Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1233-2025

for

Y7 4.3.1:1.2.9 with eHealth Application 1.1.20

from

JDM Payment Solutions SAS

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-1233-2025 (*)

eHealth: Smart Card Readers

Y7 4.3.1:1.2.9 with eHealth Application 1.1.20

from	JDM Payment Solutions SAS
PP Conformance:	Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), BSI-CC-PP-0032-V3-2023, 15.12.2022
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.4
valid until:	07 July 2030

SOGIS IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY MUTUAL RECOGNITION AGREEMENT

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, 8 July 2025

For the Federal Office for Information Security

Sandro Amendola L.S.
Director-General

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

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.4 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 Y7 4.3.1:1.2.9 with eHealth Application 1.1.20 has undergone the certification procedure at BSI.

The evaluation of the product Y7 4.3.1:1.2.9 with eHealth Application 1.1.20 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 25 April 2025. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: JDM Payment Solutions SAS.

The product was developed by: JDM Payment Solutions SAS.

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

5. Validity of the Certification Result

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

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

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

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

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 8 July 2025 is valid until 7 July 2030. 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 Y7 4.3.1:1.2.9 with eHealth Application 1.1.20 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] JDM Payment Solutions SAS
2 rue Gallien
F-93400 Saint Ouen-sur-Seine
France

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 a smart card terminal which fulfils the requirements to be used with the German electronic Health Card (eHC) and the German Health Professional Card (HPC) based on the regulations of the German healthcare system. The terminal is based on a two-chip architecture in which the security processor is used for the eHealth application.

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), BSI-CC-PP-0032-V3-2023, 15.12.2022 [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.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
Cryptographic Support	TLS 1.2 is used to authenticate the connection between TOE and all external systems (Connector, Terminal Management System (TMS), Factory Key Loading (HSM)). Cryptographic functionality complies with PKCS#1. For signature verification for the connection between the TOE and the Connector, the TOE stores a list of trusted CAs (TSP CA List). This list can be managed by the TOE administrator. Firmware, Key and Configuration updates are encrypted using AES-GCM 256. The SM-KT (Secure Module Kartenterminal) is used for the following functions: ● Key generation and protection ● Cryptographic functions based on RSA and ECSA for encryption/decryption and signature creation ● Random number generation ● A function to read out the public key Zeroisation is used to destroy keys. A logically distinct communication path is used to connect the TOE to the TMS. The connection has sole use of its TLS interface. The firmware is encrypted by AES256 GCM.
User Data Protection (FDP)	Administrative access to the TOE is controlled by roles for Direct Access. Roles are Administrator, Reset Administrator & User. Access is password controlled with a numeric pass-word that must be a minimum of 8 characters in length and may be up to 12 characters. Using the Direct Management module, the administrator can perform the initial pairing process with the connector. Access to firmware, cryptographic key and CA list management is controlled

TOE Security Functionality	Addressed issue
	through the Direct Management module. The Administrator Role is required. The TOE checks the authenticity and integrity of all updates. If a firmware, key or CA list update fails then the update is discarded and the previous state restored. There is no read access to PIN, shared secret, management credentials or secret cryptographic keys via any of the Management Roles including password and keys. There is no unauthorized reset to factory defaults implemented by the TOE. On first start-up and after reset to factory settings the TOE forces the administrator to specify a password for direct management. The TOE also ensures that the TOE administrator's credentials for local management are set before access to other TOE functionality is possible. The PIN is stored in the non-volatile memory of the secure processor and never leaves the TOE in clear text except to smart cards in local card slots. The Memory Protection Unit access control permission ensures that no other applications including the payment application can access the PIN. The PIN digits are never displayed and are replaced by asterisks. When the application processor is using the display, blue banners are displayed indicating that it is not safe to enter PIN. When the eHealth application is running and PIN entry is requested, green banners are displayed indicating that it is safe to enter PIN. Connections for the flow of information between the Connector and the TOE as well as TMS and the TOE are controlled through TLS 1.2. Exceptionally, the TOE accepts specific SICCT commands at the network interface even if the pairing process has not been established and no valid connector certificate is presented. All sensitive data (keys, PIN) received from cards or the connector are deleted immediately after use.
Identification and Authentication (FIA)	Administrator access to the Direct Management module is controlled by an error counter of incorrect password entries. The TOE blocks Administrator access from the third consecutive invalid password entry. This functionality is an authentication mechanism provided by the eHealth application subsystem. User access is defined by role: User, Administrator, Reset Administrator. Passwords are numeric with a length of at least 8 characters. There are separate authentication mechanisms for the Direct Management and SICCT modules. Each have their own error counter. PIN is displayed by asterisks only. SICCT module access requires TLS mutual authentication. The Administrator can reset or change a password.
Security Management (FMT)	Factory reset and the management of security attributes can only be handled by authorised administrators via the Direct Management module. The Direct & User Management modules have three roles – User, Administrator & Reset Administrator (with different access rights).
Protection of the TSF (FPT)	If a firmware, key, TSP CA List or configuration update fails then the update is discarded and the previous state restored. All parts of the TOE lie within the same device and do not comprise physically separated parts. The TSF uses active detection to determine whether physical tampering with the TSF's devices or TSF's elements has occurred. For this purpose, opening switches, pogo pins and wire mesh layers are used. Drilling through the casing, opening the casing and removing the display will all trigger a tamper event. All card readers are also covered by wire mesh and

TOE Security Functionality	Addressed issue
	is enclosed in the physical security zone. In the event of physical or logical tampering, the TOE is set into tamper mode. This renders the terminal inoperable and is immediately made evident to the user on the secure display. Tampered terminals are returned to the manufacturing facility where they are taken out of service and the security processor is destroyed. The TSF runs a suite of self-tests during initial start-up, every 24 hours and on user request. The integrity of the Firmware is checked and if it does not pass then the TOE will go into Tamper mode and become inoperable.
TOE Access (FTA)	The secure state of the TOE is indicated by the use of banners and pop ups on the display. When not in a secure state, blue banners and pop ups display the message “Do not enter your PIN”. Green banners and pop ups indicate when the TOE is in a secure state.
Trusted path/channels (FTP)	The TOE follows the specification detailed in PP-0032-V3-2023, Version 3.8, 15.12.2022 for the authentication of the connector by the TOE. This includes certificate / signature verification and TLS authentication. The TOE establishes a Trusted Channel from the secure processor to the connector. The SICCT protocol over TLS 1.2 with mutual authentication is used to secure the channel. A logically distinct communication path is used to connect the TOE to the TMS for update management. The connection has sole use of its TLS interface.

Table 1: TOE Security Functionalities

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

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], chapters 3.5, 3.3 and 3.4.

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:

Y7 4.3.1:1.2.9 with eHealth Application 1.1.20

The following table outlines the TOE deliverables:

No	Type	Identifier	Form of Delivery
1.	HW/ SW	Y7 4.3.1:1.2.9 with eHealth Application 1.1.20 The Y7 card terminal consists of: ● HW Rev. 4.3.1 ● yOS 1.2.9 ● eHealth Application 1.1.20 ● FPGA 1.1.12	The Y7 card terminal (based on the regulations of the German healthcare system) is delivered in a tamper evident sealed box.
2.	DOC	Y7 Operational User Guidance and Preparative Procedures, Version 0.0.2, 09.08.2024 SHA256-value: 7896ff06dde1e2e1c82a26302192105f5ca99108faa0f1f14b43358930c7337f	The User Guide is sent by email in PDF format. The sending email uses an S/MIME certificate signed by a trusted CA.
3.	DOC	Y7 User Guidance, Version 1.12, 04.03.2025 SHA256-value: a9b587644777f2eb29976a650d0e3680e5521eb9ed188493cfa1c67fe586d436	
4.	DOC	Y7 Sealing Guide, AA-001606 Y7 – Siegelaufkleber v1 (ID 6849).docx SHA256-value: 36bcf425f30d6c5143fec8144a23cec94c1b7626a1fdf4efa66b2c49fae7f010	

Table 2: Deliverables of the TOE

On the back of the terminal an identification label for hardware identification can be found. The identification is structured as follows:

- Model: This is the model identifier. It should always be Y7.
- REV: This is the version number of the terminal.
- P/N: This is the part number of the terminal. This is used internally by JDM to manage the production of terminals.
- S/N: This is the serial number of the terminal. Every terminal has a unique serial number. This number must match the number on the delivery note. If not then the terminal must be returned to JDM.

Identification of hardware and firmware version of the Y7 is provided in Android / Settings / About Tablet. At the end of the list Board Part Number and Board Serial Numbers can be found. These numbers must be identical to the P/N and S/N on the identification label.

Identification of the eHealth application is found in the eHealth App in the menu item “Selbstauskunft” (Self-Information).

Further details about identification of the TOE and the non-TOE-parts are provided in [10] [a], chapters 3.1 and 3.2.

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, OE.ADMIN, OE.CONNECTOR, OE.SM, OE.PUSH_SERVER and OE.ID000_CARDS. Details can be found in the Security Target [6], chapter 4.2.

5. Architectural Information

The Target of Evaluation (TOE) described in this report is a smart card terminal which fulfils the requirements to be used with the German electronic Health Card (eHC) and the German Health Professional Card (HPC) based on the regulations of the German healthcare system. Please refer to [11] for further information about card compatibility. The TOE fulfils the requirements to be used as a secure PIN pad entry device for applications according to [11], which specifically means that a PIN, which has been entered by a user at the TOE, never leaves the TOE in clear text, except to smart cards in local card slots.

This chapter gives an overview of the subsystems of the TOE and the corresponding TSF which were objects of this evaluation. The security functions of the TOE are:

- 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 including update of Firmware, and
- Active physical protection.

According to the TOE Design these security functions are enforced by the following four subsystems: Secure Hardware, OS Layer, OS Extension Layer and eHealth Application.

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

All TOE Security Functions have been tested on a real TOE and the TOE test configuration has been consistent with the ST. Following methods have been used to confirm functionality of TSFs:

- automatic tests of all TSFI
- manual tests of all TSFI
- Sourcecode-Reviews
- TLS – and SICCT- Tests
- RPC- Fuzzing
- Additional manual independent tests by the evaluator

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

Note that the TOE under evaluation used the eHealth Application version 1.1.19. The final TOE has eHealth Application version 1.1.20. Both versions are identical expect that version 1.1.20 uses production keys. Therefore, all evaluation results are also valid for eHealth Application version 1.1.20.

7.1. Developer Tests

Tests are performed on a TOE configuration that resembles a real device as it would be deployed in the field, but productive keys are replaced by test keys.

In the test environment such real TOE is used and connected to card emulators that are controlled by the test environment. Since a real TOE is tested interactions with the Display or the touch screen have to be done manually by the tester.

Some test cases can be performed fully automatically with execution in the test suite and some test cases need manual performance by the tester. Requirements that are not directly testable are tested by source code review.

The testing approach of the developer is to test all TSFIs by testing directly all assigned SFRs. This allows directly addressing the security relevant behaviour of TSFIs as well as subsystems. For each SFR in the ST [6] one or more dedicated test cases are given, if applicable. All TSFI are mapped to one or more SFR, and thereby transitively to one or more test cases, as explained above. Additionally, the developer implemented further test cases, which are directly derived from the gematik requirements in [11]. This ensures that beside testing SFR relevant security functionality also a great coverage of general TSFIs functionality is given. In particular the SICCT interface, interfaces for user interaction (display, touch screen) as well as card interfaces are addressed by this approach. Underlying protocols are tested implicitly with each test case. With the SFR approach also a mapping of test cases to subsystems identified in the TOE design and its interactions is given.

All test cases were executed successfully and ended up with the expected result or a reasonable justification for failed test execution was given.

7.2. Independent ITSEF Tests

The independent tests were performed on a TOE as defined in the ST [6].

The developer provided two test case sets which includes a full coverage of all security functionality of the TOE. There are test cases checking the appropriate behaviour using specification compliant parameters for every TSFI defined in the functional specification. These tests cover each SFR of the TOE the “AFOs” described in the gematik-specifications. Additional tests developed by the evaluators were executed.

All test cases were executed successfully and ended up with the expected result or a reasonable justification for failed test execution was given.

The evaluators determined that all tests were executed successfully.

7.3. Penetration Tests

All configurations of the TOE being intended to be covered by the current evaluation were tested.

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 Moderate was actually successful in the TOE’s operational environment as defined in the ST [6], provided that all measures required by the developer are applied.

8. Evaluated Configuration

This certification covers the configuration of the TOE as described in Table 2 of this report.

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.4 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), BSI-CC-PP-0032-V3-2023, 15.12.2022 [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.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 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.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Keylength in Bits	Standard of Application	Remarks
1.	Authenticity	Signature verification for TLS with support of the gSMC-K RSA signature verification with encoding RSASSA-PSS (PKCS#1) using SHA-256 or ECDSA using the curves P-256, P-384, brainpoolP256r1 and brainpoolP384r1	[RFC 8017] (PKCS#1) [FIPS 180-4] (SHA-256) [TR-03111] (ECDSA) [FIPS-186-4] (P-256, P-384) [RFC-7027] (brainpoolP256r1, brainpoolP384r1)	For RSA: 2048 bit For ECDSA: Key length according to the used curve	[12] Kap. 3.3.2	FCS_COP.1.1/SIG
2.	Authentication	Signature generation with and verification for TLS with support of the gSMC-K RSA signature verification with encoding RSASSA-PSS (PKCS#1) using SHA-256 or ECDSA using the curves P-256, P-384, brainpoolP256r1 and brainpoolP384r1	RFC 8017] (PKCS#1) [FIPS 180-4] (SHA-256) [TR-03111] (ECDSA) [FIPS-186-4] (P-256, P-384) [RFC-7027] (brainpoolP256r1, brainpoolP384r1	For RSA: 2048 bit For ECDSA: Key length according to the used curve	[12] Kap. 3.3.2	FCS_COP.1.1/SIG
3.	Key Agreement	Elliptic Curve Diffie-Hellman Key Agreement (ECDH) for TLS	[SEC1] (ECDH), [RFC 5246] (TLS v1.2)	Key length accordinbg to the used curves P-{256,384} ([FIPS 186-4])	[12] Kap. 3.3.2	FCS_CKM.1.1/Connector
4.	Authenticated Encryption	AES-128 and AES-256 in GCM Mode for TLS v1.2	[FIPS 197] (AES) [RFC 3268] (AES-TLS) [SP 800-38D] (GCM) [RFC 5289] (AES-GCM-TLS) [RFC 5116] (AEAD)	128 bit and 256 bit	[12] Kap. 3.3.2	FCS_COP.1.1/Con_Sym
5.	Trusted	TLS v1.2 with Cipher Suites	[RFC 5246] (TLS	-	[12] Kap.	FCS_CKM.1

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Keylength in Bits	Standard of Application	Remarks
	Channel	TLS_ECDHE_RSA_ WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_ WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	v1.2)		3.3.2	.1/Connector
6.	Integrity	Integrity of Update Packets ECDSA using the curve secp384r1	[TR-03111] (ECDSA) [FIPS-186-4] (secp384r1)	Keylength according to the used curve	[11]	FCS_COP.1.1/SIG_FW (1) FCS_COP.1.1/SIG_FW (2)

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.

11. Security Target

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

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

ADV	Development
AGD	Guidance Documents
AIS	Application Notes and Interpretations of the Scheme
ALC	Life-Cycle Support
ARC	Security Architecture
ASE	Security Target Evaluation
ATE	Tests
AVA	Vulnerability Assessment
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
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
KVK	Krankenversichertenkarte
LAN	Local Area Network
OSP	Organisational Security Policy
PIN	Personal Identification Number
PP	Protection Profile

SAC	Signature Application Component
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SICCT	Secure Interoperable Chip Card Terminal
SMC	Security Module Card
SM-KT	Security Module Kartenterminal
ST	Security Target
TMS	Terminal Management System
TOE	Target of Evaluation
TSF	TOE Security Functionality
VAN	Vulnerability analysis

13.2. Glossary

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

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7] https://www.bsi.bund.de/AIS

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

[6] Security Target BSI-DSZ-CC-1233-2025, Version 0.0.16 11.04.2025, ASE_ST Y7 Security Target for the Evaluation of the Product JDM Y7 of JDM Payment Solutions SAS according to the Common Criteria 3.1 Level EAL3+ Certification Id: BSI-DSZ-CC-1233, JDM Payment Solutions SAS

[7] Evaluation Technical Report, Version 1.4, 17.04.2025, Evaluation Report - Evaluation Technical Report (ETR) -, SRC Security Research & Consulting GmbH

[8] Common Criteria Protection Profile Electronic Health Card Terminal (eHCT), BSI-CC-PP-0032-V3-2023, 15.12.2022, Version 3.8, Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik - BSI)

[9] Configuration list for the TOE, CC Configuration Items List, Version 0.0.8, JDM Payment Solutions SAS (confidential document)

[10] Guidance documentation for the TOE
[a] Y7 Operational User Guidance and Preparative Procedures, Version 0.0.2, 09.08.2024, JDM Payment Solutions SAS
[b] Y7 User Guidance, Version 1.12, 04.03.2025, JDM Payment Solutions SAS
[c] Y7 Sealing Guide, AA-001606 Y7 – Siegelaufkleber v1 (ID 6849).docx, JDM Payment Solutions SAS

[7] specifically

- AIS 1, Version 14, Anwendungshinweise und Interpretationen zum Schema, AIS 1: Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 14, Version 7, Anwendungshinweise und Interpretationen zum Schema, AIS 14: Anforde-rungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 9, Anwendungshinweise und Interpretationen zum Schema, AIS 19: Anforde-rungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 45, Version 2, Erstellung und Pflege von Meilensteinplänen

[11] Elektronische Gesundheitskarte und Telematikinfrastruktur, Spezifikation eHealth-Kartenterminal, Version 3.16.0, Stand 07.07.2023

[12] Elektronische Gesundheitskarte und Telematikinfrastruktur, Übergreifende Spezifikation, Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Version 2.28.0, 09.06.2023, gematik GmbH

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