Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1106-2021

for

BDrive Windows Client
Version 3.50.89.4

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-1106-2021 (*)

Cryptographic file exchange

BDrive Windows Client, Version 3.50.89.4

from	Bundesdruckerei GmbH
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 2

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

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 May 2021
For the Federal Office for Information Security

Sandro Amendola
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

his 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]
- 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 3 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.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 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 under CCRA-2014 for all assurance components selected.

[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 BDrive Windows Client, Version 3.50.89.4 has undergone the certification procedure at BSI.

The evaluation of the product BDrive Windows Client, Version 3.50.89.4 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 26 April 2021. 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 May 2021 is valid until 30 May 2026. 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 BDrive Windows Client, Version 3.50.89.4 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
Kommandantenstraße 18
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) defined as Bdrive Windows Client version 3.50.89.4 is the client-side solution for storing and sharing of files of all types, developed to provide a secure alternative solution of cloud sharing for company data.

The TOE is a software component, which implements the client-side functions of the Bdrive System for the Windows platform. It implements a secure, distributed file storage. Each consumer device of a user receives a unique authentication certificate, and files are shared between all devices of the user. Optionally, a user has the possibility to share files and folders with several other users in the same company. The storage scheme realizes forward error correction (erase coding) together with cryptographic means for encryption and authentication.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

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 2.

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
Login	When starting the Desktop Client, the unidentified user has to authenticate on every login via authentication with authentication certificate. Only after successful verification of the user's credentials (certificate + protection password) at the IDP, the user is allowed to perform any further action.
Logout	The user decides upon the termination of the session. The private parts of the authentication and encryption keys are protected by the TOE upon session termination and Cryptographic Operation.
Management of access rights to files and folders	Every group and every user owns a unique virtual folder called *root node.* A user may be a member of several groups. All subfolders and their files refer to their root node. In order to determine all users who are allowed to access a given folder/file, its root node has to be identified. Hence, a user has access to a given file if • this file is contained in his own root node, or • this file is contained in a root node that belongs to one of his groups. User can create new groups by transforming a directory in their private root node into a root node of a new group. Furthermore, every member of a group can invite or remove users.
Generation of user-specific meta data	The user-specific meta data are generated when a file is put under control of the TOE. The user-specific meta-data contains a checksum of the plaintext file. These user-specific meta data are encrypted, authenticated and then transferred to the Bdrive server. The plain file gets encrypted, authenticated, fragmented and transferred to the Cloud storage servers.
Generation of general meta	The general meta data is generated when a file is decided to be

TOE Security Functionality	Addressed issue
data	transferred to the Bdrive System (user's choice). The list of users who have access rights to the particular file is determined via the corresponding root node. This list makes part of these general meta data, which are transmitted to the Bdrive Server together with the storage locations of this file.
Key generation	When a file is decided to be transferred to the Bdrive system (user's choice), two symmetric keys are generated by the TOE on the basis of a seed.
File encryption	Files transferred to the Bdrive system are encrypted by AES-256 in CTR mode. Big files are split into blocks with a maximum size of 20 MB which are encrypted blockwise.
File authentication	The encrypted object is authenticated by means of HMAC. In case of big files, each of the blocks is authenticated separately – the byte offset of each block is appended to the data prior to authentication. Each block gets fragmented and uploaded to the cloud storage servers. The message authentication code (MAC) is stored on the Bdrive Server along with the general meta data.
File fragmentation	After blockwise data encryption and authentication, the encrypted block is fragmented using a Reed-Solomon-Cauchy scheme into a number of data chunks and parity chunks. Those are then uploaded to independent cloud storage servers facilitating Source data exchange recovery. The exact number of data and parity chunks is added to the general meta data.
Key encryption & decryption	The keys are asymmetrically encrypted using the device-specific encryption certificates of all authorized users' devices. The TOE determines these certificates from the access list associated with the root node that will contain the previously encrypted file. All encryption certificates are validated by the TOE before usage.
Secure channels to other trusted IT products	The TOE connects to the IDP via TLS v1.2. In any case a mutually authenticated TLS handshake takes place. Hence, the channel is established with authentication of both end points. The secure channel to the Bdrive Server is inherited from the secure channel between TOE and IDP.
Certificate Validation	The TOE performs a certificate path validation of authorized encryption certificates before usage for key encryption. The path validation traces the certificates' issuer up to a self-signed root CA that is known a priori and shipped with the TOE. Additionally the revocation status of all encryption certificates is checked via OCSP.

Table 1: TOE Security Functionalities

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

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.3, 3.4 and 3.5.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification

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

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

BDrive Windows Client, Version 3.50.89.4

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	TOE (file name: Bdrive-3.50.89.4-win64-signed.exe) Hash: 27bc09450ccf94225b15ec7622a17a12a27fa0064b9ca4a7bc931541a8df25d6	3.50.89.4	Download from Service portal
2	DOC	Bdrive user's guide [8] (file name: Bdrive_Nutzerhandbuch_Release_3_50.pdf) Hash: fbcac6a252eb7af54a952ae841d83b4f1e18db19c183a8c5cd01d4ddfc18e180	3.50	Download from Service portal
3	DOC	Operating manual for Bdrive [9] (file name: Betriebshandbuch-Bdrive-v-1.1.pdf) Hash: 611a1324c2a947d4d58c532d20838b968c9f16842ba52797bdeede3164d04707	1.1	Download from Service portal
4	DOC	User interface reference document [10] (file name: UI-Reference-Bdrive.pdf) Hash: 8e6eb91d8662d8f8550cac804428ba51265961d26de5e0921f85cc512b754a83	1.0	Download from Service portal

Table 2: Deliverables of the TOE

2.1. Overview of the delivery procedure

The TOE is composed solely of the software installer. The TOE and its deliverables are delivered via a secure download from the service portal[7] of the Bundesdruckerei GmbH.

2.2. Identification of TOE by the customer

When the TOE is downloaded from the service portal of the Bundesdruckerei, the customer can ensure the validity and integrity of the software part with the code signature of the windows installer (official Microsoft code signing certificate of the Bundesdruckerei). Additionally, the customer can calculate the hash value of the installer binary and check whether it matches the hash value specified in the Security Target ([6], chapter 1.4.3]). The

[7] https://support.bundesdruckerei.de/support

detailed description how to identify the correct version can be found in [8, chapter 1.1]. The acceptance procedure reflects the steps the customer has to perform in order to accept the delivered TOE. The provided information is sufficient to make sure that the delivered TOE is the complete evaluated instance and to detect modification/masquerading of the delivered TOE.

3. Security Policy

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

- Cryptographic Support,
- User Data Protection,
- Identification and Authentication,
- Security Management,
- TOE Access, and
- 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.Installation:** All software components of the Bdrive system shall be properly installed according the user guidance documentation.
- **OE.Credentials:** Measures shall be taken to ensure that all authorized users protect their credentials in a way that they may not be disclosed to other individuals.
- **OE.Malware:** The Bdrive Client workstation shall be free from untrusted soft- and hardware which may prevent the operating system, the other software or the hardware from its intended behav-iour.
- **OE.Admin:** Administrators shall be trustworthy and well-trained in order to be aware of security risks and respective measures to protect the installations against such security risks.
- **OE.User:** Authorized users shall not actively or negligently compromise the security of the work-station on which the TOE is installed.
- **OE.Physical:** The workstation on which the TOE is installed shall not fall under temporary undetected physical control of an attacker.
- **OE.TrustedBackend:** The backend infrastructure required by the TOE shall be sufficiently protected against attackers by physical and logical security measures.
- **OE.Masterkey:** The company that uses the Bdrive system shall have measures in place in order to protect the confidentiality of the private part of the Company Masterkey and the integrity of the public part, e.g. a four-eyes-principle for access to this key.

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

5. Architectural Information

Based on the evaluation evidence described in the CC assurance family entitled TOE design (ADV_TDS) the TOE consists of 7 subsystems:

- User Interface: User-facing component providing ordinary graphical application windows, desktop notifications, both taskbar and system tray icons. Furthermore offers a convenient file explorer integration with sync status overlays and context menu entries.
- Device Authorization: Implements workflows for initial device creation and activation as well as login. Furthermore manages the system device state (e.g. LOGGED_IN, WAITING_FOR_ACTIVATION,…) as well as appropriate authorization credentials for those states.
- Public Sharing: Public resources are a means to interact with 3rd party users that do not own a Bdrive account. It allows users to either share files via a link which can be protected by password or smsTAN authorization. Also requesting files from 3rd party users is supported. This subsystem is outside the scope of this evaluation.
- Synchronization: The central file synchronization subsystem. It reacts on both file system and remote updates and keeps the local and remote states in sync. This includes adaptions for various target platforms (e.g. Windows) and might imply solving file-system level conflicts it furthermore manages data access lists for all service specific resources and takes care of enrolling or removing users and/or devices. Note that file content processing is done elsewhere, this component merely schedules the required synchronization operations.
- Cryptography: This subsystem provides all basic cryptographic primitives to other components of the desktop client. Apart from interfaces to fundamental cryptographic algorithms it provides a secure random number generator along with facilities for entropy collection and takes care of X.509 certificate handling, including validation. For collecting entropy, this component maintains taps into other system components to draw entropy from various events triggered by external actions.
- Data & File Management: The data management subsystem provides the functionality for data up- and download as well as the required data processing (i.e. erasure encoding, symmetric encryption and blockwise data handling). Other parts of the system use this component to transfer their payload data (e.g. only the file content without further meta-data) in and out of the cloud.
- Networking: The networking subsystem provides higher level interface to the network and encapsulates all necessary networking functionality. This includes access to the Bdrive server, the Identity Provider, al cloud storage providers and OCSP. Note that the contained TLS implementation is fully transparent for all other components.

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

7.1. Developer's Test according to ATE_FUN

TOE test configurations:

The security Target [6] has identified solely one configuration of the TOE which is running on two different operating systems (Windows 7 and Windows 10) under evaluation. This configuration is achieved by a strict adherence of the Guidance Documentation part [8] and [9]. The TOE is a pure software client. The developer's tests were performed with the TOE in its one configuration on both operating systems (Windows 7 and Windows 10).

Testing approach:

- Tests cover the TSFI and their behavioural aspects by testing each TSFI with its actions.
- Tests considering the different roles (unknown User and authenticated User).
- Positive and negative tests are executed.

Testing results:

- The developer's testing effort has been proven sufficient to demonstrate that the TSFIs perform as expected.

All test cases in each test scenario were run successfully on the TOE and they all PASSED according to their expected result.

7.2. Evaluator Tests according to ATE_IND

The following subsections describe the evaluator test concept according to ATE_IND.

Subset size is chosen:

The subset contains tests from every functionality and every TSFI that is tested by the developer. It contains automatic and manual tests. The evaluator also checked that all tests were performed by the developer. As the same tests can be used for all three operating systems and the same TOE behaviour and therefore the same test results are expected for all three operating systems, the evaluator decided to test only on Windows 10[8].

Verdict for the activity:

- During the evaluator's testing the TOE operated as specified.
- The evaluator verified the developer's test results by executing a subset of the developer's tests stated in the test documentation. Therefore, the TOE passed the evaluators testing. Altogether the tests confirm the TOE functionality as described in the developer documents.

Therefore, the TOE passed the evaluators testing. Altogether the tests confirm the TOE functionality as described in the developer documents.

[8] This is done because, the same TOE in the solely one existing configuration is used for all three different systems. The TOE uses some functionality of the underlying OS, like the Folder structure, which is the same for all three operating systems. Additionally the tests do not check the exact visual layout of the system during the functionality tests, but are based on the component trays behind the visual layout of the OS, which are the same for all three different operating systems. Therefore, the same tests can be used for all three operating systems and the same TOE behaviour and therefore the same test results are expected for all three operating systems.

7.3. Penetration Testing according to AVA_VAN

Potential vulnerabilities applicable to the TOE in its operational environment the evaluators devised the attack scenarios for penetration tests when they were of opinion, that those potential vulnerabilities could be exploited in the TOE's operational environment. While doing this, also the aspects of the security architecture description 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 evaluation body.

TOE test configuration and Test Setup:

The TOE is tested in the final operational environment and installed according to the guidance documentation. TOE parameters for testing were only set within the allowed limits as defined by the guidance. No invasive modifications of the TOE were done.

Penetration testing focus:

In general, the evaluator focused on suitable coverage of TSFI, subsystems and functionality, as well as secure operation of underlying components. In detail, the following was considered:

- Regarding the TSFI, the focus of penetration testing was put on the interfaces that are externally accessible by the user. Finally, each TSFI was included in the penetration testing.
- Regarding the tested subsystems and TOE functionality, the evaluator made sure, that each subsystem and with its potentially threatened functionality is sufficiently tested.
- Regarding security relevant hardware and software in the environment, the evaluator paid special attention to potential security issues that may derive from misuse and misconfiguration of underlying components.

Attack scenarios having been tested:

On basis of the above explain testing focus, a penetration testing set of attack scenarios has been created in order to test each potential vulnerability. This test set contains 11 penetration tests, which cover the explained testing focus.

Verdict for the sub-activity:

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

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

The TOE is the Bdrive Windows Client version 3.50.89.4. The Security Target [6] has identified one configuration of the TOE under evaluation, which can be installed on different Windows platforms. The configuration is achieved by strict adherence to the preparative guidance documentations [8] and [9].

The operational environment of the TOE in its evaluated configuration can be summarized as follows:

- Windows 7 Professional with Extended Security Updates,
- Windows 7 Enterprise with Extended Security Updates,

- Windows 10.

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 2 package including the class ASE as defined in the CC (see also part C of this report)

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: Product specific Security Target
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant EAL 2

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

9.2. Results of cryptographic assessment

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

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

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
1	Generation of symmetric cryptographic keys	Key Derivation through Extraction-then-Expansion using HMAC-SHA-256	[NIST SP 800-56C]	256 Bits	Yes
2	Generation of	RSA_PKCS1_v2_2	[RFC8017]	4096 Bits	Yes

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
	asymmetric cryptographic keys				
3	Generation of cryptographic keys for TLS	RSA schemes	[FIPS-186-4] Digital Signature Standard (DSS) Appendix B.3	2048 Bits or greater	Yes
4	Symmetric encryption and decryption of user data	AES-256 in CTR mode of operation and block size 256 bits with zero padding	AES standard as specified in [FIPS-196] and CTR mode as specified in [NIST SP SP800-38a]	256 Bits	Yes
5	Cryptographic hashing for TLS	SHA-256, SHA-384, SHA-512	[FIPS-180-4]	256 Bits, 384 Bits, 512 Bits	Yes
6	File authentication	HMAC using SHA-256	[FIPS180-4] for SHA, [RFC2104] for HMAC	256 Bits	Yes
7	Asymmetric encryption and decryption of TSF data	RSAES-OAEP with SHA-256 and MGF.1 as in PKCS#1 v2.2	[RFC8017]	4096 Bits	Yes
8	User private key encryption and decryption	PKCS#5 using PBKDF2 as key derivation function, PBES 2 as encryption scheme and PBMAC1 as message authentication scheme	[RFC2898]	256 Bits	Yes
9	Hash calculation of TSF data	SHA-256	[FIPS-180-4]	-	Yes

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
10	TLS cipher suite	TLS_ECDHE_WITH_AES_128_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_CCM, TLS_ECDHE_ECDSA_WITH_AES_256_CCM, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_DSS_WITH_AES_128_CBC_SHA256, TLS_DHE_DSS_WITH_AES_256_CBC_SHA256, TLS_DHE_DSS_WITH_AES_128_GCM_SHA256, TLS_DHE_DSS_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_256_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_128_CCM, TLS_DHE_RSA_WITH_AES_256_CCM	[RFC5289], [RFC7251], [RFC5246], [RFC5288], [RFC6655]	128 Bits, 256 Bits, 384 Bits,	Yes

Table 3: TOE cryptographic functionality

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
ETR	Evaluation Technical Report
FLR	Flaw remediation
IND	Independent testing
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility

OPE	Operational user guidance
OSP	Organisational Security Policy
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
TÜViT	TÜV Informationstechnik GmbH
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[9] 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-1106-2021, Version 1.00, 2021-03-16, Security Target Bdrive Windows Client, Bundesdruckerei GmbH

[7] Evaluation Technical Report, Version 5, 2021-04-16, TÜViT (confidential document)

[8] Bdrive Nutzerhandbuch, Version 3.5, 2020-06-26, Bundesdruckerei GmbH

[9] Betriebshandbuch Bdrive, Version 1.1, 2021-02-22, Bundesdruckerei GmbH

[10] Bdrive User Interface Reference, Version 1, 2020-06-25, Bundesdruckerei GmbH

[9] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

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