# DriveLock 2020.2

14.01.2021

© 2021 DriveLock SE

# Inhaltsverzeichnis


Teil I Über diese Dokumentation 4

1 Darstellungskonventionen 5

Teil II Datenverschlüsselung mit DriveLock 6

1 Verschlüsselungsverfahren 7

Teil III DriveLock bedienen 10

1 DriveLock starten und beenden 11

2 Die Oberfläche 12

Der Navigationsbereich 12
Schaltflächen 13
Kontextmenü 13
Windows-Startmenü 14

Teil IV DriveLock-Übersicht einsehen 15

1 Temporäre Freigabe beantragen 16

2 Netzwerkprofile verwalten 17

3 Sprache wählen 17

Teil V Daten verschlüsseln 18

1 Container erstellen 20

2 Container als verschlüsseltes Laufwerk verwenden 21

3 Container löschen 22

4 Kennwort für den Container ändern 22

5 Ordner verschlüsseln 23

6 Verschlüsselten Ordner verwenden 24

7 Benutzer für einen Ordner verwalten 24

8 Benutzergruppen verwalten 25

9 Verlorenes Kennwort wiederherstellen 25

10 Die Mobile Encryption Anwendung verwenden 26

Mit der Mobile Encryption Anwendung arbeiten 26
Dateien importieren und exportieren 27

11 Zertifikate verwalten 28

Zertifikat erstellen und erneuern 28
Zertifikat veröffentlichen 29
Zertifikat kopieren 29

Teil VI DriveLock-Status einsehen 30

Teil VII Daten sicher löschen 32


 © 2021 DriveLock SE

 © 2021 DriveLock SE

# Teil I

## Über diese Dokumentation

# 1 Über diese Dokumentation

Diese Benutzerdokumentation erklärt Ihnen, wie Sie als Endbenutzer mit DriveLock in einer Unternehmensumgebung arbeiten und wie Sie die portable Version Mobile Encryption Anwendung von einem mobilen Datenträger oder die DriveLock Personal Version, die auf einem persönlichen PC ohne zentrale Administration installiert werden kann, verwenden.

## 1.1 Darstellungskonventionen

In diesem Dokument werden folgende Konventionen und Symbole verwendet, um wichtige Aspekte hervorzuheben oder Objekte zu visualisieren.

**Achtung: Roter Text weist auf Risiken hin, die beispielsweise zu Datenverlust führen können**

Hinweise und Tipps enthalten nützliche Zusatzinformationen.

**Menüeinträge** oder die Namen von **Schaltflächen** sind fett dargestellt.


© 2021 DriveLock SE

# Teil II

## Datenverschlüsselung mit DriveLock

# 2 Datenverschlüsselung mit DriveLock

Mit DriveLock können Sie Ihre Daten verschlüsseln. Verschlüsseln bedeutet, sie verändern Daten so, dass diese nicht mehr klar lesbar sind und nur noch mit dem geeigneten Schlüssel wieder lesbar gemacht, das heißt, entschlüsselt werden können.

Datenverschlüsselung können Sie mit DriveLock auf verschiedenen Ebenen vornehmen:

### Verschlüsselung von Ordnern

Wenn Sie einen Ordner verschlüsseln, werden alle darin enthaltenen Dateien automatisch auch verschlüsselt. Dabei bleiben der Dateiname, beispielsweise **Geheimvertrag.docx**, die Dateigröße und das Datum weiterhin sichtbar und lesbar. Die Datei kann in der zugehörigen Anwendung, beispielsweise in Microsoft Word geöffnet werden; ohne entsprechende Berechtigung besteht der Inhalt jedoch aus einem nicht lesbaren Text.

### Verschlüsselung von Containern

Ein Container ist eine große verschlüsselte Datei, in der Sie andere Dateien und Verzeichnisse verstecken können. Wenn Sie einen Container zur Verschlüsselung verwenden, dann definieren Sie die Größe dieses Containers und verschlüsseln ihn. Alle Dateien, die sie jetzt in diesem Container speichern sind ebenfalls verschlüsselt. Im Unterschied zur Ordnerverschlüsselung ist jedoch von außen nicht ersichtlich, wie viele und welche Verzeichnisse und Dateien in diesem Container enthalten sind. Freier Speicherplatz in diesem Container ist ebenfalls verschlüsselt.

Der Container sieht von außen wie eine große Datei mit der Endung **.dlv** aus. Die Container-Datei kann auf allen Typen von Speichermedien, wie beispielsweise USB-Stick oder Festplatten sowie auf einer Netzwerkfreigabe gespeichert werden.

Damit Sie den Container verwenden können, verbindet DriveLock diesen mit einem vordefinierten oder freien Laufwerksbuchstaben; so können Sie den Container wie jedes andere Laufwerk mit dem Windows Explorer verwenden.

### Schutz durch Passwörter oder Zertifikate

Der Zugriff auf verschlüsselte Dateien und Container wird über verschiedene Methoden geschützt, beispielsweise mit Passwörtern oder Zertifikaten. Falls Sie einmal ein Kennwort vergessen, stellt der Recovery-Mechanismus von DriveLock sicher, dass Ihre Daten trotzdem nicht verloren sind. Weitere Informationen hierzu erhalten Sie von Ihrem Administrator.

> Verschlüsselung von Containern und die Verwendung von Zertifikaten sind nicht Bestandteil der Personal Versionen DriveLock Private und DriveLock Business.

## 2.1 Verschlüsselungsverfahren

### Verschlüsselungsverfahren

- **AES** - Der Advanced Encryption Standard (AES) ist ein symmetrisches Verschlüsselungsverfahren, das als Nachfolger für DES bzw. 3DES im Oktober 2000 vom National Institute of Standards and Technology (NIST) als Standard bekannt gegeben wurde. Nach seinen Entwicklern Joan Daemen und Vincent Rijmen wird er auch Rijndael-Algorithmus genannt.
  DriveLock verwendet eine Schlüssellänge von 256 Bits, (AES-256), welche nach aktuellem Stand der Technik als ausreichend sicher für die Verschlüsselung vertraulicher Informationen angesehen wird.

 © 2021 DriveLock SE

- **Triple DES** - Symmetrisches Verschlüsselungsverfahren, das auf dem klassischen DES basiert, jedoch mit der doppelten Schlüssellänge arbeitet (112 Bit). Die zu verschlüsselnden Daten werden mit einer dreifachen Kombination des klassischen DES verschlüsselt. Aufgrund der Schlüssellänge gilt Triple-DES derzeit noch als sicheres Verfahren im Gegensatz zum einfachen DES, der durch Brute-Force-Attacken (bloßes Probieren von Schlüsseln) angreifbar ist.

- **Blowfish** - Dieser sehr schnelle *Algorithmus* bietet besonders bei 32-Bit-Prozessoren eine gute Leistung. Ein Vorteil von Blowfish ist seine variable *Schlüssellänge* von 32 bis zu 448 Bits. Blowfish gilt als sehr sicher. Der Algorithmus wurde 1994 zum ersten Mal vorgestellt.

- **Twofish** - Twofish ist der AES-Beitrag von Counterpane Systems, der Firma von Bruce Schneier. Der Algorithmus benutzt eine Blockgröße von 128 Bit und kann mit Schlüsseln von 128 bis 256 Bit betrieben werden. Twofish ist sehr schnell; auf einem Pentium wird ein Byte in 18 CPU-Takten verschlüsselt. Twofish wurde bisher sehr intensiv geprüft, ohne dass Schwachstellen gefunden worden wären.

- **CAST 5** - CAST ist eine symmetrische Blockchiffre mit 64 Bit Blocklänge und einer Schlüssellänge von 40-128 Bit. Der CAST Algorithmus wurde nach seinen Entwicklern **C**arlisle **A**dams und **S**tafford **T**avares benannt und 1996 zum Patent angemeldet. Wegen seiner höheren Geschwindigkeit gegenüber DES ist CAST auch für Echtzeitanwendungen geeignet. Schlüssellängen von 80 bis 128 Bit werden als CAST-5 bezeichnet.

- **Serpent** - ist ein symmetrischer Verschlüsselungsalgorithmus, der von den Kryptografen Ross Anderson, Eli Biham und Lars Knudsen entwickelt wurde. Dieser Algorithmus war ein Kandidat für den Advanced Encryption Standard und gehörte mit Twofish, Rijndael, MARS und RC6 zu den fünf Finalisten des AES-Standard-Ausscheidungsverfahrens. Gegensatz zu den beiden anderen als hoch-sicher eingestuften Kandidaten der letzten Runde, MARS und Twofish, wurde Serpent bezüglich seiner Sicherheit nicht kritisiert und es wurde angenommen, dass dieser der sicherste Verschlüsselungsalgorithmus der fünf Finalisten sei.

### Kennwort-Verschlüsselung (Hash-Algorithmus)

Mit einem Hash-Algorithmus verschlüsselt DriveLock das Kennwort, mit welchem das verschlüsselte Laufwerk ver- bzw. entschlüsselt wird. DriveLock unterstützt folgende Hash Verfahren:

- **SHA** - Das NIST (National Institute of Standards and Technology) entwickelte zusammen mit der NSA (National Security Agency) eine zum Signieren gedachte sichere Hash-Funktion als Bestandteil des Digital Signatur Algorithm (DSA) für den Digital Signature Standard (DSS). Die Funktion wurde 1994 veröffentlicht. Diese als Secure Hash Standard (SHS) bezeichnete Norm spezifiziert den sicheren Hash-Algorithmus (SHA) mit einem Hash-Wert von 160 Bit Länge für Nachrichten mit einer Größe von bis zu 264 Bit. Der Algorithmus ähnelt im Aufbau dem von Ronald L. Rivest entwickelten MD4. Der sichere Hash-Algorithmus existiert zunächst in zwei Varianten, SHA-0 und SHA-1, die sich in der Anzahl der durchlaufenen Runden bei der Generierung des Hashwertes unterscheiden. Das NIST hat im August 2002 drei weitere Varianten („SHA-2“) des Algorithmus veröffentlicht, die größere Hash-Werte erzeugen. Es handelt sich dabei um den SHA-256, SHA-384 und SHA-512 wobei die angefügte Zahl jeweils die Länge des Hash-Werts (in Bit) angibt.

- **RIPEMD-160** - RIPEMD-160 wurde von Hans Dobbertin, Antoon Bosselaers und Bart Preneel in Europa entwickelt und 1996 erstmals publiziert. Es handelt sich dabei um eine verbesserte Version von RIPEMD, welcher wiederum auf den Design Prinzipien von MD4 basiert und in Hinsicht auf seine Stärke und Performanz dem populäreren SHA-1 gleicht. Da die Entwicklung von RIPEMD-160 offener war als die von SHA-1, ist es wahrscheinlicher, dass dieser Algorithmus weniger Sicherheitslücken aufweist.

- **WHIRLPOOL** – WHIRLPOOL ist eine kryptologische Hash-Funktion, die von Vincent Rijmen und Paulo S. L. M. Barreto entworfen wurde. Sie wurde nach der Whirlpool-Galaxie im Sternbild der Jagdhunde benannt. Whirlpool gehört zu den vom Projekt NESSIE empfohlenen kryptografischen Algorithmen und wurde von der ISO mit ISO/IEC 10118-3:2004 standardisiert.

 © 2021 DriveLock SE

In Umgebungen mit besonderen Sicherheitsanforderungen können die in DriveLock integrierten FIPS-Algorithmen verwendet werden. Der Federal Information Processing Standard (abgekürzt FIPS) ist die Bezeichnung für öffentlich bekanntgegebene Standards der Vereinigten Staaten. Diese Standards beruhen auf Modifizierung der allgemein verwendeten Standards, die durch ANSI, IEEE, ISO und ähnliche Organisationen aufgestellt werden. Im Bereich der Kryptographie ist insbesondere FIPS 140-2 bekannt (Sicherheitsanforderungen für Kryptographische Module).


© 2021 DriveLock SE

# Teil III

## DriveLock bedienen

# 3 DriveLock bedienen

DriveLock ist eine Softwarelösung zur Absicherung von Clientrechnern. Rechner, auf denen DriveLock DriveLock installiert ist, können zentral konfiguriert werden, so dass in einem Unternehmen ein einheitliches Datenzugriffskonzept installiert werden kann.

> In einer Unternemensumgebung wird DriveLock wird von einem Administrator konfiguriert. Abhängig von seinen Einstellungen können einige der hier vorgestellten Funktionen gar nicht oder in leicht abweichender Funktion zur Verfügung stehen. Details erfragen Sie bitte gegebenenfalls bei Ihrem Administrator.
> Die portablen und persönlichen Versionen von DriveLock können für Sie für die Ver- und Entschlüsselung von Dateien in Ordnern und/oder Containern verwenden. Der genaue Funktionsumfang und die Menge der Dateien, die verschlüsselt werden können hängt von ihrer Lizenz ab.

### Datenverschlüsselung

Die Datenverschlüsselung mit DriveLock bietet unterschiedliche Möglichkeiten, Daten vor unbefugtem Zugriff zu schützen: Sie können ganze Ordner und die darin enthaltenen Dateien verschlüsseln oder Sie erstellen einen verschlüsselten Container. Sie können die Daten mit einem Kennwort verschlüsseln oder mit einem persönlichen Zertifikat.

Mehr hierzu, siehe Datenverschlüsselung.

### Gerätezugriff

DriveLock bietet konfigurierbaren Zugriff auf Laufwerke wie Disketten- bzw. CD-ROM-Laufwerke oder USB-Sticks. Zusätzlich kontrolliert es externe Datenträger wie über Bluetooth gekoppelte Geräte oder mobile Endgeräte wie Palm, Blackberry und Smartphones. Ihr Administrator hat festgelegt, wer welches Gerät zu welcher Zeit nutzen kann.

### Sicheres Löschen

Mit DriveLock können Sie Dateien und Verzeichnissen so löschen, dass keine nachträgliche Wiederherstellung dieser Daten möglich ist.

## 3.1 DriveLock starten und beenden

In der Regel wird Ihr Administrator DriveLock so installiert haben, dass das Programm nach jedem Neustart Ihres Rechners automatisch gestartet wird.

Sollte dies nicht der Fall sein, oder wenn Sie DriveLock manuell geschlossen haben, können Sie es wieder starten.

### So starten Sie DriveLock:

1. Öffnen Sie das Windows-Startmenü.
2. Suchen Sie den Eintrag für DriveLock und klicken Sie ihn. Die Position und der genaue Name des Eintrags sind abhängig von den Einstellungen in Ihrem Unternehmen. Fragen Sie Ihren Administrator nach Details.

> Alternativ kann auch ein Icon auf Ihrem Desktop eingerichtet sein.

### So beenden Sie DriveLock:

Klicken Sie auf das rote Kreuz rechts oben im Programm-Fenster (Windows-Standard).

 © 2021 DriveLock SE

## 3.2 Die Oberfläche

Die DriveLock-Oberfläche ist in folgende Bereiche eingeteilt:

- Der *Menübereich* oben enthält Symbole, über die Sie die einzelnen Funktionen ansteuern können.
- Im *Arbeitsbereich* in der Mitte führen Sie die Aufgaben aus.
- Der *Werkzeugbereich* enthält Funktionen, mit denen Sie beispielsweise Ordner verwalten können.


### 3.2.1 Der Navigationsbereich

Abhängig von der verwendeten Version und Lizenz finden Sie folgende Menüs :

**Home**

DriveLock-Übersicht einsehen

Temporäre Freigabe beantragen

Netzwerkprofile verwalten

Sprache wählen

**Verschlüsselung**

Container erstellen

Ordner verschlüsseln

Zertifikate verwalten

 © 2021 DriveLock SE

**DriveLock-Status**

DriveLock-Status einsehen

**Help**

Online-Hilfe aufrufen

### 3.2.2 Schaltflächen

## Schaltflächen

Auf folgende Schaltflächen treffen sie in den unterschiedlichen Menüs:

**OK**

Bestätigt eine Aktion; speichert die Daten und kehrt zum vorherigen Fenster zurück.

**Abbrechen**

Kehrt zum vorherigen Fenster zurück, ohne zu speichern.

**Zurück**

Kehrt zum vorherigen Fenster zurück. Bei Fenstern ohne Änderungsmöglichkeiten, wie bei der Anzeige des Gerätestatus.

**Aktualisieren**

Aktualisiert die Anzeige; es gibt auch Symbole, auf denen die Pfeile in Verbindung mit einem anderen Zeichen auftreten.

**Löschen**

Löscht eine Datei oder ein Objekt, z. B. eine infizierte Datei in DriveLock Antivirus.

### 3.2.3 Kontextmenü

Alternativ zur Bedienung über Schaltflächen können Sie auch das Kontextmenü verwenden. Sie rufen das Kontextmenü auf, indem Sie mit der rechten Maustaste auf ein Symbol im Arbeitsbereich klicken.

Sie sehen die Funktionen, die Sie für dieses Element ausführen können.

Klicken Sie mit der linken Maustaste auf einen Menüeintrag, um ihn auszuwählen.

**Kontextmenü im Windows Explorer**

 © 2021 DriveLock SE

Das Kontextmenü im Windows Explorer enthält auch Funktionen von DriveLock. Sie erkennen diese speziellen Funktionen am DriveLock-Symbol.

So können Sie für Ordner und Dateien jederzeit die Funktion **Sicher Löschen** verwenden. Andere Funktionen stehen nur im richtigen Kontext zur Verfügung, beispielsweise um einen verbundenen Container zu trennen.

### 3.2.4 Windows-Startmenü

Sie können die meisten Funktionen von DriveLock auch über das Windows-Startmenü aufrufen. Sie finden die Funktionen unter den Programmgruppen von DriveLock.

 © 2021 DriveLock SE

# Teil IV

## DriveLock-Übersicht einsehen

# 4 DriveLock-Übersicht einsehen

Im Hauptmenü **Übersicht** sehen Sie auf einen Blick, ob Ihr Computer geschützt ist. Die grünen Symbole zeigen an, dass Ihr Computer geschützt und der DriveLock Antivirus aktiv und aktuell ist. Wenn Sie rote Symbole sehen, wenden Sie sich an Ihren Administrator.

Im Hauptmenü **Übersicht** können Sie weitere allgemeine Aufgaben ausführen:

- Temporäre Freigaben beantragen
- Netzwerkprofile verwalten
- Sprache wählen

## 4.1 Temporäre Freigabe beantragen

DriveLock kontrolliert den Zugriff auf angeschlossene Wechseldatenträger, Geräte oder auch Anwendungen zentral über eine Richtlinie. Wenn Sie Zugang zu einem gesperrten Gerät oder Laufwerk benötigen oder ein gesperrtes Programm ausführen müssen, können Sie eine temporäre Freigabe beantragen.

Dabei wird zwischen einer Online-Freischaltung und einer Offline-Freischaltung unterschieden.

### Online-Freischaltung

Bei einer Online-Freischaltung verbindet sich der Administrator über das Netzwerk mit Ihrem Rechner und gibt entsprechend den Unternehmensrichtlinien das von Ihnen gewünschte Gerät bzw. Anwendung frei. Sie müssen dazu nichts tun.

### Offline-Freischaltung

Bei einer Offline-Freischaltung, also wenn keine aktive Netzwerkverbindung zwischen Ihrem Rechner und dem Rechner Ihres Administrators besteht, übermitteln Sie Ihrem Administrator den Computernamen sowie einen Code. Der Administrator ermittelt aus beidem einen Antwortcode, den er dann an Sie weitergibt. Sie können dies beispielsweise telefonisch oder per E-Mail durchführen.

### So beantragen Sie eine Offline-Freischaltung:

1. Öffnen Sie das Hauptmenü **Home** und klicken Sie auf **Temporäre Freigabe**.
   Sie sehen in einem Fenster den Namen Ihres Computers sowie einen Anforderungscode.
2. Melden Sie sowohl den Computernamen als auch den Anforderungscode ihrem Administrator, der daraus einen Freischaltungscode erzeugt und Ihnen mitteilt.

> Klicken Sie auf die drei Punkte neben dem Anforderungscode. Ein Fenster öffnet sich, das den Code in Fliegeralphabet geschrieben zeigt, dies erleichtert Ihnen die telefonische Übermittlung. Zum Beispiel *YB8C* heißt hier "Ypsilon, Berta, Acht, Cäsar". Abhängig von Ihren Systemeinstellungen, können Sie sich den Text auch vorlesen lassen.

3. Geben Sie im selben Fenster den Antwortcode ein, den Sie von Ihrem Administrator erhalten haben.

 © 2021 DriveLock SE

4. Sie erhalten die Meldung, dass Ihr Computer für eine bestimmte durch den Administrator festgelegte Zeitspanne freigegeben wurde.
   Sie können nun auf die freigeschalteten Geräte oder Anwendungen zugreifen, solange die Freischaltung aktiv ist.

5. Klicken Sie auf ✓ **OK**, um das Fenster zu schließen.

## 4.2 Netzwerkprofile verwalten

Wenn Sie einen tragbaren Computer verwenden, können Sie diesen in verschiedenen Netzwerken verwenden, beispielsweise im Büro und zu Hause. Mit DriveLock legen Sie ein Netzwerkprofil für jeden dieser Arbeitsplätze ein, das jeweils die Konfiguration dieses Netzwerkes enthält. Hierzu gehören die IP-Adressen, Proxy-Einstellungen oder Druckereinstellungen.

### So fügen Sie ein neues Netzwerkprofil hinzu:

1. Öffnen Sie das Hauptmenü **Home** und klicken Sie auf **Netzwerkprofile**.
2. Klicken Sie auf + **Netzwerkprofil hinzufügen**.
3. Geben Sie einen Namen für das neue Netzwerkprofil ein und wählen Sie ein passendes Symbol.
4. Konfigurieren Sie das Netzwerkprofil. Fragen Sie Ihren Administrator nach Details.

### So bearbeiten Sie ein Netzwerkprofil:

Markieren Sie das gewünschte Netzwerkprofil und klicken Sie auf **Eigenschaften**.

### So löschen Sie ein Netzwerkprofil:

Markieren Sie das gewünschte Netzwerkprofil und klicken Sie auf **Netzwerkprofil löschen**.

## 4.3 Sprache wählen

Sie können einstellen, in welcher Sprache die DriveLock-Benutzeroberfläche angezeigt wird, wenn Sie eine andere als die Standardsprache bevorzugen.

### So wählen Sie eine andere Sprache:

1. Öffnen Sie das Hauptmenü **Home** und klicken Sie auf **Sprache wählen**.
2. Wählen Sie die gewünschte Sprache und klicken Sie auf **OK**.


© 2021 DriveLock SE

# Teil V

## Daten verschlüsseln

# 5 Daten verschlüsseln

Sie können mit DriveLock Ihre Daten verschlüsseln, sei es Dateien in einem Ordner oder in einem Container. Das Vorgehen ist dabei sehr ähnlich:

Sie erstellen eine Verschlüsselung und verbinden den Ordner oder den Container, das heißt, Sie authentifizieren sich und können dann auf die Daten in dem Ordner bzw. Container zugreifen.

### Vorüberlegungen

Wenn Sie Daten verschlüsseln wollen, sollten Sie sich einige Dinge im Voraus überlegen:

- Was passt besser zu meiner Aufgabe, ein Ordner oder ein Container?
- Welche Daten möchte ich in diesem Container sichern? Wie groß muss dieser Container also werden?
- Wie groß ist das Speichermedium, auf dem ich den Container speichern möchte? Gibt es hier Größenbeschränkungen? Wenn Sie ein externes Laufwerk auswählen, beispielsweise einen USB-Stick, wählt DriveLock automatisch eine passende Containergröße, um den zur Verfügung stehenden Platz optimal zu nutzen. Sie können den eingestellten Wert auch selbst bis zur maximal verfügbaren Größe anpassen.
- Welche Verschlüsselungsmethoden möchte ich verwenden (falls Ihre Systemkonfiguration hier eine Wahl zulässt).
- Welches Dateisystem ist das passende NTFS oder FAT? Für Dateien in einem Container von über 4 GB Größe müssen Sie NTFS verwenden.
- Wie soll der Name des Laufwerkes lauten?

Weitere Informationen finden Sie unter Datenverschlüsselung.

Folgende Aufgaben können Sie erledigen:

- Container erstellen
- Container als verschlüsseltes Laufwerk verwenden
- Container löschen
- Kennwort für den Container ändern
- Ordner verschlüsseln
- Verschlüsselten Ordner verwenden
- Benutzer für einen Ordner verwalten

- Benutzergruppen verwalten
- Verlorenes Kennwort wiederherstellen

 © 2021 DriveLock SE

## 5.1 Container erstellen

Bevor Sie einen neuen Container erstellen, sollten Sie sich die Vorüberlegungen angesehen haben.

> Es kann sein, dass Ihnen einige der hier genannten Einstellungen nicht zur Verfügung stehen. Ihr Administrator hat dann eine Unternehmensrichtlinie definiert, die diese Einstellungen enthält.

> DriveLock wählt bei externen Datenträgern eine Containergröße, die sicherstellt, dass bei Bedarf auch noch die Mobile Encryption Anwendung auf den Datenträger kopiert werden kann.

**So erstellen Sie einen neuen Container:**

1. Öffnen Sie das Hauptmenü **Verschlüsselung**.
2. Klicken Sie auf **Neu** und wählen Sie aus dem Kontextmenü die Option **Verschlüsselter Container**.
3. Definieren Sie den neuen Container mithilfe des Assistenten:
   a. Wählen Sie den Ort, an dem Sie den Container erstellen wollen: Klicken Sie auf das gewünschte Laufwerk oder externe Gerät. Alternativ können Sie auch eine gesamte Partition als Container verschlüsseln.
   b. Stellen Sie die Größe der Container-Datei ein. DriveLock wählt bei externen Datenträgern eine Containergröße, die sicherstellt, dass bei Bedarf auch noch die Mobile Encryption Anwendung auf den Datenträger kopiert werden kann.
   c. Wählen Sie das passende Dateisystem und die Clustergröße aus.

      Abhängig vom verwendeten Dateisystem ist eine bestimmte Mindestgröße erforderlich:
      FAT: 100 KB; NTFS: 3072 KB.
      Wählen Sie NTFS, wenn Sie Dateien innerhalb eines Containers mit *mehr* als 4 GB anlegen möchten, da FAT nur Dateien bis zu dieser Größe unterstützt.

      Ein Cluster ist eine logische Einheit von Blöcken auf einem Speichermedium. Gewöhnlich adressiert das Dateisystem nur komplette Cluster, d.h. es ist nicht möglich, einzelne Blöcke oder Bytes innerhalb eines Clusters anzusprechen. Daher belegen Dateien immer eine gewisse Anzahl an Clustern. Je größer die Clustergröße, desto weniger administrative Aufwand ist für große Dateien notwendig und die Fragmentierung ist minimiert. Der Nachteil großer Cluster ist, dass sie Speicherplatz ungenutzt belegen.
   d. Optional geben Sie einen Namen für die Container-Datei an. Dieser Name wird als Laufwerksname angezeigt, wenn Sie den Container verbunden haben. Er kann sich von dem Namen der eigentlichen Containerdatei unterscheiden.
   e. Wählen Sie die Verschlüsselungsmethode und das Hash-Verfahren, siehe hierzu Verschlüsselungsverfahren.
   f. Geben Sie das Kennwort für den Container an und wiederholen Sie die Eingabe.
      Folgenden Zeichen können Sie für Ihr Kennwort verwenden:
      Großbuchstaben (A-Z)
      Kleinbuchstaben (a-z)
      Zahlen (0-9)
      Sonderzeichen (z.B. !, $, #, \ oder &)
      Die farbige Anzeige unter den Kennwort-Feldern zeigt an, wie gut Ihr Kennwort ist. Ein Kennwort ist dann gut, wenn es nicht leicht erraten oder errechnet werden kann.
      Es kann in Ihrem Unternehmen zusätzlich Richtlinien geben, wie ein Kennwort aufgebaut sein muss. So kann beispielsweise vorgeschrieben sein, dass ein Kennwort immer ein Sonderzeichen und eine Zahl enthalten

 © 2021 DriveLock SE

muss. Wenn Ihr Kennwort nicht den Unternehmensrichtlinien entspricht, erhalten Sie eine entsprechende Meldung.

4. Klicken Sie auf **Weiter**. Der Container wird erstellt. Je nach Größe und Ziellaufwerk kann dies einige Sekunden dauern. Sie erhalten eine Meldung, wenn der Container erfolgreich erzeugt wurde. Sie können jetzt auch schon den Container als Laufwerk verbinden.
5. Markieren Sie **Verbinden als** und wählen Sie einen freien Laufwerksbuchstaben.
6. Markieren Sie **Nicht zur Historie hinzufügen**, wenn Sie diesen Container nur temporär mit diesem Laufwerksbuchstaben verbinden möchten und der Container nicht in der Liste der bereits verwendeten Container zu sehen sein soll.
7. Klicken Sie auf **Fertigstellen**.

## 5.2 Container als verschlüsseltes Laufwerk verwenden

Um Dateien in einem Container zu speichern, verbinden Sie ihn als Laufwerk. Dies bedeutet, dass der Container einen Laufwerkbuchstaben erhält und Sie ihn im Windows Explorer wie ein weiteres Laufwerk sehen und mit ihm arbeiten können.

> Wenn Sie einen neuen Container anlegen, wird Ihnen dort auch gleich angeboten, den neu erstellten Container als Laufwerk zu verbinden.

Im Hauptmenü **Verschlüsselung** sehen Sie eine Liste mit den zuletzt verwendeten Containern. Sie können aus dieser Liste einen auswählen, oder Sie verwenden einen Container im Dateisystem, der nicht in der Liste angezeigt wird.

**So verbinden Sie einen Container als Laufwerk:**

1. Wählen Sie den Container, den Sie zu einem Laufwerk verbinden möchten. Sie haben folgende Möglichkeiten:
   - Der Container ist bereits in der Liste der **zuletzt benutzten Laufwerke**: Doppelklicken Sie auf den Container.
   - Der Container ist nicht in der Liste: Klicken Sie auf **Verbinden** und **Verschlüsselter Container**; geben Sie den korrekten Pfad und Dateinamen ein, oder klicken Sie auf **...**, und suchen Sie die Container-Datei auf Ihrem Dateisystem.
2. Wählen Sie den gewünschten Laufwerkbuchstaben.
3. Authentifizieren Sie sich gegebenenfalls wie gefordert.
4. Markieren Sie **Nicht zur Historie hinzufügen**, wenn dieser Container *nicht* in der Liste der zuletzt verwendeten Container angezeigt werden soll.
5. Klicken Sie auf **Fertig stellen**. Sie sehen jetzt in Ihrem Windows Explorer ein neues Laufwerk mit dem gewählten Buchstaben. Dies ist der verschlüsselte Container, in dem Sie nun Ihre Dateien ablegen können.

> Den Assistenten zum Verbinden von Containern können Sie auch öffnen, indem Sie im Windows Explorer eine Container-Datei (*.dlv) doppelklicken.

Wenn Sie den Container nicht mehr als verschlüsseltes Laufwerk benötigen, oder wenn Sie das externe Speichermedium, auf dem der Container gespeichert ist, aus ihrem Computer nehmen, müssen Sie auch das Laufwerk trennen.

**Schließen Sie alle geöffneten Dateien auf diesem Laufwerk, bevor Sie es trennen. Wenn Sie ein Laufwerk trennen, während noch Dateien von diesem Laufwerk geöffnet sind, beispielsweise in Microsoft Word, kommt**

 © 2021 DriveLock SE

**es zu Datenverlusten! DriveLock DriveLock ist nicht verantwortlich für beschädigte oder zerstörte Daten, die durch Trennen eines verschlüsselten Laufwerks ohne vorheriges Schließen der enthaltenen Dateien entstehen können.**

**So trennen Sie ein verschlüsseltes Laufwerk:**

1. Klicken Sie im Hauptmenü **Verschlüsselung** mit der rechten Maustaste auf ein bereits verbundenes Laufwerk.
2. Wählen Sie im Kontextmenü die Option **Trennen**.

> Alternativ können Sie auch im Windows Explorer mit der rechten Maustaste auf den Laufwerksbuchstaben klicken und aus dem Kontextmenü die Option **Trennen** wählen.

## 5.3 Container löschen

Verschlüsselte Container löschen Sie im Windows Explorer, indem Sie die zugehörige *.dlv-Datei löschen.

Wenn der Container noch als verschlüsseltes Laufwerk verbunden ist, müssen Sie es vorher trennen; siehe Container als verschlüsseltes Laufwerk verwenden.

> Sie können eine Containerdatei auch mit der DriveLock Funktion Sicheres Löschen entfernen, siehe Daten sicher löschen.

## 5.4 Kennwort für den Container ändern

Sie können das Kennwort für einen Container ändern. Dazu muss der Container als Laufwerk verbunden sein, siehe Container als verschlüsseltes Laufwerk verwenden.

> Um das Kennwort zu ändern, benötigen Sie das aktuelle Kennwort.

**So ändern Sie das Kennwort für einen Container:**

1. Öffnen Sie den Windows Explorer.
2. Klicken Sie mit der rechten Maustaste auf das Container-Laufwerk und wählen Sie aus dem Kontextmenü **Kennwort ändern**.
3. Geben Sie das aktuelle und das neue Kennwort ein.

   Folgenden Zeichen können Sie für Ihr Kennwort verwenden:
   Großbuchstaben (A-Z)
   Kleinbuchstaben (a-z)
   Zahlen (0-9)
   Sonderzeichen (z.B. !, $, #, \ oder &)
   Die farbige Anzeige unter den Kennwort-Feldern zeigt an, wie gut Ihr Kennwort ist. Ein Kennwort ist dann gut, wenn es nicht leicht erraten oder errechnet werden kann.

   > Es kann in Ihrem Unternehmen zusätzlich Richtlinien geben, wie ein Kennwort aufgebaut sein muss. So kann beispielsweise vorgeschrieben sein, dass ein Kennwort immer ein Sonderzeichen und eine Zahl enthalten

 © 2021 DriveLock SE

> muss. Wenn Ihr Kennwort nicht den Unternehmensrichtlinien entspricht, erhalten Sie eine entsprechende Meldung.

4. Wählen Sie eine der folgenden Optionen, falls diese von Ihrem Administrator freigegeben wurden:
   - **Benutzerkennwort setzen**: Ist der Datenträger noch nicht zur Verwendung mit der Mobile Encryption Anwendung eingerichtet, können Sie ein persönliches Kennwort erstellen, das Sie beim Zugriff außerhalb des Unternehmensnetzwerkes benötigen.
   - **Benutzerkennwort entfernen**: Wenn Sie verhindern möchten, dass der Container außerhalb des Unternehmens mithilfe der Mobile Encryption Anwendung verwendet werden kann, können Sie das persönliche Kennwort entfernen. Hierzu müssen Sie das Benutzerkennwort kennen.
5. Speichern Sie Ihre Eingaben.

## 5.5 Ordner verschlüsseln

> Es kann sein, dass Ihnen einige der hier genannten Einstellungen nicht zur Verfügung stehen. Ihr Administrator hat dann eine Unternehmensrichtlinie definiert, die diese Einstellungen enthält.

**So verschlüsseln Sie einen Ordner:**

1. Öffnen Sie das Hauptmenü **Verschlüsselung**.
2. Klicken Sie auf **Neu** und wählen Sie aus dem Kontextmenü die Option **Verschlüsselter Ordner**.
3. Wählen Sie den Ordner, den Sie verschlüsseln wollen.
4. Geben Sie an, wie Sie sich authentifizieren möchten. Die Auswahlmöglichkeiten sind abhängig von Ihren Systemeinstellungen.
   - Benutzername und Kennwort. Diese Option ist nützlich, wenn Sie den verschlüsselten Ordner einer anderen Person geben möchten.
   - Windows-Benutzerverwaltung
   - DriveLock File Protection-Benutzerverwaltung
   - Ein persönliches Verschlüsselungszertifikat, siehe auch Zertifikate verwalten
5. Abhängig von Ihrer Auswahl der Authentifizierungsmöglichkeit, sind die folgenden Schritte unterschiedlich,

   Wenn Sie Benutzername und Kennwort gewählt haben, beachten Sie die Hinweise zur Kennwortvergabe:

   Folgenden Zeichen können Sie für Ihr Kennwort verwenden:
   Großbuchstaben (A-Z)
   Kleinbuchstaben (a-z)
   Zahlen (0-9)
   Sonderzeichen (z.B. !, $, #, \ oder &)
   Die farbige Anzeige unter den Kennwort-Feldern zeigt an, wie gut Ihr Kennwort ist. Ein Kennwort ist dann gut, wenn es nicht leicht erraten oder errechnet werden kann.
   Es kann in Ihrem Unternehmen zusätzlich Richtlinien geben, wie ein Kennwort aufgebaut sein muss. So kann beispielsweise vorgeschrieben sein, dass ein Kennwort immer ein Sonderzeichen und eine Zahl enthalten muss. Wenn Ihr Kennwort nicht den Unternehmensrichtlinien entspricht, erhalten Sie eine entsprechende Meldung.
6. Klicken Sie auf **Fertig stellen**.

 © 2021 DriveLock SE

Um den Ordner nutzen zu können, müssen Sie ihn verbinden, siehe Verschlüsselten Ordner verwenden.

## 5.6 Verschlüsselten Ordner verwenden

Um auf einen verschlüsselten Ordner und seine Dateien zuzugreifen, müssen Sie ihn verbinden. Das heißt, Sie authentifizieren sich wie hinterlegt, mit Kennwort oder Zertifikat. Danach können Sie mit einem verschlüsselten Ordner arbeiten wie mit jedem anderen Ordner unter Windows.

Verschlüsselte Ordner erkennen Sie im Windows Explorer an einem kleinen Vorhängeschloss auf dem Ordner-Symbol.

**So verbinden Sie einen verschlüsselten Ordner:**

1. Wählen Sie den Order, den Sie verbinden möchten. Sie haben folgende Möglichkeiten:
   - Der Ordner ist bereits in der Liste der **zuletzt benutzten Laufwerke**: Doppelklicken Sie auf den Ordner.
   - Der Ordner ist nicht in der Liste: Klicken Sie auf **Verbinden** und **Verschlüsselter Ordner**; geben Sie den Pfad und Ordner ein, oder klicken Sie auf **...**, und suchen Sie den Ordner auf Ihrem Dateisystem.
2. Authentifizieren Sie sich gegebenenfalls wie gefordert.
3. Markieren Sie **Nicht zur Historie hinzufügen**, wenn dieser Ordner *nicht* in der Liste der zuletzt verwendeten Container angezeigt werden soll.
4. Klicken Sie auf **Fertig stellen**. Sie können jetzt im Windows Explorer wie gewohnt mit den Dateien in dem verschlüsselten Ordner arbeiten.

**So trennen Sie einen verschlüsselten Ordner:**

1. Klicken Sie im Hauptmenü **Verschlüsselung** mit der rechten Maustaste auf einen bereits verbundenen Ordner.
2. Wählen Sie im Kontextmenü die Option **Trennen**.

## 5.7 Benutzer für einen Ordner verwalten

Sie können verwalten, wer Zugriff auf Ihren verschlüsselten Ordner hat. Nur Sie als Ersteller des verschlüsselten Ordners kann diese Berechtigungen vergeben oder nehmen.

> Um die Benutzerrechte zu verwalten, muss der Ordner verbunden sein, siehe Verschlüsselten Ordner verwenden.

**So verwalten Sie die Benutzer Ihres verschlüsselten Ordners:**

1. Klicken Sie mit der rechten Maustaste auf einen verbundenen Ordner.
2. Wählen Sie im Kontextmenü die Option **Eigenschaften**.
3. Wechseln Sie auf die Registerkarte **Benutzer**. Sie sehen die derzeit vorhandenen Benutzer. Zu Anfang sind dies Sie selbst sowie ein Systemnutzer, den Sie für die Wiederherstellung von Zugangsdaten benötigen, siehe Verlorenes Kennwort wiederherstellen. Für verschlüsselte Ordner, die zentral von ihrem Administrator verwaltet werden können Sie anstelle von einzelnen Benutzern auch Benutzergruppen hinzufügen.
4. Klicken Sie auf **Hinzufügen**.
5. Wählen Sie den Benutzertyp, also die Art der Authentifizierung und geben Sie die geforderten Daten ein.
6. Folgen Sie den weiteren Anweisungen und klicken dann **Fertig stellen**. Sie sehen den neuen Benutzer nun in der Liste.

 © 2021 DriveLock SE

7. Wenn der neue Benutzer Administratoren-Rechte für den Ordner haben darf, markieren Sie das entsprechende Feld.

> Für den Zertifikatsbenutzer benötigen Sie den öffentlichen Schlüssel des neuen Benutzers, siehe Zertifikat veröffentlichen.

## 5.8 Benutzergruppen verwalten

DriveLock Administratoren können zentral verwaltete verschlüsselte Ordner auf Dateiservern anlegen. Um die Benutzerverwaltung für diese Ordner zu erleichtern könne sie auch DriveLock File Protection Gruppen erstellen, die - zusätzlich zu einzelnen Benutzern - zu zentral verwalteten verschlüsselten Ordner hinzugefügt werden können. Wenn Sie Administrator einer DriveLock File Protection Gruppe sind, sind Sie berechtigt weitere Benutzer hinzuzufügen, Benutzer zu löschen und Benutzern Gruppen-Administrationsrechte zu geben oder zu nehmen.

**So verwalten Sie Gruppem:**

1. Öffnen Sie das Hauptmenü **Verschlüsselung**.
2. Klicken Sie auf  um die Liste der verfügbaren Gruppen zu öffnen.
3. Doppel-klicken Sie ein Gruppe um deren Mitglieder zu sehen und zu bearbeiten.

> DriveLock Administratoren können nur Benutzer hinzufügen, während Sie eine Gruppe anlegen. Einmal erzeugt haben sie nicht mehr Rechte als andere Benutzer, außer Benutzer wieder aus einer Gruppe zu löschen.

## 5.9 Verlorenes Kennwort wiederherstellen

Falls Sie das Kennwort für den Zugriff auf die verschlüsselten Daten vergessen haben oder dieses Kennwort aus anderen Gründen nicht mehr verfügbar ist, haben Sie folgende Möglichkeiten:

- **Administrator-Kennwort**: Sie wenden sich an Ihren Administrator, der mit dem Administratorkennwort das Benutzerkennwort zurücksetzen kann.
- **Wiederherstellungsmechanismus im Offline-Modus**: Wenn Ihr Computer nicht mit dem Firmennetz verbunden ist oder Sie keinen Zugriff auf Ihr Zertifikat haben, verwenden Sie das Offline-Verfahren. Sie generieren mit einem Assistenzprogramm aus der verschlüsselten Datei einen Anforderungscode, den Sie an den Administrator übermitteln. Dies kann auch telefonisch geschehen. Der Administrator generiert aus diesem Anforderungscode einen Antwortcode, mit dem Sie ein neues Kennwort für die verschlüsselte Datei vergeben können.
- **Wiederherstellungsmechanismus im Online-Modus**: Wenn Ihr Computer mit dem Firmennetz verbunden ist und Sie Zugriff auf Ihr Zertifikat und das Kennwort für den zugehörigen privaten Schlüssel haben, verwenden Sie das Online-Verfahren. Hierzu müssen Sie das Zertifikat vorher in eine *.pfx-Datei exportiert haben, siehe Zertifikat kopieren.

> Es hängt von den Einstellungen in Ihrem Unternehmen ab, welche Optionen Ihnen zur Verfügung stehen.

**So erstellen Sie ein neues Kennwort im Offline-Modus:**

1. Öffnen Sie das Hauptmenü **Verschlüsselung**.

 © 2021 DriveLock SE

2. Klicken Sie auf **Wiederherstellen** und dann entweder **Verschlüsselter Container** oder **Verschlüsselter Ordner**.
3. Geben Sie den Speicherort der Containerdatei bzw. den Ordnernamen an.
4. Wählen Sie die Option **Offline-Wiederherstellung**.
5. Übermitteln Sie Ihrem Administrator den angezeigten Anforderungscode.

> Klicken Sie auf die drei Punkte neben dem Anforderungscode. Ein Fenster öffnet sich, das den Code in Fliegeralphabet geschrieben zeigt, dies erleichtert Ihnen die telefonische Übermittlung. Zum Beispiel *YB8C* heißt hier "Ypsilon, Berta, Acht, Cäsar". Abhängig von Ihren Systemeinstellungen, können Sie sich den Text auch vorlesen lassen.

6. Geben Sie im folgenden Fenster den Antwortcode ein, den Sie von Ihrem Administrator erhalten haben und vergeben Sie ein neues Kennwort.
7. Klicken Sie auf **Fertig stellen**, um den Assistenten zu beenden.

**So erstellen Sie ein neues Kennwort im Online-Modus:**

1. Wählen Sie die Option **Online-Wiederherstellung**.
2. Geben Sie den Pfad zu Ihrer Zertifikatsdatei *.pfx sowie das zugehörige Kennwort ein. Klicken Sie auf **Weiter**.
3. Alternativ können Sie auch ein Zertifikat auf einer **Smartcard** oder im **Zertifikatsspeicher auf diesem Computer** angeben.
4. Geben Sie ein neues Kennwort ein und bestätigen Sie es. Klicken Sie auf **Weiter**.
5. Klicken Sie auf **Fertig stellen**, um den Assistenten zu beenden.

## 5.10 Die Mobile Encryption Anwendung verwenden

Mithilfe der Mobile Encryption Anwendung können Sie Dateien in einem verschlüsselten Container verwenden, auch wenn auf dem Rechner kein DriveLock installiert ist oder Sie auf dem Rechner keine Administratorrechte haben, um eine Anwendung zu installieren oder Laufwerke zu verbinden.

Sie können die Mobile Encryption Anwendung beispielsweise auf einem verschlüsselten USB-Stick speichern und ihn so an jedem beliebigen Rechner verwenden.

> Mobile Encryption Anwendung liegt als Windows- (`DlMobile.exe`) und MAC- (`DlMobile.MAC.zip`) Anwendung vor.

**So kopieren Sie die Mobile Encryption Anwendung auf ein Speichermedium:**

1. Wählen Sie im Windows-Startmenü **Mobile Encryption Anwendung kopieren**.
2. Geben Sie den Zielort an.
3. Die Programmdateien der Mobile Encryption Anwendung werden in den Zielordner kopiert.

### 5.10.1 Mit der Mobile Encryption Anwendung arbeiten

Die Mobile Encryption Anwendung ist ein Programm, in dem Sie einen Container öffnen, um Dateien in den Container zu kopieren oder Dateien aus dem Container zu exportieren. Sie verwenden dieses Programm, wenn Sie den Container nicht als Laufwerk verbinden wollen oder können, weil Sie beispielsweise keine Administratoren-Rechte auf dem Rechner haben.

 © 2021 DriveLock SE

Wenn Sie die Mobile Encryption Anwendung von einem Speicherort aus starten, der auch eine *.dlv Datei enthält, versucht die Mobile Encryption Anwendung automatisch diesen Container zu öffnen und fragt sofort nach einem Kennwort. In diesem Fall wird auch geprüft, ob Sie als Benutzer lokale administrative Rechte besitzen.

**So verwenden Sie die Mobile Encryption-Anwendung:**

1. Doppelklicken Sie auf die Programmdatei auf dem Datenträger, beispielsweise `DlFPMobile.exe`.
2. Wenn eine *.dlv-Datei im selben Ordner liegt wie die Programmdatei, können Sie den Container gleich verbinden:
   a. Geben Sie das Kennwort ein.
   b. Wählen Sie den Laufwerksbuchstaben, mit dem der Container verbunden werden soll, siehe Container als verschlüsseltes Laufwerk verwenden.
3. Wenn die Mobile Encryption Anwendung nicht sofort einen Container zur Verbindung anbietet, haben Sie folgende Optionen.
   a. **Container verbinden**: Wählen Sie einen Container und verbinden Sie ihn als verschlüsseltes Laufwerk, siehe Container als verschlüsseltes Laufwerk verwenden.
   b. **Laufwerk trennen**: Trennen Sie ein verbundenes Laufwerk, siehe Container als verschlüsseltes Laufwerk verwenden.
   c. **Sprache ändern**: Ändern Sie die Sprache der Oberfläche, siehe Sprache wählen.
   d. **Container öffnen**: Öffnen Sie einen Container auf einem Rechner, auf dem sie nicht über lokale Administratorenrechte verfügen. Wählen Sie hierzu die gewünschte *.dlv-Datei und geben Sie das zugehörige Kennwort ein. Sie können jetzt Dateien importieren und exportieren, siehe Dateien importieren und exportieren.
   e. **Kennwort wiederherstellen**: Stellen Sie ein verlorenes Kennwort wieder her, siehe Verlorenes Kennwort für einen Container wiederherstellen.
4. Klicken Sie auf **Schließen**, um die Mobile Encryption Anwendung zu schließen.

> Wenn Sie die Verbindung mit einem Wechseldatenträger trennen, beispielsweise den USB-Stick herausziehen, trennt DriveLock automatisch auch das verbundene Laufwerk.

### 5.10.2 Dateien importieren und exportieren

Sie können mit der Mobile Encryption Anwendung, Dateien aus einem Container auf einen lokalen Datenträger exportieren. Ebenso können Sie Dateien in den Container importieren.

Verwenden Sie diese Option, wenn Sie den Container nicht als Laufwerk verbinden können, beispielsweise weil Sie keine Administratorrechte haben.

**So exportieren Sie Dateien aus einem Container:**

1. Öffnen Sie den Container in der Mobile Encryption Anwendung.
2. Wählen Sie die gewünschten Dateien oder Verzeichnisse und klicken Sie auf **Exportieren**.
3. Wählen Sie den gewünschten Speicherort.

**So importieren Sie Dateien in den Container:**

1. Markieren Sie im Container das Verzeichnis, in das Sie neue Dateien importieren möchten.
2. Klicken Sie auf **Importieren**.

 © 2021 DriveLock SE

3. Wählen Sie die gewünschten Dateien und klicken Sie auf **Öffnen**.

> Alternativ können Sie Dateien per Drag & Drop exportieren und importieren.

**So verwalten Sie Dateien in einem Container:**

1. Um einen neuen Ordner anzulegen, klicken Sie mit der rechten Maustaste auf einen Ordner und wählen im Kontextmenü die Option **Ordner anlegen**. Geben Sie einen Namen für den Ordner ein.
2. Um Dateien aus dem Ordner zu löschen, klicken Sie mit der rechten Maustaste auf die gewünschte Datei und wählen im Kontextmenü die Option **Löschen**.

## 5.11 Zertifikate verwalten

Zertifikate sind ein Mittel, um einen Benutzer zu authentifizieren. Ein Zertifikat besteht aus einem Schlüsselpaar: einem öffentlichen Schlüssel und einem privaten Schlüssel.

Den öffentlichen Schlüssel (public key) können Sie veröffentlichen, so dass andere Benutzer Ihnen Rechte auf verschlüsselte Daten einräumen können. Zusammen mit ihrem privaten Schlüssel, können Sie die Daten dann entschlüsseln. Genauso benötigen Sie den öffentlichen Schlüssel eines anderen Benutzers, wenn Sie Daten für diesen Benutzer verschlüsseln möchten.

Folgende Aufgaben können Sie erledigen:

- Zertifikat erstellen
- Zertifikat veröffentlichen
- Zertifikat kopieren

### 5.11.1 Zertifikat erstellen und erneuern

Sie können ein persönliches Zertifikat erstellen oder eines vom DriveLock Enterprise Service beziehen. Details hierzu erfahren Sie von Ihrem Administrator.

> Sie können nur ein persönliches und ein Server-Zertifikat erstellen. Wenn Sie diese Zertifikate bereits besitzen, steht die Funktion nicht mehr zur Verfügung. Sie können dann jedoch ein Server-Zertifikat erneuern, um das Ablaufdatum zu verlängern.

**So erstellen Sie ein neues Zertifikat:**

1. Öffnen Sie das Hauptmenü **Verschlüsselung**.
2. Klicken Sie auf  **Zertifikate verwalten**.
3. Wählen Sie eine der folgenden Optionen:
   - **Neuen Benutzer erstellen**: Ein neuer DriveLock Benutzer mit Server-Zertifikat wird auf dem zentralen DriveLock Enterprise Service erstellt.
   - **Verschlüsselungszertifikat erstellen**: Windows erstellt ein persönliches Zertifikat und speichert es auf Ihrem Computer.
4. Geben Sie Ihre persönlichen Daten ein. Sie können auch ein Bild auswählen, das in ihrem öffentlichen Schlüssel angezeigt wird.

 © 2021 DriveLock SE

5. Wählen Sie aus, wo Sie das Zertifikat speichern möchten: auf Ihrem Computer oder auf einem externen Speichermedium, beispielsweise einer Smartcard.

### 5.11.2 Zertifikat veröffentlichen

Sie veröffentlichen den öffentlichen Schlüssel Ihres Zertifikats, damit andere Personen Dateien mit diesem Schlüssel für Sie verschlüsseln können. Der öffentliche Schlüssel wird in eine *.cer-Datei geschrieben, die Sie speichern oder gleich per E-Mail versenden können.

**So veröffentlichen Sie Ihr Zertifikat:**

1. Öffnen Sie das Hauptmenü **Verschlüsselung**.
2. Klicken Sie auf **Zertifikate verwalten**.
3. Wählen Sie **Zertifikat veröffentlichen**.
4. Wählen Sie das gewünschte Zertifikat.
5. Wenn Sie das Zertifikat als Datei speichern möchten, wählen Sie die entsprechende Option und geben den Dateipfad an.
6. Wenn Sie das Zertifikat gleich per E-Mail versenden, wählen Sie die entsprechende Option.

### 5.11.3 Zertifikat kopieren

Sie können ein Zertifikat, das heißt den öffentlichen *und* den privaten Schlüssel, von einem Computer auf einen anderen kopieren. Hierzu exportieren Sie zunächst das Zertifikat in eine *.pfx-Datei und importieren es dann auf dem anderen Computer.

**Wenn Sie einen neuen Computer erhalten, vergessen Sie nicht, Ihre Zertifikate von dem alten Computer auf den neuen umzuziehen, da Sie sonst nicht mehr auf Ihre verschlüsselten Daten zugreifen können.**

**So exportieren Sie Ihr Zertifikat:**

1. Öffnen Sie das Hauptmenü **Verschlüsselung**.
2. Klicken Sie auf **Zertifikate verwalten**.
3. Wählen Sie **Zertifikat zu oder von einem anderen Computer kopieren**.
4. Wählen Sie **Zertifikat exportieren**.
5. Wählen Sie das gewünschte Zertifikat und geben Sie den Dateipfad an.
6. Geben Sie ein Kennwort ein und bestätigen Sie es.

**So importieren Sie Ihr Zertifikat:**

1. Wählen Sie **Zertifikat importieren**.
2. Wählen Sie die *.pfx-Datei, die Sie exportiert haben.
3. Geben Sie das Kennwort ein, das Sie beim Exportieren vergeben haben.

Das Zertifikat wird importiert und steht auf dem neuen Computer zur Verfügung.

 © 2021 DriveLock SE

# Teil VI

## DriveLock-Status einsehen

# 6 DriveLock-Status einsehen

Sie können Informationen zu Laufwerken, Geräten und aktuell aktiven DriveLock-Richtlinien einsehen. Die Statusübersicht ist eine wertvolle Informationsquelle, wenn es darum geht herauszufinden, ob ein Gerät oder ein Laufwerk gesperrt oder freigegeben ist. Sie dient auch einem Administrator zur Fehlerermittlung.

Diese Funktion kann durch Ihren Administrator gesperrt sein.

**So sehen Sie den Status von Geräten ein:**

1. Öffnen Sie das Hauptmenü **DriveLock-Status**. Sie sehen eine Übersicht mit den verschiedenen Systemklassen:
   - **Geräte** enthält alle internen Geräte des Computers wie Netzwerk- oder Maus-Controller, Prozessoren oder USB-Schnittstellen.
   - **Laufwerke** enthält alle Datenspeicher und Datenlesegeräte wie Festplatten und CD/DVD-Laufwerke.
   - **Richtlinien** zeigt die aktuell verwendeten Richtlinien an.
   - **Smartphones** zeigt die verbundenen mobilen Telefone an.
2. Im Detailbereich sehen sie folgende Informationen zu der ausgewählten Systemklasse:
   - **DriveLock-Richtlinie**, die für die Geräte dieser Gruppe angewendet wird.
   - **Status** des Systems, beispielsweise die Zuordnung der Testumgebung.
3. Doppelklicken Sie auf die gewünschte Systemklasse, um Details zu den darin enthaltenen Geräten bzw. Richtlinien zu erhalten.
4. Klicken Sie auf **Zurück**, um wieder zu der Systemklassenübersicht zu gelangen.
5. Klicken Sie auf **Aktualisieren**, um die Übersicht zu aktualisieren.

 © 2021 DriveLock SE

# Teil VII

## Daten sicher löschen

# 7 Daten sicher löschen

Wenn Sie Dateien oder Verzeichnisse mithilfe des Windows Explorer löschen, werden die tatsächlichen Daten nicht zerstört. Windows löscht lediglich die entsprechenden Referenzen zu der Datei im Dateisystem, so dass sie nicht mehr aufgefunden werden kann. Es gibt jedoch frei verfügbare Software, die diese Dateien findet und wieder herstellen kann.

Mit DriveLock löschen Sie Dateien und Verzeichnisse so, dass die Informationen nicht mehr hergestellt werden können. Dazu wird jede gelöschte Datei mit zufälligen Daten überschrieben. Der dafür genutzte Algorithmus bestimmt, wie häufig die Datei überschrieben wird und wie zufällige Daten generiert werden.

DriveLock hat mehrere verschiedene Algorithmen integriert, um Daten sicher zu löschen. Sofern durch Ihren Administrator keine Vorgabe erfolgt, können Sie einen dieser Algorithmen wählen.

> Das Sichere Löschen kann mehrere Minuten dauern – abhängig von abhängig von Dateigröße und Lösch-Algorithmus. Besonders bei Löschvorgängen über das Netzwerk kann dies länger dauern.

**So löschen Sie eine Datei oder ein Verzeichnis endgültig:**

1. Klicken Sie im Windows Explorer mit der rechten Maustaste auf die gewünschte Datei oder das gewünschte Verzeichnis und wählen Sie im Kontextmenü die Option **Sicher Löschen**.
2. Wählen Sie den gewünschten Algorithmus und klicken Sie auf **Ja**, um die Prozedur zu starten.
3. Wenn Sie den Algorithmus nicht ändern können, hat Ihr Administrator ihn bereits vordefiniert.

 © 2021 DriveLock SE

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.

© 2021 DriveLock SE