evaluation documentation under the Certification ID BSI-DSZ-CC-0782-V2-2015 ([17], [18]).

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

Subsystem	Description of purpose
APDU Container	General APDU processing and evaluation of the APDU structure. The subsystem is invoked from the Process Handling and forwards processing to the Security Kernel, the Hardware Abstraction Layer, Error, Toolbox and System Service subsystems.
Error	General Error handling. This subsystem can be directly invoked by the System Service and Toolbox subsystem.
File System	Functionality for management of the file-system. This subsystem is directly called by the security Kernel and can call the Hardware Abstraction Layer, Toolbox, System Service and Error subsystem.
Hardware Abstraction Layer	Implements the main functionality for accessing the Hardware, e.g. for cryptographic computations. This subsystem is used mainly for accessing the Chip Hardware. Further it can call the Toolbox, the System Service and the Error subsystem.
Security Kernel	This subsystem establishes the main security functionality and can call the Hardware Abstraction Layer, the Error, System Service and Toolbox subsystem.
Process Handling	This subsystem establishes the main process handling for incoming commands and forwards processing to the APDU Container, Hardware Abstraction Layer, Error, Toolbox and System Service subsystem.
Toolbox	This subsystem provides functionality e.g. for TLV coding and memory management and can call the Chips Hardware directly, as well as calling the System Service and error subsystem.
System Services	This subsystem provides the functionality for the general system services as e.g. life cycle management and global variables and calls the chip's hardware directly. Further it can call the Toolbox and Error subsystem.
Wrapper	The Wrapper provides as the additional tool (software part) the translation of the card internal information for the external verification tool. The wrapper therefore only accesses the other subsystems indirectly/externally.

Table 7: Subsystems of the TOE with description

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:

TSF	Description
Card Life Cycle State Machine	The Embedded Software incorporates a state machine to reflect the TOE life cycle phases.
Object System Management	The TOE supports a hierarchical file system. Here, the access and modification of the contained resources are restricted by access rules.
Cryptographic Computations	The Embedded Software contains a cryptographic library to implement the cryptographic procedures made available via the respective APDU commands.
PIN Authentication and PIN Object Management	Human users can be authenticated by a correct PIN verification.
Key Object Management	Key object management relates to the Symmetric and Asymmetric Device Authentication. It is introduced by the developer to have a clear distinction between the key management and the key usage. The key management manages the keys, e.g. key reference check and key search.
Asymmetric Device Authentication	Asymmetric authentication is used by external devices to prove their authenticity to the card and optionally to secure the subsequent communication.
Symmetric Device Authentication	External devices can also authenticate themselves by a symmetric one-time challenge-response protocol.
Access Management in Usage Phase	The resources in the file system can only be accessed via APDU commands. Here, the access to the resources is restricted by access rules.
Secure Messaging	Secure Messaging provides the functionality to ensure protection of the data exchanged via APDUs by authenticity, integrity, and confidentiality using 3TDES or AES cryptography.
TSF Protection	The Embedded Software is designed to protect the TOE against fraudulent attacks.
Wrapper	The manufacturer proprietary command GET_OBJ_INFO is able to read out public (FMT_MTD.1/NE) configuration data of all objects other than files (FPT_ITE.2). It is used together with the external wrapper to export the data required for the official verification tool. Note that for files (folders and EFs) those data are exported via SELCT command, returning FCP data.

Table 8: Security functionalities covered by evaluation body testing

The evaluators have tested the TOE systematically against high attack potential during their penetration testing. The following attack scenarios have been covered:

- DFA/LFI on COS and on Cryptographic functionalities.

- SPA/DPA/SEMA/DEMA; Template attacks, Leakage analysis on Cryptographic functionalities.
- Changing the predefined sequence of invocation of components.
- Using a component in an unexpected context or for an unexpected purpose.
- Reaching limits of resources or maximum values of parameters, like filling buffers or fields.

The overall test result is that no deviations were found between the expected and the actual test results.

8. Evaluated Configuration

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

Health Insurance Card G2

There is only one configuration of the final TOE. It comprises the following items:

- The IC Infineon M7892 B11 consisting of the circuit of the chip and the IC dedicated software (BSI-DSZ-CC-0782-V2-2015 [18]),
- the embedded software (operating system) GeGKOS C1,
- the wrapper,
- the (transport) keys on the card as key containers and off card, and
- the guidance documentation

Refer to the information provided in chapter 2 of this Certification Report.

A cryptographic library internally developed by Gemalto GmbH supplies the basic cryptographic functionalities needed for these OS components, utilizing the chip's cryptographic co-processors.

The TOE covering the IC and the IC Embedded Software is delivered as a module or smart card without any 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 DATA in different command variants according to the user guidance [15], chapter 14.

9. Results of the Evaluation

9.1. CC specific results

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

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

The following guidance specific for the technology was used:

(i) Composite product evaluation for Smart Cards and similar devices (see AIS 36). According to this concept the relevant guidance documents of the underlying platform (refer to the guidance documents covered by [18]) and the document ETR for composite evaluation from the platform evaluation ([19]) have been applied in the TOE evaluation.

(ii) Guidance for Smartcard Evaluation.

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

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

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

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

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

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

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

The evaluation has confirmed:

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

The Security Target [6] and [7] use the mandatory parts of the PP and do not make use of the optional packages of the PP.

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

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

9.2. Results of cryptographic assessment

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

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
1.	Authenticity	RSA-Signature generation RSA_ISO9796-2_DS2_SIGN with SHA-256 RSA_SSA_PKCS#1v1_5 RSASSA_PSS_SIGN with SHA-256	[23], [24], SHA: [26]	Modulus length = 2048, 3072	[22] [20, 6.6.3.1]	FCS_COP.1/COS.RSA.S FCS_COP.1/SHA PSO COMPUTE DIGITAL SIGNATURE
2.	Authenticity	RSA-Signature verification RSA_ISO9796–2_DS1_ VERIFY	[23], [24], SHA: [26]	Modulus length = 2048	[22] [20, 6.6.4.1]	FCS_COP.1/COS.RSA.V FCS_COP.1/SHA PSO VERIFY CERTIFICATE
3.	Authenticity	ECDSA-signature generation COS standard curve parameters: brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, ansix9p256r1, ansix9p384r1	[27], [28], [32]	|q| = 256 |q| = 384 |q| = 512	[27] [20, 6.6.3.2] with all COS standard curves	FCS_COP.1/COS.ECDSA.S PSO COMPUTE DIGITAL SIGNATURE, with externally given hash value
4.	Authenticity	ECDSA-signature verification using SHA-256, 384, or 512 COS standard curve parameters: brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, ansix9p256r1, ansix9p384r1	[27], [28], [32], SHA: [26]	|q| = 256 |q| = 384 |q| = 512	[27] [20, 6.6.4.2] with all COS standard curves	FCS_COP.1/COS.ECDSA.V FCS_COP.1/SHA (1) PSO VERIFY CERTIFICATE, (2) PSO VERIFY DIGITAL SIGNATURE
5.	Authenticity	Fingerprint with SHA-256	[26]	-	[22] [20, 6.1.2]	FPT_ITE.1, FPT_ITE.2

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
6.	Authentication	AES encryption and decryption in CBC mode	[33, 6.5]	|k|=128 |k|=192 |k|=256 |challenge|=128	[20, 6.7.1.2, 6.7.2.2], [22]	FCS_COP.1/COS.AES (1) EXTERNAL\MUTUAL AUTHENTICATE (2) GENERAL AUTHENTICATE challenge is part of the de/encrypted data
7.	Authentication	CMAC with AES	[34]	|k|=128 |k|=192 |k|=256 |challenge|=128	[20, 6.6.1.2, 6.6.2.2], [22]	FCS_COP.1/COS.CMAC EXTERNAL AUTHENTICATE (encrypted) challenge is part of the MACed data
8.	Authentication	3TDES in CBC-Mode	[35]	|k|=168 |challenge|=64	[22], [20, 6.7.1.1, 6.7.2.1] Max. 216 message blocks with the same key (see [22, 4.4])	FCS_COP.1/COS.3TDES EXTERNAL AUTHENTICATE challenge is part of the de/encrypted data
9.	Authentication	3TDES in Retail-MAC	[20]	k|=168 |challenge|=64	[22] Max. 216 message blocks with the same key (see [22, 4.4]) [20, 6.6.1.1, 6.6.2.1] Padding: [38, 10.2.3.1]	FCS_COP.1/COS.RMAC EXTERNAL AUTHENTICATE (encrypted) challenge is part of the MACed data

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
10.	Authentication	2TDES in CBC-Mode	[36]	|k| = 112 |challenge|= 64	[38]	FCS_COP.1 / PAUTH Only during card production phases in secured environment . Not available in applicative phase.
11.	Authentication	2TDES in Retail-MAC	[25] MAC Algorithm 1 without truncation, and with triple DES taking the place of the block cipher.	|k| = 112 |challenge|= 64	[38]	FCS_COP.1 / PAUTH Only during card production phases in secured environment . Not available in applicative phase.
12.	Authentication	RSA-Signature generation RSA_ISO9796-2_ DS1_ SIGN_DS1 with SHA-256 RSA_SSA_PKCS#1v1 _5 RSASSA_PSS_SIGN with SHA-256	[23], [24] SHA: [26]	Modulus length= 2048, 3072	[22] [20, 6.6.3.1]	FCS_COP.1 /COS.RSA. S FCS_COP.1 /SHA INTERNAL AUTHENTI CATE
13.	Authentication	RSA-Signature verification RSA_ISO9796–2_DS1 _ VERIFY	[23], [24] SHA: [26]	Modulus length = 2048	[22] [20, 6.6.4.1]	FCS_COP.1 /COS.RSA. V FCS_COP.1 /SHA EXTERNAL AUTHENTI CATE
14.	Authentication	ECDSA-signature generation COS standard curve parameters: brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, ansix9p256r1, ansix9p384r1	[27], [28], [32]	|q| = 256 |q| = 384 |q| = 512	[27] [20, 6.6.3.2] with all COS standard curves	FCS_COP.1 /COS.ECDS A.S INTERNAL AUTHENTI CATE, with externally given hash value

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
15.	Authentication	ECDSA-signature verification using SHA-256, 384, or 512 COS standard curve parameters: brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, ansix9p256r1, ansix9p384r1	[27], [28], [32], SHA: [26]	|q| = 256 |q| = 384 |q| = 512	[27] [20, 6.6.4.2] with all COS standard curves	FCS_COP.1/COS.ECDSA.V FCS_COP.1/SHA EXTERNAL AUTHENTICATE
16.	Key Agreement	Derivation of 3TDES keys with SHA-256 (via MGF1)	[35]	|k| = 168	session cryptographic keys according to Key Derivation Function specified in sec. 5.6.3 in ANSI X9.63 and specified cryptographic key sizes 192 bit (168 bit effectively) that meet the following: ANSI X9.63 [20, 6.2.1]	FCS_CKM.1/3TDES_SM FCS_COP.1/SHA Derivation of 3TDES keys in authentication protocols
17.	Key Agreement	Derivation of AES keys with SHA-1 , SHA-256	[27]	|k|=128 |k|=192 |k|=256	[22] [20, 6.2.2, 6.2.3, 6.2.4]	FCS_CKM.1/AES.SM FCS_COP.1/SHA Derivation of AES keys in authentication protocols
18.	Confidentiality	AES encryption and decryption in CBC mode	[33, 6.5]	|k|=128 |k|=192 |k|=256	According [22] [20, 6.7.1.2, 6.7.2.2	FCS_COP.1/COS.AES Secure Messaging with AES session keys
19.	Confidentiality	3TDES encryption and decryption in CBC mode	[35]	|k| = 168	[22] [20, 6.7.1.1, 6.7.2.1]	FCS_COP.1/COS.AES Secure Messaging with 3TDES session keys

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
20.	Confidentiality	2TDES encryption and decryption in CBC mode	[36]	|k| = 112	[38]	FCS_COP.1 / PAUTH Only during card production phases in secured environment . Not available in applicative phase.
21.	Confidentiality	RSA encryption and decryption Encoding schemes: RSAES-PKCS1-v1_5 RSAES-OAEP	[23]	Modulusleng th = 2048 Modulusleng th = 3072	[22] Encryption: [20, 6.8.1.1, 6.8.1.2] Decryption: [20, 6.8.2.1, 6.8.2.2]	FCS_COP.1 /COS.RSA Encryption: PSO ENCIPHER PSO TRANSCIP HER Decryption: PSO DECIPHER PSO TRANSCIP HER RSAES-PK CS#1v1_5 not recommend ed [22]
22.	Confidentiality	ELC encryption and decryption COS standard curve parameters: brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, ansix9p256r1, ansix9p384r1	[27]	|q| = 256 |q| = 384 |q| = 512	[27] Encryption: [20, 6.8.1.4] Decryption: [20, 6.8.2.3]	FCS_COP.1 /COS.ELC Encryption: PSO ENCIPHER PSO TRANSCIP HER Decryption: PSO DECIPHER PSO TRANSCIP HER
23.	Integrity	CMAC with AES	[34]	-	[22] [20, 6.6.1.2, 6.6.2.2]	FCS_COP.1 /COS.CMAC Secure Messaging

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
24.	Integrity	Retail-MAC with 3TDES	[20]	|k|=168	[22], [20, 6.6.1] Padding: [39, 10.2.3.1] (referenced in [20, 6.6.1.1])	FCS_COP.1 /COS.RMAC Secure Messaging Max. 216 message blocks with the same key (see [22, 4.4])
25.	Cryptograhic primitive	Physical RNG PTG.2	[4, AIS 31]	-	[22]	FCS_RNG.1
26.	Cryptograhic primitive	SHA-1 SHA-256 SHA-384 SHA-512	SHA: [26]	-	[20, 6.1]	FCS_COP.1 /SHA
27.	Cryptograhic primitive	3TDES	Sections 3.1 and 3.1 with keying option 1 from [35]	|k|=168	[22]	-
28.	Cryptograhic primitive	2TDES	ISO/IEC 10116 [40]. Triple DES using keying option 2	|k|=112	[38]	Only during card production phases in secured environment . Not available in applicative phase.
29.	Cryptograhic primitive	AES	[31]	|k|=128 |k|=192 |k|=256	[22]	-
30.	Cryptograhic primitive	RSA	[23]	Modulusleng th = 2048 Modulusleng th = 3072	[22]	-
31.	Cryptograhic primitive	ECC	[27]	q| = 256 |q| = 384 |q| = 512	[27]	-

Table 9: TOE cryptographic functionality

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

According to [20] and [22] the algorithms are suitable for securing integrity, authenticity and confidentiality of the data stored in and processed by the TOE as a generation G2 card operating system platform that is intended to be used within the German health care system. The validity period of each algorithm is mentioned in the official catalogue [22].

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 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.

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 [16] 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 ([41]):

- 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 card product delivery (generation of the product image), application development 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 for the object system's objects. In particular, this concerns key objects, PIN objects and the TOE specific system objects (rules objects) including their assigned security attributes. Especially, the TOE specific design concept for the rules objects and their handling has to be taken into account.

  For the choice of the access rules for the object system's objects (including the rules objects themselves) one has to consider that the TOE's Wrapper is only able to export security attributes and public key data of the object system and its objects if their access rules are set appropriately for read access. For this, the access rules for the command GET OBJ INFO have to be set accordingly, refer to the user guidance [15], chapter 8. .

  For card products that undergo a later TR-conformity testing according to the Technical Guideline BSI TR-03144 ([41]) it is strongly recommended to care for the appropriate choice of the access rules for all the object system's objects (icluding the rules objects themselves). It shall be possible for the Konsistenz-Prüftool according to

the Technical Guideline BSI TR-03143 ([42]) 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 [20]).

Any object system set up on the TOE shall only make use of the TOE's functionality as described in the G2-COS specification [20] and the user guidance [15]. The object system has to be checked for taking this requirement into account. 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. It has to be taken into account that the TOE implements the functionality of the G2-COS specification [20] that is defined as mandatory, but none of the optional packages for Crypto Box, Contactless, Logical Channels, PACE for Proximity Coupling Device and USB. Concerning the TOE's command set, only the mandatory commands and command variants from the G2-COS specification [20] and the additional commands and command variants outlined in the user guidance [15], chapter 5 and 6 are part of the TOE and its evaluation. Further specific requirements for the product image are given in the user guidance [15], chapter 8.

Refer to the user guidance documentation [15], chapter 5, 6, 7, 8, 9 and 10 and [12].

- Restrictions for key usage:

  Refer to the user guidance [15], chapter 2.9.3, 2.10.3, 8, 9 and 10.

- PIN / PUK Handling:

  Refer to the user guidance [15], chapter 2.9.3, 2.10.3, 8, 9 and 10.

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

  In particular, the TOE's specific load functionality for loading a pre-configured object system (product image) onto the card in the Initialisation Phase and for the personalisation of such installed object system in the Personalisation Phase has to be taken into account.

  Refer to the user guidance documentation [15], chapter 2.8, 2.9, 5, 7, 8, 9 and 10, [16], [14] and [11].

- Security requirements and hints for Phase 8 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 [15], chapter 2.10, 6, 7, 9 and 10 and [16].

- The TOE's Wrapper and its specifics beyond the Wrapper specification [20]:

  Refer to the user guidance [13], chapter 2 and 3.

- 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 ([41]) it is strongly recommended to care for that via the TOE's specific personalisation functionality (including the TOE's specific DGI concept) as well as via the TOE's regular commands as these are available in Phase 7 respective Phase 8 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 in particular the appropriate handling of the command LOAD APPLICATION with its different command variants, the appropriate handling of the TOE specific system objects (rules objects) as well as the appropriate setting of the DGIs and access rules for the object system's objects (including the rules objects themselves).

Refer to the user guidance documentation [15], chapter 5, 6, 8 and 9, [12] and [11].

For a TR-conformity testing of a card product set up on the TOE according to the Technical Guideline BSI TR-03144 ([41]) 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 (including the TOE specific system objects as the rules objects themselves) via the TOE's Wrapper is possible without any restriction and therefore fulfills the requirements for data export in the Wrapper specification [21]. This means a check is performed that no restriction for read access to all the related objects in the object system because of an inappropriate choice of the access rules arises. Specific focus has to be set on the check of the rules objects themselves that are implemented in the card product's object system. It shall be possible for the Konsistenz-Prüftool according to the Technical Guideline BSI TR-03143 ([42]) that is used for conformity testing to get a complete picture of the object system installed in the card product for further comparison against the respective object system specification. Refer to the user guidance [15], chapter 8.

  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 (including the rules objects themselves) 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 ([41]).
- For the card product, a check for fulfilment of the requirements for the product image in the user guidance [15], chapter 8 has to be carried out.
- Note: A card product that does not fulfil each of the requirements in the user guidance [15], chapter 8 will be rejected for a TR-certificate according to the Technical Guideline BSI TR-03144 ([41]).
- For 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 ([41]) refer in particular to its specifics beyond the Wrapper specification [21] as these are outlined in the user guidance [13], chapter 2 and 3.
- For the card product, it has to be checked that via the TOE's specific personalisation functionality (including the TOE's specific DGI concept) as well as via the TOE's regular commands as these are available in Phase 7 respective Phase 8 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 in particular the appropriate

handling of the command LOAD APPLICATION with its different command variants, the appropriate handling of the TOE specific system objects (rules objects) as well as the appropriate setting of the DGIs and access rules for the object system's objects (including the rules objects themselves).

Note: If overwriting of initialised security attributes and public key data of the object system and its objects via the TOE's specific personalisation functionality (including the TOE's specific DGI concept) or via the TOE's regular commands as these are available in Phase 7 respective Phase 8 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 ([41]).

- Any object system set up on the TOE shall only make use of the TOE's functionality as described in the G2-COS specification [20] and the user guidance [15]. The card product's object system has to be checked for taking this requirement into account.

  It has to be taken into account that the TOE implements the functionality of the G2-COS specification [20] that is defined as mandatory, but none of the optional packages for Crypto Box, Contactless, Logical Channels, PACE for Proximity Coupling Device and USB. Concerning the TOE's command set, only the mandatory commands and command variants from the G2-COS specification [20] and the additional commands and command variants outlined in the user guidance [15], chapter 5 and 6 are part of the TOE and its evaluation.

  If in particular in the framework of the TR-conformity testing of a card product according to the Technical Guideline BSI TR-03144 ([41]) the Konsistenz-Prüftool according to the Technical Guideline BSI TR-03143 ([42]) 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 [20] or the user guidance [15] this has to be manually examined and valuated.

The requirements for the TOE usage are provided for in the guidance documentation for users/administrators [11], [12], [13], [14], [15] and [16].

11. Security Target

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

12. Definitions

12.1. Acronyms

2TDES Two Key DES

3TDES Three Key DES

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
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CMAC	Cipher-based Message Authentication Code
cPP	Collaborative Protection Profile
CPU	Central Processing Unit
DEMA	Differential Electromagnetic Analysis
DES	Data Encryption Standard
DFA	Differential Fault Analysis / Attack
DGI	Data Grouping Identifier
DPA	Differential Power Analysis
DRNG	Deterministic Random Number Generator
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read-Only Memory
eHC	electronic Health Card
ETR	Evaluation Technical Report
FCP	File Control Parameter
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
KMS	Key Management System
MAC	Message Authentication Code
MF	Master File
MGF1	Mask Generation Function
NVM	Non-Volatile Memory
PACE	Password Authenticated Connection Establishment
PDM	Product Data Management system
PIN	Personal Identification Number
PP	Protection Profile
PRNG	Physical Random Number Generator

PUK	Personal Unblocking Key
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
ST	Security Target
TLV	Tag-Length-Value
TOE	Target of Evaluation
TR	Technische Richtlinie (Technical Guideline)
TSF	TOE Security Functionality
USB	Universal Serial Bus
ZMK	Zone Master Key

12.2. Glossary

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

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

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

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

Informal - Expressed in natural language.

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

Package - named set of either security functional or security assurance requirements

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

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

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

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

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

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

13. Bibliography

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

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012
http://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[8]
https://www.bsi.bund.de/AIS

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

[6] Security Target BSI-DSZ-CC-0956-2016, Security Target Health Insurance Card G2 1.0.0, Version 1.13, 23.09.2016, Gemalto SA (confidential document)

[7] Security Target Lite BSI-DSZ-CC-0956-2016, Security Target Lite Health Insurance Card G2 1.0.0, Version 1.13, 23.09.2016, Gemalto SA (sanitised public document)

[8] specifically

- AIS 1, Version 13, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 8, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 23, Version 3, Zusammentragen von Nachweisen der Entwickler
- AIS 25, Version 8, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 9, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 36, Version 4, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.9, Reuse of evaluation results

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

[9] ETR BSI-DSZ-CC-0956-2016, Evaluation Technical Report (ETR) – Summary for Health Insurance Card G2 1.0.0, Version 5.0, 29.09.2016, TÜV Informationstechnik GmbH (confidential document)

[10] Configuration List BSI-DSZ-CC-0956-2016, Configuration List Health Insurance Card G2 1.0.0, Version 1.7, 28.09.2016, Gemalto GmbH (confidential document)

[11] Guidance Documentation Health Insurance Card G2 1.0.0 - Specification for Chip card Personalization for German Health Card eGK Generation 2 (GeGKOS C1 on M7892), Version 1.12, 22.09.2016, Gemalto GmbH

[12] Guidance Documentation Health Insurance Card G2 1.0.0 - Software Requirements Specification For GeGKOS Generation 2, Version B12, 22.09.2016, Gemalto GmbH

[13] Guidance Documentation Health Insurance Card G2 1.0.0 - User guidance for Wrapper, Version 1.8, 22.09.2016, Gemalto GmbH

[14] Guidance Documentation Health Insurance Card G2 1.0.0 - Card Initialization Specification, GeGKOS C1, Infineon M7892 B11, Version A05, 22.09.2016, Gemalto GmbH

[15] Guidance Documentation Health Insurance Card G2 1.0.0 - Operational User guidance ES, Electronic Health Card, Version 1.23, 13.09.2016, Gemalto GmbH

[16] Guidance Documentation Health Insurance Card G2 1.0.0 - Preparative Procedures, Electronic Health Card - GeGKOS C1, Version 1.16, 23.09.2016, Gemalto GmbH

[17] Security Target of the underlying hardware platform, Security Target M7892 B11, Version 0.3, 13 October 2015, Infineon Technologies AG, BSI-DSZ-CC-0782-V2-2015

[18] Certification Report BSI-DSZ-CC-0782-V2-2015 for Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware) from Infineon Technologies AG, November 2015, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[19] ETR for Composite Evaluation of the underlying hardware platform Infineon Security Controller M7892 B11 from certification procedure BSI-DSZ-CC-0782-V2-2015, Version 7, 21 October 2015, TÜV Informationstechnik GmbH (confidential document)

[20] Einführung der Gesundheitskarte, Spezifikation des Card Operating System (COS), Elektrische Schnittstelle, Version 3.8.0 vom 17.07.2015, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[21] Einführung der Gesundheitskarte, Spezifikation Wrapper, Version 1.7.0, 17.07.2015, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

[22] Technische Richtlinie BSI TR-03116-1 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 1 – Telematikinfrastruktur, Version 3.19, 04.12.2015, Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

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

[25] ISO/IEC 9797 - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, Second edition, 2011-03-11

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

[27] Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.0, 28.06.2012, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[28] American National Standard for Financial Services ANS X9.62-2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), November 16, 2005, American National Standards Institute.

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

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

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

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

[33] NIST SP 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, National Institute of Standards and Technology, December 2001

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

[35] NIST Special Publication 800-67 – Revision 1, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher – Revised January 2012, National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce.

[36] Federal Information Processing Standards Publication 46-3 (FIPS PUB 46-3) of U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology Data encryption standard (DES and TDES) – Reaffirmed 1999 October 25

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

[38] EMV card personalization specification, Version 1.1, July 2007

[39] ISO/IEC 7816-4:2013 – Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange, International Organization for Standardization

[40] Information technology – Security techniques – Modes of operation for an n-bit block cipher, INTERNATIONAL STANDARD ISO/IEC 10116:2006 TECHNICAL CORRIGENDUM 1, Published 2008-03-15

[41] Technische Richtlinie BSI TR-03144 eHealth – Konformitätsnachweis für Karten-Produkte der Kartengeneration G2, Version 1.1, 22.05.2015, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[42] Technische Richtlinie BSI TR-03143 “eHealth G2-COS Konsistenz-Prüftool”, Version 1.0, 08.05.2015, Bundesamt für Sicherheit in der Informationstechnik (BSI)

This page is intentionally left blank.

C. Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

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

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

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

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

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

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

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

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

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

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

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

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

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

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

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

The following table shows the assurance class decomposition.

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

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

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

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

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

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one

component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

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

“Objectives

EAL 1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

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

EAL 1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL 1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

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

“Objectives

EAL 2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL 2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

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

EAL 3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering."

Evaluation assurance level 4 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

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

EAL 4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs."

Evaluation assurance level 5 (EAL 5) - semiformally designed and tested (chapter 8.7)

"Objectives

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

EAL 5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques."

Evaluation assurance level 6 (EAL 6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL 6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL 6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs."

Evaluation assurance level 7 (EAL 7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL 7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

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

Table 1: Evaluation assurance level summary”

Class AVA: Vulnerability assessment (chapter 16)

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

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

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

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

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0956-2016

Evaluation results regarding development and production environment

The IT product Health Insurance Card G2, 1.0.0 (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 advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 28 October 2016, 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) Gemalto GmbH, Werinherstr. 81, 81541 München, (Development)

b) Gemalto GmbH, St-Martin-Str. 60, 81541 München, (Development)

c) Gemalto GmbH, Mercedesstrasse 13, 70794 Filderstadt, (Embedding, Initialization, Personalization, Delivery)

d) Atos infogerance, 4 rue des Vielles Vignes, 77183 Croissy-Beaubourg, France, (IT-Support)

e) Atos infogerance, 153 rue Jean Jaures, 93300 Aubervilliers, France, (IT-Support)

f) Gemalto S.A., 6 rue de la Verrerie CS 20001, 92197 Meudon Cedex, France, (Development)

g) Gemalto S.A., Avenue du Pic de Bretagne CS 12023, 13881 Gémenos Cedex, France, (module assembly)

h) Gemalto Sp. z o.o, ul. Skarszewska 2, 83-110 Tczew, Poland, (Embedding, Initialization, Personalization, Delivery)

i) Gemalto Pte Ltd., 12 Ayer Rajah Crescent, Singapore 139941, Singapore, (Embedding, Initialization, Delivery)

j) For development and production sites regarding the platform please refer to the Certification Report BSI-DSZ-CC-0782-V2-2015 ([18])

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

This page is intentionally left blank.