Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0623-V3-2024

for

ZEMO VML-GK2 HW V2.0.0 / FW V3.2.0

from

ZEMO 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-0623-V3-2024 (*)

eHealth: Smart Card Readers

ZEMO VML-GK2
HW V2.0.0 / FW V3.2.0

from ZEMO GmbH

SOGIS
Recognition Agreement
for components up to
EAL 4

PP Conformance:	Common Criteria Protection Profile Mobile Card Terminal for the German Healthcare System (MobCT), Version 1.4, BSI-CC-PP-0052-2015, 24 September 2014
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 3 augmented by ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, AVA_VAN.5
valid until:	7 May 2029

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, 8 May 2024
For the Federal Office for Information Security

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

Matthias Intemann L.S.
Head of Section

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

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

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

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

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

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

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

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

2. Specifications of the Certification Procedure

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

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

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

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

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

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

3. Recognition Agreements

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

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

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

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

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

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

This certificate is recognized according to the rules of SOGIS-MRA, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained the component AVA_VAN.5 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 of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

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

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

4. Performance of Evaluation and Certification

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

The product ZEMO VML-GK2, HW V2.0.0 / FW V3.2.0 has undergone the certification procedure at BSI.

The evaluation of the product ZEMO VML-GK2, HW V2.0.0 / FW V3.2.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 2 April 2024. 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: ZEMO GmbH.

The product was developed by: ZEMO GmbH.

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

5. Validity of the Certification Result

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

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

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

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

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 8 May 2024 is valid until 7 May 2029. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

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

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

6. Publication

The product ZEMO VML-GK2, HW V2.0.0 / FW V3.2.0 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] ZEMO GmbH
Franz-Mader-Straße 9
94036 Passau

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 Mobile Card Terminal “Card Reader ZEMO VML-GK2” Hardware-Version 2.0.0 / Firmware Version 3.2.0 with integrated smart card readers. The TOE fulfils the requirements to be used with the German electronic Health Card (eHC) and the German Professional Card (HPC) based on the regulations of the German healthcare system.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Common Criteria Protection Profile Mobile Card Terminal for the German Healthcare System (MobCT), Version 1.4, BSI-CC-PP-0052-2015, 24 September 2014 [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.5.

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

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

TOE Security Functionality	Addressed issue
SF_1.SPE_MEM	On reset to factory defaults the TOE will deallocate all information in the memory (except the installed firmware) and erase encrypted health insurance in the persistent storage, as well as temporary user data.
SF_2.FWDL	The TOE can be securely updated with new firmware. The secure update guarantees that only authentic firmware, electronically signed by the manufacturer, will be accepted by the TOE and installed into the TOE.
SF_3.SEC_PIN_ENTRY	When a PIN has to be entered, the TOE changes into a secure PIN-entry mode. This mode can only be activated by the TOE and is indicated to the user. For every entered PIN digit, the TOE will display an asterisk symbol. PINs and PIN digits will never be displayed in clear text and no subject can read out the administrator PIN.
SF_4.PIN_AUTH	The TOE maintains the roles of the administrator, medical supplier and associates users with roles.
SF_5.TOE_LOCK	The TOE terminates an interactive session after 15 minutes of administrator inactivity, after [1 – 60 minutes] of medical supplier inactivity and after power loss.
SF_6.SELFTEST	The TOE performs self-tests at initial start-up and following start-ups. Self-tests check the TOE’s functionality by checking TOE hardware and evaluating the integrity of the stored firmware and the integrity of TSF data.
SF_7.Storage_Encryption	The TOE encrypts health insurance data stored in the persistent storage of the TOE with the cryptographic algorithm AES GCM and cryptographic key size of 256 bit.
SF_8.Card_Communication	The TOE enables a communication the smart cards that are

TOE Security Functionality	Addressed issue
	inserted in the TOE. When an authorised card is put into one of the TOE's slots, the TOE will read out the card's X.509 certificate and check it. The Card holder PINs entered via the PIN pad is only sent to the card slot where the authorised card is plugged in.
SF_9.DMS_Communication	The TOE enables the medical supplier to transfer data records from the persistent storage to the DMS.
SF_10.Reliable_Time_Stamps	The TOE provides reliable time stamps with a clock precision of at least ±100ppm.
SF_11.Detection_of_Physical_Attack	The TOE provides the capability to determine during operation of the TOE whether physical tampering with the TOE has occurred.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.1.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 1.4.7. 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 3.1 – 3.3.

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:

ZEMO VML-GK2, HW V2.0.0 / FW V3.2.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW & SW	Card Reader ZEMO VMLGK2 SHA-256-Hash: d4958b5c881199e7952e41810d004d01119a6310ef35d0576bc032473aebe512	HW V2.0.0 / FW V3.2.0	TOE delivered by the secure delivery chain. Firmware Image initially included in the TOE.

No	Type	Identifier	Release	Form of Delivery
2	SW	Card Reader ZEMO VMLGK2 Firmware SHA-256-Hash: d4958b5c881199e7952e41810d004d01119a6310ef35d0576bc032473aebe512	FW V3.2.0	Provided by the developer on its homepage: https://zemo.de/vmlgk-downloads/
3	DOC	Bedienungsanleitung ZEMO-VML-GK2 FW 3.2.0 SHA-256-Hash: 43e9a261755b828c55fc90b7858a8fc246cde9a5ade1de4f9390d09bb9d7173e	V2.2.0, 2023-11-24	Provided by the developer on its homepage: https://zemo.de/vmlgk-downloads/
4	DOC	Kurzanleitung ZEMO VMLGK2 FW 3.2.0 SHA-256-Hash: 44ac3d9bd4af1c91533177b8b55029ab307ba9549ac5b9c1948ffbf195434815	V1.1.0, 2023-11-24	Provided by the developer on its homepage: https://zemo.de/vmlgk-downloads/
5	DOC	Beschreibung sicherer Lieferweg für das Produkt ZEMO VML-GK2 FW: V3.2.0 SHA-256-Hash: ac1abab097a44de5f602f0c409e564b375d8bee1900d01d260736e49166416fc	V3.00 2023-11-24	Provided by the developer on its homepage: https://zemo.de/vmlgk-downloads/

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. The related documentation can be found in [9], see 5. in Table 2 above.

The box with the TOE is sealed with security seals and packed into a security bag. Security seals and security bags are printed with numbers. Furthermore, each TOE contains a transport code and a verification code.

The applicant will send the recipient an e-mail with the following information to the TOE: serial number of the TOE, tracing information, IDs of security seals, ID of security bag, transport code and verification code. The e-mail is signed with an electronic signature and will be sent till 8 a.m. The TOE will be delivered till 12 a.m.

The recipient has to check the serial number of the TOE and the IDs of the security seals and security bag. Then the recipient has to follow the authentication protocol by entering the transport code and checking the verification code that is displayed at the screen. Only if all IDs and codes are correct and the TOE is delivered in time, it is allowed to use the TOE.

The hardware version is labelled at the bottom of the TOE. Furthermore, the hardware andthe firmware version are displayed at the display of the TOE.

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,
- TOE access,
- protection of the TSF.

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

4. Assumptions and Clarification of Scope

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

OE.MEDIC: The medical supplier shall be non-hostile, always act with care, and read the existing guidance documentation of the TOE.

OE.ADMIN: The administrator shall be non-hostile, always act with care, knows the existing guidance documentation of the TOE and adhere to the rules of the TOEs environment.

OE.Developer: The developer is assumed to be non-hostile, always act with care and knows the existing guidance documentation of the TOE.

OE.CARDS: The authorised cards and the eHC are smart cards that comply with the specification of the gematik.

OE.DMS: The TOE shall only be connected to a Data Management System for a practice or hospital that is trusted by the medical supplier.

OE.PHYSICAL: The secure TOE environment shall protect the TOE against physical manipulation.

OE.ENVIRONMENT: While the TOE is in use by either the medical supplier or the administrator, they shall always keep the TOE under their control. This applies to its authenticated, as well as its unauthenticated state. While the TOE (including the VML Security Card) is not in use, it is kept in a secure area.

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

5. Architectural Information

The TOE „ZEMO VML-GK2“ is a mobile smart card terminal.

The firmware is built modular with the following subsystems:

- The subsystem Komm implements the activities at the USB- and RS232-interface.

- The subsystem Card is relevant for the interaction to the smart cards.
- The subsystem Bediener realizes the user interface.
- The subsystem Control controls the logic of the TOE.

At firmware update the whole firmware is updated.

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

There is only one evaluated configuration of the TOE, see chapter 8 below.

7.1. Developer's Test according to ATE_FUN

TOE configuration tested:

The tests have been performed in part with the unmodified version of the TOE and in part with modified TOE versions that target internal behaviour.

TOE test environment configurations:

The test setup comprises a notebook with two virtual.card kits and real smart cards (eHC, HPC, SMC-B). The virtal.card kits are used to simulate special situations, for example, a smart card with wrong/invalid certificates.

Developer’s testing approach:

- Test concept is based on covering all TSFIs.
- Positive and negative tests are applied.
- Tests considering the different roles that can access the TOE.
- Tests cover all TSF subsystems in the TOE design.
- Developer provides mappings to the tested TSFI(s) and subsystem(s), which in turn map to the SFR(s).
- The test descriptions comprise (inter alia):
  - Preconditions: preparative steps,
  - test steps: core test steps, and
  - test results: expected and actual test results.

Verdict for the activity:

The developer’s testing efforts have been proven sufficient to demonstrate that the TSFIs and subsystems perform as expected.

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 configurations and test environment as the developer during functional testing.

- TSFI selection criteria:

  The evaluation body chose to cover the existing interfaces without any 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 a subset of tests covering all TSFIs. The subset includes all test scenarios used by the developer.

- Independent testing:

  The evaluator conducted independent testing consisting of penetration testing, implementation analysis and guidance testing. The testing effort covers all functional areas of concern.

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 configuration defined in the ST was tested. Furthermore, different TOE variants were used during penetration testing to verify different mechanisms.

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

- Penetration testing approach:

  The evaluation body conducted penetration testing based on Functional Areas of Concern derived from SFRs and architectural mechanisms. The areas were prioritized with regards 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 testing but could be less emphasized.

  The penetration testing activities were performed as tests and as analytical tasks. Whenever an analysis was estimated to yield better results, the evaluator chose the analytical approach.

- TOE test configurations:

  The TOE was delivered by the developer in different configurations: This includes a final operational and a special AVA variant. The AVA configuration provides debugging outputs, which allow the evaluator to have a look at internal states of the system.

- Attack scenarios having been tested:

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

  - Handling of HPC / eHC smart cards,
  - update,
  - authentication,
  - secure encryption / decryption,
  - leakage, and
  - USB connection.

- Tested security functionality:

  The evaluator ensured that all areas listed above are tested. The penetration testing was then conducted based on priorities as described above. Therefore, a complete coverage of security functional testing based on Functional 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 High was actually successful in the TOE's operational environment.

7.3. Summary of Test Results and Effectiveness Analysis

The evaluation body has not determined any derivations between the expected and the actual test results in the context of ATE_IND and AVA_VAN. The penetration testing performed has demonstrated that the TOE is resistant to attackers with a High attack potential.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

- Hardware-Version 2.0.0
- Firmware-Version 3.2.0

There is only one evaluated configuration 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.5 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Common Criteria Protection Profile Mobile Card Terminal for the German Healthcare System (MobCT), Version 1.4, BSI-CC-PP-0052-2015, 24 September 2014 [8]
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- 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.5

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

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

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Related SFR
Encryption / decryption of health insurance data	AES-256 in GCM mode	[gemSpec_Krypt, 3.5.1 / 3.6]	256	[FIPS197] [NIST800-38D].	FCS_COP. 1/AES
Cryptographic operation for signature verification of firmware updates	RSA-3072 and SHA-512	[gemSpec_Krypt, 3.7] [RFC6234]	3072	[FIPS180-4]	FCS_COP. 1/FW

Table 3: TOE cryptographic functionality

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

According to the application standards in the table above, especially the standards issued by gematik, the algorithms are suitable for for the intended purposes listed. 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.

The assumptions defined in ST [6] needs to be fulfilled. Especially OE.MEDIC, OE.PHYSICAL and OE.ENVIRONMENT are needed regarding the physical security of the TOE.

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

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
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
gematik	Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH
HBA	Heilberufsausweis
HPC	Health Professional Card
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

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

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

[6] Security Target BSI-DSZ-CC-0623-V3-2024, Version 3.02, 2024-01-29, Security Target for a Common Criteria EAL3+ Evaluation of the Product ZEMO VML-GK2 from ZEMO GmbH

[7] Evaluation Technical Report, Version 3, 2024-03-25, EVALUATION TECHNICAL REPORT SUMMARY, TÜV Informationstechnik GmbH, (confidential document)

[8] Common Criteria Protection Profile Mobile Card Terminal for the German Healthcare System (MobCT), Version 1.4, BSI-CC-PP-0052-2015, 24 September 2014

[9] Beschreibung sicherer Lieferweg für das Produkt ZEMO VML-GK2 FW: V3.2.0 der ZEMO GmbH, Version 3.00, 2023-11-24

[10] Configuration list for the TOE, Stückliste VML-GK2, HW2.0.0, Version 3.2.0; SVN Liste aller CC relevanten Dokumente, Version 1170, 2024-03-21; SVN Liste aller entwicklungsrelevanten Dokumente, Version 809, 2024-03-22, (confidential documents)

[11] Guidance documentation for the TOE, Version 2.2.0, 2023-11-24, Bedienungsanleitung ZEMO-VML-GK2 (Versichertenkarten-Mobil-Leser), ZEMO GmbH

[7] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 38, Version 2, Reuse of evaluation results

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