Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1124-V2-2022

for

CHERRY eHealth Terminal ST-1506
AFxZ FW 3.0.0, HW 4.0.0

from

Cherry Digital Health 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-1124-V2-2022 (*)

eHealth: Smart Card Readers

CHERRY eHealth Terminal ST-1506
AFxZ FW 3.0.0, HW 4.0.0

from	Cherry Digital Health GmbH
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 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
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, 11 May 2022

For the Federal Office for Information Security

Matthias Intemann
Head of Branch

L.S.

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

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

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

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

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

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

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

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

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

2. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte 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]

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 Criteria for IT Security Evaluation (CC), Version 3.1[4] [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]

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. For mutual recognition the EAL 4 components of these assurance families are relevant.

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

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

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. 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 ST-1506, AFxZ FW 3.0.0, HW 4.0.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1124-2021. Specific results from the evaluation process BSI-DSZ-CC-1124-2021 were re-used.

The evaluation of the product CHERRY eHealth Terminal ST-1506, AFxZ FW 3.0.0, HW 4.0.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 22 April 2022. 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 Digital Health GmbH.

The product was developed by: Cherry Digital Health 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

[5] Information Technology Security Evaluation Facility

maximum validity of the certificate has been limited. The certificate issued on 11 May 2022 is valid until 10 May 2027. 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,
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 ST-1506, AFxZ FW 3.0.0, HW 4.0.0 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 Digital Health GmbH
Einsteinstraße 174
81677 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 eHealth Card Terminal with Touchscreen Display, ST-1506 AFxZ 3.0.0:4.0.0. The TOE has different certified variants, due to different housing color. The different variants can be identified by the part number of the TOE: the following variants of the TOE are certified TOE versions, ST-1506 AFHZ for white and ST-1506 AFEZ for black color. Both variants have the same TOE version.

The TOE is the card terminal eHealth Terminal ST-1506 with 2 ID1 Slots (HPC and eGK) and 2 SMC Slots (SM-KT (supporting SMC-B and SMC-KT cards) and SMC-A), 720p touchscreen (also used for secure pin entry) and LAN interfaces for the use in the German healthcare system with HPC and eGK.

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
Trusted Communication Channels	For all communication functions to the connector and remote users used by eHealth applications except service discovery the TOE will always establish a trusted communication channel to the connector or remote user.
Identification & Authentication	The TOE provides several authentication mechanisms for administrators and for other users.
Secure_PIN_Entry	The TOE provides for a secure PIN entry that can only be activated by the TOE itself and it will be indicated to the user by a LED and a red card symbol that it is in secure PIN-Entry mode. PINs for a card in a slot of the TOE, for the connector or for a remote card terminal will never be stored in a non-volatile memory of the TOE when the PIN is entered. To mitigate indirect access to the pin (gathered by touch coordinates), the position of the PIN user interface is randomized. The PIN entered by the user will only be sent to the card in the card slot of the TOE or via a TLS se-cured connection to the connector to a remote card terminal for remote-PIN verification.
Network Connections	The TOE only allows one connection to one connector at a time and will accept any information arriving at the network interface from the connector only if the communication path is encrypted and the connector has been successfully authenticated. Commands to identify the TOE in the network (service discovery) will be accepted and processed even without an

TOE Security Functionality	Addressed issue
	encrypted or authenticated connection.
Secure_Update	The TOE enforces that a modification of the firmware of the TOE only is allowed after the integrity and authenticity of the firmware has been verified by checking the signature over the update file. Signature verification on the new update file containing the new firmware signed by the manufacturer uses the cryptographic ECDSA algorithm with the curve brainpoolP384r1 and a size of the cryptographic key of 384 bit.
Secure Data Deletion	The TOE ensures that memory no longer used for storage of PINs, passwords, health data, crypto-graphic data and all information that is received by a card in a slot of the TOE or by the connect-or (except the shared secret) will be erased by overwriting with 0x00 before it is deallocated and then be made available for further use. Memory areas for PINs will be overwritten with 0x00 as soon as the PIN has been sent to the chip card.
Secure Management Functions	The TOE is aware of three roles: administrators, the TOE Reset Administrator, and user (meeting FMT_SMR.1). To identify and authenticate these roles the TOE provides PIN based identification and authentication. The secure management functions are only available to the TOE administrator after successful identification and authentication.
Self-Test	The TOE performs self-tests during initial start-up and after activation by an authorised user to demonstrate the correct operation of the TSF. The self-tests include tests of the cryptographic primitives for the AES and the hash algorithms and the RSA verification algorithm by performing known answer tests.
Secure Fail-State	The TOE ensures that it maintains a secure fail state when • an alarm condition indicates possible tampering or if a • self-test detects an error. The TOE will then turn to an unrecoverable non-functional state and has to be sent in for service.
Physical Protection of the TOE	The TOE is constructed as one part and is protected against opening attacks to the casing of the TOE by using full volumetric protection covers. For active protection against probing and drilling attacks, the TOE has an alarm function constantly checking a drill and probing protection foil for alarm conditions which are a short-cut or interruption of the circuit paths on the foil caused by drilling and probing attacks. On alarm (indi-cating possible tampering) the alarm function will display a message on the TOE display and will put the TOE in a secure non-functioning state. The alarm condition remains after a TOE restart.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 9.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.2 . 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:

CHERRY eHealth Terminal ST-1506, AFxZ FW 3.0.0, HW 4.0.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Hardware of the eHealth Card Terminal with Touchscreen Display, ST-1506 AFxZ	4.0.0	Delivery via secure delivery chain
2	SW	Firmware Image SHA-256-Hashsum: fd78c76bd22acbaa0dcf6e391936b267a5ddcd850b3b85309b0aa25739ec76db	3.0.0	Initially included in the TOE or as software update
3	DOC	eHealth Terminal ST-1506 - Handbuch für Administratoren (Teilenummer: 64410079) SHA-256-Hashsum: c7d2d64acdbbbbb6631116c5fbaa0799aca7aecccb4badf6b6cb74156876f2db	Apr 2022 / 04	Provided by the developer on their homepage https://www.cherry.de/eHealth
4	DOC	eHealth Terminal ST-1506 - Kurzanleitung für Benutzer (Teilenummer: 64410078) SHA-256-Hashsum: b1bc472ff8294e27e44fa0fa6e47c0ff1fedf28610f1c213f453c845feb74d39	Apr 2022/ 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 [11].

According to [11] the TOE is stored in the secure production area at Theobroma in Wien. The TOE will be send to the central dispatch warehouse of Cherry. The transport is secured with a seal (”Plombe”) and the seal number is sent to the warehouse by a signed e-mail.

The TOE will be delivered from central dispatch warehouse of Cherry to companies with a certified secure delivery chain, e.g. CGM (CompuGroup Medical Deutschland AG) and T-

Systems. From that point the secure delivery chain is identical to the related certified secure delivery chain.

The service technician or the end user installs the product eHealth Card Terminal with Touchscreen Display, ST-1506 AFxZ within the premises of the end user. The guidance 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. As an additional measure, the seal band (“Siegelband”) has to be checked.

The TOE can be identified within the management menu as following:

- Einstellungen > Status

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

- Artikelnummer: ST-1506 AFHZ (for white color)

  Firmwareversion: 3.0.0

  Hardwareversion: 4.0.0
- Artikelnummer: ST-1506 AFEZ (for black color)

  Firmwareversion: 3.0.0

  Hardwareversion: 4.0.0

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 6.1 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 […]. The card terminal prevents (not visible) physical manipulations for at least 10 minutes.

- 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.
- 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 TOE administrator is responsible for the correct operation of the Push Server.
- 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 3.5 and 4.2.

5. Architectural Information

The following figure is an overview of the TOE architecture:

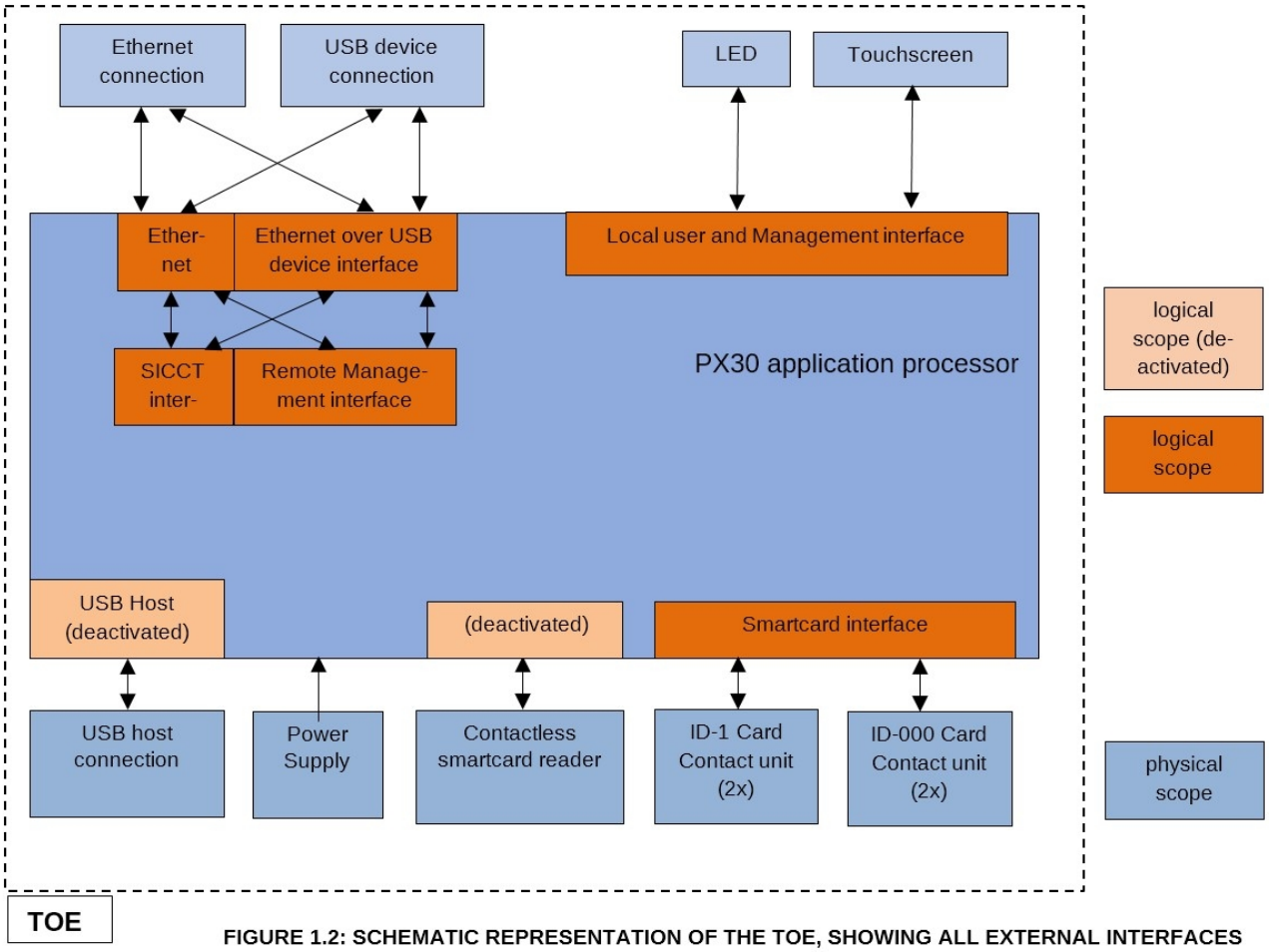

Figure 3: TOE Architecture

The figure presents the main building blocks of the TOE and their relation to the environment.

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. Developer's Test according to ATE_FUN

TOE configuration tested:

The Security Target [6] has identified solely one configuration of the TOE eHealth Card Terminal with Touchscreen Display, ST-1506 AFxZ 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:

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.

Independent Testing according to ATE_IND

- TOE test configurations:

  The evaluation body used the same test configuration 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 most of the local management tests[7] and a subset of the firmware update tests[8]. For the local management test sampling was conducted.

- Verdict for the sub-activity:

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

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 are two configurations 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 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:

[7] The evaluator covered most gui functionality during their regular interaction with the TOE. A few local management tests regarding access control were repeated to verify the developer's results and to ensure that the administrators function can only be accessed after entering the login credentials.

[8] The TOE does not support firmware downgrade. Due to the irreversible process of the firmware update, the evaluator has repeated a subset of the update tests.

  - C1: TOE without any modifications. The setup comprises of the TOE connected to a computer via LAN or USB,
  - C2: TOE with debug capabilities. The TOE offers a SSH interface for the evaluation to inspect the operating system and its configuration.

- Attack scenarios having been tested:

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

  - SecureCommunication,
  - DataProtection,
  - Update,
  - AccessControl,
  - CardCommunication,
  - SecurePIN-Entry,
  - FactoryReset,
  - SecureManagement,
  - SecureStates,
  - SelfProtection,
  - TOE-Interface,
  - PhysicalSecurity,
  - SecBoot,
  - DomainSeparation,
  - SystemHardening,
  - CobraApplet,
  - RNG,
  - ThirdPartySoftware, and
  - StaticCodeAnalysis.

- SFRs penetration tested:

  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

There is only one evaluated configuration of the TOE. The difference between the article numbers ST-1506 AFHZ and ST-1506 AFEZ is only related to the color 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.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-1124-2021, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on ADV, AGD, ATE and AVA with ATE_IND.

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 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 tables give 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	Implementation Standard	Key Size in Bits	Security Level above 100 Bits	Comments
1.	Trusted Channel	TLS_DHE_RSA_WITH_AES_128_CBC_SHA and TLS_DHE_RSA_WI	RFC 5246 (TLS 1.2, DHE) FIPS 197 (AES-GCM, AES-	128 bit resp. 256 bit (AES) 160bit (SHA)	yes	[12], [13]

No.	Purpose	Cryptographic Mechanism	Implementation Standard	Key Size in Bits	Security Level above 100 Bits	Comments
		TH_AES_256_CBC_SHA; TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 curves for ECDHE: P-256, P-384, brainpoolP256r1, brainpoolP384r1 with cryptographic primitives: Diffie-Hellman key exchange (DH group for RSA: 14) sym. de-/ encryption and MAC-calculation with AES-CBC Hash-calculation with SHA verification (certificate) with RSASSA-PKCS#1 v2.2 in FCS_CKM.1.1/Connector, FCS_COP.1.1/Con_Sym, FCS_COP.1.1/SIG	CBC) FIPS PUB 180-2 (SHA) RFC 8017 (RSASSA-PKCS#1 v2.2) RFC 4492 (ECC for TLS) RFC 5639 (Brainpool)	2048 bit (RSA) 384 bit (ECDHE)		
2.	Trusted Channel / web-management FCS_CKM.1.1/Management, FCS_COP.1.1/Management	TLS v1.2 Cipher Suite TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_C	RFC 5246 (TLS 1.2, DHE, ECDHE) FIPS 197 (AES-GCM, AES-CBC) FIPS PUB 180-2 (SHA) FIPS 180-4 (SHA256) RFC 8017 (RSASSA-PKCS#1 v2.2) ANSI X9.62	256 bit resp. 384 bit (P-256, P-384, brainpool) 128 bit resp. 256 bit (AES) 160 bit (SHA) 256 bit (SHA256) 384 bit (SHA384) 2048 bit (RSA)	yes	[12], [13]

No.	Purpose	Cryptographic Mechanism	Implementation Standard	Key Size in Bits	Security Level above 100 Bits	Comments
		BC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 with cryptographic primitives: ECDHE Diffie-Hellman key exchange (curves P-256, P-384, brainpoolP256r1, brainpoolP384r1]) symm. de-/ encryption and MAC-calculation with AES-GCM resp. AES-CBC Hash-calculation with SHA256 resp. SHA384 resp. SHA-2 Signaturverification (certificate) with RSASSA-PKCS#1 v2.2 Signature verification ECDSA	(ECDSA)			
3.	Password verification (all user, but TOE Reset Administrator) in FIA_UAU.5	Password verification by SHA-256-Hash via password and individual Salt with cryptographic primitives: SHA-256	FIPS 180-4 (SHA)	256 bit (SHA)	yes	[12], [13]
4.	Password verification (TOE Reset Administrator) in FIA_UAU.5	Password verification via HOTP Challenge-Response With cryptographic primitives: SHA-256	RFC 4226, with SHA-256 used Hash-Function SHA-2 Hash-Funktion, s. FIPS 180-4	256 bit (SHA)	yes	[12], [13]

Table 3: TOE cryptographic functionality for the trust channels

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

No.	Purpose	Cryptographic Mechanism	Implementation Standard	Key Size in Bits	Application Standard
1.	Authentification of the correct Firmware (FW-Update)	ECDSA Signaturverification with brainpool with cryptographic primitives: ECDSA with curve brainpoolP384r1 Hash-calculation with SHA in FCS_COP.1.1/SIG_FW	ANSI X9.62 (ECDSA) FIPS 180-4 (SHA256)	384 bit (brainpool) 256 bit (SHA-256)	[14]
2.	Authentification TSL (TSP CA LIST Update)	ECDSA Signaturverification with brainpool with cryptographic primitives: ECDSA with curve brainpoolP384r1 Hash-calculation with SHA in FCS_COP.1.1/SIG_TSP	ANSI X9.62 (ECDSA) FIPS 180-4 (SHA256)	384 bit (brainpool) 256 bit (SHA)	[14]

Table 4: TOE cryptographic functionality for the firmware update

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 [12] and [14] the algorithms are suitable for the corresponding purpose. 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.

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
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
eGK	Elektronische Gesundheitskarte
eHC	Electronic Health Card
eHCT	Electronic Health Card Terminal
ETR	Evaluation Technical Report
FLR	Flaw remediation

HPC	Health Professional Card
IND	Independent testing
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
OSP	Organisational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
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[9] 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-1124-V2-2022, Version 4.8, 2022-04-06, Security Target EAL3+ for eHealth Terminal ST-1506, Cherry Digital Health GmbH

[7] Evaluation Technical Report, Version 2, 2022-04-21, ETR SUMMARY, 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 May 2017

[9] Configuration list for the TOE, ALC_CMS_HW, V1.1.0, 2022-03-21, ALC_CMS_SW, V1.13, 2022-04-06, BOM, V4.0.0, 2022-03-07 Bibliography V4.5, 2022-04-07 (confidential document)

[10] eHealth Terminal ST-1506 - Handbuch für Administratoren (Teilenummer: 64410079) , Version 4, 2022-04, Cherry Digital Health GmbH

[11] Common-Criteria-3.1 Dokument, ALC_DEL.1, Version 0.9, 2020-10-27 Cherry Digital Health GmbH, (confidential document)

[12] gematik, Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Version 2.20.0, Stand 02.09.2021

[13] gematik, Spezifikation eHealth-Kartenterminal, Version 3.13.3, 30.06.2021

[14] Technical Guideline BSI TR-03111 Elliptic Curve Cryptography, Version 2.10, 01.06.2018, Federal Office for Information Security (BSI).

[9] specifically

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

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