Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1171-2023

for

Electronic Health Card Terminal eHealth GT900
Hardwareversion: 2.1.0, Firmwareversion: 2.0.1

from

GT German Telematics Gesell. für Telematik mbH

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-1171-2023 (*)

eHealth: Smart Card Readers

Electronic Health Card Terminal eHealth GT900
Hardwareversion: 2.1.0, Firmwareversion: 2.0.1

from	GT German Telematics Gesell. für Telematik mbH
PP Conformance:	Common Criteria Protection Profile Electronic Health Card Terminal (eHCT) Version 3.7, BSI-CC-PP-0032-V2-2015-MA-01, 22 May 2017
Functionality:	PP conformant 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
for components up to
EAL 4

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 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

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

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

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

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 30 March 2023

For the Federal Office for Information Security

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

Sandro Amendola L.S.
Head of Division

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

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

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

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

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

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

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

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

2. Specifications of the Certification Procedure

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

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

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

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

3 BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

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

3. Recognition Agreements

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

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

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

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

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

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

This certificate is recognized according to the rules of SOGIS-MRA, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained the component AVA_VAN.4 that is not mutually recognised in accordance with the provisions of the SOGIS MRA.

3.2. International Recognition of CC – Certificates (CCRA)

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

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

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

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

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

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 Electronic Health Card Terminal eHealth GT900, Hardwareversion: 2.1.0, Firmwareversion: 2.0.1 has undergone the certification procedure at BSI.

The evaluation of the product Electronic Health Card Terminal eHealth GT900, Hardwareversion: 2.1.0, Firmwareversion: 2.0.1 was conducted by Deutsche Telekom Security GmbH. The evaluation was completed on 24 February 2023. Deutsche Telekom Security GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: GT German Telematics Gesell. für Telematik mbH.

The product was developed by: GT German Telematics Gesell. für Telematik mbH.

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

5. Validity of the Certification Result

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

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

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

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

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 30 March 2023 is valid until 29 March 2028. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

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,
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 Electronic Health Card Terminal eHealth GT900, Hardwareversion: 2.1.0, Firmwareversion: 2.0.1 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] GT German Telematics Gesell. für Telematik mbH
Libellenstraße 9
14129 Berlin

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 eHealth Card Terminal GT900 Hardware version: 2.1.0, Firmware version: 2.0.1.

It is an eHealth Card Terminal with 2 ID-1 Slots (HPC and eGK) and 2 ID-000 SMC Slots (supporting SMC-KT and SMC-B cards), a disinfectable liquids resistant 20 key keypad also usable for secure pin entry and LAN + USB interfaces with interoperability to the eHealth Connectors TI 1.0 and to the High Speed Connectors (HSK) for TI 2.0 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 May 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 all 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.SECDOWN	Secure update of TSP CA list, firmware list and/or firmware core
SF.DRILLSEC	Protection against physical manipulation
SF.SELFTEST	Self-tests
SF.I&A	User identification and authentication
SF.CLRMEM	Residual information protection
SF.MNGT	Management functions
SF.PINCMD	Protected PIN entry
SF.TRUSTCH	Protected data exchange between the TOE and a connector
SF.ADMCH	Protected data exchange between the TOE and a remote TOE administrator

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, 3.4 and 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:

Electronic Health Card Terminal eHealth GT900,
Hardwareversion: 2.1.0, Firmwareversion: 2.0.1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Hardware - Version: 2.1.0 colour white	Version 2.1.0	Delivered as a package
		Hardware - Version: 2.1.0 SW colour black	Version 2.1.0	Delivered as a package
		Hardware - Version: 2.1.0 SI colour silver	Version 2.1.0	Delivered as a package
2	SW	Firmware	Version 2.0.1	Integrated into #1
3	DOC	Short guidance [10]	Version 1.0.1	Delivered together with #1

Table 2: Deliverables of the TOE

2.1. Overview of the Delivery Process

The TOE is delivered to the customer by the GT German Telematics Gesellschaft für Telematikdienste mbH using the following delivery procedure:

The TOE is delivered in a package from the storage from in GT German Telematics Gesellschaft für Telematikdienste mbH directly to the customer. The short guidance document [10] is delivered as part of this package. This document contains unambiguous references to the official guidance document [11], which can be downloaded from the developer’s website.

2.2. Identification of TOE

The TOE can be identified using the sticker attached to the TOE’s housing at the bottom, which lists the hardware version number. The firmware version can be identified on the screen as described in section 2.3 of [11]. The values can be then compared to the information in [6].

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. Specifically it is assumed:

- The card terminal prevents (not visible) physical manipulations for at least 10 minutes. The environment ensures beyond these 10 minutes that the card terminal is protected against unauthorized physical access or such is perceptible,
- That the user handles his PIN with care; specifically that the user will keep their PIN secret,
- That the user can enter the PIN in a way that nobody else can read it,
- That the user only enters the card PIN when the TOE indicates a secure state,
- That the medical supplier checks the sealing and the physical integrity of the TOE regularly before it is used,
- The medical supplier sends the TOE back to the manufacturer in case he suspects an unauthorized reset to factory defaults has been performed by unauthorized personnel, and
- That the network of the medical supplier is appropriately secured so authorized entities are trustworthy.

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. The administrator and the medical supplier shall be responsible for the secure operation of the TOE. Specifically it shall be ensured:

- That they enforce the requirements on the environment (see A.ENV),
- That the administrator ensures that the medical supplier received the necessary guidance documents (especially for firmware updates),
- That the physical examination of the TOE is performed according to the process described by the manufacturer in the evaluation process (e.g. seal checking),
- That the administrator checks the integrity of the terminal before the initial start-up procedure (every new pairing process) and the medical supplier checks the integrity of the terminal before every start-up procedure,

- That they react to breaches of environmental requirements according to the process described by the manufacturer (e.g. reshipment to the manufacturer), and
- That the administrator checks the secure state of the TOE regularly

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. The connector has to undergo an evaluation and certification process in compliance with the corresponding Protection Profiles. Further the connector has to periodically check the pairing state with the TOE and warn the administrator accordingly.

OE.SM: The TOE will use a secure module (SM-KT) that rep-resents the cryptographic identity of the TOE in form of an X.509 certificate. It is assumed that the cryptographic keys in this module are of sufficient quality and the process of key generation and certificate generation is appropriately secured to ensure the confidentiality, authenticity and integrity of the private key and the authenticity and integrity of the public key/certificate. The random number generator of the SM-KT shall provide entropy of at least 100 bit for key generation. It is further assumed that the secure module is secured in a way that protects the communication be-tween the TOE and the module from eavesdrop-ping and manipulation and that the SM-KT is securely connected with the TOE (according to TR-03120). The secure module has undergone an evaluation and certification process in compliance with the corresponding Protection Profile and complies with the specification.

OE. PUSH_SERVER: The internal network of the medical supplier is equipped with a so called Push Server for automatic firmware updates according to the push update mechanism. The TOE administrator is responsible for the operation of the Push Server and able to select the particular firmware version that the server is allowed to install on the card terminals. Every time an update pro-cess is performed for a card terminal the push server logs the following information: identifier of involved card terminal, version of firmware to install, result of the update process.

OE.ID000_CARDS: All smartcards of form factor ID000 shall be properly sealed after they are brought into the TOE. Further, the developer shall provide guidance documentation on how a TOE administrator could renew a sealing after an ID000 card is replaced by another one.

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

5. Architectural Information

The architecture of the complete system is shown in 1.

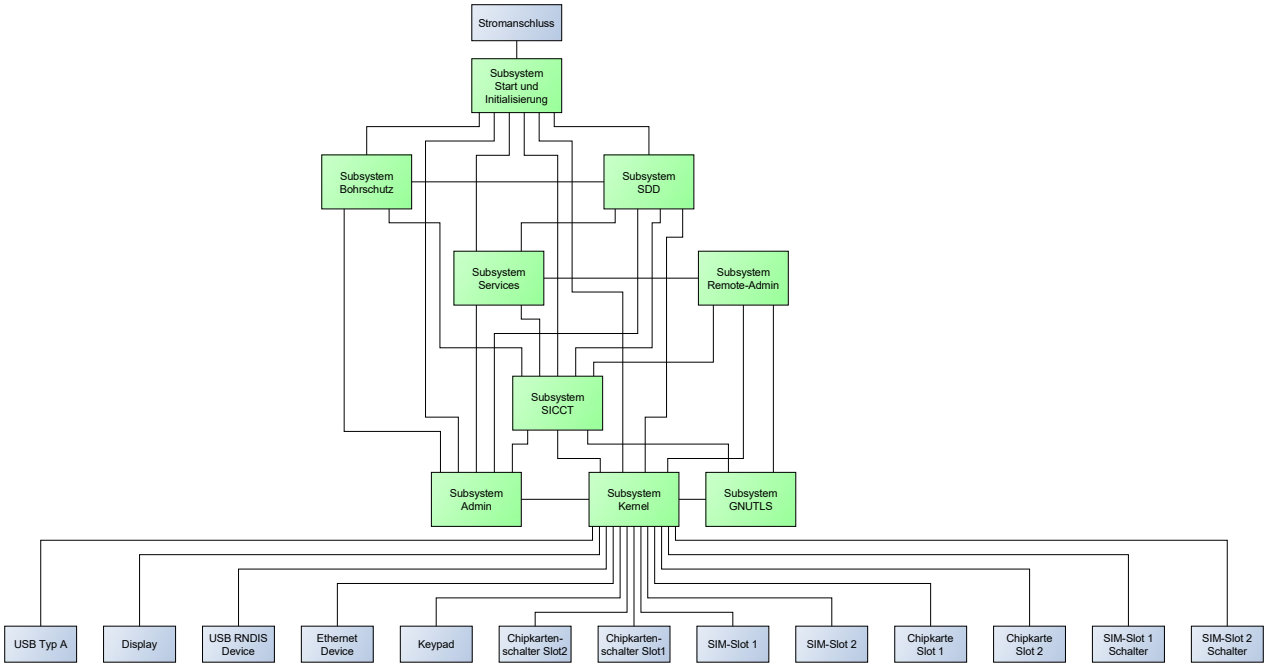

Figure 1: Architecture of the complete system

Internally TOE consists of nine subsystems as shown in the following table:

Subsystem	Description
Start und Initialisierung	The subsystem is used for the superordinate task scheduler of the TOE. Through this subsystem all other subsystems are started and their return values are processed. The subsystem implements parts of SF.SELFTEST: Checking for incomplete firmware updates, checking of messages of SF.DRILLSEC, checking if there was a security alarm, checking if the TOE was disconnected from power-, checking the integrity of files, checking the signature of the PIC32MM key, hash values of important files, installed CA certificates and cross certificates, and processing self-tests of the cryptographic functions.
Admin	This subsystem includes functionality for the local configuration (SF.MNGT) including firmware and CA certificates and updates. The subsystem implements the SF.SECDOWN, parts of SF.SELFTEST, SF.I&A for the administrator roles, and SF.CLRMEM for PINS.
Bohrschutz	This subsystem implements SF:DRILLSEC and supports SF.SELFTEST by monitoring the security sensors of the TOE. For this, the drill protection foil, the keyboard foil, the SIM slots, and the PIC32MM micro controller on the display board are monitored so that an alarm is raised in case of a security critical event.
Kernel	This subsystem is the basic OS functionality provided by the Linux kernel, which includes drivers and CPU specific functions to communicate with the internal hardware components.
SICCT	This subsystem implements SF.TRUSTCH, SF.PINCMD and parts of SF.SELFTEST, SF.I&A, SF.MNGT, and SF.CLRMEM and enables the SICCT communication with the connector including using TLS secured channels.
Remote-Admin	This subsystems enables a remote administrator to access the TOE over a secured TLS channel (SF.ADMINCH, SF.I&A, and SF.MNGT).
GNUTLS	This subsystems implements the cryptographic functions of SF.TRUSTCH and SF.ADMINCH used for TL.
Services	This subsystem provides services to other subsystems, namely the managing of passwords and password-related error counters, temporary locking mechanisms, handling of configuration files, and handling of network configuration.
SICCT Service Discovery (SDD)	This subsystem implements the service discovery functionality of the SICCT port.

Table 3: Subsystems of the TOE

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

7.1. Description of the Test Concept for ATE_FUN

The developer considered the TOE environment as defined in the Security Target. The developer tests cover all subsystems.

Moreover, aspects of the security architecture of the TOE are also covered by tests conducted by the developer. Each test is implemented as a manual test with assistance of the following tools: Konnektorsimulator, virtual.card.kit, VirtualCardKitTestSystemInterface, PuTTY, GT900 LAN Setup, Gencode2, OpenSSL, Packet Sender, and Wireshark. All tests are executed and evaluated manually by the tester.

The test documentation consists of a test coverage and depth of testing analysis and test specifications divided into sections for SF.SECDOWN, SF.DRILLSEC, SF.SELFTEST, SF.I&A, SF.CLRMEM, SF.MNGT, SF.PINCMD, SF.TRUSTCH, and SF.ADMCH. All security functions as defined in the ST are covered by the developer tests. For each of the security functions the developer defined a set of tests that shall demonstrate the correct behaviour of the involved modules/subsystems of the TOE.

Each test specification has the same structure. It consists of:

- test case ID,
- short description,
- test requirements,
- test steps,
- an expected result, and
- the actual test result.

For each test different configurations and parameters where used to do positive and negative tests. By testing the security functionality of the TOE, the correct behaviour is also tested because the functions of the TOE are used for the tests.

The test result logs show that the tests identified in the test coverage and depth of testing analysis have been executed as expected by the developer.

7.2. Description of the Test Concept for ATE_IND

Overview:

The independent testing was performed using the developer’s testing environment.

Since the TOE has only one configuration, all configurations of the TOE being intended to be covered by the current evaluation were tested.

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

Independent testing approach:

The TOE was independently tested with respect to three specific subject areas: a) The processing of firmware updates over the publicly available USB and SICCT interface, b) the connection handling to the gSMC-KT, and c) the correct functionality of the management interface.

TOE test configurations:

No special configuration is made. The TOE has only one single configuration, and the TOE is always this default configuration state.

The TOE under test is “electronic Health Card Terminal eHealth GT900” consisting of the following components:

- Hardware-Version: 2.1.0
- Firmware-Version 1.22.4

Note that section 1.1 of [6] lists firmware version 2.0.1. The evaluators confirm, that all of the tests and their respective test results remain valid for the version 2.0.1 as this is only a version that includes security relevant fixes that do not change the validity of the test results compared to the version under test. The evaluators checked by source code reviews that each change between 1.22.4 and 2.0.1 does not affect the code relevant for the test cases listed in ATE. Therefore, the functionality tested in all test cases is not affected by the changes.

Independent test subset chosen incl. a short justification:

The TSFIs tested by independent evaluator tests are TSFI1, TSFI5, TSFI6, TSFI7, and TSFI8. This includes all major interface functionalities like USB firmware update, communcication with the gSMC-KT as well as network capabilities. Because these interfaces are most critical for the security that the TOE provides, the selection of independent evaluator tests has a good coverage of the possible attack paths an attacker can use from outside the TOE.

Developer’s test subset repeated incl. a short justification:

The evaluators repeated developer tests for no specific subject areas: The tests covered the whole range of TSFIs, most of the modules, and most SFRs. This include tests that cover a broad code fraction of the TOE’s implementation. All those tests cover critical security functionalities of the TOE and are backed by developer-coded implementations.

Verdict for the sub-activity:

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

7.3. Description of the Test Concept for AVA

Overview:

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

All configurations of the TOE being intended to be covered by the current evaluation were tested.

The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential High was actually successful.

Penetration testing approach:

The evaluator examined the developer document [11] to find relevant information about how to bring the TOE in a proper and known state. He then searched for potential vulnerabilities through CVE entries based on the development documents for ARC and TDS. In addition to that the evaluator searched for potential vulnerabilities for the current TOE whilst evaluating the developer contributions for the single evaluation aspects in the context of the assurance classes ADV, AGD and ATE. The evaluator then derived attack

scenarios which cover all potential vulnerabilities. For these scenarios the evaluator created penetration tests, so that every attack scenario is tested by at least one relevant penetration test.

TOE test configurations:

No special configuration is made. The TOE has only one single configuration, and the TOE is always this default configuration state.

The TOE under test is “electronic Health Card Terminal eHealth GT900” consisting of the following components:

- Hardware version: 2.1.0
- Firmware version: 1.22.4

Note that section 1.1 of [6] lists firmware version 2.0.1. The evaluators confirm, that most of the tests and their respective test results remain valid for the version 2.0.1 as this is only a version that includes security relevant fixes that do not change the validity of the test results compared to the version under test. The evaluators checked by source code reviews that each change between 1.22.4 and 2.0.1 does not affect the code relevant for the test cases listed in AVA. Therefore, the functionality tested in all test cases is not affected by the changes.

The TOE is connected via Ethernet to the test network of the valuation facility, which contains apert from the TOE other network devices used to penetrate the TOE’s network interfaces.

Attack scenarios having been tested:

12 attack scenarios have been tested, e.g. eavesdropping, manipulation of firmware, malicious data, network interfaces.

SFRs penetration tested:

- FCS_COP.1/SIG_FW
- FDP_ACF.1/Terminal
- FDP_ACF.1/Management
- FMT_SMF.1
- FPT_FLS.1
- FDP_IFC.1/PIN
- FDP_IFF.1/PIN
- FCS_CKM.1/Connector
- FCS_COP.1/Con_Sym
- FCS_COP.1/Management
- FCS_CKM.1/Management
- FPT_FLS.1
- FPT_PHP.1
- FPT_PHP.2
- FPT_TST.1
- FDP_IFF.1/NET

- FIA_UAU.5
- FIA_UAU.7
- FCS_CKM.1/Management
- FTP_ITC.1/Connector
- FCS_COP.1/SIG
- FDP_IFC.1/NET

The remaining SFRs were analyzed, but not penetration tested due to non-exploitability of the related attack scenarios in the TOE's operational environment also including an attacker with a Moderate attack potential.

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 as defined in [6] provided that all measures required by the developer are applied.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

The TOE is only available in one evaluated configuration. The hardware case can be of three different colors (white, black silver), which are treated as one configuration because they provide the same functionality.

The versions are detailed in Table 2: Deliverables of the TOE.

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.

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 May 2017 [8]
- for the Functionality: PP conformant
  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.

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	TLS 1.2 (Konnektor) Ciphersuite	TLS_DHE_RSA_AES_128_CBC_SHA1 (0x00, 0x33)	RFC3447, RFC3526, RFC5246, RFC3268, RFC2104	128	yes	FCS_CKM.1.1/ Connector, FCS_CKM.1.1/Management, FCS_COP.1.1/Con_Sym, FCS_COP.1.1/Management
2	TLS 1.2 (Konnektor) Ciphersuite	TLS_DHE_RSA_AES_256_CBC_SHA1 (0x00, 0x39)	RFC3447, RFC3526, RFC5246, RFC3268, RFC2104	256	yes	FCS_CKM.1.1/ Connector, FCS_CKM.1.1/Management, FCS_COP.1.1/Con_Sym, FCS_COP.1.1/Management
3	TLS 1.2 (Konnektor) Ciphersuite	TLS_DHE_RSA_AES_128_CBC_SHA256 (0x00, 0x67)	RFC3447, RFC3526, RFC5246, RFC3268, RFC2104	128	yes	FCS_CKM.1.1/ Connector, FCS_CKM.1.1/Management, FCS_COP.1.1/Con_Sym, FCS_COP.1.1/Management
4	TLS 1.2 (Konnektor) Ciphersuite	TLS_DHE_RSA_AES_256_CBC_SHA256 (0x00, 0x6b)	RFC3447, RFC3526, RFC5246, RFC3268, RFC2104	256	yes	FCS_CKM.1.1/ Connector, FCS_CKM.1.1/Management, FCS_COP.1.1/Con_Sym, FCS_COP.1.1/Management
5	TLS 1.2 (Konnektor) Ciphersuite	TLS_ECDHE_RSA_AES_128_CBC_SHA1 (0xc0, 0x13) with secp256r1 and secp384r1	RFC3447, RFC3526, RFC5246, RFC3268, RFC2104, RFC4492, RFC5480	128	yes	FCS_CKM.1.1/ Connector, FCS_CKM.1.1/Management, FCS_COP.1.1/Con_Sym, FCS_COP.1.1/Management
6	TLS 1.2 (Konnektor) Ciphersuite	TLS_ECDHE_RSA_AES_256_CBC_SHA1 (0xc0, 0x14) with secp256r1 and secp384r1	RFC3447, RFC3526, RFC5246, RFC3268, RFC2104, RFC4492, RFC5480	256	yes	FCS_CKM.1.1/ Connector, FCS_CKM.1.1/Management, FCS_COP.1.1/Con_Sym, FCS_COP.1.1/Management
7	TLS 1.2 (Konnektor) Ciphersuite	TLS_ECDHE_RSA_AES_128_CBC_SHA256 (0xc0, 0x27) with secp256r1 and secp384r1	RFC3447, RFC3526, RFC5246, RFC3268, RFC2104, RFC4492, RFC5480	128	yes	FCS_CKM.1.1/ Connector, FCS_CKM.1.1/Management, FCS_COP.1.1/Con_Sym, FCS_COP.1.1/Management
8	TLS 1.2 (Konnektor) Ciphersuite	TLS_ECDHE_RSA_AES_256_CBC_SHA384 (0xc0, 0x28) with secp256r1 and	RFC3447, RFC3526, RFC5246, RFC3268,	256	yes	FCS_CKM.1.1/ Connector, FCS_CKM.1.1/Management,

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
		secp384r1	RFC2104, RFC4492, RFC5480			FCS_COP.1.1/Con_Sym, FCS_COP.1.1/Management
9	TLS 1.2 (Konnektor) Ciphersuite	TLS_DHE_RSA_AES_128_GCM_SHA256 (0x00, 0x9e)	RFC3447, RFC3526, RFC5246, RFC3268, RFC2104	128	yes	FCS_CKM.1.1/ Management, FCS_COP.1.1/Management
10	TLS 1.2 (Konnektor) Ciphersuite	TLS_ECDHE_RSA_AES_128_GCM_SHA256 (0xc0, 0x2f) with secp256r1 and secp384r1	RFC3447, RFC3526, RFC5246, RFC3268, RFC2104, RFC4492, RFC5480	128	yes	FCS_CKM.1.1/ Management, FCS_COP.1.1/Management
11	Signature generation and checking for Konnektor certificate and Konnektor pairing	RSASSA-PSS [PKCS#1] mit SHA256	RFC 3447	2048	yes	FCS_CKM.1.1/ Management, FCS_COP.1.1/Management
12	Signature check for firmware updates	PKCS#1 v2.1 RSASSA-PKCS-v1_5	RFC 3447	4096	yes	FCS_COP.1.1/SIG_FW
13	Signature check for TSP CA update	PKCS#1 v2.1 RSASSA-PKCS-v1_5	RFC 3447	4096	yes	FCS_COP.1.1/SIG_TSP
14	Checking exchange of gSMC-KT and challenge response	RSA	RFC 3447	2048	yes	-
15	Communication between mainboard and display board	RSA and AES-CBC	RFC 3447, RFC 5246, NIST SP 800-38A	2048 (RSA), 192 (AES)	yes	-

Table 4: TOE cryptographic functionality

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

According to the application standards in the table above, especially the standards issued by gematik, the algorithms are suitable for the intended purposes listed above. An explicit validity period is not given.

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:

- The user has to follow the instructions of the document “Checkliste sichere Lieferkette” referenced in section 1.3 of [11] before the first use of the TOE.
- Furthermore the user has to check the case’s integrity according to section 1.3.1 of [11] and the seals’ integrity according to section 1.3.2 of [11]. Please note that the seals do not contribute to the 10 minutes attack resistance that the TOE has to provide against physical attacks but are considered as a additional security feature.
- During the operation of the TOE the user has to follow the instructions of section 1 of [11], especially the hint in section 1.4 covering the requirements for unoccupied storage of the TOE for a longer period than 10 minutes.
- In case the TOE is put out of order, the user has to follow the instructions of section 11 of [11].

11. Security Target

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

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

ADV	Development
AGD	Guidance Documents
AIS	Application Notes and Interpretations of the Scheme
ALC	Life-Cycle Support
ARC	Security Architecture
ASE	Security Target Evaluation
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
CLEF	Commercial Licensed Evaluation Facilities
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
eGK	Elektronische Gesundheitskarte
eHC	Electronic Health Card
eHCT	Electronic Health Card Terminal
ETR	Evaluation Technical Report
IND	Independent testing
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
KVK	Krankenversichertenkarte
LAN	Local Area Network
OSP	Organisational Security Policy
PIN	Personal Identification Number
PP	Protection Profile
RSA	Asymmetrical Cryptographie (Rivest, Shamir und Adleman)
SAC	Signature Application Component
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SMC	Security Module Card
SM-KT	Security Module Kartenterminal
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
VAN	Vulnerability analysis

13.2. Glossary

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

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

14. Bibliography

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

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

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[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-1171-2023, Version 1.9.5, 2022-12-07, Electronic Health Card Terminal eHealth GT900 Security Target, gt german telematics GmbH

[7] Evaluation Technical Report, Version 1.0, 2023-02-16, Deutsche Telekom Security 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 May 2017

[8] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

[9] Configuration list for the TOE, Version 1.8.2, 2023-02-16, Chipkartenterminal eHealth GT900 - Dokumentation des Produktlebenszyklus - Konfigurationsliste, gt german telematics GmbH (confidential document)

[10] Kurzanleitung Kartenterminal eHealth GT900, gt german telematics GmbH, Version 1.0.1

[11] Kartenterminal eHealth GT900 –Benutzerhandbuch–, gt german telematics GmbH, Version 2.1.4, 2022-11-21

C. Excerpts from the Criteria

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

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3, Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

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

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report