Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0519-V2

for

ORGA 6141 online Version 3.7.2:1.2.0

from

Ingenico 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-0519-V2 (*)

eHealth: Smart Card Readers

ORGA 6141 online
Version 3.7.2:1.2.0

from	Ingenico Healthcare GmbH
PP Conformance:	Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), Version 3.7 vom 21. September 2016, BSI-CC-PP-0032-V3
Functionality:	Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 3 augmented by ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, AVA_VAN.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 and CC Supporting Documents as listed in the Certification Report 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 only

Bonn, 02 March 2018

For the Federal Office for Information Security

Joachim Weber
Head of Branch

L.S.

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

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 under SOGIS-MRA for all assurance components selected.

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.

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

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

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 ORGA 6141 online, Version 3.7.2:1.2.0 has undergone the certification procedure at BSI.

The evaluation of the product ORGA 6141 online, Version 3.7.2:1.2.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 10 November 2017. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

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

The product was developed by: Ingenico 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 02 March 2018 is valid until 01 March 2023. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

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,

[5] Information Technology Security Evaluation Facility

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 ORGA 6141 online, Version 3.7.2:1.2.0 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] Ingenico Healthcare GmbH

Konrad-Zuse-Ring 1
24220 Flintbek

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) ORGA 6141 online, version 3.7.2:1.2.0, is a eHealth card terminal with graphical display. It fulfils the requirements to be used with the German electronic Health Card (eHC) and the German Health Professional Card (HPC) based on the regulations of the German healthcare system and can to be used as a secure PIN pad entry device.

It has a card terminal with 2 ID1 Slots (HPC and eGK) und 2 SMC Slots (SM-KT (supporting SMC-B and SMC-KT cards) and SMC-A), 20 key keypad, USB and LAN interfaces for the use in the German healthcare system with KVK, HPC and eGK generation 1+ and generation 2. Connection to a connector is possible via LAN and TCP/IP-protocol.

In its core functionality the TOE is not different from any other smart card terminal which provides an interface to one or more smart cards including a mean to securely enter a PIN.

Additionally the TOE provides a network interface which allows routing the communication of a smart card to a remote IT product outside the TOE.

Altogether the TOE provides the following main functions:

• Access to one or more slots for smart cards,

• Secure network connectivity,

• Secure PIN entry functionality,

• Enforcement of the encryption of communication,

• User authentication,

• Management functionality including firmware updates,

• Passive and active physical protection.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), Version 3.7 vom 21. September 2016, BSI-CC-PP-0032-V3 [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.4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

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

TOE Security Functionality	Addressed issue
SF_1	Trusted Communication Channels: For all communication functions used by eHealth applications to the connector and remote users via the trusted channel the TOE will always establish a trusted communication channel to the connector or remote user that is logically distinct from other communication channels and provides assured identification of its end points and

TOE Security Functionality	Addressed issue
	protection of the channel data from modification or disclosure. The card terminal permits the connector and remote users to initiate com-munication via the trusted channel. The TOE only allows one connection to one connector at a time.
SF_2	Identification & Authentication: The TOE provides several authentication mechanisms for administrators and for other users: • a PIN based local authentication mechanism • a remote authentication mechanism for the SICCT-interface • an interface for authentication of the administrator by performing a Challenge & Response operation with the TOE To perform the secured management function the administrator of the TOE first must identify and authenticate himself.
SF_3	Network Connections: The TOE will accept any information arriving at the network interface from the connector only if the communication path is encrypted and the connector has been successfully authenticated. A connector authentication is not required for SICCT commands by unauthorized users as listed in the following paragraph. The TOE accepts the following SICCT commands arriving at the network interface even if no pairing process is established and no valid connector certificate is required(FDP_IFF.1.4/NET): • SICCT CT INIT CT SESSION • SICCT CT CLOSE CT SESSION • SICCT GET STATUS The TOE accepts the following SICCT commands arriving at the network interface even if no pairing process is established, no valid connector certificate is presented for administrator (FDP_IFF.1.4/NET): • SICCT CT INIT CT SESSION • SICCT CT CLOSE CT SESSION • SICCT GET STATUS • SICCT SET STATUS • SICCT CT DOWNLOAD INIT • SICCT CT DOWNLOAD DATA • SICCT CT DOWNLOAD FINISH The TOE additionally accepts the following EHEALTH commands arriving at the network interface if no pairing process is established but a valid con-nector certificate is presented: • EHEALTH TERMINAL AUTHENTICATE.
SF_4	Secure Update: The TOE enforces that a modification of the firmware of the TOE only is allowed after the integrity and authenticity of the firmware has been verified by checking the signature over the update file.
SF_5	Secure PIN-entry:

TOE Security Functionality	Addressed issue
	For PIN entry the TOE supports a secure PIN-entry mode. This mode can only be activated by the TOE and is indicated by a padlock symbol for every PIN digit that has to be entered. For every entered PIN digit the padlock symbol is replaced by an asterisk symbol. PINs and PIN digits will never be displayed. The administrator-PIN will never leave the TOE.
SF_6	Secure Data Deletion: Memory no longer used for storage of PIN, cryptographic keys and all information that is transferred by a card in a slot of the TOE or by the connector (except the shared secret), will be erased by overwriting with 0x00 and then be made available for further use. Memory areas for PINs will be overwritten with 0x00 as soon as the PIN has been sent to the chip card. When selected by an authenticated TOE administrator (excluding SICCT interface) pairing information from all three possible pairing processes (initial pairing, review of pairing- information and maintenance-pairing) will securely deleted and written with 0x00.
SF_7	Secure Management-Functions: The TOE is aware of three roles: administrator, reset administrator and user. To identify and authenticate the roles administrator and reset administrator the TOE provides PIN based identification and authentication. The secure management functions are only available to the TOE administrator after successful identification and authentication. The detailed description of the management functions has been provided within [6].
SF_8	Self-Test: The TOE can perform a self-test on power-on and after activation by an authorised user. The detailed description of the self-test is provided within [6].
SF_9	Secure Fail-State: In case of • an alarm condition indicates possible tampering or if a • self-test detects an error or • failure during firmware update the TOE will be put into a secure fail state.
SF_10	Physical Protection of the TOE: The TOE is protected against unnoticed tampering by security seals which will be visibly destroyed on attempts to tamper with the TOE body (see SM_1). The TOE has an alarm function constantly checking switches triggering an alarm on opening the TOE housing and a drill and probing protection foil for alarm conditions which are drilling and probing attacks to the bottom side, the left and right side and the rear side of the TOE causing short-cuts or interruption of the circuit paths on the foil. On alarm (indicating possible tampering) the alarm function will put the TOE in a secure but safe non-functioning state (see SF_9) and will display a message on the TOE display. The alarm condition remains even after a TOE reset.
SM_1	Sealing: The TOE is protected against unnoticed manipulations by security seals. The seals are sticky seals and carry authenticity attributes. The seals are placed over the jointing of the body parts. Seal positions, their look and how to identify broken security seals with be described in the guidance documents.

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 3.1. 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 – 3.5.

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:

ORGA 6141 online, Version 3.7.2:1.2.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	ORGA 6141 online	1.2.0	Must be according the documentation in no. 3, 4 and 5.
2	FW	Firmware Image SHA256-Hashsum: 286739490dd3f17a61b529cc783f9385b1a752122d3793b5f3714b0b0fef4669	3.7.2	As part of a new TOE and via download from the developer. The delivery must be according the documentation in no. 3, 4 and 5.
3	DOC	user guide (Bedienungsanleitung Stationäres eHealth Kartenterminal ORGA 6141 online mit Firmware-Version 3.7.2)	7.10.2	Provided by the developer on their homepage: *www.ingenico.de/healthcare*
4	DOC	brief instruction (Kurzanleitung Stationäres eHealth Kartenterminal ORGA 6141 online mit Firmware-Version 3.7.2)	7.10.2	Delivered with the delivery package of the TOE.
5	DOC	Endnutzer-Checkliste „Sichere Lieferkette“	7.10.2	Provided by the developer on their homepage: *www.ingenico.de/healthcare*

Table 2: Deliverables of the TOE

The user has to verify the SHA256-checksum of the firmware image (see no. 2 in table 2) before updating 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,
- Protection of the TSF,
- TOE Access,
- Trusted path/channels.

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.ENV: It is assumed that the TOE is used in a controlled environment.
- OE.ADMIN: The administrator of the TOE and the medical supplier shall be non-hostile, well trained and have to know the existing guidance documentation of the TOE environment.
- OE.CONNECTOR: The connector in the environment has to be trustworthy and provides the possibility to establish a Trusted Channel with the TOE including a mean for mutual authentication.
- OE.SM: The TOE will use a secure module (SM-KT) that represents the cryptographic identity of the TOE in form of an X.509 certificate.
- OE.PUSH_SERVER: The internal network of the medical supplier is equipped with a so called Push Server for automatic firmware updates.
- OE.ID000_CARDS: All smartcards of form factor ID000 shall be properly sealed after they are brought into the TOE.

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

5. Architectural Information

A high level description of the IT product and its major components can be found in the

Security Target [6], chapter 1.3.1 + 1.3.2.

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

7.1. Developer Tests according to ATE_FUN

The test setup comprises a laptop, a Connector, a TOE and three virtual card kits. Further hardware is used to create a LAN, to connect all used components.

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), 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.

7.2. Evaluator Tests

All testing activity of the evaluation body is covered by testing in the scope of ATE_IND and AVA_VAN.

7.2.1 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 broadly cover the existing interfaces without specific 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 all tests but in the end six tests were not repeated due to their complexity. No deviations were found between the expected and the actual test results.

7.2.2 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 Moderate 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 regard 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, but could be less emphasized, if developer tests were found to be sufficient.

The penetration testing activities were performed as tests and as analytical tasks. When an analysis was estimated to yield better results, the evaluators chose the analytical approach. Analytical activities were especially applied in the areas Update, Random Number Generation and Hardening Mechanisms. Combined approaches were also applied.

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

- TLS Connections
- Update
- Hardening Mechanisms
- Self-Protection
- Network Services

A complete coverage of security functional testing based on technical areas of concern is performed.

8. Evaluated Configuration

The evaluation results are only valid for the single configuration defined in the Security Target [6].

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 for those components up to EAL 5 extended by advice of the Certification Body for components beyond EAL 5.

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) plus the components ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, AVA_VAN.4 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), Version 3.7 vom 21. September 2016, BSI-CC-PP-0032-V3 [8]
- for the Functionality: Common Criteria Part 2 conformant
- 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.4

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

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 cryptographic algorithms are used by the TOE to enforce its security policy:

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
1	TLS key establishment	Diffie-Hellman as part of TLS cipher suites TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA	[RFC4346], [RFC5246]	2048	[RFC3526], DH group = 14, DH min exponent length = 384 bits, Forward secrecy = yes	FCS_CKM.1.1/Connector
2	TLS Peer Authentication	RSA-2048 as part of TLS cipher suites TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA	[RFC4346], [RFC5246]	2048	Limited support for TLS v1.1 and v1.2, according to [gemSpec_Krypt]	FCS_CKM.1.1/Connector
3	TLS payload encryption	AES-128 (TLS_DHE_RSA_WITH_AES_128_CBC_SHA), AES-256 (TLS_DHE_RSA_WITH_AES_25	[RFC4346], [RFC5246]	128, 256	Limited support for TLS v1.1 and v1.2, according to [gemSpecKrypt]	FCS_CKM.1.1/Connector

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
		6_CBC_SHA) in CBC mode				
4	TLS Message Authentication	HMAC-SHA as part of TLS cipher suites TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA	[RFC4346], [RFC5246]	512	Limited support for TLS v1.1 and v1.2, according to [gemSpec_Krypt]	FCS_CKM.1.1/Connector
5	TLS Signature Verification	SHA-256 with RSA	[PKCS#1]	2048	[FIPS180-4]	FCS_CKM.1.1/Connector
6	TSF Signature Verification	RSASSA-PKCS1-V1_5 with SHA-256	[PKCS#1]	2048	[FIPS180-4]	FCS_COP.1.1/SIG

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:

- Usage of the TOE only in a trustworthy environment as described in the security target [6] and the documentation, see table 2,

- Delivery of the TOE as described in the documentation, see table 2.
  Deliveries are only allowed to the central store VSP (CGM) according [14]. The further delivery must be according the way for connectors for transportation within Germany (“innerdeutschem Transport“) as described in „Delivery Procedures (ALC_DEL) für die KoCoBox MED+, Version: 1.1.7, 20.10.2016, Verfahren BSI-DSZ-CC-0950-V2-2017“. The technical, organisational und personnel minimum requirements for connectors in the aforementioned document must be fulfilled. Ingenico has to bind CGM by contract accordingly.

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

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
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2. Glossary

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

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

13. Bibliography

[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, Revision 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

[7] specifically

- AIS 1, Version 13, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- 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)

[6] Security Target BSI-DSZ-CC-0519-V2, Version 3.27, 2017-10-25, Ingenico Healthcare GmbH

[7] Evaluation Technical Report, Version 2, 2017-11-10, TÜVIT, (confidential document)

[8] Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), Version 3.7 vom 21. September 2016, BSI-CC-PP-0032-V3

[9] Bedienungsanleitung Stationäres eHealth Kartenterminal ORGA 6141 online mit Firmware-Version 3.7.2, Version 7.10.2, 2017-10-20, Ingenico

[10] Kurzanleitung Stationäres eHealth Kartenterminal ORGA 6141 online mit Firmware-Version 3.7.2, Version 7.10.2, 2017-10-20, Ingenico

[11] Endnutzer-Checkliste „Sichere Lieferkette“, Version 7.10.2, 2017-10-27, Ingenico

[12] HW-Konfigurationsliste: Datensatz AGILE ORGA_6141_online.pdx, 2017-10-04, Ingenico

[13] SW-Konfigurationsliste (SVN Log-Dateien): SVN_log_ORGA 6141_online.zip, Version 3.7.2, 2017-10-26, Ingenico

[14] Sichere Lieferkette für stationäre und mobile Gesundheitskartenleser im OPB1 der Ingenico Healthcare GmbH nach der Common Criteria Stufe EAL3+, Version 15, 2017-11-10, Ingenico

[15] Maßnahmenkatalog zur Lagerung von eHealth-Geräten, Version 1, 2017-10-27, Ingenico

[16] Lebenszyklusunterstützung, Version 2.11, 2017-09-18, Dr. Neuhaus GmbH

Quoted standards:

[FIPS180-4] FIPS PUB 180-4 Secure Hash Signature Standard (SHS), NIST, 2012-03

[gemSpec_Krypt] Einführung der Gesundheitskarte – Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik), Version 2.3.0, 17.06.2014

[RFC3526] More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), 2003-05

[RFC4346] T. Dierks, E.Rescorla. RFC4346: The Transport Layer Security (TLS) Protocol Version 1.1, 2006-04

[RFC5246] T. Dierks, E.Rescorla. RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2, 2008-08.

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 10.5
- 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 detailled 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 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.

Annex B: Evaluation results regarding development and production environment

Annex C: Overview and rating of cryptographic functionalities implemented in the TOE

Annex B of Certification Report BSI-DSZ-CC-0519-V2

Evaluation results regarding development and production environment

The IT product ORGA 6141 online, Version 3.7.2:1.2.0 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 2 March 2018, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.3, ALC_CMS.3, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1)

are fulfilled for the development and production sites of the TOE listed below:

a) Development:
Ingenico Healthcare GmbH, Konrad-Zuse-Ring 1, 24220 Flintbek, Germany

b) Production:
Dr. Neuhaus Telekommunikation GmbH, Messestraße 20, 18069 Rostock, Germany

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6]) are fulfilled by the procedures of these sites.

Annex C of Certification Report BSI-DSZ-CC-0519-V2

Overview and rating of cryptographic functionalities implemented in the TOE

See Chapter 9.2, table 3.

Note: End of report