Federal Office
for Information Security

Certification Report

BSI-CC-PP-0032-V3-2023

for

Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), Version 3.8

developed by

Federal Office for Information Security

Federal Office for Information Security (BSI), Postfach 20 03 63, 53133 Bonn, Germany
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-CC-PP-0032-V3-2023

Common Criteria Protection Profile

Common Criteria Protection Profile Electronic Health Card Terminal (eHCT)
Version 3.8

developed by Federal Office for Information Security

Assurance Package claimed in the Protection Profile:
Common Criteria Part 3 conformant
EAL 3 augmented by
ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, and AVA_VAN.4

valid until 5 February 2033

SOGIS Recognition Agreement

Common Criteria

The Protection Profile identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 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 Protection Profile and in conjunction with the complete Certification Report.

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 Protection Profile by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the Protection Profile 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

Bonn, 6 February 2023
For the Federal Office for Information Security

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

Sandro Amendola
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 Act on the Federal Office for Information Security (BSIG), the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products as well as for Protection Profiles (PP).

A PP defines an implementation-independent set of IT security requirements for a category of products which are intended to meet common consumer needs for IT security. A PP claimed by a user, consumer or stakeholder for IT gives them the possibility to express their IT security needs without referring to a specific product. Product certifications can be based on Protection Profiles. For products which have been certified based on a Protection Profile an individual certificate will be issued but the results from a PP certification can be re-used for the Security Target evaluation within a product evaluation when conformance to the PP has been claimed.

Certification of the Protection Profile is carried out on the instigation of the BSI or a sponsor. A part of the procedure is the technical examination (evaluation) of the Protection Profile according to Common Criteria [1]. The evaluation is usually 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.

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 (BSIG)[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], including PP Certification
- 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, Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Internal procedure for the issuance of a PP certificate

3 Recognition Agreements

In order to avoid multiple certification of the same Protection Profile in different countries a mutual recognition of IT security certificates - as far as such certificates are based on CC - under certain conditions was agreed. Therefore, the results of this evaluation and certification procedure can be re-used by the product certificate issuing scheme in the evaluation of a Security Target within a subsequent product evaluation and certification procedure.

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 up to and including Common Criteria (CC) Evaluation Assurance Levels EAL 4, and in addition at higher recognition levels for IT-Products related to certain technical domains only. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

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.

Details on recognition, the signatory nations, technical domains and the agreement itself can be found at https://www.sogis.eu.

3.2 International Recognition of CC – Certificates (CCRA)

The international Common Criteria Recognition Arrangement (CCRA) became effictive in September 2014 in its current version. It defines the recognition of certificates for IT-products 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 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.

Details on recognition, the signatory nations and the agreement itself can be found at https://www.commoncriteriaportal.org.

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

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 PP Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), Version 3.8 has undergone the certification procedure at BSI. This is a re-certification based on BSI-CC-PP-0032-V2-2015. Specific results from the evaluation process based on BSI-CC-PP-0032-V2-2015 were re-used.

The evaluation of the PP Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), Version 3.8 was conducted by the ITSEF Deutsche Telekom Security GmbH (Bonn). The evaluation was completed on 5 January 2023. The ITSEF Deutsche Telekom Security GmbH (Bonn) is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Federal Office for Information Security.

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 only applies to the version of the Protection Profile as indicated.

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

For the meaning of the CC concepts and terms please refer to CC [1] Part 1 for the concept of PPs, to CC [1] Part 2 for the definition of Security Functional Requirements components (SFR) and to CC [1] Part 3 for the definition of the Security Assurance Components, for the class AVA Vulnerability assessment and for the cross reference of Evaluation Assurance Levels (EALs) and assurance components.

The validity of this certificate ends as outlined on the certificate. The applicant and the sponsor of this certificate are recommended to review the technical content of the Protection Profile certified according to the evolvement of the technology and of the intended operational environment of the type of product concerned as well as according to the evolvement of the evaluation criteria. Such review should result in an update and a re-certification of the Protection Profile accordingly. Typically, technical standards are reviewed on a five years basis.

The limitation of validity of this PP certificate does not necessarily impact the validity period of a product certificate referring to this Protection Profile, but the certification body issuing a product certificate based on this Protection Profile should take it into its consideration on validity.

[5] Information Technology Security Evaluation Facility

6 Publication

The PP Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), Version 3.8 has been included in the BSI list of the certified Protection Profiles, 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.

The Certification Report may be obtained in electronic form at the internet address stated above.

B Certification Results

The following results represent a summary of

- the certified Protection Profile,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Protection Profile Overview

The Protection Profile Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), Version 3.8 [6] is established by the Federal Office for Information Security as a basis for the development of Security Targets in order to perform a certification of an IT-product, the Target of Evaluation (TOE).

The Target of Evaluation described in the Protection Profile (PP) BSI-CC-PP-0032-V3-2023 is a smart card terminal, which fulfils the requirements to be used with the German electronic Health Card (eHC) and the German Health Professional Card (HPC) based on the regulations of the German healthcare system.

Furthermore, the TOE fulfils the requirements to be used as a secure PIN pad entry device for applications according to [15]. In case of a stand-alone card terminal the physical scope of the TOE comprises:

- The hardware and if applicable sealed cage of the smart card terminal,
- The firmware of the smart card terminal, and
- The related guidance documents.

Compared with the earlier version of this PP, among other things, the optional support for secure contactless card access was added and updates to the CC and the gematik specification have been taken into account.

In its core functionality the TOE is not different from other smart card terminals that provide an interface to one or more smart cards including a mean to securely enter a PIN. Additionally the TOE provides a network interface which allows routing the communication of a smart card to a remote IT product outside the TOE.

The TOE provides the following main functions:

- Access to one or more slots for smart cards,
- Secure network connectivity,
- Secure PIN entry functionality,
- Enforcement of the encryption of communication,
- User authentication,
- Management functionality including update and downgrade of Firmware,
- Passive physical protection, and
- Optional: Secure contactless card access.

The TOE must work with a cryptographic key for i.e. authentication, integrity assurance and to ensure the confidentiality of data transmitted over the LAN interface. Due to the high protection requirements of the information objects transmitted over the LAN interface, a secure key store (SM-KT) is required for the key. The TOE has to support the gSMC-KT as the security module of the card terminal (SM-KT). The support of IPv4 is mandatory. To ensure the sustainability of the TOE, it should be able to support IPv6 in addition to IPv4 only with a firmware update.

In its environment, the TOE communicates with a so called connector. This connector is the secure connection between the local network of the medical supplier and the remote network of the telematic infrastructure. It provides the medical supplier with secure access

to the services of the telematic infrastructure. The connector will be evaluated separately according to the requirements in the corresponding Protection Profile BSI-CC-PP-0098 [9].

For the connection of the TOE to a connector via the LAN interface, the protocol with the SICCT commands is mandatory. The interfaces of the TOE and communication partners using them are provided in Figure 1.

The TOE may support contactless access of smartcards according to ISO/IEC 14443. In this case the communication to the card is secured regarding integrity and confidentiality

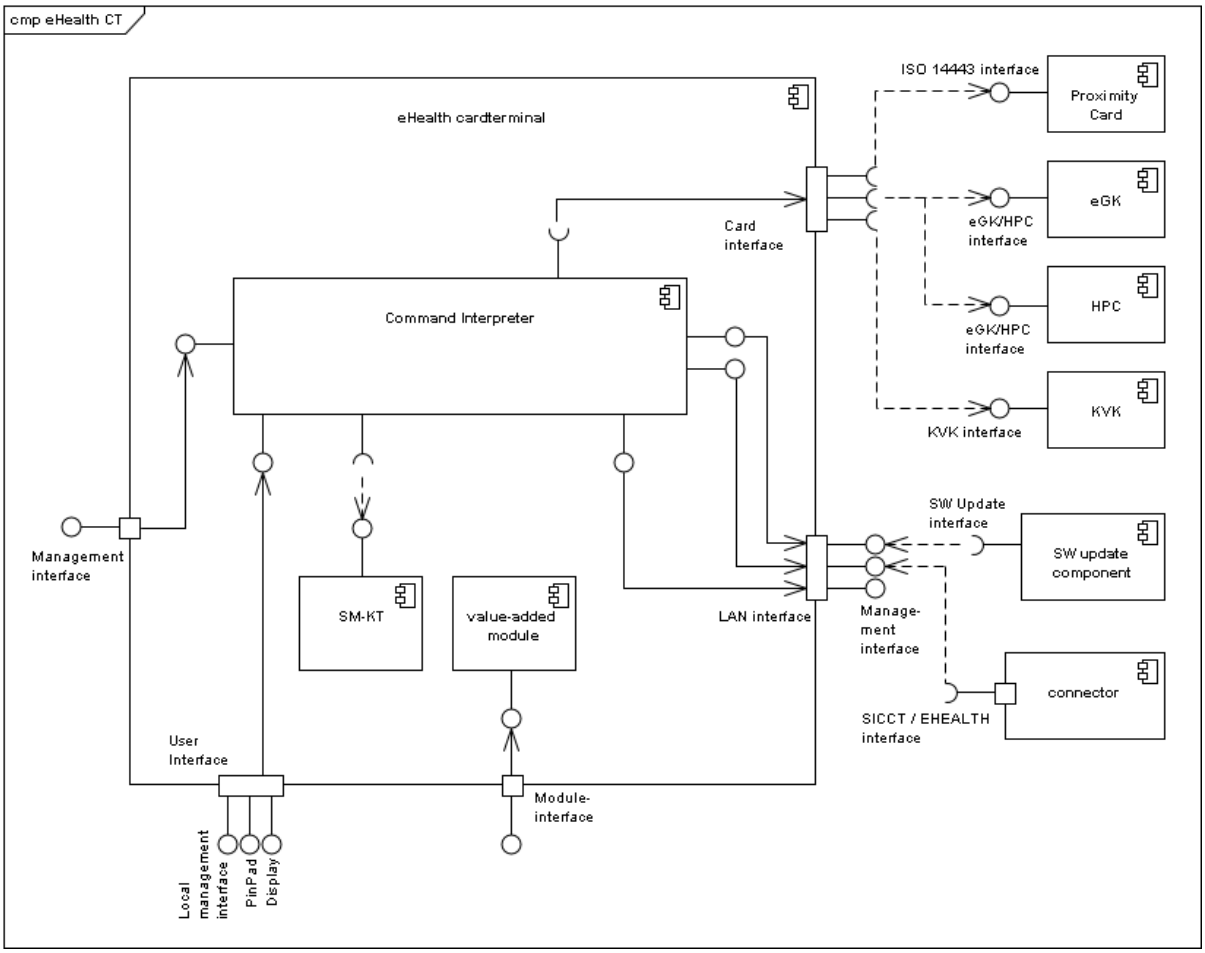

Figure 1: TOE architecture (logical perspective)

The assets to be protected by a TOE claiming conformance to this PP are defined in the Protection Profile [6], chapters 3.1 and 7.1.1. Based on these assets the security problem definition is defined in terms of assumptions, threats and organisational security policies. This is outlined in the Protection Profile [6], chapters 3 and 7.1.

These assumptions, threats and organisational security policies are split into security objectives to be fulfilled by a TOE claiming conformance to this PP and security objectives to be fulfilled by the operational environment of a TOE claiming conformance to this PP. These objectives are outlined in the PP [6], chapters 4 and 7.2.

The Protection Profile [6] requires a Security Target based on this PP or another PP claiming this PP to fulfil the CC requirements for strict conformance.

2 Security Functional Requirements

Based on the security objectives to be fulfilled by a TOE claiming conformance to this PP the security policy is expressed by the set of security functional requirements (SFR) to be implemented by a TOE. It covers the following issues:

- FCS: Cryptographic Support
- FDP: User data protection
- FIA: Identification and Authentication
- FMT: Security Management
- FPT: Protection of the TSF
- FTA: TOE Access
- FTP: Trusted path/channels

The SFRs describe the following tasks of the eHCT:

- Cryptographic key generation and destruction
- Cryptographic operations for signatures. connector and proximity card communication and remote management
- Security attributes and access control for terminal functions and management
- Security attributes and information flow control for card holder CAN and PIN
- Residual information protection
- User attributes and authentication mechanisms with timing and failure handling
- Security roles and secure security attribute initialization and management
- Self-testing
- Trusted paths for connector communication and remote management

These TOE security functional requirements are outlined in the PP [6], chapters 6.1 and 7.3.1. They are all selected from Common Criteria Part 2. Thus the SFR claim is called:

Common Criteria Part 2 conformant

3 Assurance Requirements

The TOE security assurance package claimed in the Protection Profile is based entirely on the assurance components defined in part 3 of the Common Criteria. Thus, this assurance package is called:

Common Criteria Part 3 conformant
EAL 3 augmented by
ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, and AVA_VAN.4

(for the definition and scope of assurance packages according to CC see [1], part 3 for details).

4 Results of the PP-Evaluation

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 Application Notes and Interpretations of the Scheme (AIS) [4] as relevant for the TOE.

As a result of the evaluation the verdict PASS is confirmed for the assurance components of the class APE (Protection Profile evaluation).

The following assurance components were used:

APE_INT.1 PP introduction
APE_CCL.1 Conformance claims
APE_SPD.1 Security problem definition
APE_OBJ.2 Security objectives
APE_ECD.1 Extended components definition
APE_REQ.2 Derived security requirements

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-CC-PP-0032-V2-2015, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the added optional support for contactless access to proximity cards, the update to CC v3.1 R5 and changes to the gematik specification.

The results of the evaluation are only applicable to the Protection Profile as defined in chapter 1.

5 Obligations and notes for the usage

The following aspects need to be fulfilled when using the Protection Profile:

- The Protection Profile contains application notes, the author of a product specific security target needs to consider.

6 Protection Profile Document

The Protection Profile Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), Version 3.8 [6] is being provided within a separate document as Annex A of this report.

7 Definitions

7.1 Acronyms

AES AES Advanced Encryption Standard

AIS Application Notes and Interpretations of the Scheme

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

CA Certification Authority

CAN Card Access Number

CCRA Common Criteria Recognition Arrangement

CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
DF.KT	Dedicated File Kartenterminal
EAL	Evaluation Assurance Level
eHC	Electronic Health Card
eHCT	Electronic Health Card Terminal
ETR	Evaluation Technical Report
gSMC-KT	Gerätespezifisches Security Module Card Type Kartenterminal
HPC	Health Professional Card
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
KSR	Configuration and Software Repository- Service of the telematic
LAN	Local Area Network
PIN	Personal Identification Number
PP	Protection Profile
SAC	Signature Application Component
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SICCT	Secure Interoperable ChipCard Terminal
SMC-B	Security Module Card Typ B
SM-KT	Security Module Kartenterminal
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	Trust-Service Provider that issues connector certificates
VAM	Value-added module

7.2 Glossary

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

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

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.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

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 - A set of software, firmware and/or hardware possibly accompanied by guidance.

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.

8 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, Revision 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[6].

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website

[6] Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), BSI-CC-PP-0032-V3-2023, Version 3.8, 15.12.2022, Federal Office for Information Security

[7] Evaluation Technical Report, Version 1.5, 21.12.2022, Evaluation Technical Report BSI-CC-PP-0032, Deutsche Telekom Security GmbH (confidential document)

[8] Common Criteria Protection Profile Card Operating System Generation 2, BSI-CC-PP-0082, Federal Office for Information Security

[9] Common Criteria Protection Profile Schutzprofil 2: Anforderungen an den Konnektor, BSI-CC-PP-0098, Federal Office for Information Security

[6] specially

- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile für Evaluationen nach CC
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR für Evaluationen nach CC
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

8.1 Cryptography

[10] BSI TR-03116-1, Technische Richtlinie TR-03116-1, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1: Telematikinfrastruktur, in its current version[7]

[11] BSI TR-03120, Technische Richtlinie „Sichere Kartenterminalidentität (incl. Kartenterminalschutz)“, Version 1.1

[12] BSI TR-03120 Appendix, „Anhang: Kartenterminalschutz“ zur Technischen Richtlinie BSI TR-03120, Version 1.1

[13] BSI TR-03110-2, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2: Protocols for electronic Identification, Authentication and trust Services (eIDAS), Version 2.21, 21.12.2016

[14] Federal Information Processing Standards Publication 180-2 SECURE HASH STANDARD U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1

8.2 Specifications

[15] gematik: Spezifikation eHealth-Kartenterminal, Version 3.15.0, Stand 16.05.2022

[16] TeleTrusT SICCT-Spezifikation as referenced by [15]

[17] gematik: Spezifikation der gSMC-KT – Objektsystem, Version 3.9.0, Stand 24.08.2016 (for card generation G2) and
gematik: Spezifikation der gSMC-KT – Objektsystem, Version 4.3.0, Stand 12.05.2022 (for card generation G2.1)

[18] gematik: Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, in its current version[8]

[7]The ST author will have to specify the actual version that was used for the TOE. The currently valid version can be found on the website of the BSI via “Themen” > “Technische Richtlininen” (current direct link: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116.html).

[8]The ST author will have to specify the actual version that was used for the TOE. The currently valid version can be found as “gemSpec_Krypt” on the gematik “fachportal” document search site (https://fachportal.gematik.de/dokumentensuche) by searching for [Typ = “Produkttyp”], [Produkttyp = “eHealth-Kartenterminal”], [Produkttypversion = highest available number].

C Annexes

List of annexes of this certification report

Annex A: Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), Version 3.8 [6] provided within a separate document.

Note: End of report