BDRIVE SECURITY
WHITEPAPER

13 June 2018

Bundesdruckerei GmbH
Kommandantenstraße 18
10969 Berlin

Contents

1. Introduction

Bdrive, Bundesdruckerei's cloud solution, allows you to share and work on data with others – both within your company as well as in exchange with partners. You remain in control of the data at all times so that neither third parties nor Bundesdruckerei as the Bdrive operator can access or manipulate your data. While developing Bdrive, Bundesdruckerei focused on both security and usability. In close co-operation with renowned research institutes working in this field, we have been able to develop a high-security cloud solution that can also be easily integrated into your company's IT systems.

As a high-security company with government tasks, we not only know about security standards, we are also experts when it comes to compliance with legal regulations in national and international business transactions. This expertise is reflected in all of our products. Bdrive fully meets all compliance requirements.

This document will provide detailed information about the security measures implemented in Bdrive and the current status of external security evaluation, so that you can decide whether or not our solution can be combined and used in conjunction with the security guidelines in place at your company.

The document is broken down as follows:

- **Bdrive cloud** – Cryptographic methods and protocols to secure the files released in Bdrive
- **Link shares and drop pads** –Cryptographic methods and protocols to secure the files sent via link shares and drop pads
- **Network security** – Safeguarding communication between all the participants, including identity management and mutual authentication
- **Platform security** – Measures to secure the Bdrive and D-Trust platforms
- **Security management** – Procedure to implement information security management systems
- **Security evaluation** – Status of security evaluation for the Bdrive system in its entirety (Bdrive client, Bdrive service, D-Trust and cloud storage services)
- **Scientific support** – Presentation of the scientific facilities involved

2. Bdrive cloud

All cryptographic methods used in Bdrive are recommended by the German Federal Office for Information Security (BSI) (see [3] and [4]). What's more, the cryptographic procedures used in Bdrive are described in a crypto concept that was developed according to BSI's specifications.

The aim is to implement end-to-end security using cryptographic methods. End-to-end security means that neither third parties nor Bundesdruckerei as the operator of Bdrive can read or manipulate your data. Bdrive only manages the keys used and the encrypted data.

The security functionalities described in this section are implemented by the Bdrive client software provided by Bdrive for the user end devices. This software is currently available for Windows OS. From summer 2018, mac OS will also be supported. Versions for iOS and Android are planned.

2.1 File encryption and authentication

Files are encrypted together with the file name and hash value on the user's device. The encryption method used is AES in counter mode with a key length of 256 bits. In order to guarantee the authenticity of the data, a checksum is generated from the encrypted data using the HMAC-Sha256 method. Keys with a length of 256 bits are also used here.

The keys used are generated on the user devices; they differ for each file and are additionally regenerated when the file is updated. A secure random number generator is used to calculate the keys (see also section 2.5). The same applies to the required initialization vectors for the counter mode used.

All Bdrive users have RSA key pairs which are used to encrypt the keys for file encryption and authentication (we use RSA-EME-OAEP here). The RSA key pairs are also generated by the Bdrive client based on the secure random number generator and have a length of 4,096 bits. RSA-EME-OAEP is a probabilistic encryption method and therefore requires random values, which are also provided by the random number generator described in section 2.5.

In order to enable not just the data owners but also persons authorized by them to access the data, the file encryption and authentication keys are also encrypted with the public RSA keys of such authorized persons.

To ensure that the keys for file encryption and authentication can in fact only be accessed by authorized persons, all public RSA keys used in Bdrive receive a certificate from a trusted certification authority (see section 5.1). This makes it possible to uniquely assign the public RSA keys to the key owner.

The AES and HMAC keys can therefore only be decrypted by those persons who have been authorized to do so by the data owners. This also means that the files can only be decrypted by these authorized persons. In other words, even Bundesdruckerei, as the operator of Bdrive, cannot access the decrypted files.

2.2 Data availability

When only one cloud storage service is used, this can result in a loss of availability if the service fails. To ensure a very high level of availability, Bdrive uses several independent cloud storage services to provide your data.

The encrypted data together with the checksum are divided into several fragments using an erasure coding procedure, so that only a few fragments are sufficient for recovery. For example, four fragments can be created so that only two fragments are needed to reconstruct the encrypted file including the checksum.

The fragments generated are uploaded to independent cloud storage services. If one (or more) of these services fails, the file can be restored despite the missing fragments. The number of generated fragments can be adjusted depending on the availability requirements.

Simply providing availability of the encrypted file fragments is not enough. If, for instance, the key pair used to encrypt and decrypt the symmetric keys is lost, the corresponding data can no longer be decrypted. In order to meet with the availability requirements, each participating company generates a key pair and also has the public key certified, just like in the case of regular user key

pairs. The respective symmetric keys for encrypting the data of the employees of the company are also encrypted with the company's public master key.

These private keys must be protected accordingly. We recommend the use of Shamir's secret sharing method to transfer key parts to four persons, two of whom can assemble the company's secret master key (four-eyes' principle). The four key parts should be stored securely on external memory areas (e.g. USB sticks).

In addition, the availability of metadata must also be guaranteed (see section 2.3).

2.3 Securing the file metadata

To ensure file management on the part of Bdrive, information about the file fragments is stored centrally in Bdrive. This information, also called metadata, is generated on the user devices and consists of:

- Size in bytes (source file, encrypted file, fragments)
- Local folder structure via folder and file IDs
- Timestamps
- The Sha256 checksum of the encrypted file fragments
- Erasure coding parameters
- Storage coordinates in the cloud storage services
- Encrypted symmetric keys (for all authorized users) with corresponding user IDs
- Initialization vector

The metadata does not contain any information about the content of the file (neither the name of the file nor the names of the folders and subfolders from which it might be possible to draw conclusions about the file content). Folder and file IDs are values that are assigned randomly when the file is created. User IDs are assigned during registration for the Bdrive service and uniquely identify users.

Once the metadata has been generated on the user devices, this metadata is TLS-secured (mutual authentication always takes place, see also section 5.2) and uploaded to the secure environment of the Bdrive service where they are encrypted and stored with secured integrity in databases. Two redundant databases are used to ensure data availability. The contents of the databases are additionally saved daily on independent storage media.

2.4 Secure key deletion and storage

Volatile keys, such as the symmetric keys required to encrypt the files, their names and hash values, are deleted immediately after use in the Bdrive client. The same applies to the secret parameters and keys used to establish the TLS connection.
However, non-volatile secrets must be stored securely in the Bdrive client. These are:

- The internal state of the deterministic random number generator

- The private key of the RSA key pair for encrypting and decrypting the symmetric keys (see section 2.1)

- The private key of the RSA key pair for user authentication[1] (see section 5.3)

Secure storage (i.e. encrypted and with secured integrity) of these secrets is based on a password. When authentication certificates are used, users must assign a device password in order to use the Bdrive client. When the GoID card is used, the password consists of two parts: Part of the password is stored on the user's device. The second part is stored securely in the Bdrive service and transferred to the Bdrive client via the established TLS connection after the users have successfully registered.

Password-Based Encryption Scheme 2 (PBEC2) is used to encrypt these secrets and password-based MAC 1 (PBMAC1) is used to authenticate the keys (see [6]). In both cases, a key with a length of 256 bits is first derived from the password and a salt using a so-called key derivation function (we also use PBKDF2 from [6]). We use 100,000 iterations to derive the key within the key derivation function. This makes brute force attacks on the device password virtually impossible.

The salts are different (i.e. different salts for generating the encryption keys and the authentication keys), they have a length of 100 bits and are randomly selected (once) by the random number generator described in section 2.5.

2.5 Random number generators

The security of the cryptographic procedures and protocols used depends to a large extent on the entropy (simply put, on the unpredictability) of the keys used and the other cryptographic parameters. Bdrive uses random number generators to generate these values, which are recommended by official bodies such as the Federal Office for Information Security (BSI) and the National Institute for Standard and Technology (NIST) for use in highly sensitive areas.

The required random values are generated using the deterministic random number generator (DRNG) HMAC-DRNG from [7]. The HMAC function is based on Sha256. DRNGs require a so-called seed from which they can calculate random values. In order to obtain a high entropy of the output random values, this seed must also have a high entropy.

The Bdrive client uses different values to generate the seed: user interactions (e.g. times during various actions and between keyboard strokes, mouse positions, system states, network traffic, etc.). The quality of these random values is proven in the external security evaluation.

The Bdrive service uses a physical random number generator to generate the seeds, which BSI has analysed and certified with regard to security for this purpose.

[1] Bdrive also allows the GoID Card issued by Bundesdruckerei to be used for authentication in relation to Bdrive. In this case, no authentication certificates are required.

3. Link shares and drop pads

In addition to exchanging files within companies and between their employees who use our service, Bdrive can also be used to share files in a secure manner with employees of companies that are not registered with Bdrive by sending them via link shares or receiving them via drop pads.

3.1 Link shares

Link shares can be used to securely transfer files to employees whose companies are not registered with Bdrive. To do this, a password must first be selected from which an encryption key and an authentication key are derived.

The file is then encrypted and authenticated with these keys and the encrypted file is securely stored in the Bdrive cloud together with an initialization vector, the checksum and a salt value. The recipients of the file receive a link which they can use to download this data. The connection between the browser and the Bdrive cloud is TLS-secured. Using the password, the file can then be decrypted and its authenticity checked. The decryption and verification of authentication take place completely in the browser.

We also use AES in counter mode here for encryption and HMAC-Sha256 for data authentication. Both keys have a length of 256 bits and are derived from the selected password with additional salt using the key derivation function PBKDF2 from [6]. In order to practically prevent brute force attacks, we use 100,000 iterations within the key derivation function. All the required random values (initialization vector and the two salt values) are generated with the random number generator described in section 2.5.

The password can be transmitted via a secure channel (e.g. secure instant messengers such as Telegram or Signal).

3.2 Drop pads

Drop pads are another functionality which users of companies not registered with Bdrive can also use to securely transfer data to Bdrive customers. For this purpose, the files are secured on the basis of the encryption certificates issued to Bdrive customers.

Two keys (for file encryption and authentication) and the initialization vector for encryption are generated in the user's browser. Both keys are encrypted with the public key contained in the encryption certificate and all the data (encrypted file, checksum, encrypted key and initialization vector) is securely uploaded to the Bdrive cloud. The file then appears in the Bdrive customers' drop pad folder.

The file is encrypted and authenticated again using AES in counter mode and HMAC Sha256. To encrypt the two required keys we use the asymmetric encryption method RSA-EME-OAEP, as already described in section 2.1.

4. Network security

Secure implementation of the Bdrive service not only requires securing the individual systems, such as the Bdrive client, the Bdrive service, certification service provider and cloud services, but especially requires securing communication between the individual systems. Besides encrypting communication via TLS, this also means authenticating the communication partners.

4.1 Identity management

The basis for the secure exchange of data is that the communication partners must always be certain about who they are sharing the data with. To implement this requirement in Bdrive, all users receive authentication and encryption certificates. In addition to the user public keys, the certificates also contain the name, the company, the user ID and the issuing Certification Authority.

Authentication certificates are used for authentication in relation to Bdrive (see also section 5.3). Encryption certificates are used to encrypt the symmetric keys for file encryption and authentication for people who are to be permitted to access these files (see section 2.1).

High security requirements must therefore be met when these certificates are issued. All certificates are issued by D-Trust, an established and secure certification service provider (see also section 8.3). To ensure that the certificates can also be assigned to users, they must be clearly identified during the issuing process. This task is assumed by the respective company where the users are employed.

4.2 Secure communication channels

In order to implement the protection goals of confidentiality and authenticity during the transmission of metadata between users and Bdrive, the transmission is secured by Transport Layer Security (TLS). The data is therefore both encrypted and authenticated. The cipher suite DHE_RSA_WITH_AES_256_CBC_SHA256 is used here.

Both communication partners must authenticate themselves when the TLS connection is established. Bdrive authenticates itself to users via server authentication certificates which are also issued by D-Trust. Users have several ways to authenticate themselves to Bdrive (see section 5.3).

4.3 User authentication

Bdrive authenticates itself to users by means of server authentication certificates. There are currently two ways for users to authenticate themselves to Bdrive:

1. Using the authentication certificate issued

2. Using the GoID Card issued by Bundesdruckerei

Companies can decide for themselves which authentication procedure they want to use for the Bdrive service and can then adapt the procedure chosen to their required security level.

5. Platform security

Bdrive processes the metadata of the file fragments. No conclusions can be drawn from this data regarding the file contents, however, it shows which users are working together on files. This information must therefore be protected in terms of confidentiality. What's more, the platform must also ensure that any attempt to manipulate (protection goal: authenticity) or delete (protection goal: availability) the metadata does not go unnoticed.

Identity management is another important element of Bdrive. Users must be certain at all times about who they are exchanging their data with. This is why the D-Trust certification service provider's platform has the protection required to prevent attackers from forging authentication and encryption certificates by intruding the system.

5.1 Intrusion detection and prevention

Bdrive and D-Trust use virus scanners and firewalls from various providers to protect themselves against external attacks. Virus signatures and configurations are regularly updated and adapted to the current security situation.

These measures alone are not enough to protect the platform. This means, for instance, that so-called zero-day exploits (security holes that were previously unknown) cannot be detected. In order to be able to react to current attacks, we have implemented various intrusion detection and intrusion prevention systems on all platforms which can detect attacks via anomaly detection and initiate appropriate countermeasures.

What's more, all activities are recorded and stored and regularly checked for anomalies by our security experts using established tools, so that system security can also be checked manually.

5.2 Software quality and penetration test

When developing software, we attach great importance to its quality in order to minimize security gaps that result from software errors. Our software undergoes several quality assurance tests before it can be used in the existing system.
We attach particular importance to the prevention of attacks with code injection. All input fields are clearly specified and are only processed further by the system if the contents correspond to the specification. In this way, we can prevent malware from being imported into the system via these input fields and endangering security.
But even with extensive tests and clear specifications, errors cannot be fully ruled out. That's why we have regular penetration tests carried out in order to be able to detect and eliminate security gaps at an early stage.

5.3 Hosting

All the required IT components (servers, databases) are located in specially secured areas within D-Trust. Only Bdrive administrators can access these premises according to the four-eyes principle, i.e. two administrators must authenticate themselves at the secured doors using personalized chip cards and a PIN in order to gain access. Every access is logged in an auditable form and regularly analysed by the Bdrive security team.

The premises (doors and windows) are fitted with alarm systems so that break-ins are detected at all times and reported to the responsible security team.

6. Security management

In addition to the use of cryptographic algorithms to secure the data, other technical, organizational and personnel measures must also be implemented to ensure secure operation of Bdrive.
The necessary security measures are not only developed and implemented by our competent staff with the support of renowned research institutions, but are also evaluated externally with a view to completeness and effectiveness (see section 7).

The necessary security measures to be implemented are developed on the basis of established procedure models. Besides the implementation of the latest security measures, these also include activities for maintaining ongoing operations (e.g. emergency management, procedures in the event of security incidents and adjustments to the measures with regard to the current security situation).

6.1 Security team

Our security team is made up of one information security officer and several security experts. In addition to developing personnel, organizational, technical and infrastructural security measures, the security team's tasks also include implementing these measures and maintaining them during ongoing operations. This requires not only regular training of all employees, but also adjustments to the current security situation and responding to any security incidents that may occur.

The security of Bdrive is constantly being improved. We are supported by renowned research institutions, such as the Hasso Plattner Institute of the University of Potsdam and the ID Management Group of Freie Universität Berlin.

6.2 Background checks on employees

Before being hired, all employees are thoroughly examined with a view to their qualifications for the tasks which they are to assume. We check their training and previous employment on the basis of training certificates and job references. Employees who are to be deployed to highly sensitive areas must also present a police clearance certificate.

6.3 Security training courses

Bundesdruckerei regularly conducts security training courses to raise awareness for IT security and data protection. Training is not only mandatory for technical staff (e.g. system administrators and developers), but also for administrative staff and is adapted to the respective target groups. The training courses cover all relevant topics of IT security and data protection, current threats, attackers' actions (including social engineering), consequences of successful attacks and methods to minimize risks.

We also invite renowned researchers to our annual Campus Week to present the latest topics from their work and to discuss their results with us. This gives us an insight into innovative technologies so that we can continuously improve our own solution.

6.4 Vulnerability and security incident management

Software can have errors. Some of these errors can also lead to security holes. The same applies to all security measures implemented, be it of a personnel, organizational, technical or infrastructural nature. Despite evaluating these security measures, security holes may arise that were not identified during evaluation.

Our security team therefore regularly checks the effectiveness of the measures implemented, also by simulating our own attacks (hacking, but also phishing attacks, for instance), thus testing the effectiveness of our security measures and security training.

If security holes become apparent, e.g. through our own observations or from actual attacks, we are prepared to deal with this. Our security team has already run through possible attack scenarios and has prepared appropriate countermeasures. These can range from short-term shutdown of security-critical services to shutting down Bdrive until security is restored.

We also regularly monitor the current security situation and collect information, e.g. from the Computer Emergency Response Team of the Federal Office for Information Security, about current security gaps and attacks so that we can then initiate appropriate countermeasures.

7. Security evaluation

All components of the Bdrive infrastructure have been evaluated and certified according to established process models. In addition to checking whether appropriate security measures have been implemented for all security risks, we also examine how effective these measures are (i.e. whether they suitably minimize risks). This evaluation looks at both the current status of implementation and at whether it is possible to respond appropriately to security incidents or current developments with regard to attacks.

7.1 Bdrive client

The Bdrive client is software that is needed to use Bdrive. This software implements essential security functions, such as key generation, encryption and decryption, file authentication, etc. For this purpose, we are aiming for certification according to Common Criteria EAL 4.
EAL stands for Evaluation Assurance Level, i.e. the implemented trust level. EAL 4 means that the app is methodically developed, tested and reviewed and is thus highly likely to fulfil the claimed security functionality.

7.2 Bdrive service

Bundesdruckerei is aiming for certification according to SEAL-3 (Security Assurance Level 3) for the entire Bdrive system. Certification is planned to be completed by the end of 2018 and will then be repeated regularly for new releases.

This certification is carried out by TÜV Informationstechnik GmbH.

7.3 Certification service provider

The certificates used in Bdrive are the security anchor for secure data exchange. All certificates are issued by certification service provider D-Trust. D-Trust is a wholly-owned subsidiary of Bundesdruckerei and has been established in this field for many years. D-Trust issues advanced and qualified certificates in accordance with the German Act on Digital Signature. For this purpose,

the security of all the processes for issuing certificates is evaluated and the evaluation is confirmed by the Federal Network Agency on the basis of a BSI certificate.

7.4 Cloud services

Bdrive works exclusively with independent and ISO-certified cloud storage providers whose data centres are operated in Germany. This means that the data (or better, the encrypted and authenticated data fragments) is (are) stored exclusively on German servers.

8. Scientific assistance

Bdrive is being continuously further developed and tested with a view to security. In this context, we have the support of two renowned research institutions, i.e. the ID Management Group at Freie Universität Berlin under the direction of Prof. Dr. Margraf and the Hasso Plattner Institute of the University of Potsdam under the direction of Prof. Dr. Meinel.

8.1 ID Management Group at Freie Universität Berlin

The ID Management Group at Freie Universität Berlin is working on the design, creation and evaluation of usable and secure software and IT systems. The main research topics of the working group are: physical unclonable functions, cryptanalysis, usable security, IT security management, security management as a service.

8.2 Hasso Plattner Institute

The Hasso Plattner Institute (HPI) is unique in the German university landscape: It offers a unique practice and innovation-based course in IT Systems Engineering that ends with a Bachelor or Master of Science, as well as an additional course in the Design Thinking innovation methodology. Organized as an independent Digital Engineering Faculty of the University of Potsdam, HPI combines excellent research and teaching, as well as the advantages of a privately financed institute and free studies.

Glossary

AES: Symmetric encryption algorithm used in Bdrive to encrypt files and metadata
Authentication certificate: Certificate issued by a CA that is linked to an asymmetric key pair for authentication

Bdrive cloud: The infrastructure used in Bdrive for secure storage of files and metadata

Bdrive client: Software that a company administrator or a Bdrive user installs on a device in order to use this as a client-side interface to the Bdrive service.

Bdrive customer: Company that has entered into an agreement to use the Bdrive service

Bdrive user: Employee of a Bdrive customer who uses the Bdrive service and has registered with the service for this purpose

Certification Authority (CA): Trusted body that issues certificates that can be used to check the link between cryptographic keys and key owner

Drop pads: Encrypted files that can be transmitted to Bdrive customers by employees of companies that are not signed up to Bdrive

GoID Card: Proof of identity issued by Bundesdruckerei for employees of a company that allows the card holder to be identified with certainty

Link shares: Encrypted files that can be transmitted by Bdrive customers also to employees of companies that are not signed up to Bdrive

MAC/HMAC: Method for authenticating data

The German ID card: Proof of identity for German citizens which allows the holder to be identified more securely and which can be used for online services (use of the online ID function)

RSA: Asymmetric encryption method with which symmetric encryption and authentication keys are encrypted in Bdrive

Transport Layer Security (TLS): Hybrid encryption protocol for secure data transmission on the Internet

Encryption certificate: Certificate issued by a CA and linked to an asymmetric key pair for encrypting data

Certificate: A digital data record that confirms certain features of a person or object and whose authenticity and integrity can be verified using cryptographic methods.

References

[1] T. Bray: The JavaScript Object Notation (JSON) Data Interchange Format, Request for Comments (RFC): 7159.

[2] BSI: IT Baseline Protection catalogues, Federal Office for Information Security.

[3] BSI: TR 02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2016-01, 15. February 2016, Federal Office for Information Security.

[4] BSI: TR 02102-2, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 - Verwendung von Transport Layer Security (TLS), Version 2016-01, Federal Office for Information Security.

[5] D. Hardt: The OAuth 2.0 Authorization Framework, Internet Engineering Task Force (IETF), Request for Comments (RFC): 6749

[6] B. Kaliski: PKCS#5: Password-Based Cryptography Specification Version 2.0, Request for Comments (RFC): 2898.

[7] NIST: Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 01/2012

[8] FIPS: Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, 2013.