Federal Office
for Information Security

Certification Report

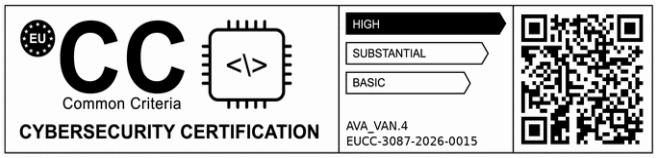
EUCC-3087-2026-0015
Administration ID
BSI-DSZ-CC-1124-V4-2026

for

CHERRY eHealth Terminal ST-1506, FW 5.0.0, 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 9582-11

Contents

A. Certification

1. Preliminary Remarks

The Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 [EUCC-VO] establishes a Union-wide cybersecurity certification scheme for TOEs and Protection Profiles for conformity assessments using the requirements of Common Criteria.

By implementing the Cybersecurity Act[1], certification activities at assurance level 'high' and in duly justified cases at assurance level 'substantial' are reserved to the National Cybersecurity Certification Agency of a Member State.

In accordance to BSIG[2] Act, the Federal Office for Information Security (BSI) issues certificates for information technology products.

Certification of a product is carried out at the request of a developer, vendor or a distributor, hereinafter called the applicant.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria referenced in the above mentioned Implementing Regulation (EU) 2024/482 as well as relevant application notes and interpretations published by the certification body of the BSI.

Evaluation facilities notified by the German National Cybersecurity Certification Authority carry out the evaluation.

This Certification Report is the result of the certification activities carried out by the certification body of the BSI in conclusion of the technical evaluation. 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 carries out its activities according to the criteria laid down in the following:

- Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) [EUCC-VO]
- EUCC state-of-the-art documents of relevance to the TOE [EUCC_SOTA]
- Act on the Federal Office for Information Security[2]

[1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[2] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 2 December 2025, BGBl. 2025 Nr. 301, S. 2

- BSI Certification and Approval Ordinance[3]
- BMI Regulations on Ex-parte Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior and Community)
- ISO/IEC 15408 as published on the day of issuance of this certificate and as mirrored by the Common Criteria for IT Security Evaluation (CC), Version CC:2022 [CC]
- ISO/IEC 18045 as published on the day of issuance of this certificate and as mirrored by the Common Methodology for IT Security Evaluation (CEM), Version CEM:2022 [CEM]
- DIN EN ISO/IEC 17065 standard
- EUCC programme: Scheme documentation describing the certification process (EUCC) [EUCC_PROG]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [AIS]

3. Recognition Agreements

In order to avoid multiple certifications 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. International Recognition of CC – Certificates (CCRA)

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

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

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

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 5 EAL 2 and ALC_FLR components.

4. Performance of Evaluation and Certification

- The certification body monitors each individual evaluation to ensure a uniform application and interpretation of the criteria as well as uniform ratings.

[3] Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung – BSIZertV) of 02 December 2025, Bundesgesetzblatt 2025, no. 301

[4] 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

- The TOE CHERRY eHealth Terminal ST-1506, FW 5.0.0, HW 4.0.0 has been certificied by the certification body of the Federal Office for Information Security (BSI) based on administration ID BSI-DSZ-CC-1124-V3-2023. Specific results from the evaluation process were re-used.
- The evaluation of the product CHERRY eHealth Terminal ST-1506, FW 5.0.0, HW 4.0.0 was carried out by TÜV Informationstechnik GmbH, located at
  Unternehmensgruppe TÜV NORD
  Am TÜV 1
  45307 Essen.
- The evaluation was completed on 12 August 2026. TÜV Informationstechnik GmbH is a notified evaluation facility (ITSEF).
- This certification was applied for: Cherry Digital Health GmbH.
- The assessed TOE was developed by: Cherry Digital Health GmbH.
- The certification activities are concluded with the comparability check and the production of this Certification Report. This work was completed by the certification body of the BSI.

This Certification Report applies only to the version of the TOE as identified in this document. The confirmed assurance package is valid on the condition that

- all statements and indications regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in an environment 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 issued Certificate confirms the assurance of the product claimed in the Security Target [ST] on certificate’s issuance day. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be reassessed. Therefore, the holder of the certificate should involve the assurance continuity program of the EUCC Certification Scheme (e.g. by a re-assessment or re-certification) in its obligations to monitor the certified product. Specifically, if certification results should be 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 reassessment on a regular e.g. annual basis.

In order to prevent an indefinite certificate usage where evolving attack methods justify a recent reassessment of the product’s resistance, the maximum validity period of the certificate is limited. The certificate issued on 17 August 2026 is valid until 16. August 2031 and its validity can be renewed by certifying the TOE again.

The holder of this certificate is obliged:

1. to meet the obligations from the Implementing Regulation (EU) 2024/482, in particular but not exclusively to respect the rules for certificate usage, to monitor the conformity of the certified TOE, to inform the certification body about subsequently detected vulnerabilities or irregularities with relevance to the security of the TOE and to maintain vulnerability management and disclosure procedures,

Should changes be introduced into the certified version of the TOE, the validity period of its related certificate can be extended in order to cover the changed TOE, provided the holder of the certificate applies for measures under EUCC scheme’s assurance continuity

(i.e. recertification or maintenance) and the changed TOE then meets the assurance requirements.

5. Publication

The TOE CHERRY eHealth Terminal ST-1506, FW 5.0.0, HW 4.0.0 has been notified to ENISA for publication on the website on European cybersecurity certification schemes and has also been included in BSI's list of certified products, which is published regularly (see [EUCC_CERT]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

This holder of the certificate[5] has to publish on its website this Certification Report and supplementary information. The Certification Report may also be obtained in electronic form at the internet address stated above.

[5] Cherry Digital Health GmbH
Rosental 7
80331 München

B. Certification Results

The following chapters summarise the assessment results of the

- the applicant’s Security Target specified for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes, statements and indications from the certification body.

1. Executive Summary

The Target of Evaluation is the eHealth Card Terminal with Touchscreen Display, ST-1506 AFxZ 5.0.0:4.0.0. 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 product CHERRY eHealth Terminal ST-1506, FW 5.0.0, HW 4.0.0 has been certified under the EUCC scheme in accordance to the provisions of the Implementing Regulation (EU) 2024/482. Specific results from the evaluation process based on administration ID BSI-DSZ-CC-1124-V3-2023 were re-used. The TOE deliverables are listed in table 1.

The evaluation of the product CHERRY eHealth Terminal ST-1506, FW 5.0.0, HW 4.0.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 12 August 2026. TÜV Informationstechnik GmbH is a notified evaluation facility (ITSEF).

The Evaluation Technical Report (ETR) [ETR] was provided by the ITSEF according to the Common Criteria [CC], the Methodology [CEM], the requirements of the Scheme [EUCC-VO],[EUCC_PROG].

The evaluation has confirmed:

- CC Version and Release: see [CC] and [CEM]
- PP Conformance: Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), BSI-CC-PP-0032-V3-2023, 15.12.2022 [PP]
- Assurance Level: EUCC High with component AVA_VAN.4
- Assurance Package: EAL 3
- Augmentation: ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, AVA_VAN.4

The Security Target [ST] is the basis for this certification. It is based on the certified Protection Profile Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), BSI-CC-PP-0032-V3-2023, 15.12.2022 [PP].

A detailed description of the security functionality, addressed threats, organisational security policies and the operational environment can be found in the Security Target [ST].

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

The vulnerability assessment results stated in this certificate do not express an appraisal of the strength and suitability of the cryptographic algorithms implemented in the TOE (see BSIG Section 52, Para. 4, Clause 2).

The certification results apply only to the version of the product indicated in the certificate and on the condition that all the statements and indications are kept as detailed in this Certification Report. Neither the BSI nor any other organisation that recognises or gives effect to this certificate implicitly or explicitely guarantee or endorse the certified TOE.

2. Identification of the TOE

The Information and communications technology product is identified as follows:

CHERRY eHealth Terminal ST-1506, FW 5.0.0, HW 4.0.0

Holder of the certificate: Cherry Digital Health GmbH
Rosental 7
80331 München
https://embedded.cherry.de/st-1506-security/

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: a96447661463072e342c91dd25356a1f6e7a2cbea34c495ef93149c6a9a112b5	5.0.0	Initially included in the TOE or as a software update
3	DOC	eHealth Terminal ST-1506 - Handbuch für Administratoren (Teilenummer: 64410079) SHA-256-Hashsum: 06b40eaa6a16a5d728de8a002bafb3b696a26cf8b5fd52eb32b48264dd412f2b	Jul 2026 / 11	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: c1affb988741179142916ebf019daf2ffcd9991071caaa312075ddc131c7f0cd	Jul 2026 / 07	Delivered with the de-livery package of the TOE

Table 1: Deliverables of the TOE

2.1. TOE Delivery Process

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

According to [ALC_DEL] 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 send 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.

2.2. TOE Identification

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: 5.0.0
  Hardwareversion: 4.0.0
- Artikelnummer: ST-1506 AFEZ (for black color)
  Firmwareversion: 5.0.0
  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 mentioned security policies can be found in sections 6.1 of the [ST].

For vulnerability handling, information can be found on the following website: https://embedded.cherry.de/st-1506-security/

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 uncovered aspects need to be provided for by specific security objectives that have to be met by the TOE environment. They are in particular:

- 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-hos-tile, 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 [ST].

5. Architectural Information

Figure 1.2 in [ST] presents the main building blocks of the TOE and their relation to the environment.

6. Supplementary Cybersecurity Information

The evaluated documentation as outlined in table 1 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.

Regarding the secure PIN entry mode, there are two different security levels of the TOE, which can be configured within the menu (see [AGD, 24.3]). The activation of the randomized presentation of the virtual PIN keyboard is mandatory for the evaluated configuration of the TOE (menu: “Verwürfelung PIN-Eingabe (ein)”). This is the default configuration after the delivery of the TOE.

As described in [AGD, 22] the TOE can be configured to enter the PIN of the SMC-B via Web Service. This is deactivated by default and it is not allowed to activate it for the evaluated TOE configuration as mentioned by the security note in that chapter.

As described in [ST, 1.4.1] and [AGD, 15.6] the TOE must not be connected to the PIN-Pad. The use of the external PIN-Pad is not allowed for the certified version of the TOE.

As described in [ST, 7.10] the developer implemented the physical protection mechanisms by using metal drill covers and other detection measures within the TOE casing to protect physical tamper attacks against the TOE. The requirement based on O.PROTECTION (see [PP, 4.1] and [ST, 4.1]) is fulfilled by this security mechanism.

As described in [AGD, 14.1] the TOE can be configured to perform a remote pairing with a connector. This is deactivated by default and it is not allowed to activate it for the evaluated TOE configuration as mentioned by the security note in that chapter.

There are no other requirements for the TOE usage, except those provided for TOE users/administrators in the guidance documentation [AGD] and [AGD Quick].

The developers website as stated in chapter 2 provides the following supplementary information:

- the period during which support is offered (esp. security related updates)
- contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers
- a reference to online repositories listing publicly disclosed vulnerabilities related to the TOE/ICT, ICT service or ICT process and to any relevant cybersecurity advisories

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

All tests have been carried out by ITSEF:
TÜV Informationstechnik GmbH,
Unternehmensgruppe TÜV NORD
Am TÜV 1
45307 Essen
under the responsibility of certification Body

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87
Postfach 20 03 63
D-53175 Bonn

Please refer to chapter 1 for details on assurance levels or packages involved into testing.

7.1. Developer's testing approach

The TOE was tested for the aspect ATE in the configuration defined in the ST and for EBT testing with an additional test configuration with debug capabilities.

- 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 Testing Approach:

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.

All interfaces were considered during testing.

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

Penetration Testing according to AVA_VAN

The penetration testing was partially performed using the developer's testing environment, partially using the test environment of the ITSEF.

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.

Verdict for the sub-activity:

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

8. Evaluated Configuration

This certificate covers the following configurations of the TOE:

Artikelnummer: ST-1506 AFHZ (for white color)
Firmwareversion: 5.0.0
Hardwareversion: 4.0.0

Artikelnummer: ST-1506 AFEZ (for black color)
Firmwareversion: 5.0.0
Hardwareversion: 4.0.0

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 and no differences of the hard- or software of the TOE.

9. Results of the Evaluation

9.1. CC specific results

The ITSEF produced and provided the Evaluation Technical Reports (ETR) [ETR] according to the requirements of the Scheme [EUCC-VO],[EUCC_PROG], the Common Criteria [CC], the Common Evaluation Methodology [CEM], and all relevant interpretations and guidelines of the Scheme (AIS) [AIS].

On advise by the Certification Body and consent by the certificate holder the following guidance further specific for the technology of the product [AIS] were applied:

AIS 14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 2010-08-03, Bundesamt für Sicherheit in der Informationstechnik.,

AIS 19, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 9, 2014-11-03, Bundesamt für Sicherheit in der Informationstechnik.

AIS 32, CC-Interpretationen im deutschen Zertifizierungsschema, Version 7, 2011-06-08, Bundesamt für Sicherheit in der Informationstechnik.

AIS 46, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, Version 3, 2013-12-04, Bundesamt für Sicherheit in der Informationstechnik.

As a result of the evaluation, the verdict PASS is confirmed for the assurance components that are identified in chapter 1 of this report and claimed by the Security Target [ST] for the corresponding TOE. The corresponding TOE is identified in chapter 2 of this report.

The certificate

- is uniquely identified by: EUCC-3087-2026-0015, administration ID BSI-DSZ-CC-1124-V4-2026
- was issued on: 17 August 2026
- is valid until: 16 August 2031

The results of the evaluation are only applicable to the TOE as defined in chapter 1 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

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

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application
Trusted Channel in FCS_CKM.1.1/ Connector, FCS_COP.1.1/Con_Sym, FCS_	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 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: Ephemeral Diffie–Hellman key exchange (ECDHE) sym. de-/encryption and integrity protection with AES-GCM (128 bit / 256 bit) Hash-calculation with SHA-256 / SHA-384 verification (certificate) with RSASSA-PKCS#1 v1.5 / ECDSA	RFC 5246 (TLS 1.2) RFC 4492 (ECC / ECDHE for TLS) RFC 5289 (TLS ECDHE + AES-GCM cipher suites) FIPS 197 (AES-GCM) FIPS PUB 180-2 (SHA-256 / SHA-384) RFC 8017 (RSASSA-PKCS#1) RFC 5639 (Brainpool curves) SEC 2 / FIPS 186-4 (NIST curves P-256, P-384 / ECDSA)	128 bit resp. 256 bit (AES) 256 bit resp. 384 bit (SHA) 2048 bit (RSA) 256 bit resp. 384 bit (ECDHE / ECDSA)	[gemSpec_Krypt], [gemSpec-KT]..
Trusted Channel / web-management FCS_CKM.1.1/ Management, FCS_COP.1.1/ Management	TLS v1.2 Cipher Suite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 with cryptographic primitives: ECDHE Diffie-Hellman key	RFC 5246 (TLS 1.2) RFC 4492 (ECC / ECDHE for TLS) RFC 5289 (TLS ECDHE + AES-GCM cipher suites) FIPS 197 (AES-GCM) FIPS PUB 180-4 (SHA-256 / SHA-384) RFC 8017 (RSASSA-PKCS#1 v1.5) RFC 5639 (Brainpool curves) FIPS 186-5 (NIST curves P-256 / P-384 und ECDSA)	128 bit resp. 256 bit (AES) 256 bit resp. 384 bit (SHA) 2048 bit (RSA) 256 bit resp. 384 bit (ECDHE / ECDSA)	[gemSpec_Krypt], [gemSpec-KT]

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application
	exchange (curves P-256, P-384, brainpoolP256r1, brainpoolP384r1) symm. de-/encryption and integrity protection with AES-GCM Hash-calculation with SHA-256 resp. SHA-384 Signature verification (certificate) with RSASSA-PKCS#1 v1.5 / ECDSA			
Password verification (all user, but TOE Reset Adminis-trator) 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)	[gemSpec_Krypt], [gemSpec-KT]
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)	[gemSpec_Krypt], [gemSpec-KT]
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)	[TR-03111]
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)	[TR-03111]

Table 2: TOE cryptographic functionality

The strength of the these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 52, Para. 4, Clause 2).

According to [gemSpec_Krypt], [gemSpec-KT] the algorithms are suitable to enforce its security policy for the respective functionalities of the TOE An explicit validity period is not given.

10. Obligations and Notes for the Usage of the TOE

Table 1: Deliverables of the TOE outlines the documents that contain necessary information on the intended use of the TOE including all security related information, conditions and instructions to be taken into account by the user. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target and not covered by the TOE itself need to be met by the operational environment of the TOE.

The customer or user of the TOE shall take the statements of this certificate into account in its system risk management process. The user should define measures in its risk management that respond to emerging and new attack methods and techniques to the TOE until the TOE has been reassessed.

The user also has to consider in its risk management the limited validity for the usage of cryptographic algorithms as outlined in chapter 9.

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. Until the TOE has been re-certified, the user should examine the use 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 [ST] of the TOE / Information and communications technology (ICT) product is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

None

12.1. Acronyms

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

ETR Evaluation Technical Report

ICT Information and communications technology

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

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

12.2. Glossary

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

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

13. Bibliography

[EUCC-VO] Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)
and
Implementation Regulation (EU) 2025/2462 of 8 December 2025 amending Implementing Regulation (EU) 2024/482 as regards definitions, ICT product series certification, assurance continuity and state-of-the-art document

[CC]	ISO 15408:2022, Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model - Part 2: Security functional components - Part 3: Security assurance components - Part 4: Framework for the specification of evaluation methods and activities - Part 5: Pre-defined packages of security requirements https://www.iso.org/standard/72891.html https://www.iso.org/standard/72892.html https://www.iso.org/standard/72906.html https://www.iso.org/standard/72913.html https://www.iso.org/standard/72917.html as mirrored by CCRA's edition: CC:2022 R1, Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model - Part 2: Security functional components - Part 3: Security assurance components - Part 4: Framework for the specification of evaluation methods and activities - Part 5: Pre-defined packages of security requirements https://www.commoncriteriaportal.org
[CEM]	ISO 18045:2022: Information technology Security techniques Methodology for IT security evaluation https://www.iso.org/standard/72889.html as mirrored by CCRA's edition: CEM:2022 R1, Common Methodology for Information Technology Security Evaluation https://www.commoncriteriaportal.org
[EUCC_SOTA]	EUCC state-of-the-art documents: https://certification.enisa.europa.eu/publications/eucc-state-art-documents_en
[EUCC_PROG]	EUCC program of the BSI: Scheme documentation describing the certification process (EUCC), https://www.bsi.bund.de/zertifizierung
[EUCC_CERT]	EUCC Certificates, periodically updated list published on ENISA's website on European cybersecurity certification schemes (https://certification.enisa.europa.eu/) but also on BSI's website (https://www.bsi.bund.de/zertifizierungsreporte)
[AIS]	Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[6] https://www.bsi.bund.de/AIS
[ST]	Security Target BSI-DSZ-CC-1124-V4-2026, Version 6.5, 07.08.2026 Security Target EAL3+ for eHealth Terminal ST-1506, Cherry Digital Health GmbH

[6]specifically

- see chapter 9.1

[PP]	Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), BSI-CC-PP-0032-V3-2023, 15.12.2022
[ETR]	Evaluation Technical Report, Version 3, 12.08.2026, EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY), TÜV Informationstechnik GmbH, (confidential document)
[ConfList]	Configuration list for the TOE: [ALC_CMS_SW], [ALC_CMS_HW], [BOM] and [Bibliography] (confidential documents)
[ALC_CMS_SW]	Cherry ST-1506 Security Evaluation Configuration Management Scope of Software Development ALC_CMS_SW, Version 3.1, 26.07.2026, Cherry Digital Health GmbH (confidential document)
[ALC_CMS_HW]	ALC_CMS_HW_vx.y.z.xlsx, Version 1.1.1, 31.01.2023, Cherry Digital Health GmbH (confidential document)
[BOM]	BOM_Package_v4.0.0_2023-02-01 Version 4.0.0, 01.02.2023, Cherry Digital Health GmbH (confidential document)
[Bibliography]	ST-1506 Bibliography, Glossary and Acronyms, Version 6.3, 07.08.2026, Cherry Digital Health GmbH (confidential document)
[AGD]	eHealth Terminal ST-1506 - Handbuch für Administratoren, Version 64410079-11, July 2026, Cherry Digital Health GmbH
[AGD Quick]	eHealth Terminal ST-1506 - Kurzanleitung für Benutzer, Version 64410078-07, July 2026, Cherry Digital Health GmbH
[gemSpec-KT]	gematik- Spezifikation eHealth-Kartenterminal, Version 3.17.0, 12.02.2024.
[gemSpec_Krypt]	gematik - Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Version 2.29.0, Stand 30.01.2024.
[ALC_DEL]	Common-Criteria-3.1 Dokument ALC_DEL.1, V1.1, 17.01.2023, Cherry Digital Health GmbH (confidential document)

Note: End of report