Certificate

The certification body of TÜV Informationstechnik GmbH
hereby awards this certificate to the company

Bundesdruckerei GmbH
Kommandantenstraße 18
10969 Berlin, Germany

to confirm that its IT system

BDrive v. 2.0.51.4

fulfils all requirements of the criteria

Security Qualification (SQ),
Version 10.0
Security Assurance Level SEAL-3

of TÜV Informationstechnik GmbH. The requirements are summarized in the appendix to the certificate.

The appendix is part of the certificate and consists of 7 pages.

The certificate is valid only in conjunction with the evaluation report.

Security
TÜViT®
2018 Trusted Site
Certificate ID: 9558.18
© TÜViT – TÜV NORD GROUP – www.tuvit.de

20

Certificate valid until
2020-10-31

Essen, 2018-10-30

Dr. Christoph Sutter
Head of Certification Body

TÜV Informationstechnik GmbH
Member of TÜV NORD GROUP
Langemarckstr. 20
45141 Essen, Germany
www.tuvit.de

Certification Scheme

The certification body of TÜV Informationstechnik GmbH performs its certification on the basis of the following certification scheme:

- German document: ”Zertifizierungsprogramm (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH“, version 1.0 as of 2015-08-24, TÜV Informationstechnik GmbH

Evaluation Report

- German document: “Sicherheitstechnische Qualifizierung BDrive v. 2.0.51.4” of Bundesdruckerei GmbH, version 1.5 as of 2018-10-22, TÜV Informationstechnik GmbH.

Evaluation Requirements

- German document: “Sicherheitstechnische Qualifizierung (SQ) der TÜV Informationstechnik GmbH“, version 10.0 as of 2011-03-21, TÜV Informationstechnik GmbH
- System-specific Security Requirements (see below)

The Evaluation Requirements are summarized at the end.

Evaluation Target

The target of evaluation is the IT System BDrive v. 2.0.51.4 of Bundesdruckerei GmbH.

BDrive v. 2.0.51.4 is a platform for the secure storage and transfer of confidential data. Data is broken down into fragments and distributed redundantly to different cloud provider storage systems, which are not necessarily part of the BDrive platform. The data is protected by encryption mechanisms on the client, so that the data is only available decrypted on the client.

In addition, individual folders can be shared with other BDrive participants.

It is also possible to share files via a shared link as a download for non-BDrive participants. With the Droppad function, it is possible to upload files to a user's BDrive folder. For both the Shared link and the Droppad function, it is possible to assign a password in order to restrict access to the respective function.

Detailed descriptions of the functions are included in the evaluation report.

Evaluation Result

- All applicable evaluation requirements for the security qualification with Security Assurance Level SEAL-3 of IT systems are fulfilled.
- The system-specific security requirements are fulfilled.

The recommendations of the evaluation report have to be regarded.

System-specific Security Requirements

The following system-specific security requirements are the basis of the certification and have been checked.

1 Authentication

- An initial registration or release of the user by the administrator (company Admin) is necessary for the saving and sharing of files as well as folders via the BDrive services. Exceptions are the Droppad and Shared-Link functions.
- Authentication of users and their devices is done through strong authentication mechanisms using certificates. In addition, password authentication is required every time the BDrive client is started.

2 Access Control

- Access to data, which can be shared via the shared-link function and the use of the Droppad function, can be limited in time. After the specified time has elapsed, access is no longer possible.
- Users of a company cannot access data from users of other companies. The exception is the explicit linking of companies (trusted-company function), which allows to exchange files between pre-defined companies.
- Users can share files in BDrive Folders. To do this, users can assign access permissions on their own folders to other users. Users without permission cannot access these folders.
- Data, services and functions worth protecting are protected against unauthorized access.

3 Data Security

- Files worth protecting are saved in a BDrive folder on the IT system on which the BDrive client software is installed. They are stored in unencrypted form only in this place. Before these files are transferred to external cloud storage, each file is encrypted with its own file key, integrity-protected, and then fragmented. These encrypted file fragments are stored in different, external cloud stores.
- The transfer of files worth protecting as well as access to the BDrive services is carried out via secure connections, which ensure confidentiality and integrity.

4 Cryptographic

- Cryptographic algorithms that comply with the state of the art are used for authentication, encryption and data transmission.

5 User Session Management

- The security-relevant session features used by the BDrive services are securely generated and validated to protect the confidentiality and integrity of session data.

6 Validation of Input/Output Data

- All the input and output data is validated by the web interfaces of the BDrive services before processing, so that no data that can damage the system is processed or outputted.

7 System Harding

- The components and server processes accessible from the Internet have no known exploitable vulnerabilities.
- No confidential information about the internal structure and components is disclosed by the systems and applications used.

Summary of the requirements for the Security Qualification (SQ), version 10.0

1 Technical Security Requirements

The technical security requirements must be documented, consistent and verifiable. The specification must be made in accordance with ISO / IEC 17007. In addition, technical security requirements must be derived in the framework of an individual threat and risk analysis, they must be derived from previously defined protection profiles, or they must conform to published security requirements of recognized authorities or bodies of IT security. Furthermore, they must be appropriate to the intended use of the IT product and meet applicable security demands.

2 Architecture and Design

The IT system must be structured reasonably and understandable. Its complexity must not have any impact on security. The hardening and protection measures must be adequate and effective. It must not contain any conceptual vulnerability that allows bypassing or disabling security-relevant components.

3 Operating Instructions (as of SEAL-4)

The existing control measures must be effective. The monitored events must be able to identify security incidents promptly and reliably. Administration is performed through a trusted path/channel for confidentiality and integrity. The documentation must be clear and understandable. The documentation must be known to authorized person and always be readily accessible.

4 Vulnerability Assessment and Penetration Testing

The security measures of the IT system must withstand penetration testing. It must not be possible to break or circumvent security measures. The IT system must be configured securely, must meet all of the defined technical security requirements and must not have any exploitable vulnerabilities.

5 Change Management (as of SEAL-5)

Patch management must be completely documented and suitable for the IT system. The procedure for amendments of the IT system must be clearly defined and appropriate for the IT system. Persons involved must be familiar with it and responsibilities must be clearly defined. Amendments of the IT system must not lead to a reduction of the security level achieved.

Security Assurance Level

The following table shows the applicable criteria for the security assurance level. A certificate can be issued for IT systems having successfully passed the evaluation and reaching an overall level of at least SEAL-3.

Security Assurance Level Evaluation Criteria	SEAL-1	SEAL-2	SEAL-3	SEAL-4	SEAL-5
Technical Security Requirements	X	X	X	X	X
Architecture and Design			X	X	X
Operating Instructions				X	X
Vulnerability Assessment and Penetration Testing		X	X	X	X
Change Management					X

Table: Evaluation Criteria and Security Assurance Level of IT systems