Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0513-V2-2018

for

CHERRY eHealth Terminal G87-1505 FW-Version 3.0.1 HW-Version 1.1.1

from

Cherry GmbH

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0513-V2-2018 (*)

eHealth: Smart Card Readers

CHERRY eHealth Terminal G87-1505
FW-Version 3.0.1 HW-Version 1.1.1

from	Cherry GmbH
PP Conformance:	Common Criteria Protection Profile Electronic Health Card Terminal (eHCT) Version 3.7, BSI-CC-PP-0032-V2-2015-MA-01, 22. Mai 2017
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 3 augmented by ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, AVA_VAN.4

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 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
recognition for components
up to EAL 2

Bonn, 28 March 2018

For the Federal Office for Information Security

Joachim Weber
Head of Branch

L.S.

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

This page is intentionally left blank.

Contents

This page is intentionally left blank.

A. Certification

1. Preliminary Remarks

Under the BSIG1 Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

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

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

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

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

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

2. Specifications of the Certification Procedure

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

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

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

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

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

- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045.
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

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

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

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

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

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

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

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

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

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

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

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

4. Performance of Evaluation and Certification

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

The product CHERRY eHealth Terminal G87-1505 FW-Version 3.0.1 HW-Version 1.1.1 has undergone the certification procedure at BSI.

The evaluation of the product CHERRY eHealth Terminal G87-1505 FW-Version 3.0.1 HW-Version 1.1.1 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 28. February 2018. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

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

The product was developed by: Cherry GmbH.

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

5. Validity of the Certification Result

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

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

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

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

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 28 March 2018 is valid until 27 March 2023. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

[5] Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product CHERRY eHealth Terminal G87-1505 FW-Version 3.0.1 HW-Version 1.1.1 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Cherry GmbH
Cherrystraße
91275 Auerbach/Opf
Deutschland

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 smart card keyboard “G87-1505” version 3.0.1:1.1.1 with integrated smart card readers. It fulfils the IT security requirements to be used with the German electronic Health Card (eHC) and the German Health Professional Card (HPC) based on the regulations of the German healthcare system.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Common Criteria Protection Profile Electronic Health Card Terminal (eHCT) Version 3.7, BSI-CC-PP-0032-V2-2015-MA-01, 22. Mai 2017 [8].

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 3 augmented by ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, AVA_VAN.4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. They are selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

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

TOE Security Functionality	Addressed issue
SF.1	Secure Communication
SF.2	Memory Rework
SF.3	Secure PIN Entry
SF.4	Secure Update
SF.5	User Authentication
SF.6	TOE Management
SF.7	Protection against Counterfeiting

Table 1: TOE Security Functionalities

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

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.3 - 3.5.

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:

CHERRY eHealth Terminal G87-1505
FW-Version 3.0.1 HW-Version 1.1.1

The following both variants of the TOE are certified TOE versions:

- G87-1505LBZDE-2
- G87-1505LBZDE-10

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Cherry eHealth Terminal G87-1505 variants: • G87-1505LBZDE-2 • G87-1505LBZDE-10	1.1.1	As part of the secure delivery chain, see description of TOE delivery process below
2	SW	Firmware Image SHA-256-Hashsum: 66b4c2b970825088e9240c5140214883ee7cbab85582df8e6edd6b2a3cccea77	3.0.1	Initially included in the TOE
3	DOC	User guide [10]: (Handbuch für Administratoren eGK Tastatur G87-1505) SHA-256-Hashsum: a5f4c01823242299f5f20d5df610866a6a85778b2bd30b2159e7098457f44594	Feb 2018 / 6440650-04	Provided by the developer on their homepage https://www.cherry.de/eHealth
4	DOC	Brief instruction [11]: (Kurzanleitung für Benutzer eGK Tastatur G87-1505)	Feb 2018 / 6440649-04	Delivered with the delivery package of the TOE

Table 2: Deliverables of the TOE

The TOE is delivered to the end user in such a way as defined by the secure delivery chain [12].

The transport to the user is also defined in the concept of the secure delivery chain, see [13]. That document describes the complete chain. The guidance [10] defines all steps the end user has to perform to check if the secure delivery chain was correctly used and to check that the TOE is not manipulated or replaced and therefore the integrity and authenticity of the TOE is guaranteed.

3. Security Policy

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

- Cryptographic Support,
- User Data Protection,

- Identification and Authentication,
- Security Management,
- Protection of the TSF,
- TOE Access,
- Trusted Path/Channels.

Specific details concerning the above mentioned security policies can be found in chapter 6 of the Security Target [6].

4. Assumptions and Clarification of Scope

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

OE.ENV: It is assumed that the TOE is used in a controlled environment.

OE.ADMIN: The administrator of the TOE and the medical supplier shall be non-hostile, well trained and have to know the existing guidance documentation of the TOE environment.

OE.CONNECTOR: The connector in the environment has to be trustworthy and provides the possibility to establish a Trusted Channel with the TOE including a mean for mutual authentication.

OE.SM: The TOE will use a secure module (SM-KT) that represents the cryptographic identity of the TOE in form of an X.509 certificate.

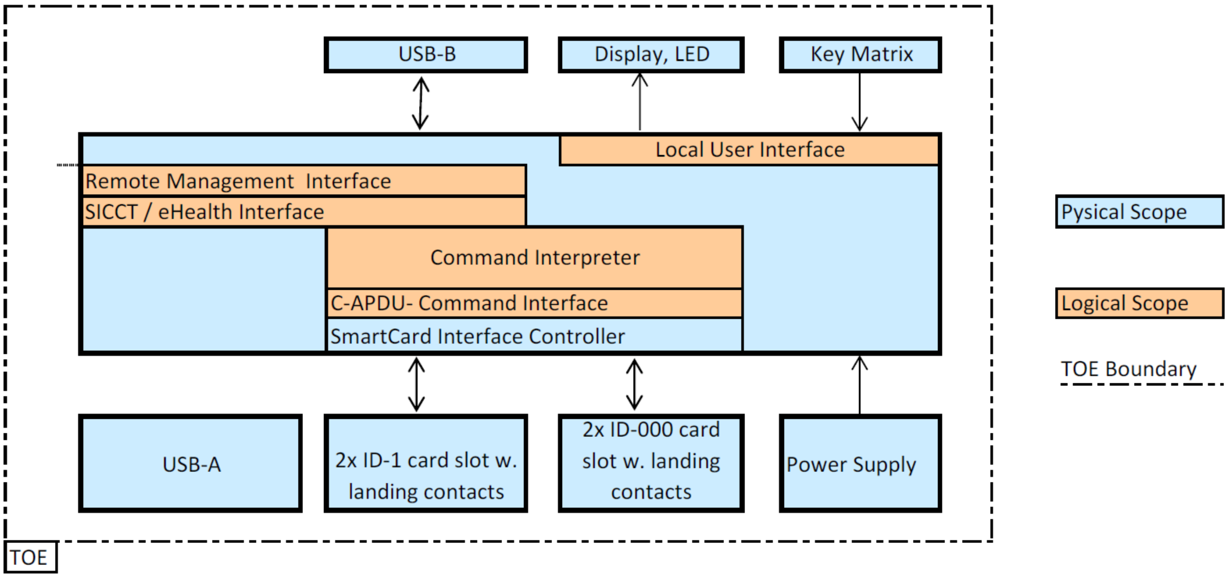
OE.PUSH_SERVER: The internal network of the medical supplier is equipped with a so called Push Server for automatic firmware updates.

OE.ID000_CARDS: All smartcards of form factor ID000 shall be properly sealed after they are brought into the TOE.

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

5. Architectural Information

The figure below presents the main building blocks of the TOE and their relation to the environment. A high level description of the IT product and its major components can be found in the Security Target [6], chapter 1.3.


USB-B
Display, LED
Key Matrix
Local User Interface
Remote Management Interface
SICCT / eHealth Interface
Command Interpreter
C-APDU- Command Interface
SmartCard Interface Controller
USB-A
2x ID-1 card slot w. landing contacts
2x ID-000 card slot w. landing contacts
Power Supply
TOE
Pysical Scope
Logical Scope
TOE Boundary

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.

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 TOE was tested in the configuration defined in the ST [6].

7.1. Developer's Test according to ATE_FUN

TOE configuration tested:

The Security Target [ST] has identified solely one configuration of the TOE G87-1505 under evaluation. The tests have been performed with the unmodified TOE within a special test framework simulating the real operational environment.

TOE test environment configurations:

The security objectives for the operational environment stated within [ST] are considered in ATE_FUN. All applicable objectives for the operational environment have been applied for the test environment. The test setup comprises a host PC with the test suit, a TOE and four virtual card kits.

Developer’s testing approach:

- Positive and negative tests are applied,
- Tests considering the different roles that can access the TOE,
- Tests covering all TSF subsystems in the TOE design,
- Developer provides mappings to the tested TSFI(s), SFR(s) and subsystem(s),
- The test descriptions comprise (inter alia):
  - Pre conditions: preparative steps,
  - Test steps: core test steps,
  - Post conditions: clearance steps to tidy up before the next test.

Verdict for the activity:

- All test cases were executed successfully on the TOE,
- The developer’s testing results demonstrate the TOE behaviour as expected.

All tests are passed.

7.2. Evaluator Tests

All testing activity of the evaluation body is covered by testing in the scope of ATE_IND and AVA_VAN.

7.2.1. Independent Testing according to ATE_IND

TOE test configurations:

- The evaluation body used the same test configurations and test environment as the developer during functional testing.

TSFI selection criteria:

- The evaluation body chose to broadly cover the existing interfaces without specific restrictions.

TSFI tested:

- All interfaces were considered during testing.

Developer tests performed:

- The evaluation body chose to inspect all developer tests. They also chose to repeat all tests except three.

Verdict for the sub-activity:

No deviations were found between the expected and the actual test results.

7.2.2. Penetration Testing according to AVA_VAN

Overview:

The penetration testing was partially performed using the developer’s testing environment, partially using the test environment of the evaluation body.

There is only one configuration of the TOE under evaluation and addressed by testing.

No attack scenario with the attack potential Moderate has actually been successful.

Penetration testing approach:

The evaluation body conducted penetration testing based on functional areas of concern derived from SFRs and architectural mechanisms. The areas were prioritized with regard to various factors, e.g. attack surface, estimated flaw likelihood, developer testing coverage, detectability of flaws during developer testing.

Medium and high areas were guaranteed to be penetration tested, with a stronger emphasis on high priorities. Low priorities were also considered during penetration, but could be less emphasized, if developer tests were found to be sufficient.

The penetration testing activities were performed as tests and as analytical tasks. Whenever an analysis was estimated to yield better results, the evaluators chose the analytical approach. Analytical activities were especially applied in the areas like Update, Random Number Generation and Hardening Mechanisms. Combined approaches were also applied.

TOE test configurations:

The TOE has been tested in the following TOE test configurations:

- TOE without any modifications. The setup comprises of the TOE connected to a Host PC via USB.

Attack scenarios having been tested:

The evaluation body considered security analysis and penetration testing in the following areas:

- Physical Security,
- TLS Connections,

- SICCT Access Control,
- Update,
- Remote Management,
- Identification & Authentication,
- Operation Mode of the TOE,
- Buffer Overflow,
- Card Slots of the TOE,
- Leakage.

Tested security functionality:

The evaluator ensured that all areas listed above are tested. Actually, the evaluation body used a more detailed list during the analysis and testing. The penetration testing was then conducted based on priorities as described above. Therefore, a complete coverage of security functional testing based on technical areas of concern is performed.

Verdict for the sub-activity:

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential Moderate was actually successful in the TOE's operational environment.

8. Evaluated Configuration

This certification covers the following configurations of the TOE: There is only one evaluated configuration of the TOE. The evaluation results are only valid for the single configuration defined in the Security Target [6].

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] 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.

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

- All components of the EAL 3 package including the class ASE as defined in the CC (see also part C of this report)
- The components ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, AVA_VAN.4 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Common Criteria Protection Profile Electronic Health Card Terminal (eHCT) Version 3.7, BSI-CC-PP-0032-V2-2015-MA-01, 22. Mai 2017 [8]

- for the Functionality: PP conformant plus product specific extensions
  Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant
  EAL 3 augmented by ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, AVA_VAN.4

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 table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines the standard of application where its specific appropriateness is stated.

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
Authenticity and Integrity	RSA signature verification with encoding RSASSA-PKCS1-V1_5 using SHA-256	[PKCS#1] (RSA), [FIPS180-4] (SHA)	2048	[gemSpec_Krypt], [gemSpec]	FCS_COP.1/SIG
Authenticity and Integrity	RSA signature verification with encoding RSASSA-PSKCS1-v1_5 using SHA-256	[PKCS#1] (RSA), [FIPS180-4] (SHA)	2048	[gemSpec_Krypt], [gemSpec]	FCS_COP.1/SIG_TSP for update of the TSP CA list
Authentication	RSA signature verification with encoding RSASSA-PKCS1-1.5 using SHA-256	[PKCS#1] (RSA), [FIPS180-4] (SHA)	2048	[gemSpec_Krypt], [gemSpec]	FCS_COP. 1/SIG
Key Agreement	Diffie-Hellman with TLS key derivation function	[HaC] (DH) [RFC2526] (dh-roup), [FIPS180-4] (SHA), [RFC1321] (MD5), [RFC2104] (HMAC), [RFC4346] (TLSv1.1) [RFC5246] (TLSv1.2)	2048 (dh-group 14) with DH exponent length = 320 bits	[gemSpec_Krypt], [gemSpec]	FCS_CKM.1/Connector
Confiden-tiality	AES in CBC-mode	[FIPS197] (AES), [RFC3602] (AES-CBC)	128, 256	[gemSpec_Krypt], [gemSpec]	FCS_COP.1/Con_Sym
Integrity	HMAC with SHA-1 (TLS)	[FIPS180-4] (SHA), [RFC2104] (HMAC), [RFC2404] (HMAC-SHA-1)	160	[gemSpec_Krypt], [gemSpec]	FCS_COP.1/Con_Sym
Trusted Channel	TLS v1.1 and TLS v1.2	[RFC4346] (TLSv1.1), [RFC5246] (TLSv1.2)		[gemSpec_Krypt], [gemSpec]	FTP_ITC.1/Connector
Trusted Channel	TLS v1.1 and TLS v1.2	[RFC4346] (TLSv1.1), [RFC5246] (TLSv1.2)		[gemSpec_Krypt], [gemSpec]	FTP_TRP.1/Management

Table 3: TOE cryptographic functionality

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

According to [gemSpec_Krypt], [gemSpec], and [TR03116-1] the algorithms are suitable for the corresponding purpose.

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

In addition, the following aspects need to be fulfilled when using the TOE:

- Usage of the TOE only in a controlled environment as described in the security target [6] and the related TOE user documentation, see table 2.
- The TOE is only allowed to be delivered to the end user in such a way as defined by the secure delivery chain [12] and [13]. The guidance [10] defines all steps the end user has to perform to check if the secure delivery chain was correctly used and to check that the TOE is not manipulated or replaced and therefore the integrity and authenticity of the TOE is guaranteed.

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Definitions

12.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
ATE	Tests
AVA	Vulnerability Assessment
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile

EAL	Evaluation Assurance Level
eGK	elektronische Gesundheitskarte
eHC	electronic Health Card
eHCT	electronic Health Card Terminal
ETR	Evaluation Technical Report
HPC	Health Professional Card
KT	Card Terminal
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
IND	Independent testing
KSR	Configuration and Software repository Service of the telematics infrastructure
LAN	Local Area Network
LEI	Supplier (Leistungserbringer-Institution)
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SSEK	Shared Secret Encryption Key
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	Trust-Service Provider that issues connector certificates

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[7] https://www.bsi.bund.de/AIS

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

[6] Security Target BSI-DSZ-CC-0513-V2-2018, Version 2.17, 28.02.2018, Common-Criteria 3.1-Document Security Target EAL3+ for G87-1505, Cherry GmbH

[7] Evaluation Technical Report, Version 2, 28.02.2018, TÜV Informationstechnik GmbH, (confidential document)

[8] Common Criteria Protection Profile Electronic Health Card Terminal (eHCT) Version 3.7, BSI-CC-PP-0032-V2-2015-MA-01, 22. Mai 2017

[9] Configuration list for the TOE, Version 1.47, 28.02.2018 (confidential document)

[10] Handbuch für Administratoren eGK Tastatur G87-1505, Version 6440650-04, Feb 2018, Cherry GmbH

[11] Kurzanleitung für Benutzer eGK Tastatur G87-1505, Version 6440649-04, Feb 2018, Cherry GmbH

[7] specifically

- AIS 1, Version 13, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- 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)

[12] Common-Criteria-3.1 Dokument ALC_DEL.1, Version 1.45, 25.01.2018, Cherry GmbH, (confidential document)

[13] Sichere Lieferkette, Version 1.7, 27.02.2018, Cherry GmbH, (confidential document)

Quoted standards:

[FIPS180-4] FIPS PUB 180-4 Secure Hash Signature Standard (SHS), NIST, 2012-03,

[FIPS197] Federal Information Processing Standards Publication 197: ADVANCED ENCRYPTION STANDARD (AES), NIST, November 2001,

[gemSpec] Spezifikation eHealth-Kartenterminal, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Version 3.5.0, 17.06.2014,

[gemSpec_Krypt] Einführung der Gesundheitskarte – Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik), Version 2.3.0, 17.06.2014,

[HaC] A. Menezes, P. van Oorschot und O. Vanstone. Handbook of Applied Cryptography. CRCPress, 1996,

[PKCS#1] B. Kaliski: PKCS #1: RSA Encryption, Version 2.1, RFC 3447, Version 2.2, October 2012,

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, „HMAC: Keyed-Hashing for Message Authentication", February 1997,

[RFC2404] The Use of HMAC-SHA-1-96 within ESP and AH, Network Working Group, November 1998,

[RFC3268] Chown, P., Advanced Encryption Standard (AES) Cipher suites for Transport Layer Security (TLS), June 2002,

[RFC3602] S .Frankel, R. Glenn, S. Kelly: The AES-CBC Cipher Algorithm and Its Use with IPsec. September 2003,

[RFC4346] The Transport Layer Security (TLS) Protocol Version 1.1, T. Dierks, E. Rescorla, April 2006,

[RFC5246] The Transport Layer Security (TLS) Protocol Version 1.2, RFC 5246, Network Working Group,

[SP800-38A] Recommendation for Block Cipher Modes of Operation – Methods and Techniques, December 2001,

[SP800-38B] Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005,

[TR03116-1] Technische Richtlinie BSI TR-03116-1, Kryptographische Vorgaben für die eCard-Projekte für der Bundesregierung, Teil 1: Telematikinfrastruktur, Technische Arbeitsgruppe TR-03116, 30.01.2014 (Version 3.18).

This page is intentionally left blank.

C. Excerpts from the Criteria

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

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.4
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 11
- On the detailled definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 12 to 16
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

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

This page is intentionally left blank.

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report