Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1125-2019

for

Bundesdruckerei Document Application with tamper-evident casing, Document Application Version 2.2.1; (Firmware Vers. 1.1.12, HW Vers. 0)

from

Bundesdruckerei 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-1125-2019 (*)

Hoheitliche Dokumente: Software

Bundesdruckerei Document Application with tamper-evident casing,
Document Application Version 2.2.1; (Firmware Vers. 1.1.12, HW Vers. 0)

from	Bundesdruckerei GmbH
PP Conformance:	Common Criteria Protection Profile for Document Management Terminal DMT-PP, BSI-CC-PP-0064-V2-2018, Version: 2.0, 2018-06-06, Federal Office for Information Security (BSI)
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 3

SOGIS
Recognition Agreement

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.

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

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.

Bonn, 31 October 2019

For the Federal Office for Information Security

Bernd Kowalski
Head of Division

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

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: 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.

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

[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 Bundesdruckerei Document Application with tamper-evident casing, Document Application Version 2.2.1; (Firmware Vers. 1.1.12, HW Vers. 0) has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1093. Specific results from the evaluation process BSI-DSZ-CC-1093 were re-used.

The evaluation of the product Bundesdruckerei Document Application with tamper-evident casing, Document Application Version 2.2.1; (Firmware Vers. 1.1.12, HW Vers. 0) was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 2 October 2019. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Bundesdruckerei GmbH.

The product was developed by: Bundesdruckerei 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 31 October 2019 is valid until 30 October 2024. 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

[5] Information Technology Security Evaluation Facility

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 Bundesdruckerei Document Application with tamper-evident casing,, Document Application Version 2.2.1; (Firmware Vers. 1.1.12, HW Vers. 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] Bundesdruckerei GmbH
Oranienstraße 91
10969 Berlin

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 Bundesdruckerei Document Application with tamper-evident casing 2.2.1.

The Document Application is running on a Document Management Terminal (DMT). It is used to read the German Passport (ePass), to read and update the electronic data of the German identification card ("Personalausweis (PA)") and electronic resident permit ("elektronischer Aufenthaltstitel (eAT)") as well as to verify the document's authenticity and the integrity of its data.

The TOE is operated by governmental organisations, e.g. municipal office, police, government or other state approved agencies. The TOE is specifically applied in registration offices to allow card holders to verify that their ePass, PA or eAT is working correctly. In case of PA and eAT it is further possible to update the address information of the card holder, the card holder's PIN for eID applications, and the community ID ("Gemeindeschlüssel"). In addition, the eID application functionality of the PA or eAT can be activated or deactivated. Additionally the TOE ensures secure communication to external control software and provides a tamper-evident enclosure.

Necessary protocols for the communication of the TOE with the electronic identity documents like the ePass, PA or eAT are described in [ICAO_9303] and [TR-03110-1], [TR-03110-2], [TR-03110-3].

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Common Criteria Protection Profile for Document Management Terminal DMT-PP, BSI-CC-PP-0064-V2-2018, Version: 2.0, 2018-06-06, Federal Office for Information Security (BSI) [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.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.2. 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.PROTOCOLS	SF.PROTOCOLS ensures that the protocols for communication between itself and electronic identity documents are enforced according to [TR-03110-1], [TR-03110-2], [TR-03110-3] and [ICAO_9303] (FIA_UAU.4, FIA_UAU.5, FIA_UAU.6 and FIA_API.1).
SF.MANAGEMENT	SF.MANAGEMENT enforces that the following management functions are accessible to the Administrator of the TOE (FIA_UAU.2, FIA_UID.2 FMT_SMR.1, FMT_SMF.1, FMT_MTD.1/TOE-Config, FMT_MTD.1/EnableOpAccKeyStore and FMT_MTD.1/ReadVersion).
SF.AUDIT	The TOE generates audit data (FAU_GEN.1) which is then stored by the environment.

TOE Security Functionality	Addressed issue
SF.PROTECTION	SF.PROTECTION allows the user to detect physical tampering of the base unit (FPT_PHP.1/ BaseUnit) and provides a trusted communication path between TOE and control software (FTP_TRP.1/ControlSoftware). Detection of physical tampering is realized by a seal that is carried by the base unit. This seal will be broken and therewith indicated physical tampering of the base unit. The communication between Control Software and TOE is secured by a trusted channel.

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 3.2. 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 3.4 – 3.6.

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:

Bundesdruckerei Document Application with tamper-evident casing, Document Application Version 2.2.1; (Firmware Vers. 1.1.12, HW Vers. 0)

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Bundesdruckerei Document Application with tamper-evident casing	2.2.1	Included in 2 or via Update.
2	HW	TOE Casing	0	Physical delivery.
3	DOC	VISOTEC® V-ÄNDERUNGSTERMINAL Handbuch Installation und Bedienung	1.160	Via secured web-portal.

Table 2: Deliverables of the TOE

The complete terminal that operates the TOE is delivered to the user via standard delivery services (e.g. DHL). The delivery however, is tracked and the terminal can only be operated using an operator, administrator and revisor smart card which are shipped separately. The delivery includes also non-TOE components like the computer hardware and peripherals.

For terminals that are already delivered to the customer, the update functionality may be used to deliver the TOE-SW (as part of the firmware).

The guidance documentation is not delivered together with the terminal as this would allow an attacker to steal a packet and manipulate a terminal as well as the guidance. Instead, the guidance documentation is downloaded by the users via a secured web portal.

The Guidance Version 1.160 has the following hash value (SHA256):

17eda6c33237c026a51d2b5667faee564b5f3d907abe3c383a5bdd10ce0e571d

The guidance documentation informs the administrator about the security characteristics of an authentic terminal. The following aspects ensure the authenticity:

- A Type-Label of Bundesdruckerei, that is in fact a seal,
- Six seals on the terminal (4 on the bottom and 2 on the top of the terminal),
- The security characteristics of the box used for shipment.
- The version of the casing is “0” coded by the 7th character of the S/N, the “0” after “V-AETx”, see [10, chap. 2.5.4].

The version of the software and casing can be verified. This enables the authorized users, Operator, and Administrator to identify the TOE by its version number.

3. Security Policy

The Security Policy enforced is defined by the selected set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Security Audit,
- Communication,
- Cryptographic Support,
- User Data Protection,
- Identification and Authentication,
- Security Management,
- Protection of the TSF, and
- Trusted Path/Channels.

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

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to

specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

OE.AuthenticationMeans:

Operators (S1), Administrators (S2) and Revisors (S3) must be authenticated by at least two authentication factors from different categories, whereby at least the categories possession-based authentication factor and knowledge-based authentication factor must be taken into account. [10, chap. 3.1], [10, chap. 4.4.2], [10, chap. 5.5.2].

OE.SecureBoot[7]:

The components in the TOE environment that are required for the operation of the Document Management Terminal must provide mechanisms to boot the Document Management Terminal's OS and the device drivers in a secure way so that an initial secure state without protection compromise is guaranteed. The devices drivers of any external input and output device (O5+O6+O7) must also be protected by secure booting mechanisms. [10, chap. 4.4.2], [10, chap. 5.5.2].

OE.Date:

The Operator (S1) shall check the correctness of the current date and time of the TOE at the beginning of his duty. For this the Operator has to use a reliable reference (e.g. DCF-77 Clock, GPS Clock). [10, chap. 5.5.2].

OE.ChipPassword:

The environment must enable the Operator (S1) or the Electronic identity document holder (S5) to ensure during entering or updating the chip password (R.ChipPassword) or the personal chip password (R.PersonalChipPassword) that any person who is not authorised to know that password is not able to skim it. Therefore, a special distance between the Document Management Terminal and any other person shall be enforced. Additionally, the touchscreen is protected against skimming by a privacy filter. [10, chap. 3.2.2], [10, chap. 4.3].

OE.CheckLogData:

The stored log data (R.LogData) shall be revised regularly to discover malfunctions or attacks. This shall be done by a Revisor (S3) who is not the same person as the Administrator (S2). [10, chap. 5.7].

OE. CheckTerminalIntegrity

The integrity of the entire Document Management Terminal hardware shall be checked regularly by Operator (S1), but at least at the beginning of his duty or if the terminal is returned from state "PKSDisabled[8]" (c.f. OE.TAKeyManagement).

The Operator (S1) shall verify that the Document Management Terminal is authentic and has not been manipulated.

If external in- or output devices are connected to the Document Management Terminal the Operator (S1) shall check their cable connection. [10, chap. 5.1] [10, chap. 5.2], [10, chap. 5.5.2], [10, chap. 9.1].

[7]See also Application Note 8 in [8]

[8]PKSDisabled means that the certificates required for operational use are deleted. The TOE cannot be operated regularly in this state.

OE.TrainedUser:

The Users – Operators (S1), Administrators (S2) and Revisors (S3) – of the Document Management Terminal shall be well-trained and trustworthy in a sense not to compromise the TOE installation itself or the assets secured by the TOE and the TOE environment. [10, chap. 3.2.1], [10, chap. 4.3].

OE.SecureAdministration:

The administration of the Document Management Terminal as well as the TOE itself shall be maintained securely. Only authorised personnel shall be allowed to administer the Document Management Terminal and the TOE. The administration personnel will not install any malicious soft- or hardware at the Document Management Terminal. [10, chap. 3.1], [10, chap. 3.2.1], [10, chap. 4.3].

OE.SecureComponents:

If any input and/or output device (O5+O6+O7) necessary for the operation of the Document Management Terminal is situated outside of the tamper-evident environment according to OT.TamperEvidence, they must be directly connected to the base unit by cable. In particular, no hubs or active cables are allowed in the connection between the baseunit and the input and/or output device. The devices must remain in close proximity to the base unit during operation, i.e. they must remain in sight of the Operator (S1). [10, chap. 4.3].

OE.TAKeyManagement:

The terminal may only remain in the state "PKSLocked[9]" if one of the following conditions is fulfilled and must be returned to state "PKSDisabled" otherwise:

1. In case of stationary use, the Document Management Terminal must be installed permanently at its intended environment (e.g. at the working places of a municipal office).

2. In case of mobile use, the terminal may remain in the state "PKSLocked" if the terminal is left unattended by the Operator (S1) for a short time period or if the terminal is stored in a secure environment. The environment is considered secure if physical and remote access to that environment is restricted to the Operator (S1). The terminal must be returned to state "PKSDisabled" if the Document Management Terminal shall be left unattended and cannot be stored in a secure environment. [10, chap. 5.1], [10, chap. 5.5.3], [10, chap. 5.5.4].

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

5. Architectural Information

The TOE is a software which is capable of reading or updating electronic identity documents. Furthermore, the TOE includes a tamper-evident environment that protects the software of the TOE itself as well as the required components for the operation of the TOE.

Subsystem	Description
Reverse Proxy	Provides the secure channel with Control PC.
Chip Daemon	Communication with ID document and SAM.

[9]PKSLocked means that the certificates required for operational use are installed but need to be unlocked by the operator for the TOE to operate fully.

Subsystem	Description
Management Daemon	Configuration of the connection to the Control PC
Physical Enclosure	The tamper-evident environment of the TOE

Table 3: Subsystems of the TOE

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

As the TOE is a software application that is executed within an operating system that runs on a smart card terminal, the developer of the TOE has chosen a software based concept for testing. They developed a dedicated test framework to test the TOE and that can be run on the same hardware on which the TOE will be operated in practice.

TOE test configurations:

- C1: CC test TOE - It is used for developer testing and comes with SSH access and further modification, like the CC test controller daemon, to allow the test suite to access all TOE functionalities.
- C2: PKI TOE - with the only difference that a developer PKI is used for document related operations. This enables the TOE to connect to the developers PKI over the internet. This is not possible with the original PKI since it is restricted to registration office.
- C3: debug TOE - with SSH access and a so called soft SAM, a software based implementation of the SAM. This allows the evaluator to perform tests that change certificates that are usually stored inside the SAM and thus cannot be changed.

The C1 test configuration provides a dedicated test interface (accessible via SSH) that can be used to start test cases that are contained in the test framework. This is the only way to directly address the interfaces that the TOE provides during testing. The test cases of the developer cover the complete security functionality of the TOE.

The evaluator conducted penetration tests based on all test configurations including direct manipulations of the environment of the TOE (even though such manipulations are not formally necessary due to dedicated assumptions in the Security Target).

The further penetration tests are performed regarding the physical tamper of the the enclosure. For this the developer assessed the security label according to [4, AIS48]. The penetration tests included the whole enclosure to verify that the TOE fulfills the requirement of detection of physical tampering.

For the Re-evaluation, the C3 TOE configuration was not used.

7.1. Developer's Test according to ATE_FUN

TOE test configurations:

- The developer used a TOE with software additions for their testing approach (C1).

TOE test environment configurations:

- The test setup comprises a laptop, a COMPRION CLT One with antenna, a TOE with display.

Testing approach:

- 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) and subsystem(s).
- Different testing approaches are used:
  - 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.

For the Re-evaluation the developer repeated successfully all test cases and they all PASSED according to their expected result.

7.2. Evaluator Tests

Independent Testing according to ATE_IND

TOE test configurations:

- The ITSEF used the same test configurations and test environment as the developer during functional testing (C1).

TSFI selection criteria:

- The ITSEF chose to broadly cover the existing interfaces without specific restrictions.

TSFI tested:

- All interfaces were considered during testing.

Developer tests performed:

- The ITSEF chose to inspect all developer tests. They also chose to repeat all tests.

Verdict for the sub-activity:

For the Re-evaluation the evaluator repeated a subset of tests, no deviations were found between the expected and the actual test results.

7.3. Penetration Testing according to AVA_VAN

Overview:

- The penetration testing was partially performed using the developer's testing environment, partially using the test environment of the ITSEF.
- The Security Target [6] has identified solely one configuration of the TOE under evaluation. Nevertheless there are three test configurations that were used for penetration testing (C1, C2 and C3).
- No attack scenario with the attack potential Basic has actually been successful.

Penetration testing approach:

- Based on a list of potential vulnerabilities applicable to the TOE in its operational environment created within the work unit AVA_VAN.2-5 the evaluators devised the attack scenarios for penetration tests when they were of the opinion, that those potential vulnerabilities could be exploited in the TOE's operational environment.
- While doing this, also the aspects of the security architecture described in ADV_ARC were considered for penetration testing. All other evaluation input was used for the creation of the tests as well. Specifically the test documentation provided by the developer was used to find out if there are areas of concern that should be covered by tests of the ITSEF.
- As the TOE is a document application with the enclosure of the Base Unit (the mainboard) that heavily relies on the security measures of the environment (including the terminal in, which the TOE is integrated). The ARC document also covers some of the security measure that are applied by the terminal. The evaluator considered the fact that the TOE is delivered in such a way and widened the scope of the vulnerability analysis to cover specific security aspects of the whole terminal.
- The evaluator also paid attention to the TSFI in the FSP. As the TSFI are quite simple with few options that can be varied and the TOE is deeply integrated into a terminal when it is delivered, the vulnerability assessment needed to focus on mechanisms that are operational inside the TOE or the terminal.

In summary, 11 different attack scenarios having been tested as part of this activity.

Verdict for the sub-activity:

- No deviations were found between the expected and the actual test results.
- Regarding the Re-evaluation: The Evaluator repeated a subset of tests, no deviations were found between the expected and the actual test results.

7.4. Summary of Test Results and Effectiveness Analysis

Verdict for the sub-activity:

No attack scenario with the attack potential Basic was actually successful in the TOE's operational environment as defined in [6] provided that all measures required by the developer are applied.

Please note:

The TOE is only a small part of the whole terminal and it heavily relies on the secure functioning of the rest of the terminal. The overall security significantly depends on the secure environment in which the terminal is operated. Therefore, it's strongly advised that the responsible personnel is well-trained to uphold security, i.e. secure operation, detection of manipulations, checking of seals, general security awareness; see guidance documentation [10] as well as chapter 4 and 10 for further details.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

Item	Exact version
TOE software	2.2.1
Rest of the terminal firmware (including the operating system)	1.1.12
TOE Casing	0

Table 4: Exact version information of the TOE configuration

This certification covers only one configuration as described in table 4 above.

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 RNG assessment the scheme interpretations AIS 20 was used (see [4]).

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)

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-1093, re-use of specific evaluation tasks was possible. The main update of the firmware is related to the use of foreign addresses.

The focus of this Re-evaluation was on ATE and a subset of AVA and ATE_IND, with the subset being chosen in conjunction with the performed changes of the TOE.

The developer updated the document [11] that includes the TOE interfaces and modules.

The evaluation has confirmed:

- PP Conformance: Common Criteria Protection Profile for Document Management Terminal DMT-PP, BSI-CC-PP-0064-V2-2018, Version: 2.0, 2018-06-06, Federal Office for Information Security (BSI) [8]
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 3

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	Key Size in Bits	Standard of Application	Evaluator's comments
1.	BAC ChallengeGen	RNG DRG.3	[FIPS186-2] Appendix 3, Section 3.1	112	[ICAO_9303]#4.3.1	-
2.	BAC Encryption of Challenge/ Response	3DES-CBC IV=0, No Padding	[ANS X9.52] (3DES) [SP800-38A] (CBC)	112	[ICAO_9303]#4.3.3.1 [ICAO_9303]#9.7.1.2	3DES not recommended[10]
3.	BAC Key Derivation	SHA1	[FIPS180-4] (SHA)	128	[ICAO_9303]#9.7.1.1	SHA-1 not recommended[10]
4.	BAC Authentication (MAC)	Retail-MAC (DES-CBC) IV=0, Padding Method 2 MAClen=8Bytes	[FIPS PUB 46-3] (DES) ISO/IEC 9797-1:2011 (Retail MAC)	112	[ICAO_9303]#4.3.3.2 ISO9797-1 Mode 3	-
5.	PACE KeyGen (Ephemeral)	RNG DRG.3	[FIPS186-2] Appendix 3, Section 3.1	256	[TR-03110-2] [ICAO_9303]#4.4 [TR-03116]	-
6.	PACE Nonce	RNG DRG.3	[FIPS186-2] Appendix 3, Section 3.1	-	[TR-03110-2] [ICAO_9303]#4.4	-
7.	PACE Encryption/ Decryption	AES-CBC	[FIPS 197] (AES), [SP800-38A] (CBC)	128	[TR-03116] [TR-03110-2] [ICAO_9303]#4.4	-
8.	PACE KeyAgreement PACE Mapping	ECKA/ECKA-GM(ECDH)	[TR-03110-1]	-	[TR-03110-1] [ICAO_9303]#4.4 [TR-03116]	-
9.	PACE MAC	AES-CMAC	[FIPS 197] (AES), [SP800-38B] (CMAC)	128	[TR-03110-2] [ICAO_9303]#4.4 [TR-03116]	-

[10]See [TR-02102] but required by [ICAO_9303].

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Evaluator's comments
10.	PACE Key Derivation	SHA-1	[FIPS180-4] (SHA)	128	[TR-03110-2] [ICAO_9303]#4.4 [TR-03116] [TR-03111]#4.3.3.2	SHA-1 not recommended[10]
11.	TAv2 KeyGen (Ephemeral)	(RNG DRG.3)	[FIPS186-2] Appendix 3, Section 3.1	256 (brainpool P256r1)	[TR-03110-2]#3.3 [TR-03116]	-
12.	TAv1/TAv2 Sign	ECDSA-SHA256	[ISO/IEC 15946-2-2002], Part 2 (ECDSA) [FIPS180-4] (SHA)	256 (StaticKey : brainpoolP 256r1)	[TR-03116] [TR-03110-2]#3.3 [TR-03110-1]#3.5	-
13.	PKI Passive Authentication (CSCA)	ECDSA-SHA256 ECDSA-SHA384 ECDSA-SHA512	[ISO/IEC 15946-2-2002], Part 2 (ECDSA) 256 384 512	[TR-03116] [ICAO_9303]#5.1 [TR-03110-1]#1.1	-	
14.	Passive Authentication Document Signer	ECDSA-SHA224 ECDSA-SHA256 ECDSA-SHA384	ISO/IEC 15946-2-2002], Part 2 (ECDSA) [FIPS180-4] (SHA)	224 256 384	[TR-03116] [ICAO_9303]#5.1 [TR-03110-1]#1.1	SHA-224 not recommended[10]
15.	PKI Passive Authentication DG-Hash	SHA256 SHA384	[TR-3110-1]	none	[TR-03116] [ICAO_9303]#5.1 [TR-03110-1]#1.1	-
16.	PKI Terminal Authentication CVCA	ECDSA-SHA2	ISO/IEC 15946-2-2002], Part 2 (ECDSA) [FIPS180-4] (SHA)	256	[TR-03116] [TR-03110-1]#3.5 [TR-03110-2]#3.3	-
17.	CAv1 KeyGen	(ECC: RNG DRG.3)	[FIPS186-2] Appendix 3, Section 3.1	256 (brainpool P256r1)	[TR-03116] [TR-03110-1]#3.4	-
18.	CAv2 KeyGen (Generated	(ECC: RNG DRG.3)	[FIPS186-2] Appendix 3,	-	[TR-03116] [TR-03110-2]#3.4	-

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Evaluator's comments
	during TAv2)		Section 3.1			
19.	CAv1/CAv2 KeyAgreement	ECKA(ECDH)	[TR-03116]	256	[TR-03116] [TR-03110-1]#3.4 [TR-03110-2]#3.4	-
20.	CAv1 Encryption	3DES- CBC AES-CBC	[ANS X9.52] (3DES) SP800-38A (CBC)	112 128	EUCOM (2006) 2909 [TR-03116] [TR-03110-1]#3.4	3DES not recommended[10]
21.	CAv1 Authentication (MAC)	3DES RetailMAC AES-CMAC	[FIPS PUB 46-3] (DES) ANS X9.52 (3DES) ISO/IEC 9797-1:2011 (Retail MAC) [FIPS 197], [FIPS SP800-38B] (AES-CMAC)	112 128	EUCOM (2006) 2909 [TR-03116] [TR-03110-1]#3.4	3DES not recommended[10]
22.	CAv2 Encryption	AES-CBC	[FIPS 197] (AES), [SP800-38A] (CBC)	128	[TR-03116] [TR-03110-2]#3.4	-
23.	CAv2 Authentication (MAC)	AES-CMAC	[FIPS 197], [FIPS SP800-38B] (AES-CMAC)	128	[TR-03116] [TR-03110-2]#3.4	-
24.	Firmware Signature Verification	ECDSA	[ISO/IEC 15946-2-2002], Part 2 (ECDSA)	256	[FIPS186-4]#Kap 6	-
25.	Firmware Signature Hash	SHA256	[FIPS180-4] (SHA)	-	[FIPS180-4]	-
26.	SAM-Access/ Authentication PACE	ECKA/ECDH	[TR-03111]	384	[TR-03111]	-
27.	SAM- SecureMessaging	AES-CBC AES-CMAC	[FIPS 197] (AES), [SP800-38A] (CBC) [FIPS 197], [FIPS SP800-38B] (AES-CMAC)	128	SYM) AES: [FIPS197] CBC: [SP800-38A] CMAC: [SP800-38B]	-

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Evaluator's comments
28.	TLS	ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-SHA384 ECDHE-ECDSA-AES128-SHA256 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES128-SHA256	ISO/IEC 15946-2-2002], Part 2 (ECDSA) [FIPS 197] (AES), [FIPS180-4] (SHA)	128 256	[RFC5246]	-

Table 5: 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). 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 order to highlight the information provided for TOE users (Administrator, Operator, and Revisor) in the guidance documentation the following hints and requirements are of specific importance and are therefore mentioned here explicitly:

- The Security Target [6] contains assumptions about the physical environment of the TOE. The operators, administrators and revisors have to ensure that the TOE is stored in a secure environment when left unattended or that it is brought into a secure state (state PKSDisabled) otherwise.
- The terminal that operates the TOE shall be powered off every evening/workday [10, chap. 5.1].
- The correct operation of the software environment of the TOE (i.e. the Operating System/Firmware) is of specific importance to the secure operation of the TOE. As such, the certificate for the TOE is only be valid for the operation using the exact version of the Operating System/Firmware as it has been available during evaluation, see table 4.
- The use of the software HDSupport is mandatory. The requirements in [10, chap. 4.4.4] need to be fulfilled.

The overall security depends on the secure environment in which the terminal is operated. Therefore, its advised that the responsible personnel is well trained to uphold security, i.e. secure operation, detection of manipulations, checking of seals, general security awareness, see [10, chap. 2.5.2] for details regarding the checks of the seals.

The TOE is only a small part of the whole terminal and it relies on the secure functioning of the rest of the terminal, see chapter 4 for further details.

11. Security Target

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

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

AIS Application Notes and Interpretations of the Scheme

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

BSIG BSI-Gesetz / Act on the Federal Office for Information Security

CCRA Common Criteria Recognition Arrangement

CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
eID	Electronic Identification
eAT	Elektronischer Aufenthaltstitel (electronic resident permit)
ePass	Elektronischer Reisepass (electronic passport)
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PA	Personalausweis (Identity document)
PIN	Personal Identification Number
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

13.2. Glossary

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

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

14. Bibliography

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

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

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[11] 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 Bundesdruckerei Document Application BSI-DSZ-CC-1125-2019, V 1.52, 2019-09-12, Bundesdruckerei GmbH

[7] Evaluation Technical Report, V 2, 2019-10-01, BSI-DSZ-CC-1125, TÜV Informationstechnik GmbH, (confidential document)

[8] Common Criteria Protection Profile for Document Management Terminal DMT-PP, BSI-CC-PP-0064-V2-2018, Version: 2.0, 2018-06-06, Federal Office for Information Security (BSI)

[9] Configuration list for the TOE, V1.27, 2019-09-12 Configurationlist, File: ALC_CMS_DMT-V1.xx.xlsx, Bundesdruckerei GmbH (confidential document)

[10] VISOTEC® V-ÄNDERUNGSTERMINAL Handbuch Installation und Bedienung, V 1.160, 2019-09-12, Bundesdruckerei GmbH

[11] ADV_FSP - Functional Specification, V 1.54, 2019-09-06, Bundesdruckerei GmbH, (confidential document)

[11] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 48, Version 1, Anforderungen an die Prüfung von Sicherheitsetiketten

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 https://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.