Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0623-V2-2018

for

ZEMO VML-GK2,
FW-Version 3.1.0, HW-Version 2.0.0

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-V2-2018 (*)

eHealth: Smart Card Readers

ZEMO VML-GK2
FW-Version 3.1.0, HW-Version 2.0.0

from	ZEMO GmbH
PP Conformance:	Common Criteria Protection Profile Mobile Card Terminal for the German Healthcare System (MobCT), Version 1.4, BSI-CC-PP-0052-2015, 19 January 2015
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, and AVA_VAN.5

SOGIS
Recognition Agreement
for components up to
EAL 4

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 4

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

Bonn, 28 June 2018

For the Federal Office for Information Security

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

Bernd Kowalski
Head of Division

L.S.

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

This page is intentionally left blank.

A. Certification

1. Preliminary Remarks

Under the BSIG1 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]
- BSI Schedule of Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- 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] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

- 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.sogisportal.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: http://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 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 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, FW-Version 3.1.0, HW-Version 2.0.0 has undergone the certification procedure at BSI.

The evaluation of the product ZEMO VML-GK2, FW-Version 3.1.0, HW-Version 2.0.0 was conducted by datenschutz cert GmbH. The evaluation was completed on 15 June 2018. datenschutz cert GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the 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 28 June 2018 is valid until 27 June 2023. 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, FW-Version 3.1.0, HW-Version 2.0.0 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] 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 ZEMO VML-GK2, Version 2.0.0 (Hardware) / 3.1.0 (Firmware) by ZEMO GmbH. The TOE is a smart card terminal used for the German healthcare system as a Mobile Card Terminal (MobCT). It is used by medical suppliers during visits to read out insurance data from a German electronic Health Card (eHC) of a health insured person.

The Security Target [6] and its addendum [13] are the basis for this certification. It is based on the certified Common Criteria Protection Profile Mobile Card Terminal for the German Healthcare System (MobCT), Version 1.4, BSI-CC-PP-0052-2015, 19 January 2015 [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, and 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 memory (except for the installed firmware) and erase encrypted health insurance data 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 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 between the smart cards that are inserted in the TOE. When an authorised card is put into one

TOE Security Functionality	Addressed issue
	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 ±100 ppm.
SF_11.Detection_ of_Physical_Attack	The TOE provides the capability to determine during operation of the TOE whether physical tampering of 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.

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, FW-Version 3.1.0, HW-Version 2.0.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Mobile smart card terminal VML-GK2	2.0.0	Sealed Box
2	SW	Firmware	3.1.0	Installed on card terminal
3	SW	Update file VML-GK2_V3.1.0_G5.GK2 Hash value (SHA-256): c2 16 85 af 4f ad ae 18 a0 14 1d fd 4b bb ac fe ac 8c 8b f0 7c 04 8e 76 01 d4 16 9c 40 7f aa 3a	3.1.0	E-Mail from ZEMO GmbH
4	SW	Update file VML-GK2_V3.1.0_G5_Upd.GK2 Hash value (SHA-256): 61 c2 d7 67 f4 6e 3e ca f2 f8 3b c7 43 61 21 ea a2 8d d0 5f 59 b3 35 00 95 2e f8 24 32 92 20 48	3.1.0	E-Mail from ZEMO GmbH

No	Type	Identifier	Release	Form of Delivery
5	DOC	Guidance [10] Hash value (SHA-256): 0a a0 79 91 71 6e 6e 47 ea fe e5 be f3 e2 e9 fb 72 de b7 83 59 67 4a 7c a8 9a 91 05 54 30 9f ef	1.1.4	Download from website https://zemo.de/vmlgk-downloads/
6	DOC	Description of Delivery Procedure [11] Hash value (SHA-256): de 05 9f f0 bc 72 c8 44 4d fd ea e8 3f c0 cf f1 a8 71 49 5f f9 b1 50 0e f3 8a 9c 52 2e 5c 96 66	1.3	Download from website https://zemo.de/vmlgk-downloads/

Table 2: Deliverables of the TOE

The delivery procedure is documented in [11] and is available at the ZEMO website https://zemo.de/vmlgk-downloads/ together with the guidance documentation. The delivery procedure contains the following key items:

- The box with the TOE is sealed with security seals and packed into a security bag. Security seals and security bags are printed with individual IDs. Furthermore, each TOE contains a transport PIN and a verification code.
- The TOE will be delivered overnight till 12 noon of the next day.
- ZEMO GmbH will send the recipient an e-mail with the date of delivery and the following information about the TOE: serial number of the TOE, tracing information, IDs of security seals, ID of security bag, transport PIN and verification code. The e-mail is signed with an electronic signature and will be sent at 8 a.m. on the day of delivery.
- 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 PIN and checking the verification code that is displayed on screen. Only if all IDs and codes are correct and the TOE is delivered in time, the recipient is allowed to use the TOE.

The TOE is labelled with its hardware version at the bottom of the case. Furthermore, the hardware and the firmware version are displayed on the display of the TOE. Both the delivery documentation as well as the guidance documentation are secured by an electronic signature.

3. Security Policy

The Security Policy of the TOE is defined by the Security Functional Requirements and the security functions that are implemented.

This includes the following items: The health insurance data is stored inside the TOE only temporary and encrypted. To read out and to display the health insurance data a role concept is implemented. Functions for the administrator require authentication and are separated from functions for the medical supplier. For details see [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, read 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 always keep the TOE under their control. This applies to its authenticated as well as its unauthenticated state. While the TOE 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 between 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

The TOE was tested in the following configuration: firmware version 3.1.0 and hardware version 2.0.0. This is conform to the ST [6].

7.1. Developer Tests

The developer performed about 80 tests in the context of the evaluation both manually and with tool support. The test documentation describes the tests that are systematically defined based on the subsystems and TSFI of the TOE. Furthermore, the developer performed gematik tests.

All results of the developer tests correspond with the expected results. Overall, the developer tests show that the TOE behaves as specified in the ST [6], in the functional specification, and in the TOE design.

7.2. Evaluator Tests

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

Independent tests were performed by the evaluator. The security functions were tested by triggering the external interfaces of the TOE. In addition, internal states of the TOE were tested, too. The following security functions were tested: SF_2.FWDL, SF_3.SEC_PIN_ENTRY, SF_4.PIN_AUTH, SF_5.TOE_LOCK, SF_11.Detection_of_Physical_Attack. In total, 44 independent tests were performed. All interfaces were tested by the evaluator. As a result the tests showed that the TOE is operating correctly as specified in the ST [6], the functional specification, and the TOE design.

Based on the vulnerability analysis the evaluator performed the following penetration tests: manipulation of the seals, misuse of the display and keypad, attacks at the USB and smart card interfaces. As a result the tests showed that there are no vulnerabilities that could be exploited in the intended environment.

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

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

- Hardware Version: 2.0.0
- Firmware Version: 3.1.0

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, and 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, 19 January 2015 [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, and 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 strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context) only.

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
Authentication and Integrity	RSASSA-PKCS1-v1_5 signature verification using SHA-256 hash function	PKCS#1 (RSA), FIPS 180-4 (SHA)	2048	Yes

Table 3: TOE cryptographic functionality

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
Confidentiality and Integrity	AES in GCM-mode	FIPS-197 (AES), NIST SP 800-38D (AES-GCM)	256	gemSpec_Krypt [12]

Table 4: TOE cryptographic functionality

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

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in Table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

11. Security Target

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

12. Definitions

12.1. Acronyms

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
C2C	Card-to-Card-Authentication
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
CT	Card Terminal
DMS	Data Management System
EAL	Evaluation Assurance Level
eHC	Electronic Health Card

eHCT	Electronic Health Card Terminal
ETR	Evaluation Technical Report
gematik	Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH
HPC	Health Professional Card
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MobCT	Mobile Health Card Terminal
PP	Protection Profile
ppm	Parts per Million
RTC	Real Time Clock
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SMC	Secure Module Card
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

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012, http://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-V2-2018, Version 2.15, 04.06.2018, Security Target for a Common Criteria EAL3+ Evaluation of the Product ZEMO VML-GK2, ZEMO GmbH

[7] Evaluation Technical Report, Version 1.0 10.06.2018, Evaluation Technical Report – Summary, datenschutz cert 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, 19 January 2015

[9] Configuration list for the TOE, 18.04.2018, Konfigurationsliste (confidential document)

[10] Guidance documentation for the TOE, Version 1.1.4, 18.04.2018, Bedienungsanleitung ZEMO-VML-GK2 V3.1.0

[11] Delivery procedure "Beschreibung sicherer Lieferweg für das Produkt ZEMO VML-GK2 der ZEMO GmbH", Version 1.3, 04.06.2018

[12] Gematik crypto specification "Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur", gemSpec_Krypt, Version 2.3.0, 17.06.2014, gematik

[13] Addendum to the Security Target for a Common Criteria EAL3+ Evaluation of the Product ZEMO VML-GK2 from ZEMO GmbH", Version 2.00, 02.04.2015

[7] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)

Referenzierte Standards:

[FIPS 180-4] FIPS PUB 180-4 Secure Hash Signature Standard (SHS), NIST, 2012-03

[FIPS 197] Federal Information Processing Standards Publication 197: ADVANCED ENCRYPTION STANDARD (AES), NIST, November 2001

[PKCS#1] PKCS #1 v2.2: RSA Cryptography Standard, October 2012

[NIST SP 800-38D] Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007

This page is intentionally left blank.

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 10.4
- 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 11
- On the detailled definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 12 to 16
- 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 http://www.commoncriteriaportal.org/cc/

This page is intentionally left blank.

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report