DriveLock 2022.1

3/30/2022

Table of Contents

Part I

About this documentation

1 About this documentation

This documentation explains how you as the end user can work with DriveLock in an enterprise environment and with the portable version Mobile Encryption Application to be started from an mobile storage media or the personal versions of DriveLock which can be installed without central administration on a personal PC.

1.1 Representation conventions

In this document the following conventions and symbols are used to highlight important aspects or visualize objects.

Caution: Red text indicates hazards that could possibly cause data loss

> Notices and tips contain useful information.

Menu Items or the names of **buttons** are displayed in bold.

Part II

Data encryption with DriveLock

2 Data encryption with DriveLock

With DriveLock you can encrypt your data. Encrypting means altering the data in such a way that it is no longer readable with common means, and can only be made readable again with the appropriate key.

You can perform a data encryption with DriveLock on various levels:

Encryption of folders

If you encrypt a folder, all files contained therein are automatically encrypted as well. The file name, for example, **Geheimvertrag.docx**, the file size and date will continue to be visible and readable. The file can be opened in its native application, such as Microsoft Word, but without the respective authorization the content, however, will be displayed in form of a non-readable text.

Encryption of containers

A container is a large encrypted file in which you can hide other files and directories. If you use a container for the encryption, you must define the size of this container and encrypt it. Any files that you subsequently save in this container are also encrypted. In contrast to the folder encryption it is not visible from the outside, how many and which directories and files are contained in this container. The free space in this container is also encrypted.

On the outside, the container appears as a large file with the extension **.dlv** . The container file can be saved to all types of storage media such as a USB stick or hard drive and onto a network share.

For you to be able to use the container DriveLock will connect (map) it with a predefined or free drive letter, enabling you to use the container with the Windows Explorer just like any other drive.

Protection through passwords or certificates

Access to encrypted files and containers is protected by various methods, such as passwords or certificates. If you forget a password, the recovery mechanism of DriveLock will ensure that your data won't be lost. For more information on this topic, contact your administrator.

> Encryption of containers and the usage of certificates are not part of the personal versions DriveLock Private und DriveLock Business.

2.1 Encryption Methods

Encryption Methods

- **AES** - The Advanced Encryption Standard (AES) is a symmetric cryptosystem and the successor of the DES or respectively 3DES, which was announced as the standard in October 2000 by the National Institute of Standards and Technology (NIST). Named after its developers Joan Daemen and Vincent Rijmen it is also referred to as Rijndael algorithm.
  DriveLock uses a 256-bit key (AES-256), which is considered sufficient also for top secret information (U.S. CNSS (Committee on National Security Systems)).
- **Triple DES** - Symmetric encryption method which is based on the classic DES, but utilizes double the key length (112 bit). The data is encrypted with a triple combination of the classic DES. Due to the key length Triple-DES is currently still regarded as a safe procedure in contrast to the simple DES, which is vulnerable to brute-force attacks (the mere tasting of keys).

- **Blowfish** - This very fast *algorithm* delivers a very good performance especially with 32-bit processors. One advantage of Blowfish is its variable *key length* from 32 to 448 bits. Blowfish is considered to be very safe. The algorithm was first introduced in 1994.

- **Twofish** Twofish is the AES contribution from Bruce Schneier's company Counterpane Systems. The algorithm uses a block size of 128 bits and can be operated with keys from 128 to 256 bits. Twofish is very fast. On a Pentium processor a single byte is encrypted in 18 CPU cycles. Twofish has been tested very intensively and no weaknesses have been found to date.

- **CAST 5** - CAST is a symmetric block cipher with a 64-bit block length and a key length from 40 to 128 bits. The CAST algorithm was named after its developers, **C**arlisle **A**dams und **S**tafford **T**and a patent was filed in 1996. Because of its higher speed compared to DES, CAST is also suitable for real-time applications. Key lengths from 80 to 128 bits are referred to as CAST-5.

- **Serpent** - is a symmetric encryption algorithm that was developed by the cryptographers Ross Anderson, Eli Biham and Lars Knudsen. This algorithm was a candidate for the Advanced Encryption Standard and was one of the five finalists of the AES Standard elimination procedure along with Twofish, Rijndael, MARS and RC6. Unlike the other two candidates MARS and Twofish that were classified as highly secure in the last round, Serpent was not criticized regarding its security and it was assumed that this was the most secure encryption algorithm of the five finalists.

Password encryption (hash algorithm)

DriveLock encrypts the password with which the encrypted drive is encrypted or decrypted using a hash algorithm. DriveLock supports the following encryption methods:

- **SHA** - The NIST (National Institute of Standards and Technology) in collaboration with the NSA (National Security Agency) developed a hash function which was intended for signing, as a part of the Digital Signature Algorithm (DSA) for the Digital Signature Standard (DSS). The function was published in 1994. The standard which is known as Secure Hash Standard (SHS) specifies the secure hash algorithm (SHA) which has a hash value of 160 bits in length, for messages with a size of up to 264 bits. The algorithm is similar to the MD4 which was developed by Ronald L. Rivest. The secure hash algorithm primarily exists in two versions, SHA-0 and SHA-1, which differ in the number of cycles performed when the hash value is generated. In August 2002 the NIST published, three additional versions ("SHA-2") of the algorithm to generate the larger hash values. These are SHA-256, SHA-384 and SHA-512 whereas the appended number indicates the length of the hash value (in bits).

- **RIPEMD-160** - RIPEMD-160 was developed in Europe by Hans Dobbertin, Antoon Bosselaers und Bart Preneel and first published in 1996. This is an improved version of RIPEMD, which in turn is based on the design principles of the MD4 and in terms of strength and performance matches the more popular SHA-1. Since the development of RIPEMD-160 was more open than that of SHA-1, it is more likely that this algorithm will show fewer vulnerabilities.

- **WHIRLPOOL** – WHIRLPOOL is a cryptographic hash function designed by Vincent Rijmen and Paulo S. L. M. Barreto. It was named after the Whirlpool galaxy in the constellation of Canes Venatici. Whirlpool is one of the cryptographic algorithms recommended by the NESSIE project and has been standardized by the ISO with ISO / IEC 10118-3:2004.

For environments with special security requirements, the FIPS algorithms can be used which are included in DriveLock. The Federal Information Processing Standard (in short FIPS) is the name for publicly announced standards of the United States. These standards are based on modifications of the commonly used standards that are established by ANSI, IEEE, ISO, and similar organizations. In the field of cryptography the FIPS 140-2 is especially well known (security requirements for cryptographic modules).

Part III

Operating DriveLock

3 Operating DriveLock

DriveLock is a software solution for protecting client computers. Computers on which DriveLock is installed can be configured centrally, so that a uniform data protection concept can be implemented within a company.

> In an enterprise environment DriveLock is configured by an administrator in your company. Depending on the settings he performed, some of the functions presented here may not be available at all or with a slightly different functionality. For details, please contact your administrator if necessary.
> The portable and personal versions of DriveLock you can use to en-/decrypt files in folders and/or containers. The functions you can use and the amount of data you can encrypt depends on your license.

Data encryption

Data encryption with DriveLock offers various possibilities to protect data from unauthorized access: You can encrypt entire folders as well as the files contained therein or create an encrypted container. You can encrypt the data with a password or a personal certificate.

For more information on this, see Data encryption.

Device Control

DriveLock offers a configurable access control for drives such as floppy disks or CD-ROM drives as well as USB sticks. In addition, it controls external media such as devices connected via Bluetooth or mobile devices such as Palm, Blackberry and smartphones. Your administrator has specified who is allowed to use which device at what time.

Secure deletion

With DriveLock you can delete files and folders so that a subsequent recovery of this data is not possible.

3.1 Starting and ending DriveLock

In general, your administrator will have installed DriveLock in such a way, that the program will start automatically whenever you restart your computer.

If this is not the case, or if you closed DriveLock manually, you can start it again.

To start DriveLock:

1. Open the Windows Start menu.
2. Find the entry for DriveLock and click on it.. The position and the exact name of the entry depend on the settings of your organization. Ask your Administrator for details.

> Alternatively, an icon can also be present on your desktop.

To terminate DriveLock:

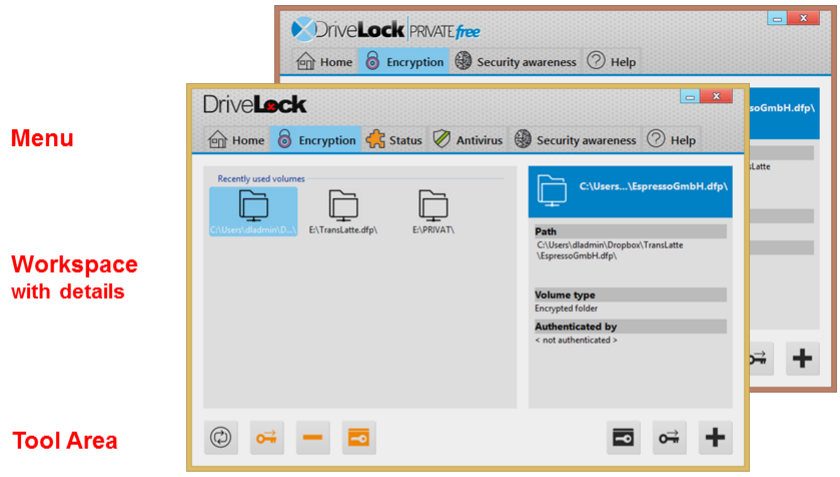
Click on the red cross in the top right of the program window (Windows default).

3.2 The interface

The DriveLockinterface is divided into the following areas:

- The *Menu* contains icons with which you can control the individual functions.
- In the *Workspace* in the middle, you can execute the tasks.

- The *Tool Area* contains functions that allow you to, for example, create your certificate or to manage folders.



3.2.1 The Navigation Pane

Depending on your version and license you will find the following menus:

Home

DriveLock overview display

Request temporary authorization

Manage network profiles

Language selection

Encryption

Create containers

Encrypt folders

Certificate management

DriveLock status

DriveLock status display

Help

Online Help

3.2.2 Buttons

Buttons

The following buttons can be found in the different menus:

OK

Confirms actions, stores the data and returns to the previous window.

Abort

Returns to the previous window without saving.

Back

Returns to the previous window. For windows without changing options, for example, the display of the device status.

Refresh

Refreshes the display. There are also symbols, where the arrows occur in conjunction with a different character.

Delete

Deletes a file or object, such as an infected file in DriveLock Antivirus.

3.2.3 Context Menu

Alternatively to the operation via buttons you can also use the context menu. You can access the context menu by clicking the right mouse button on an icon in the workspace.

You will see the functions that can be performed for that element.

With the left mouse button, click on a menu item to select it.

Context menu in the Windows Explorer

The context menu in the Windows Explorer also contains functions of DriveLock. You recognize these special features with the DriveLock icon.

For folders and files this enables the function **Secure deletion** at any time. Other functions are only available in the context, for example, to disconnect a connected container.

3.2.4 Windows Start menu

Most of the functions of DriveLock can also be accessed via the Windows Start menu. You can find the functions under the DriveLock program group.

Part IV

DriveLock overview display

4 DriveLock overview display

In the main menu **Overview** you are able to see at a glance whether your computer is protected. The green icons indicate that your computer is protected and that the DriveLock Antivirus is active and up-to-date. If you see red icons, contact your administrator.

In the main menu **Overview** you can perform other common tasks:

- Request temporary authorizations
- Manage network profiles
- Language selection

4.1 Request temporary authorization

DriveLock centrally controls access to the attached removable media devices or applications via a policy. If you need access to a locked device or drive or need to run a locked program, you can apply for a temporary authorization.

Hereby it is distinguished between an online activation and an offline authorization.

Online Authorization

With an online authorization, the administrator connects to your computer through the network and authorizes the device or application you requested in accordance with the company policies. You are not required to do anything.

Offline Authorization

With an offline authorization, in case there is no active network connection between your computer and the computer of your administrator, your computer name as well as a code must be transmitted to the administrator. From these two information elements the administrator will create a response code, which he will convey to you. You can perform this process, for example, via phone or e-mail.

To request an offline authorization:

1. Open the main menu **Home** and click on the **Temporary authorization**.
   You will see a window with the name of your computer as well as a request code.
2. Convey the computer name as well as the request code to the administrator, will then generates an activation code and notify it to you.

> Click on the three dots next to the request code. A window will open that displays the code written in the phonetic aviator alphabet, which makes it easier to communicate the code via telephone. For example *YB8C* will be displayed here as “Yankee, Bravo, Alpha, Charlie”. Depending on your system settings, you can also have the text read out loud to you.

3. Enter the response code you received from your administrator in the same window.

4. You will receive a message that your computer has been authorized for a certain period of time specified by the administrator.
   You can now access the activated devices or applications, as long as the authorization is active.

5. Click on ✓ **OK** to close the window.

4.2 Managing network profiles

If you use a portable computer you can use it on different networks, for example, in the office and at home. With DriveLock you can specify a network profile for each of these workplaces, which will then always contain the configuration for every specific network. This includes IP addresses, proxy settings or printer settings.

To add a new network profile:

1. Open the main menu **Home** and click on **Network profiles**.
2. Click on + **Add network profile**.
3. Enter a name for the new network profile, and select an appropriate icon.
4. Configure the network profile. Ask your administrator for details.

To edit a network profile:

Highlight the desired network profile and click on **Properties**.

To delete a network profile:

Highlight the desired network profile and click on **Delete network profile**.

4.3 Language selection

You can set the language in which the DriveLock user interface will be displayed, if you prefer a language other than the default language.

To select a different language:

1. Open the main menu **Home** and click on **Language selection**.
2. Select the desired language and click **OK**.

Part V

Data encryption

5 Data encryption

With DriveLock you are able to encrypt your data, whether they are files in a folder or in a container. The procedure is very similar:

You create an encryption and connect the folder or container, which means that you must authenticate and are then able to access the data in the folder or container.

Foregoing considerations

If you want to encrypt the data, you should consider a few things in advance:

- What will be the better choice for my intended use, a folder or a container?
- What I want to backup data in this container? How big does the container have to be?
- How big is the storage medium onto which I want to save the container? Are there any size limitations? If you select an external drive such as a USB stick, DriveLock automatically selects an appropriate container size to optimally use the available space. You can also adjust the set value to the maximum size available yourself.
- Which encryption method do you want to use (if your system configuration allows a selection here).
- What file system is the appropriate, NTFS or FAT? For files in a container that is larger than 4 GB, you must use NTFS.
- What should the name of the drive be?

More details can be found under Data encryption.

You can perform the following tasks:

- Create containers
- Use the container as an encrypted drive
- Delete containers
- Change the password for the container
- Encrypt folders
- Use encrypted folders
- Manage users for a folder

- Managing user groups
- Recover a lost password

5.1 Creating containers

Before you create a new container, you should examine the foregoing considerations.

> It is possible that some of the settings referred to here may not be available. Your administrator then have defined a corporate policy that contains these settings.

> For external data carriers DriveLock selects a container size, which ensures that, when required, the Mobile Encryption Application can also be copied to the data carrier.

This is how you can create a new container:

1. Open the main menu **Encryption**.
2. Click on **New** and from the context menu select the option **Encrypted container**.
3. Define the new container with the help of the setup wizard:
   a. Select the location where you want to create the container: Click on the desired drive or external device. Alternatively, you can also encrypt an entire partition as a container.
   b. Set the size of the container file. DriveLock selects a container size for external data carriers, which ensures that, when required, the Mobile Encryption Application can also be copied to the data carrier.
   c. Select the appropriate file system and the cluster size.

      Depending on the file system used, a certain minimum size is required:
      FAT: 100 KB; NTFS: 3072 KB.
      Select NTFS if you wish to store files inside a container with *more* than 4 GB, since FAT only supports files up to this size.

      A cluster is a logical unit of blocks on a storage medium. Usually the file system only addresses the entire cluster, i.e. it is not possible to address individual blocks or bytes within a cluster. Therefore files always occupy a certain number of clusters. The larger the cluster size, the less administrative effort is required for large files, and the fragmentation is minimized. The disadvantage of large clusters is that they occupy space which is unused.
   d. Optionally, enter a name for the container file. This name will then appear as the drive name, when you connect to the container. It may be different from the name of the actual container file.
   e. Select the encryption method and the hash method, for this see Encryption Methods.
   f. Enter the password for the container, and then repeat the entry.
      Following characters you can be used for your password:
      Uppercase letters (A-Z)
      Lowercase letters (a-z)
      Numbers (0-9)
      Special characters (e.g. !, $, #, \ or &)
      The colored display in the password fields indicates how good your password is. A password is good if it can not be easily guessed or calculated.
      It is possible that there are additional policies within your company regarding the structure of passwords. For example, there may be a requirement that a password must always contain a special character and a number. If your password does not comply with the company policy, you will receive a message.

4. Click on **Next**. The container will be created. Depending on the size and destination drive this can take several seconds. You will receive a message after the container was created successfully. Now you are already able to connect the container as a drive.
5. Select **Connect as** and select an available drive letter.
6. Select **Do not add to history**if you only want to temporarily connect the container with this drive letter and the container should not appear in the list of already used containers.
7. Click on **Finish**.

5.2 Using the container as an encrypted drive

To store files in a container, map it as a drive. This means that the container will receive a drive letter and you can work with it in the Windows Explorer as if it were an additional drive.

> When you create a new container, you will also immediately be offered the option to map the newly created Container as a drive.

In the main menu **Encryption** you can see a list of recently-used containers. You can select from this list, or you can use a container within the file system, which does not appear in the list.

To map a container as a drive:

1. Select the container that you want to connect as a drive. You have the following options:
   - The container is already in the list of **recently used drives**: Double-click on the container.
   - The container is not in the list: Click on **Connect** and **Encrypted container**, Enter the correct path and file name, or click on **...**and locate the container file in your file system.
2. Select the appropriate drive letter.
3. Authenticate as required if necessary.
4. Select **Do not add to history**if this container should *not* should appear in the list of recently used containers.
5. Click on **Complete**. You will now see a new drive with the selected letter in your Windows Explorer. This is now the encrypted container in which you can store your files.

> The wizard for connecting containers can also be opened by double-clicking on a container file (*.dlv) in the Windows Explorer.

If you do not need the container as an encrypted drive anymore, or if you disconnect the external storage media on which the container is stored from your computer, you must also disconnect the drive.

> **Close all open files on that drive before disconnecting it. If you disconnect a drive while files are still open on that drive, for example, in Microsoft Word, a data loss will occur! DriveLock is not responsible for damaged or destroyed data, which may result from the separation of an encrypted disk without first closing the files contained therein.**

To disconnect an encrypted disk:

1. In the main menu in **Encryption** right-click on an existing mapped drive.
2. From the context menu, select **Disconnect**.

Alternatively, in the Windows Explorer you can right-click on the drive letter and from the context menu perform a **Disconnect** selection.

5.3 Deleting containers

Encrypted containers can be deleted in the Windows Explorer, by deleting the associated *.dlv file.

If the container is still connected as an encrypted drive, you must disconnect it prior to the deletion, see Using the container as an encrypted drive.

You can also delete a container file with the DriveLock feature Secure Deletion, see Secure data deletion.

5.4 Changing the password for the container

You are able to change the password for a container. This requires that the container is connected as a drive, see Using the container as an encrypted drive.

To change the password, you will need the current password.

To change the password for a container:

1. Open the Windows Explorer.
2. With the right mouse button click on the container-drive and from the context menu choose **Change Password**.
3. Enter the current and new password.

   Following characters you can be used for your password:
   Uppercase letters (A-Z)
   Lowercase letters (a-z)
   Numbers (0-9)
   Special characters (e.g. !, $, #, \ or &)
   The colored display in the password fields indicates how good your password is. A password is good if it can not be easily guessed or calculated.

   It is possible that there are additional policies within your company regarding the structure of passwords. For example, there may be a requirement that a password must always contain a special character and a number. If your password does not comply with the company policy, you will receive a message.

4. Choose one of these options, if they were authorized by your administrator:
   - **Set user password**: If the data carrier has not yet been set up for use with Mobile Encryption Application , you can create a personal password that you will require when accessing from outside the corporate network.
   - **Remove user password**: If you want to prevent a usage of the container outside the company with the help of the Mobile Encryption Application , you can remove the personal password. To perform this the user password must be known to you.
5. Save your entries.

5.5 Encrypting folders

It is possible that some of the settings referred to here may not be available. Your administrator then have defined a corporate policy that contains these settings.

To encrypt a folder:

1. Open the main menu **Encryption**.
2. Click on **New** and from the context menu select the option **Encrypted folder**.
3. Select the folder you want to encrypt.
4. Specify how you want to authenticate. The available choices depend on your system settings.
   - Username and password. This option is useful when you want to pass the encrypted folder to another person.
   - Windows User Manager
   - DriveLock File Protection user manager
   - A personal encryption certificate, see Managing certificates
5. Depending on your authentication option selection, the following steps could be different,

   If you selected a username and password, observe the instructions for the password assignment:

   Following characters you can be used for your password:
   Uppercase letters (A-Z)
   Lowercase letters (a-z)
   Numbers (0-9)
   Special characters (e.g. !, $, #, \ or &)
   The colored display in the password fields indicates how good your password is. A password is good if it can not be easily guessed or calculated.
   It is possible that there are additional policies within your company regarding the structure of passwords. For example, there may be a requirement that a password must always contain a special character and a number. If your password does not comply with the company policy, you will receive a message.
6. Click on **Complete**.

To use the folder, you need to connect it, see Using encrypted folders.

5.6 Using encrypted folders

To access an encrypted folder and its files, it must be connected. This means an authentication with the stored credentials, either with a with password or certificate. Then you can work with an encrypted folder just like with any other folder in Windows.

Encrypted folders in Windows Explorer can be identified with their small padlock on the folder icon.

To connect an encrypted folder:

1. Select the folder that you want to connect as a drive. You have the following options:
   - The folder is already in the list of **recently used drives**: Double-click on the folder.
   - The folder is not in the list: Click on **Connect** and **Encrypted folder**; specify the correct path and folder name, or click on **...**and locate the folder in your file system.
2. Authenticate as required if necessary.

3. Select **Do not add to history** if this folder should *not* appear in the list of recently used containers.
4. Click on **Complete**. You can now work with the encrypted folder as usual in the Windows Explorer.

To disconnect an encrypted folder:

1. In the main menu on **Encryption** right-click on an existing mapped drive.
2. From the context menu, select **Disconnect**.

5.7 Managing users for a folder

You are able to manage who has access to your encrypted folder. Only you as the owner of the encrypted folder can assign or revoke these permissions.

> To manage user rights, the folder must be connected, see Using encrypted folders.

To manage the users of your encrypted folder:

1. Right-click on a connected (mapped) folder.
2. From the context menu, select the option **Properties**.
3. Switch to the tab **Users**. You will see, the currently existing users. Initially, these will be yourself as well as a system user, which you might need for the recovery of access data, see Lost password recovery. For encrypted folders which are centrally managed by your DriveLock administrator, you may also add groups of users instead of single users.
4. Click on **Add**.
5. Select the type of user, meeting the type of authentication, and enter the required data.

> For the certificate user you need the public key of the new user, see Certificate publication.

6. Follow the further instructions and then click **Complete**. You will now see the new user in the list.
7. If the new user is allowed to have administrator rights for the folder, mark the appropriate field.

5.8 Managing user groups

DriveLock administrators may create centrally managed encrypted folders on a file server. To ease managing users for these folders, they also may create DriveLock File Protection Groups which can be assigned to centrally managed encrypted folders additionally to single users. If you are group administrator of a DriveLock File Protection Group, you are allowed to add additional users, to delete users and to grant or revoke group administrator rights to those users.

This is how you manage groups:

1. Open the main menu **Encryption**.
2. Click on  to open the list of groups you can manage
3. Double click a group to see and edit it's members

> DriveLock administrators only can add users, while they create the group. Once created they don't have more permissions than other users but to delete users from a group.

5.9 Lost Password Recovery

If you forget the password to access the encrypted data or the password is not available for other reasons, you have the following options:

- **Administrator password**: Contact your administrator who can then use the administrator password to reset the user password.
- **Recovery mechanism in offline mode**: If your computer is not connected to the corporate network, or you do not have access to your certificate, use the offline method. Use the assistance program to generate a request code from the encrypted file, which you must then submit to the Administrator. This can also be done over the phone. The administrator will use the request code to generate a response code with which you can assign a new password for the encrypted file.
- **Recovery mechanism in online mode**: If your computer is connected to the corporate network and you have access to your certificate and the password for the corresponding private key, use the online method. For this purpose, you must have previously exported the certificate to a *.pfx file, see Certificate Copying.

> It depends on the company specific settings, which options will be available to you.

To create a new password in the offline mode:

1. Open the main menu **Encryption**.
2. Click on  **Restore** and then either on **Encrypted container** or **Encrypted folder**.
3. Specify the location of the container file or the folder name.
4. Select the option **Offline recovery**.
5. Submit the displayed request code to your administrator.

> Click on the three dots next to the request code. A window will open that displays the code written in the phonetic aviator alphabet, which makes it easier to communicate the code via telephone. For example *YB8C* will be displayed here as “Yankee, Bravo, Alpha, Charlie”. Depending on your system settings, you can also have the text read out loud for you.

6. Enter the response code you received from your administrator to assign a new password in the following window.
7. Click on **Complete**to exit the wizard.

To create a new password in the online mode:

1. Select the option **Online recovery**.
2. Enter the path to your *.pfx certificate file as well as the associated password. Click on **Next**.
3. Alternatively, you can read a certificate from a **Smart Card** or from the **certificate storage location on this computer** .
4. Enter a new password and confirm it. Click on **Next**.
5. Click on **Complete**to exit the wizard.

5.10 Using the Mobile Encryption Application

With the help of the Mobile Encryption Application you can use files in an encrypted container or folders, even if the computer does not have DriveLock installed or you do not have administrator rights on the computer to install an application or to connect drives.

The Mobile Encryption Application can, for example, be saved to an encrypted USB flash drive thus making it usable on any computer.

> Mobile Encryption Application is available as Windows- (`DLMobile.exe`) and MAC- (`DLMobile.MAC.zip`) Application

To copy the Mobile Encryption Application to a storage medium:

1. From the Windows start menu, select Copy Mobile Encryption Application.
2. Specify the target location.
3. The program files of the Mobile Encryption Application will then be copied to the destination folder.

5.10.1 Working with the Mobile Encryption Application

The Mobile Encryption Application is a program in which you open a container in order to copy files to the container or to export files from the container. You can use this program if you do not want to connect the container as a drive or are unable to do so, for example, because you have no administrator rights on the computer.

If you execute the Mobile Encryption Application start from a storage location that also contained contains a *.dlv file Mobile Encryption Application will automatically try to open that container and immediately ask for a password. In this case, it will also be examined whether you possess local administrative rights.

How to use the Mobile Encryption Application:

1. Double-click on the program file on the data carrier, for example, `DlMobile.exe`.
2. If a *.dlv file is contained in the same folder as the executable, you can directly map the container:
   a. Enter the password.
   b. Select the drive letter to be used for the connection to the container, see Using the container as an encrypted drive.
3. If the Mobile Encryption Application does not immediately offer a container for the connection, you have the following options:
   a. **Connect container**: Select a container and map it as an encrypted drive, see Using the container as an encrypted drive.
   b. **Disconnect drive**: Disconnect a mapped drive, see Using the container as an encrypted drive.
   c. **Change language**: Change the language of the interface, see Language selection.
   d. **Open container**: Open a container on a computer on which you do not have local administrator rights. For this, select the desired *.dlv file and enter the corresponding password. You can now import and export files, see Importing and exporting files.
   e. **Lost Password Recovery**: Recover a lost password, see Recover lost password for a container.
4. Click on **Close**To close the Mobile Encryption Application .

> If you sever the connection to a removable data carrier, for example, remove the USB stick, DriveLock will automatically disconnect the mapped drive.

5.10.2 Importing and exporting files

With the Mobile Encryption Applicationyou are able to export files from a container to a local disk. You can also import files into the container.

You can use this option if you do not want to connect the container as a drive, for example, because you have no administrator rights.

To export files from a container:

1. Open the container in the Mobile Encryption Application.
2. Select the desired files or folders and click on **Export**.
3. Select the desired storage location.

To import files into the container:

1. In the container, mark the the directory in which you want to import new files into.
2. Click on **Import**.
3. Select the desired files and click on **Open**.

> Alternatively, you can also export and import files via drag & drop.

To manage files in a container:

1. To create a new folder, click the right mouse button on a folder and in the context menu select the option **Create Folder**. Enter a name for the folder.
2. To delete files from the folder, click the right mouse button on a file and in the context menu select the option **Delete**.

5.11 Managing certificates

Certificates are a means to authenticate a user. A certificate consists of a pair of keys: a public key and a private key.

The public key can can be published, so that other users can grant you rights to encrypted data. Together with your private key, you can then decrypt the data. Accordingly, you will need the public key of another user if you want to encrypt data for that user.

You can perform the following tasks:

- Create a certificate
- Publish a certificate
- Copy a certificate

5.11.1 Certificate creation and renewal

You can create a personal certificate or obtain one from the DriveLock Enterprise Service. For more information on

this topic, contact your administrator.

> You can only create one personal and one server certificate. If you already have this certificates, the function will no longer be available but you may renew your server certificate to extend the expiration date.

To create a new certificate:

1. Open the main menu **Encryption**.
2. Click on  **Certificate management**.
3. Select one of the following options:
   - **Create new user**: A new DriveLock user with a server certificate is created on the centralized DriveLock Enterprise Service.
   - **Create encryption certificate**: Windows creates a personalized certificate and stores it on your computer.
4. Enter your personal information. You can also select an image that is displayed in your public key.
5. Choose where you want to save the certificate: on your computer or on an external storage medium, such as a smart card.

5.11.2 Certificate publication

You publish the public key of your certificate so that other people can encrypt files with this key for you. The public key is written to a *.cer file that you can save or send by e-mail.

To publish your certificate:

1. Open the main menu **Encryption**.
2. Click on  **Certificate management**.
3. Select **Certificate publication**.
4. Select the desired certificate.
5. If you want to save the certificate as a file, select the appropriate option, and specify the file path.
6. If you want to immediately send the certificate by e-mail, select the appropriate option.

5.11.3 Certificate copying

You are able to copy a certificate, meaning the public *and* the private key, from one computer to another. To do this, you must first export the certificate to a *.pfx file and then import it on the other computer.

> **If you receive a new computer, do not forget to transfer your certificates from the old computer to the new one, since otherwise you will not be able to access your encrypted data.**

To export your certificate:

1. Open the main menu **Encryption**.
2. Click on  **Managing certificates**.
3. Select **Copy certificate to or from another computer**.
4. Select **Export Certificate**.

5. Select the desired certificate and specify the file path.
6. Enter a password and confirm it.

To import your certificate:

1. Select **Import Certificate**.
2. Select the *.pfx file that you exported.
3. Enter the password that you assigned during the export.

The certificate is imported and will be available on the new computer.

Part VI

DriveLock status display

6 DriveLock status display

You can display information about drives, devices and currently active DriveLockpolicies. The status report is a valuable source of information to determine whether a device or drive is locked or unlocked. It also an administrator to perform an error detection.

> This feature can be disabled by your administrator.

To see a status of devices:

1. Open the main menu **DriveLock status**. You will see an overview of the different system classes:
   - **Devices** contains all internal devices of the computer such as network or mouse controllers, processors or USB interfaces.
   - **Drives** contains all data storage and reading devices such as hard drives and CD/DVD drives.
   - **Policies** displays the policies currently used.
   - **Smartphones** displays the connected mobile phones.
2. In the details pane, you will see the following information for the selected system class:
   - **DriveLock Policy**which is applied for the devices of this group.
   - **Status** of the system, for example, the assignment of the test environment.
3. Double-click the desired system class to obtain details about the devices or policies contained therein.
4. Click on **Back**to return to the system class overview.
5. Click on **Update**to update the overview.

Part VII

Secure data deletion

7 Secure data deletion

When you delete files or folders using the Windows Explorer, the actual data is not destroyed. Windows only deletes the corresponding references to the file in the file system so that it can no longer be found. However, there is free software that can locate and restore these files again.

With DriveLock you can delete files and directories in such a way that the information can not be restored. For this, each deleted file will be overwritten with random data. The algorithm used for this will determine how often the file will be overwritten, and how the random data is generated.

DriveLock has several different algorithms integrated to securely delete data. Unless otherwise specified by your administrator, you can choose one of these algorithms.

> The secure deletion can take several minutes - depending on the file size and the deletion algorithm. Especially when deleting over the network this process can take longer.

To delete a file or folder permanently:

1. In the Windows Explorer, right-click on the desired file or the folder and in the context menu select the option **Secure deletion**.
2. Select the desired algorithm and click on **Yes**to start the procedure.
3. If you are unable to change the algorithm, then your administrator will have predefined it.

DriveLock

Die in diesen Unterlagen enthaltenen Angaben und Daten, einschließlich URLs und anderen Verweisen auf Internetwebsites, können ohne vorherige Ankündigung geändert werden. Die in den Beispielen verwendeten Firmen, Organisationen, Produkte, Personen und Ereignisse sind frei erfunden. Jede Ähnlichkeit mit bestehenden Firmen, Organisationen, Produkten, Personen oder Ereignissen ist rein zufällig. Die Verantwortung für die Beachtung aller geltenden Urheberrechte liegt allein beim Benutzer.
Unabhängig von der Anwendbarkeit der entsprechenden Urheberrechtsgesetze darf ohne ausdrückliche schriftliche Erlaubnis der DriveLock SE kein Teil dieser Unterlagen für irgendwelche Zwecke vervielfältigt oder übertragen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln, elektronisch oder mechanisch, dies geschieht.
Es ist möglich, dass DriveLock SE Rechte an Patenten bzw. angemeldeten Patenten, an Marken, Urheberrechten oder sonstigem geistigen Eigentum besitzt, die sich auf den fachlichen Inhalt dieses Dokuments beziehen. Das Bereitstellen dieses Dokuments gibt Ihnen jedoch keinen Anspruch auf diese Patente, Marken, Urheberrechte oder auf sonstiges geistiges Eigentum, es sei denn, dies wird ausdrücklich in den schriftlichen Lizenzverträgen von DriveLock SE eingeräumt.
Weitere in diesem Dokument aufgeführte tatsächliche Produkt- und Firmennamen können geschützte Marken ihrer jeweiligen Inhaber sein.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.
DriveLock and others are either registered trademarks or trademarks of DriveLock SE or its subsidiaries in the United States and/or other countries.
The names of actual companies and products mentioned herein may be the trademarks of their respective owners.