Federal Office
for Information Security

# Certification Report

# BSI-DSZ-CC-0596-V3-2023

for

# Mobiles eHealth Kartenterminal ORGA 930 M online 4.9.0: 1.0.0

from

# Worldline Healthcare 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-0596-V3-2023** (*)

eHealth: Smart Card Readers

**Mobiles eHealth Kartenterminal ORGA 930 M online**
4.9.0: 1.0.0

| | |
|---|---|
| from | Worldline Healthcare GmbH |
| 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<br>Common Criteria Part 2 extended |
| Assurance: | Common Criteria Part 3 conformant<br>EAL 3 augmented by AVA_VAN.5, ALC_TAT.1, ADV_TDS.3, ADV_IMP.1, ADV_FSP.4 |

SOGIS
Recognition Agreement
for components up to
EAL 4

Common Criteria

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

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 18 January 2023

For the Federal Office for Information Security

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

Sandro Amendola L.S.
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 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 Mobiles eHealth Kartenterminal ORGA 930 M online, 4.9.0: 1.0.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0596-V2-2018. Specific results from the evaluation process BSI-DSZ-CC-0596-V2-2018 were re-used.

The evaluation of the product Mobiles eHealth Kartenterminal ORGA 930 M online, 4.9.0: 1.0.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 11 January 2023. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the applicant is: Worldline Healthcare GmbH.

The product was developed by: Worldline Healthcare 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 18 January 2023 is valid until 17 January 2028. 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 Mobiles eHealth Kartenterminal ORGA 930 M online, 4.9.0: 1.0.0 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] Worldline Healthcare GmbH
Konrad-Zuse-Ring 1
24220 Flintbek
Deutschland

# 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 “ORGA 900” with integrated smart card readers. The TOE fulfills the requirements to be used with the German electronic Health Card (eHC) and the German Profession 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 AVA_VAN.5, ALC_TAT.1, ADV_TDS.3, ADV_IMP.1, ADV_FSP.4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6. 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 | Secure Identification & Authentication<br>The TOE provides several authentication mechanisms for the roles administrator, medical supplier and developer and associates users with roles. Each user has to be successfully identified and authenticated before being allowed to perform any TSF-mediated action. |
| SF_2 | Secure Residual<br>The TOE terminates an authenticated session and thereby delete all unencrypted sensitive information from the memory: On dropping of the authenticated state, power loss and deallocation of the resource from temporary data in the persistent storage of the TOE and in the volatile memory of the TOE. |
| SF_3 | Secure Self-Tests<br>The TOE performs self-tests at initial start-up and are able to be started manually via management. The selftests check the TOE's functionality by evaluating the integrity of the stored data. This includes the integrity of the firmware in processor flash (loader and application) and integrity of TSF SFLASH-Page with configuration data. |
| SF_4 | Secure Data Protection<br>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 bits and with a symmetric cryptographic key. The generation of the symmetric cryptographic key is initiated and performed by the authorised card of the user. |
| SF_5 | Secure Management<br>The TOE grants access to the management functions i.e. installing firmware, import of cross CVCs, management of time settings, resetting to factory defaults, management of the administrator login credentials, and printer control, to the administrator who has to authenticate himself by PIN entry or for the latter perform a successful Challenge & Response operation with the TOE. |

| TOE Security Functionality | Addressed issue |
|---|---|
| SF_6 | Secure Card Communication<br>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: whether the card claims to be an authorised card, whether the X.509 certificate of this authorised card is mathematically correct, and whether the current date is given by the TOE falls within the validity period of the certificate before permitting any other interaction with a card.<br>The Card holder PIN entered via the PIN pad is only sent to the card slot where the authorised card is plugged in. No PIN is sent to the card slot where the eHC is plugged in. |
| SF_7 | Secure DMS Communication<br>The TOE enables the medical supplier to transfer data records from the persistent storage to the DMS only. The transmission takes place via error detection code (EDC).<br>After the data record has been transferred to the DMS successfully it is been deleted from the devices. |
| SF_8 | Secure Firmware-Update<br>On firmware update 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 on the TOE. For signature verification purposes the TOE firmware contains the public cryptographic key and the TOE performs a signature verification for firmware updates with cryptographic algorithms SHA and RSA and cryptographic key sizes of: SHA-512 and RSA-4096. |

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.

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 3.3.

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:

**Mobiles eHealth Kartenterminal ORGA 930 M online,** 4.9.0: 1.0.0

The following table outlines the TOE deliverables:

| No | Type | Identifier | Release | Form of Delivery |
|---|---|---|---|---|
| 1 a) | HW+FW | ORGA 930 M online<br>HW and Firmware Image “orga_930_130_PU_PK_sig.dfu”<br>(SHA-256: 8d62b2d83c8a16085b1888b6bbbc40270e7110790c69092618d615fccd24c35f) | 4.9.0:1.0.0 | TOE delivered by the Secure delivery chain. Firmware Image initially included in the TOE. |
| 1 b) | FW | ORGA 930 M<br>Firmware Image Package “ORGA_930_M_online_FW_4.9. 0.ppu”<br>(SHA-256: 25019f3c55bd632bf5b44e8bdd2e83664a4809ae67745eac6cc62b1f52dc1fe5) | 4.9.0:1.0.0 | Provided by the developer on its homepage. |
| 2 | DOC | Bedienungsanleitung Mobiles eHealth Kartenterminal ORGA 930 M online mit Firmware- Version 4.9.0<br>(SHA-256: a5709a5d4f979b88fdb7a84f071147b0919e2d168fd3acca599af61fad04c75b) | 22.9.1 | Provided by the developer on its homepage. |
| 3 | DOC | Kurzanleitung Mobiles eHealth Kartenterminal ORGA 930 M online mit Firmware-Version 4.9.0<br>(SHA-256: 1792aae9950454d88630151b297235a7ebf14e861f7662c617678422e761a309) | 22.9.2 | Provided by the developer on its homepage. |
| 4 | DOC | Endnutzer-Ckeckliste „Sichere Lieferkette“<br>(SHA-256: 65ffff99a99b641502d859fc4ea980aa1158250ea08ff1020fd655abffbecf53) | 22.9.1 | Provided by the developer on itshomepage. |
| 5 | DOC | Prüfung der Versandverpackung durch den Empfänger<br>(SHA-256: a41f6c4aed6468cc6f246ae9a96ae85103262f864e72289a5cc76706d2c6bc8e) | 22.10.3 | Provided by the developer on its homepage. |

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 first option is, to do a secure delivery of the TOE from the developer Worldline to the company CGM (CompuGroup Medical Deutschland AG), T-Systems or a participant of the Konnektor delivery chain. From this point, the secure delivery chain is identical to the certified secure delivery chain with the Cert.-ID.: BSI-DSZ-CC-0950-V2-2018 (CGM) or BSI-DSZ-CC-0928 (T-Systems).

The direct transport to the end user is the second allowed transport of the secure delivery chain. The service technician or the end user installs the product Mobile Card Terminal ORGA 900 within the premises of the end user. The guidance defines all steps the end user has to perform to check, if the secure delivery chain was correctly used and to check that the TOE is not manipulated or replaced and therefore the integrity and authenticity of the TOE is guaranteed.

The TOE can be identified within the management menu \Service\Status\. There, the product version 4.9.0:1.0.0 is displayed.

# 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

# 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.

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

# 5. Architectural Information

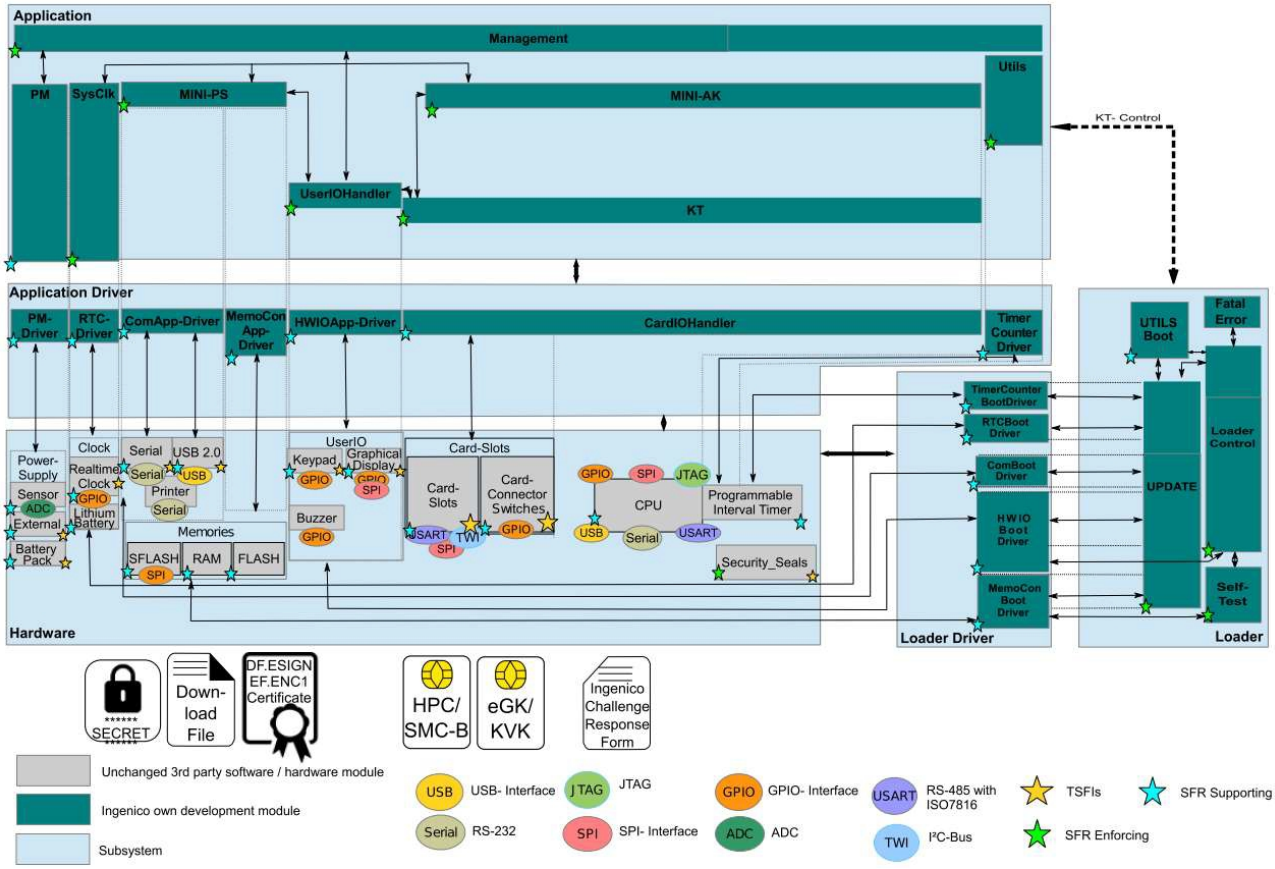


**Figure 1: TOE Architecture**

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

The TSF is broken down into the following 5 subsystems:

- Loader: This subsystem contains the bootloader of the TOE, which executes the start-up process.
- Application: This subsystem involves the applications of the device.
- Loader Driver: This subsystem includes the drivers of the hardware from the TOE for the interaction with subsystem “Loader”.
- Application Driver: This subsystem includes the drivers of the hardware from the TOE for the interaction with subsystem “Application”.
- Hardware: The hardware contains all electronic and mechanical components of the main processor and the connected peripherals.

# 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 (with 2 variants) of the TOE.

## 7.1. Developer's Testing

TOE test configurations

The Security Target [6] has identified two configurations of the TOE, which are identical except their configuration ID. Therefore, only one configuration need to be tested.

The test setup comprises a laptop with the test suite Qumate, a TOE and two virtual.card kits and real smart cards (eGK, HBA, SMC-B). The virtal.card kits are used to simulate special situation, for example, a smart card with wrong/invalid certificate.

Testing approach

- Coverage and depth tests are done together.
- Tests considering the different roles that can access the TOE.
- Tests covering all TSF subsystems in the TOE design.
- Developer provides mappings to the tested TSFI(s), SFR(s), subsystem(s), SFR-enforcing modules and use cases.
- Different testing approaches are used:
  - Code analysis,
  - Test suite (automatic and manual test).
- The test descriptions comprise (inter alia):
  - Pre conditions: Preparative steps,
  - Test steps: Core test steps,
  - Post conditions: Clearance steps to tidy up before the next test.

Verdict for the activity

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

## 7.2. Independent Testing

TOE test configurations

The evaluation body used the same test configurations and test environment as the developer during functional testing.

Testing approach

The evaluation body chose to cover the existing interfaces broadly without specific restrictions. All interfaces were considered during testing.

The evaluation body chose to inspect all developer tests. They also chose to repeat all tests, except for nine tests that were not repeated due to their duration and additional hardware requirements.

The evaluator conducted independent testing covering the stationary mode and guidance testing.

Verdict for the sub-activity

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

## 7.3. Penetration Testing

Test Configurations

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.
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 the running system.

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.

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.

Attack scenarios

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

o Handling of HPC / eHC / KVK smart cards,

o Update,

o Authentication,

o Secure encryption / decryption,

o Leakage.

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 provided that all measures required by the developer are applied.

# 8. Evaluated Configuration

This certification covers the following configurations of the TOE: There is only one evaluated configuration (with 2 variants) of the TOE.

ORGA 930 M online, mobile card terminal, graphical display, 2 full size slots (eHC / KVK and HPC / SMC-B). This involves the delivery of new ORGA 930 M online devices.

- TOE Version: 4.9.0:1.0.0

The TOE version includes the following versions:

- Version Hardware: 1.0.0
- Manufacturing code: HC 00 04 00 00
- Version Loader: 7.5.1
- Version Application: 4.9.0
- Version Configuration: 1.0.0/930MONLINE

ORGA 930 M: This product is identical to ORGA 930 M online except for ALC_DEL and the configurations after updating the application and the loader to the same version of ORGA 930 M online.This is just the delivery of updates to existing ORGA 930 M eGK devices.

- TOE Version: 4.9.0:1.0.0
- Version Configuration: 1.0.0/930M

# 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 AVA_VAN.5, ALC_TAT.1, ADV_TDS.3, ADV_IMP.1, ADV_FSP.4 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0596-V2-2018, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on minor changes of the TOE as product optimizing and Updates of the Open Source components. The Secure Delivery Chain was improved, as it is now independent from the forwarder with new security measures.

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 AVA_VAN.5, ALC_TAT.1, ADV_TDS.3, ADV_IMP.1, ADV_FSP.4

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

## 9.2. Results of cryptographic assessment

The 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 |
|---|---|---|---|---|
| Cryptographic operation for signature verification of firmware updates | RSASSA-PKCS1-v1_5 with RSA-4096 and SHA-512 | [PKCS#1] [RFC6234] | 4096 | Yes |
| Challenge & Response mechanism | SHA-1 | [RFC3174] | 160 | No |
| Integrity of the TSF | SHA-512 | [RFC6234] | 512 | Yes |

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 |
|---|---|---|---|---|
| Encryption / decryption of health insurance data | AES-256 in GCM mode | [18] | 256 with a tag-length of 256 | [FIPS197] [NIST800- 38D] |

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 the intended purposes listed above. 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.

In addition, the following aspects need to be fulfilled when using the TOE: For the certified use as a mobile card terminal, the stationary mode “stationäre Betriebsart” is not allowed. As described in the installation manuals [10] and [11], the administrator is however required to temporarily change the mode to “stationäre Betriebsart” for the duration of an update of the TOE to a newer certified version.

# 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

**AES-GCM** AES in Galois Counter Mode (GCM)

**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

**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 |
| **SM-KT** | Sicherheitsmodul Kartenterminal |
| **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 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-0596-V3-2023, Version 3.33, 2022-11-02, Common Criteria Security Target for the Evaluation of the Product ORGA 900, Worldline Healthcare GmbH

[7] Evaluation Technical Report Summary, Version 2, 2023-01-06, 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] Configuration list for the TOE, Version 1.19.0, 2022-11-11, ConfigList Document References Listing of CC Documents from Evaluation of the Product ORGA v 6141 online and ORGA 930 online, Worldline Healthcare GmbH (confidential document)

[10] Bedienungsanleitung Mobiles eHealth Kartenterminal ORGA 930 M online mit Firmware-Version 4.9.0, Version 22.9.1, Worldline Healthcare GmbH

[11] Kurzanleitung Mobiles eHealth Kartenterminal ORGA 930 M online mit Firmware-Version 4.9.0, Version 22.9.2, Worldline Healthcare GmbH

[12] Endnutzer-Checkliste „Sichere Lieferkette“, Version 22.9.1, Worldline Healthcare GmbH

[13] Prüfung der Versandverpackung durch den Empfänger, Version 22.10.3, Worldline Healthcare GmbH

[14] Liste der Lieferketten, Version 0.7, Worldline Healthcare GmbH

[7] specifically

- AIS 1, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC
- AIS 19, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC
- AIS 23, Zusammentragen von Nachweisen der Entwickler
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 41, Guidelines for PPs and STs
- AIS 45, Erstellung und Pflege von Meilensteinplänen
- AIS 46, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[15] Produktbeschreibung „Versandverpackungssiegelband“, Version 0.1, Worldline Healthcare GmbH

[16] Produktbeschreibung „Versandverpackungssiegel“, Version 0.3, Worldline Healthcare GmbH

[17] Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Version 2.21.0, 2022-01-31, gematik

[18] Spezifikation Mobiles Kartenterminal, Version 2.15.0, 2022-02-24, gematik

# 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