Handbuch

Dok.-Nr.: ACL-HB-8.11.3
Ausgabedatum: 07.01.2021
Ausgabe-Nr.: 191

ArchiCrypt Live

D-85521 Ottobrunn
Telefon (089) 66000893
Telefax (089) 66000875
Email Info@ArchiCrypt.com

Inhalt

4 Bestellen / Registrieren

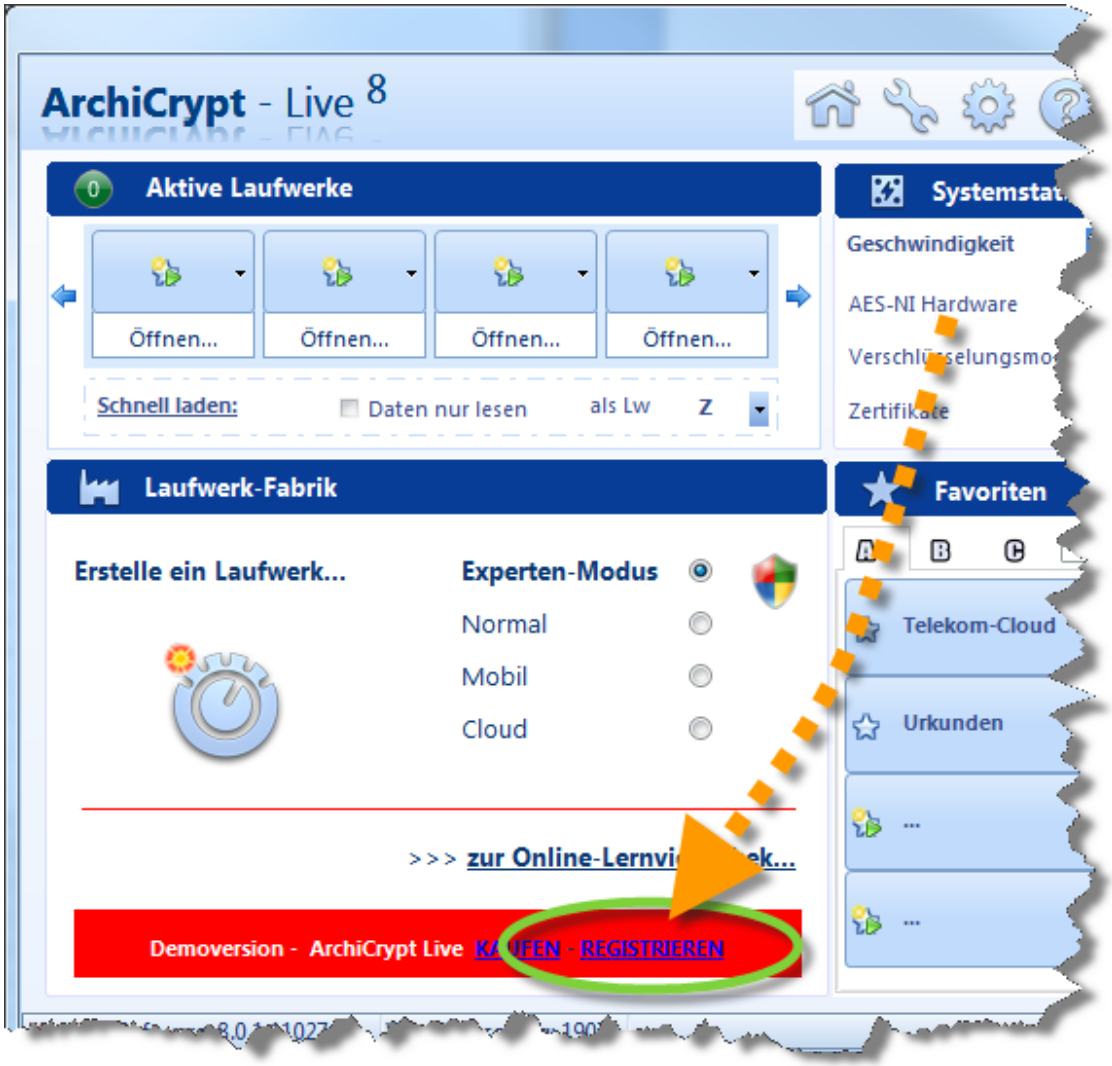
Bestellen bei ArchiCrypt

ArchiCrypt Live im Shop

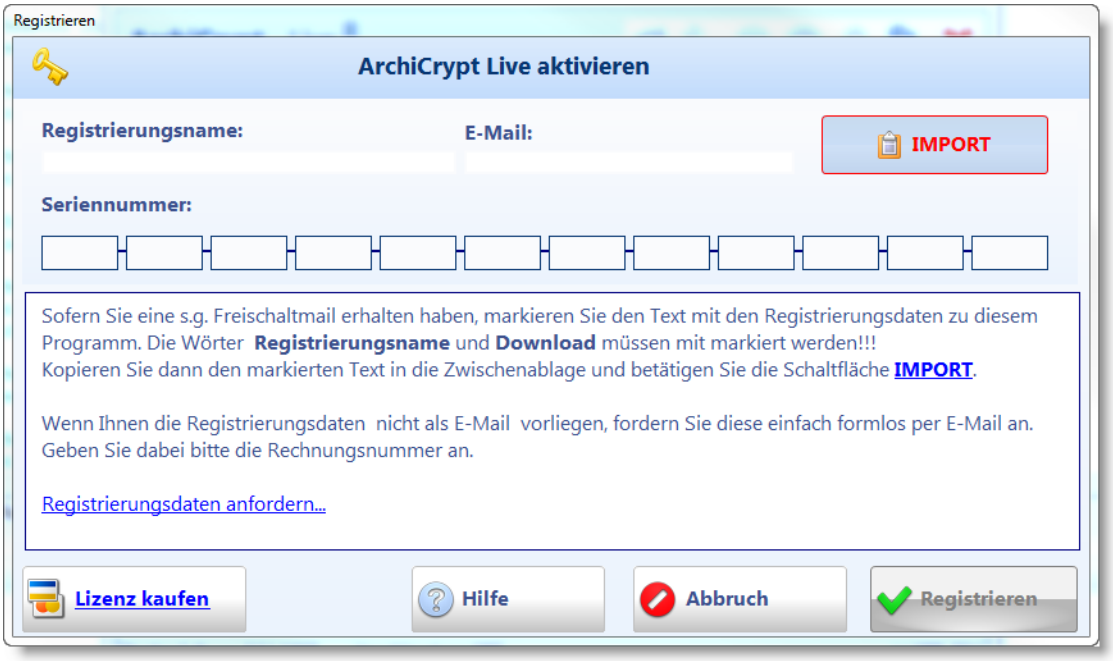
Weitere Bestellmöglichkeiten >>

So schalten Sie ArchiCrypt Live frei

Nach Erhalt der Seriennummer starten Sie bitte das Programm.
Klicken Sie auf Registrieren.



Es erscheint der folgende Dialog:



1. In den meisten Fällen wurden Ihnen die Daten per E-Mail zugestellt. Für diesen Fall gibt es eine sehr einfache Methode, die Software zu aktivieren.
2. Öffnen Sie die E-Mail mit den Daten zum Programm.
3. Markieren Sie die Daten des Programms mit der linken Maustaste.
4. Der markierte Text **muss dabei mindestens** die Begriffe **Registrierungsname** und **die komplette Seriennummer** enthalten. Es sollte in etwa wie folgt aussehen:

```
*** ab hier kopieren ***
Registrierungsname:
Mustermann9876
E-Mail:
Max.Mustermann@MaxMustermannsSeite.de
Seriennummer:
2424-C569-8354-A7A1-A1AF-8663-B777-12BB-C3FB-C797-DA71-6D
Download:
http://download.archicrypt.de/Live_Vollversion.zip
***bis hier kopieren***
```

5. Klicken Sie jetzt auf *IMPORT*

6. Die Daten werden jetzt in das Registrierungsformular übertragen und die Registrierung abgeschlossen. Ein Dialog der zum Neustart der Anwendung auffordert, wird angezeigt.

Weitere Bestellmöglichkeiten

Weitere Bestellmöglichkeiten		
Online-Shop	**zum Online-Shop**	Sobald Sie den Bestellvorgang starten, wird eine verschlüsselte SSL-Verbindung aufgebaut. Alle Daten, die zwischen Ihrem Rechner und unserem Bestellsystem übertragen werden, sind dadurch gegen fremden Zugriff geschützt. Internet-Shopping auf sichere Art!
Telefon	**(089) 66000-893** Dienstag - Donnerstag 09.00 - 12.00 Uhr	Teilen Sie uns die Rechnungsanschrift mit und halten Sie einen Stift und ein Stück Papier bereit. Der Bearbeiter teilt Ihnen das Passwort zur Freischaltung sofort am Telefon mit, das Produkt kann sofort produktiv eingesetzt werden. Gerne beantworten wir auf diesem Wege auch offene Fragen.
Anonym	**Anschrift:** Softwareentwicklung Dipl.-Ing. Patric Remus Am Brunneck 6 85521 Ottobrunn	Voraussetzung für den anonymen Bezug der Software ist ein E-Mail-Zugang bei einem Anbieter, der ihre persönlichen Angaben nicht überprüft. Senden Sie uns einen Brief mit Bargeld in EURO in Höhe des Produktpreises. Fügen Sie dem Brief die E-Mail Adresse bei. Sie erhalten Ihre Registrierungsdaten dann an diese Mailadresse.

5 Hilfe zur Hilfe

Nutzen Sie die Hilfe

Die Hilfe zu ArchiCrypt Live ist sehr umfangreich. Dennoch sollten Sie sich die Zeit nehmen, und die wichtigsten Kapitel zumindest überfliegen.

Als Anwender sollten Sie mindestens die folgenden Kapitel lesen.

- Tipps für den Umgang mit der Software
- Installationshinweise
- Systemvoraussetzungen
- Bedienung
- Datensicherung

Grundsätzlich gilt.
Wenn man sich über die Auswirkung einer Aktion nicht sicher ist, sollte der Blick in das Handbuch erfolgen.

Symbole in der Hilfedatei

Innerhalb der Hilfe sind besondere Textstellen durch bestimmte Symbole hervorgehoben.

➡ UNBEDINGT LESEN

Textstellen, die mit einem solchen Symbol gekennzeichnet sind, sollten Sie unbedingt lesen. Sie weisen häufig auf Gefahrenquellen und Fehlerfallen hin oder beschreiben wichtige Sachverhalte.


WICHTIGE HINWEISE

Textstellen, die mit einem solchen Symbol gekennzeichnet sind, enthalten wichtige Informationen über Verhaltensweisen der Software und technische Hintergründe.


TIPPS und Tricks

Textstellen, die mit einem solchen Symbol gekennzeichnet sind, enthalten Hinweise zu Möglichkeiten, die Ihnen die Arbeit mit ArchiCrypt Live erleichtern.


Grafik interaktiv
Die Grafik bietet interaktive Elemente. Klicken Sie auf den Bereich der Grafik über den Sie mehr erfahren möchten.


TECHNIK
Hier werden Ihnen technische Hintergründe erläutert.

6 Tipps für den Umgang mit der Software

Fertigen Sie sofort eine Kopie einer Schlüsseldatei oder ArchiCrypt Card an

JEDE Datei ist anfällig für Störungen, eine Schlüsseldatei ist keine Ausnahme! Smartcards können ebenfalls zerstört werden oder verloren gehen. Solche Vorkommnisse sind selten, aber überaus dramatisch in ihren Folgen. Ohne Schlüssel ist MIT KEINEM Mittel ein Zugriff auf die Daten in einem Live Laufwerk möglich. Arbeiten Sie daher stets mit der Kopie eines Schlüssels. Planen Sie beim Einsatz von Smartcards für jeden Nutzer 2-3 Karten ein.

Master PIN

Beim Einsatz einer ArchiCrypt Card können Sie diese mit einer PIN zusätzlich absichern. Wird die PIN 4 Mal falsch eingegeben, wird die Karte gesperrt. Die Sperre (*PIN Fehler zurücksetzen*) kann im Personalisieren Dialog zurückgesetzt werden. Wenn Sie die Karte zusätzlich mit einer Master PIN abgesichert haben, dann ist für bestimmte Operationen die Master PIN einzugeben. Wird diese 3 Mal falsch eingegeben, wird die komplette ArchiCrypt Card unbrauchbar. Es kann also auch kein PIN Fehler zurückgesetzt werden, wodurch Sie in der Folge eventuell keinen Zugriff mehr auf Laufwerksinhalte haben, sofern Sie keine Maßnahmen im Vorfeld ergriffen haben.!

Also MASTER PIN MERKEN

Sie können im Vorfeld folgende Maßnahmen ergreifen:

1. Fertigen Sie nach dem Erzeugen des Schlüssels auf der ArchiCrypt Card einen Klon an. Diesen Klon können Sie bei Verlust oder dann, wenn Sie PIN/Master PIN vergessen haben, nochmals verwenden. Verwahren Sie diese Karte an einem sicheren Ort.

2. Sie können die Laufwerke zunächst mit einem klassischen (sehr langen Passwort absichern). Dieses Passwort notieren Sie und verwahren es an einem sicheren Ort. Anschließend fertigen Sie eine Schlüsselsicherung durch Verwaltung - Key-Sicherung. Jetzt ändern Sie den Zugang auf SmartCard. Geht die SmartCard verloren oder Sie vergessen die PIN/Master PIN, können Sie die Schlüsselsicherung zurückspielen und mit dem Passwort auf das Laufwerk zugreifen. Achten Sie darauf, dass Sie dies für ein normales Live Laufwerk ebenso durchführen müssen, wie für das Geheimfach.

 Richten Sie nach dem Erstellen einen Gastzugang ein

Sie können für ein Laufwerk direkt nach dem Erstellen einen Gastzugang einrichten, den Sie alternativ zum Beispiel mit einem "normalen" Passwort absichern. So haben Sie selbst dann noch Zugriff zu Ihrem Laufwerk, wenn Schlüsseldatei, Smartcard oder Token zerstört sind. Das funktioniert nicht für das Geheimfach, da es hier nur einen Zugang gibt! Hier müssen Sie eine Schlüsselsicherung mit normalem Passwort wie oben beschrieben ausführen.
siehe: Verwaltung - Zugang

Führen Sie nach dem Erstellen eines Laufwerks eine Schlüssel-Sicherung durch

Nutzen Sie die Möglichkeiten des Key Backup, um ein s.g. Notfallpasswort zu erzeugen, mit dem Sie jederzeit an den Inhalt eines Laufwerks gelangen können.
siehe: Verwaltung - Key-Sicherung

Führen Sie regelmäßig Backups durch

Sichern Sie die Trägerdatei (*Datei die Ihr ArchiCrypt Laufwerk beherbergt*) je nach Wichtigkeit in regelmäßigen Abständen! Ein ArchiCrypt Live Laufwerk ist für Ihr Windowssystem eine ganz normale Datei. Diese Datei kann, wie jede andere Datei auch, beschädigt oder versehentlich gelöscht werden. In diesem Fall sind all Ihre Daten für immer verloren!

Beachten Sie die Eigenheiten bestimmter ArchiCrypt Live Laufwerke

Sie können beim Erzeugen neuer Laufwerke die Optionen Wachsendes Laufwerk oder Ultraschnelles Erstellen auswählen. Im Umgang mit diesen Laufwerken sind einige Besonderheiten zu beachten.
NTFS Laufwerke benötigen immer exklusiven schreibenden Zugriff. Somit ist das Laden solcher Laufwerke von CD/CDRW und DVD (*allgemein Medium mit Schreibschutz*) nicht unter allen Betriebssystemen möglich!

Binden Sie Netzverzeichnisse als Netzlaufwerke ein

Sie können ArchiCrypt Live Laufwerke im Netzwerk freigeben. Bedenken Sie jedoch, dass alle Daten im Klartext über das Netzwerk übertragen werden. Wenn Sie hingegen ein ArchiCrypt Live Laufwerk

von einer Netzwerkressource laden, erfolgt die Übertragung voll verschlüsselt.

Merken Sie sich Ihr Passwort und bewahren Sie stets eine Kopie Ihrer Schlüsseldatei auf

ArchiCrypt Live besitzt keinen Hauptschlüssel oder eine sonstige "Backdoor" (*Hintertür*). Wenn Sie Ihren Schlüssel (*Passwort/Schlüsseldatei/SmartCard/etc.*) verlieren, gibt es keinerlei Möglichkeit mehr, an die Daten zu gelangen! Auch wir als Entwickler haben keine Chance, ohne Passwort an die Daten zu gelangen.

7 Energiespar-Funktionen

WARNUNG: Als Anwender wird man regelmäßig davon ausgehen, dass der Rechner beim Herunterfahren bzw. beim Betätigen des Netzschalters tatsächlich alle Programme beendet und insbesondere die Daten aus dem Speicher des Systems entfernt werden. Bei Vorhandensein entsprechender Hardware ist dies jedoch nicht der Fall. In der Folge kann dies gerade im Zusammenhang mit ArchiCrypt Live dazu führen, dass geschlossen geglaubte Live Laufwerke nach dem vermeintlichen Neustart ohne Angabe eines Passwortes zur Verfügung stehen. Bei Fremdzugriff hätte also jemand, der einfach nur den Rechner startet Zugriff auf zuletzt offene Live Laufwerke.

So sichern Sie sich ab!

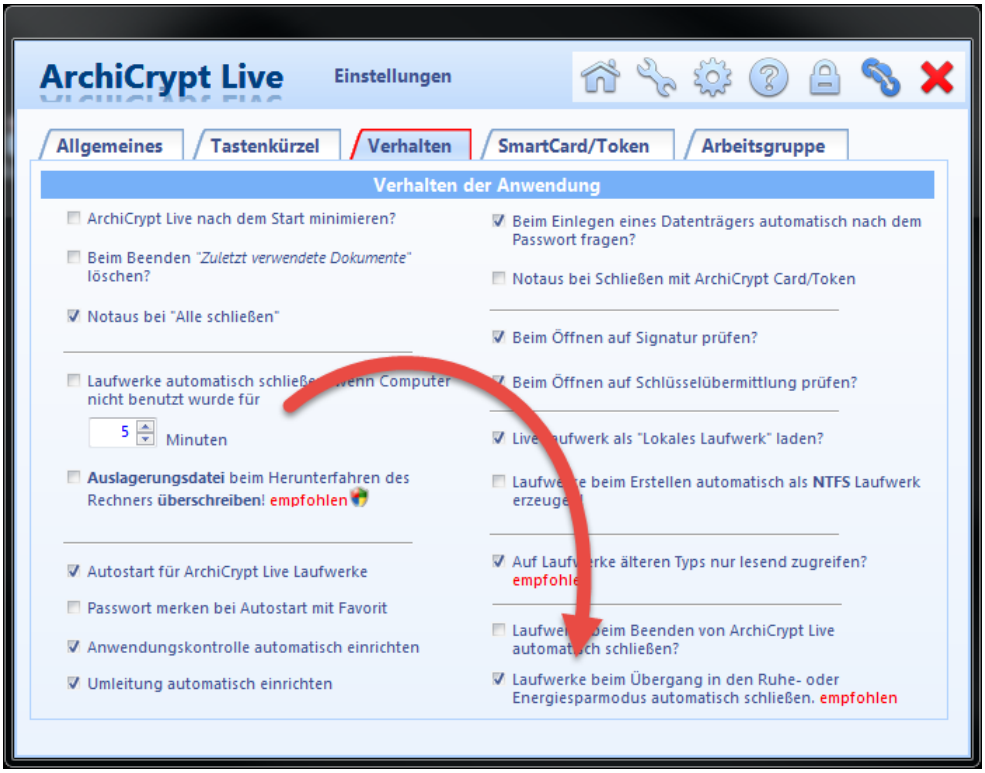
1. Laden Sie ein Live Laufwerk und prüfen Sie, ob nach Herunterfahren und Neustart das Laufwerk noch geöffnet ist.
2. Testen Sie dies ebenso für den Fall, dass Sie den Rechner mit Hilfe des Netzschalters herunterfahren.

Bleibt bei einem der Versuche ein Laufwerk geöffnet, beendet Windows sich nicht komplett, sondern speichert aufgrund der Energiespar-Optionen den Zustand des Systems bis zum nächsten Start zwischen.

Um zu verhindern, dass Live Laufwerke geöffnet bleiben, haben Sie zwei Möglichkeiten:

1. Gehen Sie in die Einstellungen von ArchiCrypt Live und wechseln Sie zu der Registerkarte Verhalten.
Hier aktivieren Sie bitte die Option
"Laufwerke beim Übergang in den Ruhe- oder Energiesparmodus automatisch schließen."

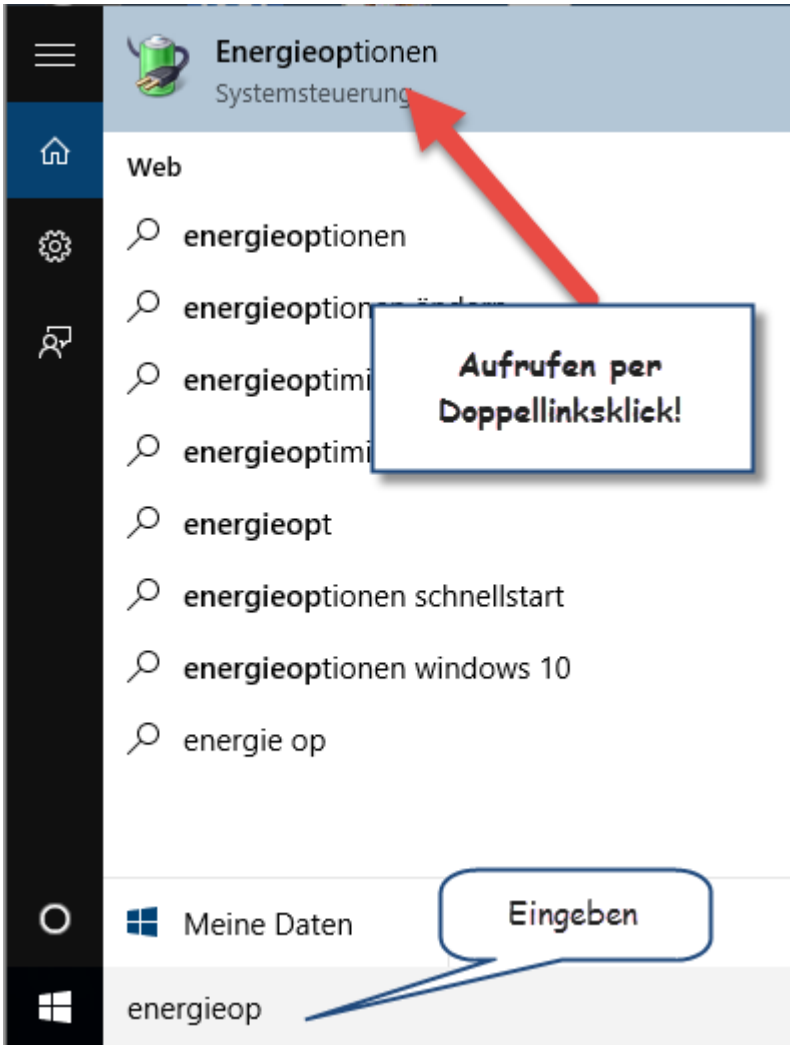
Damit ArchiCrypt Live auf solche Ereignisse wie den Übergang in den Energiesparmodus reagieren kann, muss ArchiCrypt Live auch aktiv sein (*Ruhen im Systemtray genügt*).



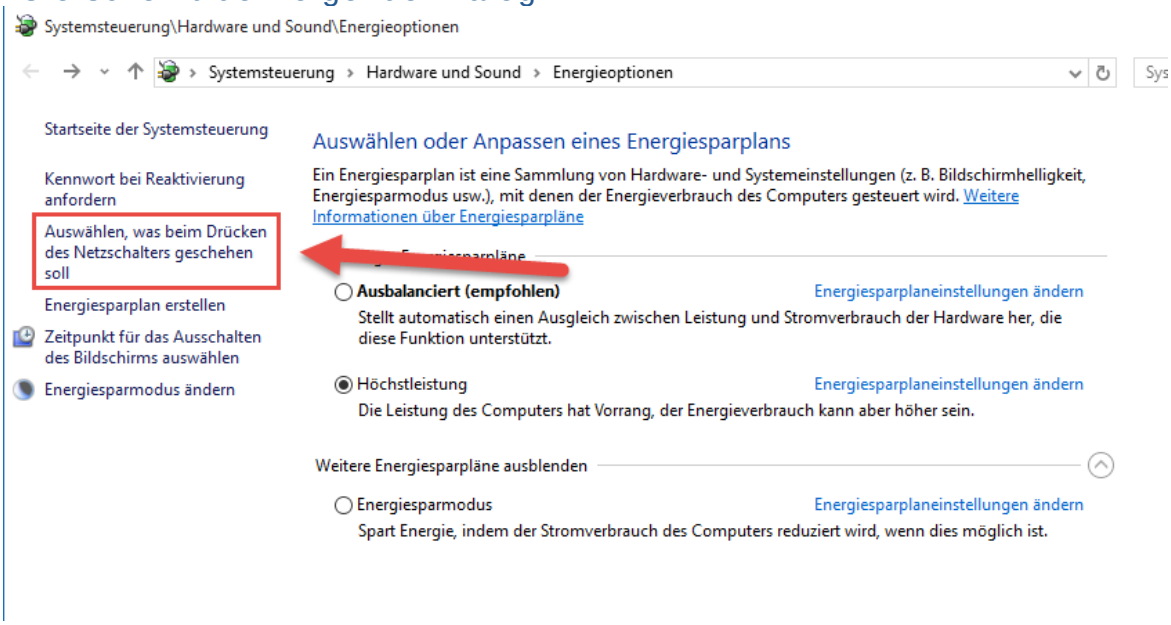
Beim Übergang in ganz bestimmte Energiesparmodi meldet das System dies nicht an Anwendungen wie ArchiCrypt Live weiter. ArchiCrypt Live kann folglich nicht reagieren und die Laufwerke bleiben offen. Testen Sie also unbedingt das Verhalten beim Herunterfahren erneut.

2. Wenn Variante 1 nicht korrekt arbeitet, müssen Sie Änderungen an den Energiespareinstellungen vornehmen. Nachfolgend wird das Vorgehen exemplarisch für Windows 10 gezeigt.

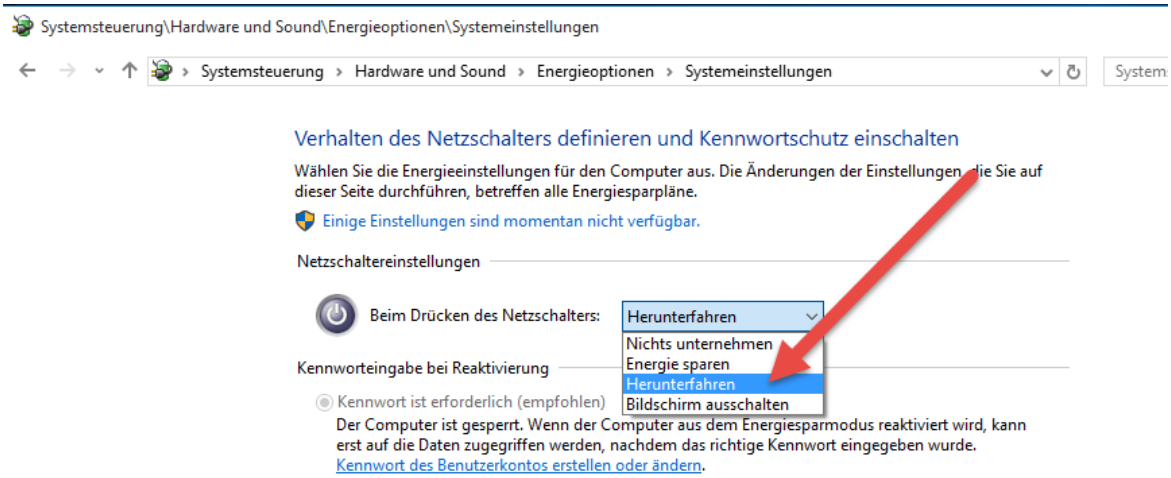
Geben Sie "Energieoptionen" in das Suchfeld ein und rufen Sie die **Energieoptionen** auf.



Es erscheint der folgende Dialog:



Wählen Sie "**Auswählen, was beim Drücken des Netzschalters geschehen soll**"



Wählen Sie im Auswahlfeld die Option **Herunterfahren** aus.

Klicken Sie im gleichen Dialog auf "**Einige Einstellungen sind momentan nicht verfügbar**". Weiter unten im Dialog bei "**Einstellungen für das Herunterfahren**" nehmen Sie das Häkchen bei **Schnellstart aktivieren (empfohlen)** heraus.

Gehen Sie jetzt auf "**Änderungen speichern**".

8 Einleitung

8.1 Willkommen

Vielen Dank, dass Sie sich für ArchiCrypt Live© entschieden haben.

Die Menge vertraulicher Daten und deren Schutzbedürfnis steigt mit dem Wachstum der öffentlichen und firmeninternen Netzwerke. In

dieser neuen "Digitalen Welt" besteht die größte Herausforderung darin, eigene Informationen vor Unbefugten zu schützen.

Einfachheit, Sicherheit und Leistungsfähigkeit sind die Schlagworte, die man guten Gewissens im Zusammenhang mit ArchiCrypt Live nennen kann.
Wir haben es uns zur Aufgabe gemacht, Verschlüsselung aus der "Ecke" des Mystischen und Komplizierten herauszuholen. Einfachste Handhabung für normale Anwender und gleichzeitig Sicherheit auf Augenhöhe mit staatlichen Institutionen und Regierungsbehörden.

ArchiCrypt Live setzt in Version 8 auf pfiffige Funktionen, ausgefeilte Bedienkonzepte. Was die Verschlüsselungsverfahren angeht, setzen wir kompromisslos auf internationale Standards.
Bei der Realisierung der neuen Version standen die Punkte Sicherheit, Bedienkomfort und Cloud-Schutz im Vordergrund unserer Bemühungen.

Schützen Sie Ihre Privatsphäre, gehen Sie verantwortungs- und vertrauensvoll mit Ihren Kundendaten um, schützen Sie das Know-how Ihres Unternehmens.

ArchiCrypt Live © ist ideal für

- Firmen und Behörden die mit sensiblen Daten umgehen
- Banken und Versicherungen
- Rechtsanwälte und Notare
- Steuerberater und Finanzdienstleister
- Unternehmens- und Personalberatungen
- Ärzte

und alle, die Daten mit den besten Methoden unüberbietbar schnell schützen möchten.

Die neusten Entwicklungen können Sie wie gewohnt unter www.ArchiCrypt.de einsehen.

Dipl.-Ing. Patric Remus

8.2 Neu in dieser Version

Neu in Version 8

Video - Neues in Version 8

Sollten sich das Video im Browser nicht anzeigen lassen, so können Sie das Video alternativ direkt in Youtube auf unserem ArchiCrypt Kanal ansehen.

ArchiCrypt Live glänzt in Version 8 erneut mit pfiffigen und einzigartigen Funktionen. Was die Verschlüsselungsverfahren angeht, setzen wir kompromisslos auf internationale Standards. Bei der Realisierung der neuen Version standen die Punkte Komfort, Geschwindigkeit und Sicherheit im Vordergrund unserer Bemühungen. Wie immer spielten neben den technischen Entwicklungen die Anregungen unserer treuen Kunden eine maßgebliche Rolle.

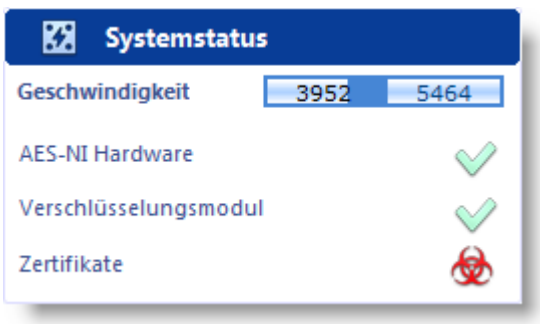
Optik und Bedienung

ArchiCrypt Live 8 bringt eine umstrukturierte und moderne Bedienoberfläche. Bei der Neukonzeption wurde sorgfältig darauf geachtet, dass das bewährte Bedienkonzept erhalten bleibt. Langjährige Nutzer finden sich sofort zurecht, neuen Anwendern

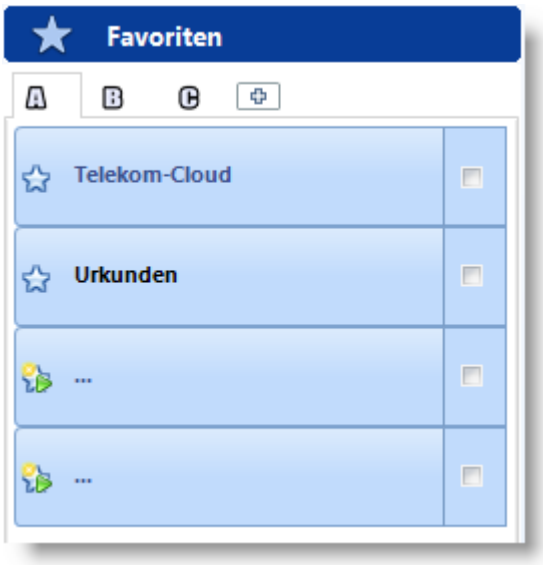
fällt der Einstieg leicht. Das Laden einzelner Laufwerke geht schneller von der Hand.

Linksklick, Live-Datei auswählen und fertig. Neu ist auch die Möglichkeit, eine Live-Datei einfach per Drag und Drop auf einen freien Slot zu ziehen. Einfach loslassen und das Laufwerk wird nach Passworteingabe geladen.

Neu hinzu gekommen ist die Systemstatus-Ansicht, die Auskunft über Performance und Sicherheit gibt.



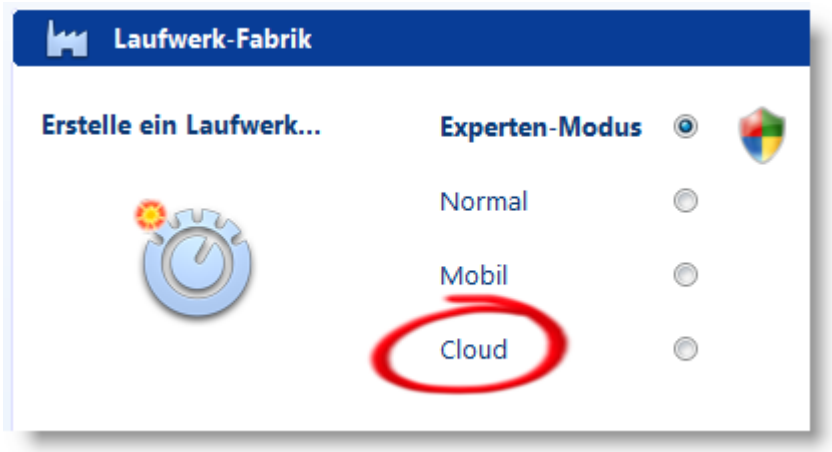
Die Favoriten sind jetzt auf Reiterseiten organisiert. Statt 8 haben jetzt 12 Favoriten Platz.



Das Erstellen neuer Laufwerke kann wahlweise im Expertenmodus oder in etwas verkürzter Form erfolgen.

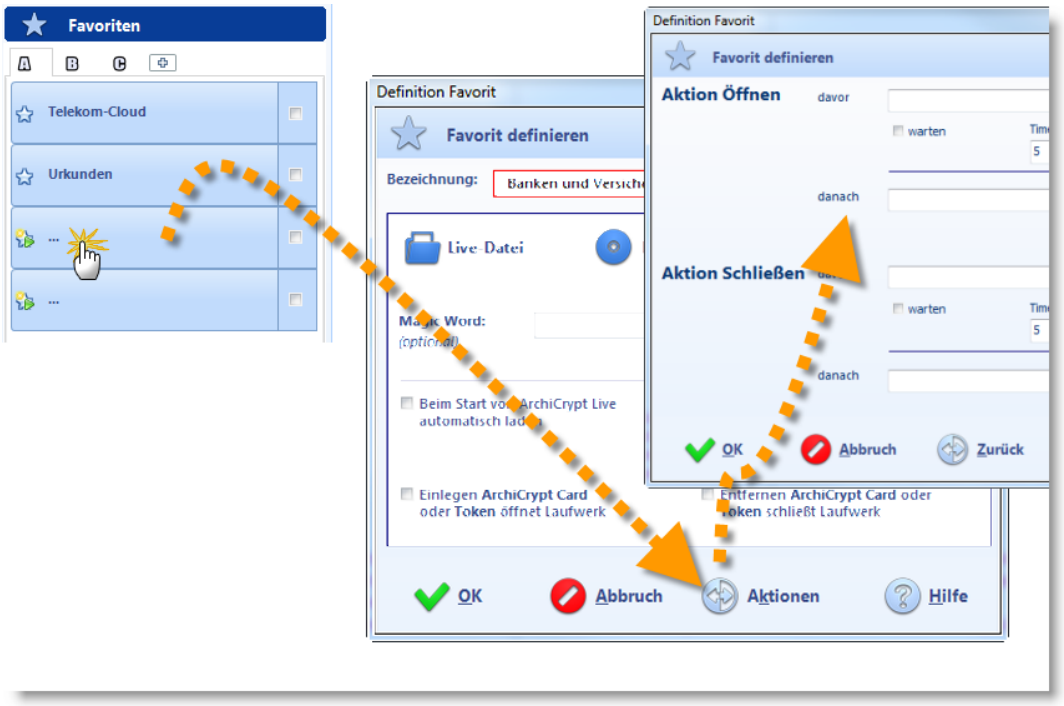
Schutz für die Cloud

Sensible Daten gehören nicht ungeschützt in die Cloud! Das sollte inzwischen wirklich jedem klar sein. Gleichzeitig ist es natürlich extrem bequem, die Daten auf Rechner A schnell und effektiv mit denen auf Rechner B zu synchronisieren.
Auf der Arbeit den Vertrag in die Cloud laden und zu Hause daran weiter arbeiten. Findet ArchiCrypt Live auf Ihrem Rechner einen bekannten Cloud-Dienst (*Dropbox, Google Drive, One Drive, Telekom-Cloud bzw. MagentaCLOUD und Strato HiDrive*) können Sie in der Laufwerk-Fabrik die entsprechende Option auswählen. ArchiCrypt Live legt dann im passenden Verzeichnis ein Laufwerk an. Alle Daten werden vor der Übertragung in die Cloud in Echtzeit verschlüsselt. Der Cloud-Anbieter sieht ausschließlich Datenmüll, mit dem ohne Passwort nichts anzufangen ist.



Aktionen für Laufwerksoperationen

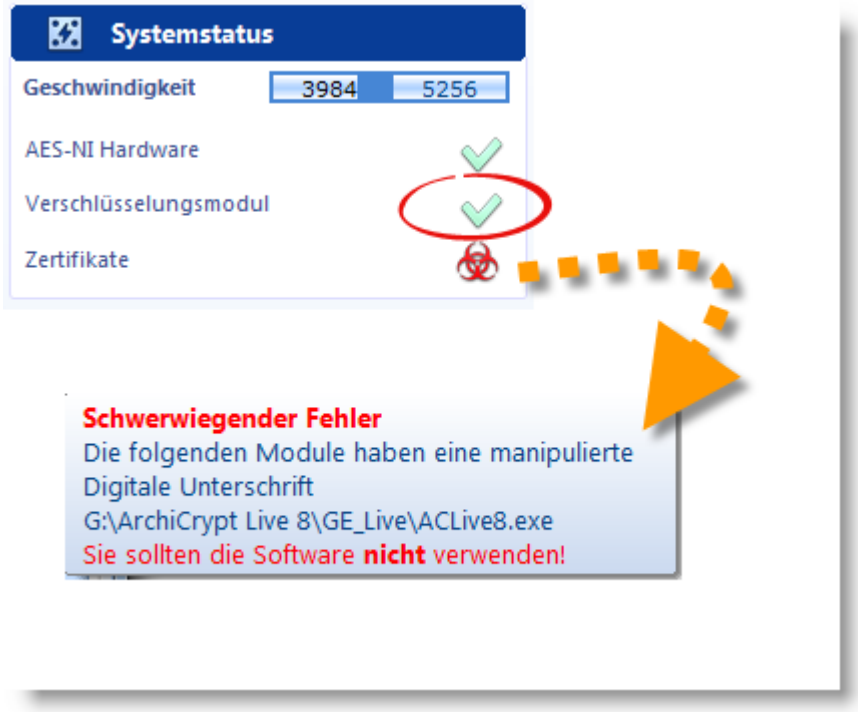
Kenner wissen, dass man mit Favoriten diverse Möglichkeiten hat, die man im Zusammenhang mit dem "normalen" Laden von Laufwerken nicht hat.



Mit Hilfe dieser Aktionen ist es möglich, zahlreiche Aufgaben zu automatisieren. Mit Hilfe spezieller Kommandos ist es zum Beispiel auch möglich, Anwendungen zu beenden.

Sicherheit und Selbsttest

Manipulierte Sicherheitssoftware ist gefährlich. Man wähnt seine Daten in Sicherheit, während in Wahrheit Unbefugte vollen Zugriff auf die Daten haben. Um solchen Manipulationen vorzubeugen, führt die Software verschiedene Selbsttests durch. Hierbei wird geprüft, ob Verschlüsselungsroutinen und Kernmodule in Takt sind.



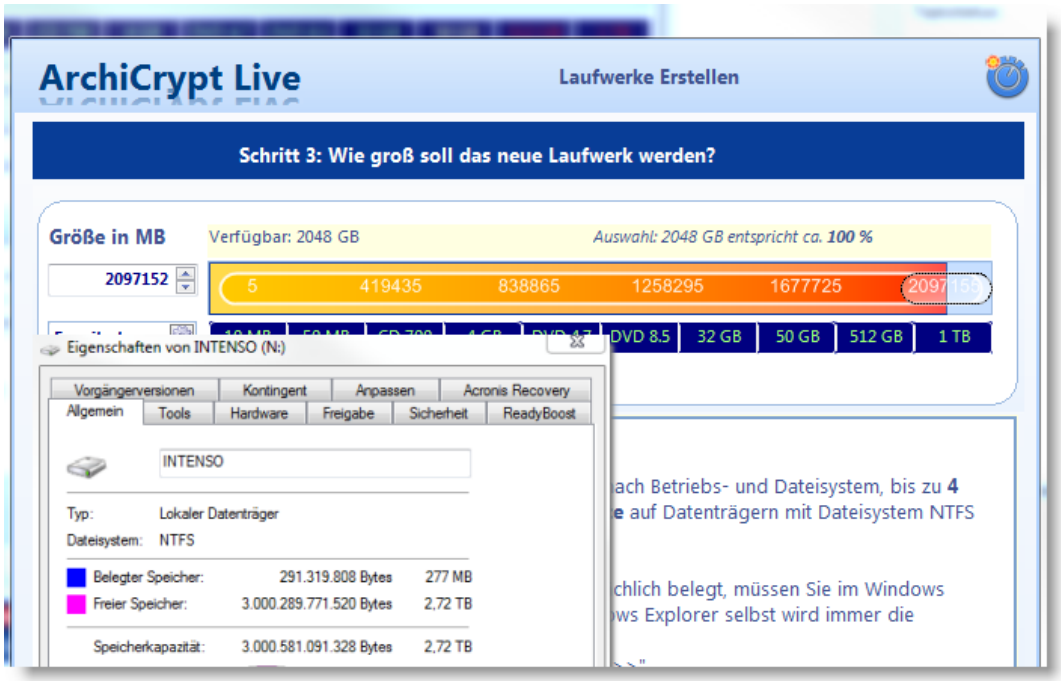
AES-NI Hardware Unterstützung

Prozessoren, die nach 2008 produziert wurden, bieten inzwischen nahezu alle den s.g. AES-NI Befehlssatz an. AES Verschlüsselung kann hier direkt als Prozessorbefehl ausgeführt werden, wodurch bei der Verschlüsselung enorme Geschwindigkeitsvorteile gegenüber der Verschlüsselung im Programmcode entstehen. ArchiCrypt Live unterstützt diese Befehle für alle mit AES verschlüsselten Laufwerke. Laufwerke, die mit Version 7 erstellt werden, profitieren bereits davon und müssen nicht konvertiert werden.

AES NI Support

Unterstützung großer externer Festplatten

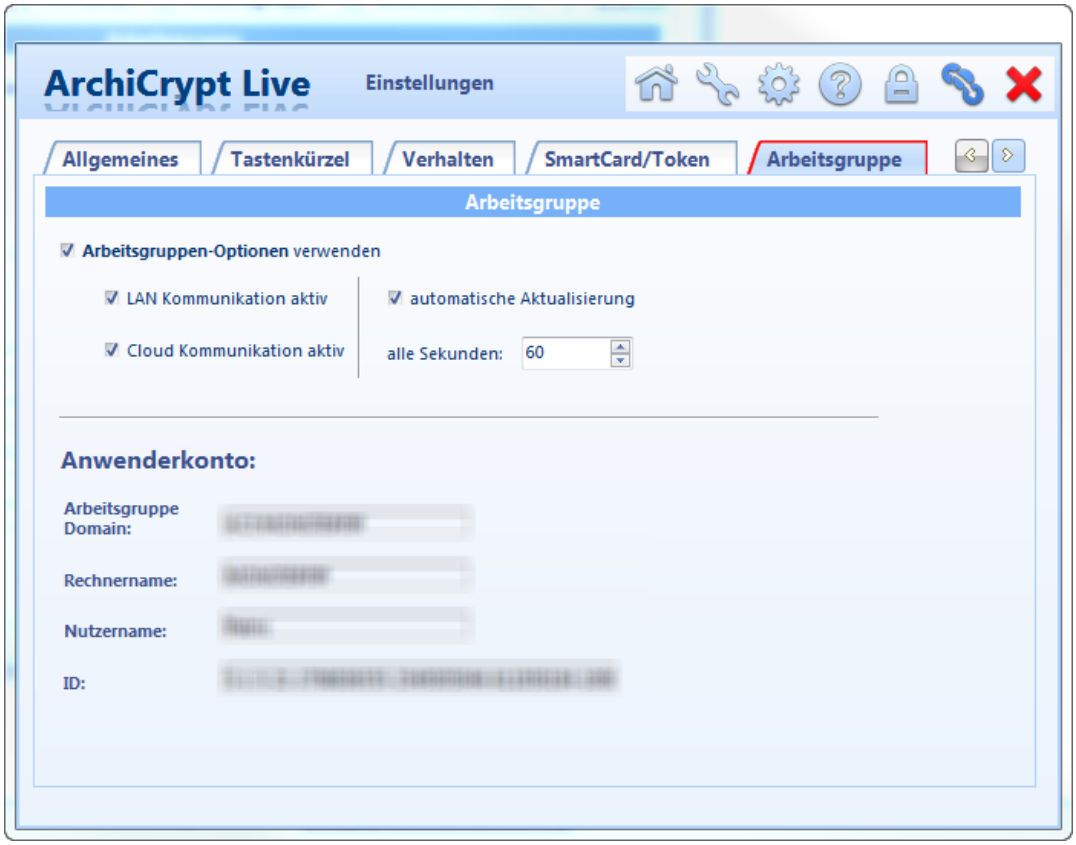
Die Kapazitäten externer Festplatten und Datenträger steigen weiter an. Inzwischen sind Laufwerke jenseits der 2 Terabyte keine Seltenheit mehr. Um mit existierenden Betriebssystemen weitgehend kompatibel zu sein, werden dem Betriebssystem bestimmte Parameter vorgegaukelt. ArchiCrypt Live wurde so angepasst, dass diese Datenträger korrekt angesprochen werden. Einzelne Live Laufwerke selbst können 2 Terabyte an Daten aufnehmen.



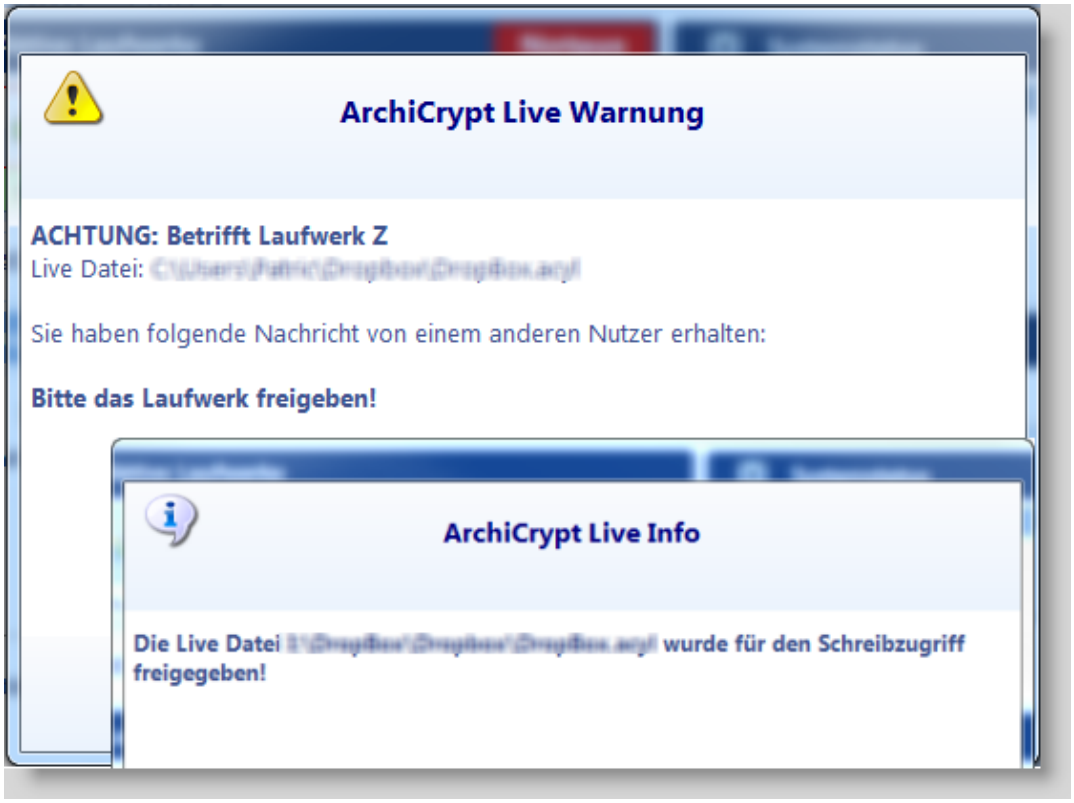
Externe Festplatte verschlüsseln

Unterstützung für kleine Arbeitsgruppen

Wenn Sie Live Laufwerke an einem Speicherort ablegen, der durch mehrere Nutzer angesprochen werden kann (*Netzwerkfreigabe*, *NAS-Server*), dann können diese Nutzer auch gemeinsam das Live-Laufwerk laden. Damit kann ein Anwender schreibend (*er kann Daten lesen, schreiben, löschen, ändern*) und eine beliebige Anzahl an Anwendern lesend auf die Daten zugreifen.



Möchte man schreibend zugreifen und das Laufwerk ist bereits durch einen anderen Anwender entsprechend geöffnet, kann man diesem eine Nachricht senden. Wird das Laufwerk von diesem freigegeben, erhält man eine entsprechende Benachrichtigung.



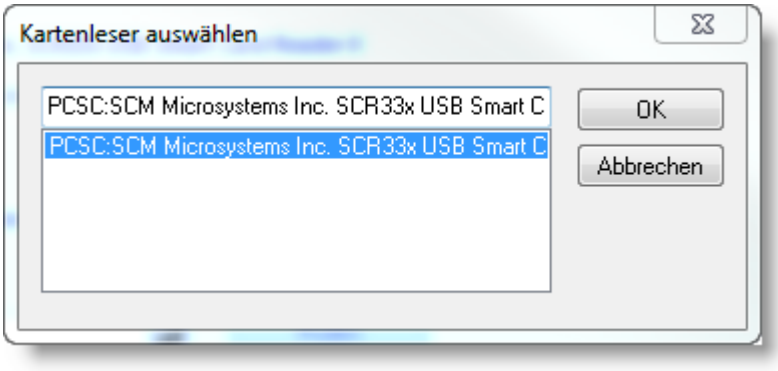
Verschlüsselung Arbeitsgruppe

9 Allgemeine Informationen

9.1 Installationshinweise

Das Programm wird mit einer eigens entwickelten Installationsroutine geliefert, die Ihnen die Arbeit abnimmt. Um die Installation durchführen zu können, müssen Sie sich als lokaler Administrator anmelden. Die Installation erfolgt automatisch so, dass Sie für jeden Nutzer eingerichtet wird.

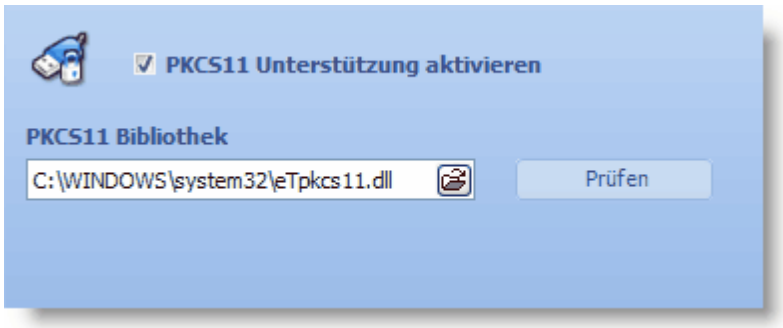
Falls Sie die ArchiCrypt Card nutzen möchten, müssen Sie das ArchiCrypt Card Modul installieren. Starten Sie nach der Installation zunächst den Rechner neu. Nach dem Neustart des Rechners starten Sie bitte ArchiCrypt Live und wechseln zur Funktion Einstellungen-Allgemeines. Betätigen Sie die Schaltfläche SmartCard Lesegerät auswählen. Markieren Sie den gewünschten Leser so, dass die Bezeichnung im oberen Eingabefeld zu sehen ist! Die aufgeführten Kartenleser mit den Bezeichnungen Debug:.... bitte NICHT auswählen. Sie dienen lediglich Testzwecken!



Jetzt bitte die Schaltfläche OK betätigen und ArchiCrypt Live neu starten!

Falls Sie ein Security-Token (einfach: Token) besitzen können Sie den Token nutzen, um darauf Schlüssel für Ihre ArchiCrypt Laufwerke abzulegen. Wichtig ist, dass Ihr Token den s.g. PKCS#11 Standard erfüllt und eine entsprechende Bibliothek (DLL) mitbringt, mit deren Hilfe ArchiCrypt Live auf die Funktionen zugreifen kann. Sollte die Dokumentation Ihres Token darüber keine Auskunft geben, kontaktieren Sie bitte den Hersteller Ihres Token.

Unter Einstellungen-SmartCard/Token können Sie die Bibliothek auswählen. Klicken Sie nach der Auswahl auf "*Prüfen*". ArchiCrypt Live versucht nun, die entsprechenden Funktionen der Bibliothek zu ermitteln und gibt an, ob die Bibliothek geeignet ist.



➡ACHTUNG:

- Falls eine Vorversion installiert ist, deinstallieren Sie diese Version mit dem zugehörigen Deinstallationsprogramm. Zum Zeitpunkt der Deinstallation darf kein Laufwerk geladen sein. Sie erreichen die Deinstallationsroutine über die Systemsteuerung, indem Sie den Eintrag Software auswählen und anschließend den Eintrag für ArchiCrypt Live auswählen.

- Inhalte von ArchiCrypt Live Laufwerken, welche mit einer älteren Version erstellt wurden, sollten Sie vor der Installation der neuen Version unverschlüsselt speichern.

9.2 Systemvoraussetzungen

Um ArchiCrypt Live verwenden zu können, muss Ihr System folgende Voraussetzungen erfüllen:

Betriebssystem

Windows 7/8/10 (*auch 64 BIT Versionen*)

Hinweis: Die mitgelieferten Treiber sind mit einem speziellen Digitalen Zertifikat (*EV Certificat*) digital signiert.
Diese Zertifikate sind unter Windows 7 ohne SP1 nicht verwertbar, so dass eventuell ein Fehlermeldung erscheint,
die angibt, die Treiber seien nicht signiert. Für Windows 7 stellt Microsoft einen Patch bereit: Security Advisory 3033929

Minimale Anforderungen

Microsoft Windows 7 (SP1, 32 BIT)
Bildschirmauflösung 800x600 mit 256 Farben
ca. 30 MB freier Festplattenplatz
Intel Pentium oder kompatibler Prozessor 1,4 GHz
2 GB RAM
CD-ROM oder DVD-ROM-Laufwerk

Empfohlene Systemkonfiguration

Microsoft Windows 10
Bildschirmauflösung 1024x768, true color
50 MB freier Festplattenplatz
4GB RAM
Intel Core i5 oder kompatibler Prozessor

- OPTIONAL: Internetzugang für Online-Tutor
- OPTIONAL: Falls Sie eine ArchiCrypt Card nutzen wollen (empfohlen), benötigen Sie einen Smartcard Reader, der den PC/SC Standard erfüllt. Sie erhalten die ArchiCrypt Card in unserem Online Shop unter http://shop.ArchiCrypt.de
  (nahezu alle aktuellen SmartCard Lesegeräte erfüllen diese Anforderung) und eine ArchiCrypt Card.
- OPTIONAL: Falls Sie einen Token nutzen möchten, muss dieser den PKCS#11 Standard erfüllen

HINWEIS: ***Die ArchiCrypt Card ist ein eigenständiges Produkt und muss separat erworben werden.***

10 Bedienung

10.1 Überblick

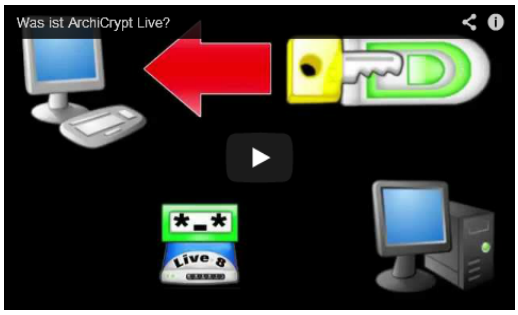
siehe auch: Wichtige Begriffe - Begriffserläuterungen

Sollten sich die nachfolgenden Videos im Browser nicht anzeigen lassen, so können Sie die Videos alternativ direkt in Youtube auf unserem ArchiCrypt Kanal ansehen.

Überblick über ArchiCrypt Live

ArchiCrypt Live verfolgt eine zukunftsweisende Methode, um sensible Dateien in Sicherheit zu bringen. Es legt einfach ein virtuelles ArchiCrypt Live - Laufwerk an, das mit einem eigenen Laufwerksbuchstaben versehen wird und sich in der Folge wie eine ganz normale Festplatte ansprechen lässt. Texte, Bilder, Videos, Musiken und Anwendungen werden einfach auf das virtuelle Laufwerk kopiert bzw. darauf installiert.

Video - Einleitung



Video - Was ist ArchiCrypt

Video - 60 Sekunden Demo

Wo kommen die ArchiCrypt-Laufwerke her?

ArchiCrypt Live 8 kann bis zu acht dieser virtuellen Laufwerke gleichzeitig kontrollieren, wobei jedes Laufwerk bis zu zwei Terabyte (*das sind gigantische 2048 Gigabyte*) groß sein darf und einen eigenen Laufwerksbuchstaben bekommt. Den Speicherplatz "borgt" sich das Programm von der normalen Festplatte aus. Hier wird einfach ein Bereich für das virtuelle Laufwerk reserviert. Durch eine spezielle Technik (Ultraschnelles Erstellen) kann ArchiCrypt Live selbst gigantisch große Laufwerke von mehreren hundert Gigabyte in wenigen Sekunden erstellen. Diese "Wachsenden Laufwerke" belegen zunächst nur sehr wenig Platz und wachsen dann bei Bedarf bis zu ihrem Limit an. ArchiCrypt Live-Laufwerke können auch auf einem NAS-Server oder einer Netzwerkfreigabe erstellt und von dort auch von kleinen Arbeitsgruppen gemeinsam genutzt werden. Wer die sicheren Laufwerke auf einem USB-Stick anlegt, kann diesen in der Folge dann mal an diesen und mal an jenen Rechner anschließen und verwenden. Sogar ArchiCrypt-Laufwerke auf CD oder DVD sind möglich. Wer seine Daten ungeschützt in der Cloud speichert, begeht einen schweren Fehler. ArchiCrypt erkennt installierte Cloud-Dienste (*Dropbox, Google Drive, OneDrive und Telekom-Cloud*) und kann hier ein Live Laufwerk bereitstellen, welches dafür sorgt, dass alle Daten vor der Übertragung in die Cloud in Echtzeit verschlüsselt werden. Ein Verlust oder Diebstahl der Datenträger fällt zum Glück nicht mehr gleich in die Kategorie "Katastrophe": Wer das passende Kennwort nicht besitzt, ist auch nicht in der Lage, auf die enthaltenen Dateien zuzugreifen. Der ausschließliche Einsatz von offenen und praxisbewährten Verschlüsselungsverfahren und -standards garantiert dabei maximale Sicherheit.

Weitere Besonderheiten der Software

- Unterstützung von modernen Mehrkernprozessoren (*inzwischen auf nahezu jedem modernen Heim-PC zu finden*) führt zu einer deutlichen Geschwindigkeitssteigerung.
- Unterstützung erweiterter Befehlssätze von modernen Prozessoren (AES-NI).
- ArchiCrypt Live kann Daten auf den internen Festplatten, Speicherkarten, USB-Sticks, NAS-Servern, Netzwerkfreigaben, CDs, DVDs und externe Festplatten schützen.
- Legen Sie ein Live Laufwerk in die Cloud. Durch die Cloud-Anbindung werden die Daten vor der Übertragung in die Cloud in Echtzeit verschlüsselt. Unterstützt werden die Cloud-Dienste Dropbox, Google Drive, One Drive und die Telekom-Cloud.
- Unterstützung kleiner Arbeitsgruppen. ArchiCrypt Live kann die speziellen Live Laufwerke von einem Netzlaufwerk (*Netzwerkfreigabe, NAS-Server)* laden. Dabei können mehrere Personen gleichzeitig auf ein solches Laufwerk zugreifen. Ein Schreiber, der Daten beliebig ändern oder erstellen kann und eine beliebige Anzahl von "Lesern", die das Laufwerk nutzen können, wie eine CD. Wer als Leser Daten schreiben möchte, sendet dem aktuellen Schreiber einfach eine kurze Nachricht.
- Geheimbereiche: Ihr digitales Geheimfach. Dabei handelt es sich um einen Bereich des ArchiCrypt-Live-Laufwerks, der nur mit einem speziellen Passwort zugänglich ist. Die Existenz dieses besonderen Bereichs ist ohne Kenntnis dieses Schlüssels nicht nachweisbar (*Prinzip der Plausiblen Verleugnungsmöglichkeit*).
- Wer seine Datensafes verschleiern möchte, kann so genannte Steganografische Laufwerke erstellen. ArchiCrypt Live vermischt dabei einen Datensafe zum Beispiel mit einem Video, einem Musikstück, einem Bild oder einer Windows-Anwendung. Man kann das Video oder Bild anschließend normal betrachten, das Musikstück anhören und die Anwendung in gewohnter Weise nutzen und ebenso als ArchiCrypt-Live-Laufwerk laden.
- Erstellen Sie mobile Datensafes, die nur aus einer einzigen Datei bestehen. Mobile Datensafes stellen nach Eingabe des Passwortes auf jedem Windows XP, Windows Vista und Windows 7/8 Rechner ein Laufwerk mit Echtzeit-Verschlüsselung (Lese-/Schreibzugriff) bereit. Mobile Datensafes sind zudem ideal dazu geeignet, sensible Daten bequem und sicher an Dritte weiterzugeben. Der Empfänger kann die Inhalte des Laufwerks nach belieben ändern und Ihnen das Ergebnis so wieder zukommen lassen. Sicherer Datenaustausch und nur einer benötigt eine Lizenz!
- Mit ArchiCrypt Live können Sie die Laufwerke einfach mit mit Public-Key-Private-Key Verfahren hochsicher mit anderen tauschen. Sogar der Versand über das unsichere Internet stellt somit kein Problem dar. Sofern Sie kein eigenes Zertifikat von

einer Zertifizierungsstelle besitzen, erstellt Ihnen ArchiCrypt Live ein X.509-Zertifikat mit Schlüssellängen bis zu 2048 Bit (RSA).

- Die verschlüsselten Laufwerke lassen sich mit der separat zu erwerbenden ArchiCrypt-Card schützen. Sie arbeitet mit allen PC/SC-kompatiblen Lesegeräten zusammen. Sobald eine Karte an den Rechner angeschlossen wird, kann man bestimmte Laufwerke automatisch laden, beim Entfernen automatisch schließen lassen.
- Neben dem Schutz der ArchiCrypt Laufwerke durch konventionelles Passwort oder ArchiCrypt Card, werden auch s.g. Security-Token (*PKCS#11 Geräte*) unterstützt. Auf diesen Token kann man die Schlüssel für seine ArchiCrypt Live Laufwerke ablegen und bei Bedarf eine für den Token nötige PIN über ein hochsicheres PIN-PAD eingeben. Sobald ein Token an den Rechner angeschlossen wird, kann man bestimmte Laufwerke automatisch laden, beim Entfernen automatisch schließen lassen.
- Wer möchte, vergibt Notfall- und Gastpasswörter. Gäste haben so zum Beispiel zeitlich begrenzt Zugriff auf die Daten, ohne dass Sei IHR Passwort herausgeben müssen.
- Die Notaus-Funktion schließt Laufwerke sofort ab, auch wenn sie gerade in Gebrauch sind.
- Mit einem zuvor definierten "Magic Word" lassen sich Laufwerke aus jeder Anwendung heraus ganz besonders schnell öffnen und auch wieder abschließen.
- Fortgeschrittene Nutzer haben die Möglichkeit, ArchiCrypt Live-Laufwerken über Kommandozeile zu laden bzw. zu schließen. Einer Einbindung in eigene Programme steht damit nichts mehr im Wege.
- Mit der Umleitungsfunktion leiten Sie alle Dateien aus einem Verzeichnis des "normalen" Rechners um auf ein verschlüsseltes Live Laufwerk. Ganz ohne Einstellungen am System oder einem Programm zu ändern.
- Durch die Anwendungskontrolle können Sie festlegen, welche Programme auf die Inhalte eines Live Laufwerks zugreifen dürfen. Durch s.g. Whitelisting haben nur die Programme Zugriff, die explizit die Erlaubnis haben.
- Live-Laufwerke können als Favorit angelegt werden. Damit hat man schnellen Zugriff und kann spezielle Eigenschaften und Aktionen festlegen.
- Legen Sie Kommandos und Befehle fest, die vor dem Öffnen, nach dem Öffnen, vor dem Schließen und nach dem Schließen von Live Laufwerken ausgeführt werden sollen.
- Mit Hilfe eines optional erhältlichen Zusatzprogramms (*ArchiCrypt Live ToGo*) können Sie ArchiCrypt Live Laufwerke sogar über das Internet laden. Legen Sie das Live Laufwerk

einfach z.B. per FTP auf Ihrem Server ab und greifen Sie mit Live ToGo unterwegs bequem auf die Inhalte zu.

Weiter zur Einstieg >>

1 ACHTUNG: Das Verschlüsseln der Systempartition ist nicht möglich!!!!

10.2 Einstieg

ArchiCrypt Live vereint alle Funktionen unter einer zentralen Oberfläche, die über die Home-Seite erreichbar sind.

siehe auch: Werkzeuge für das Laufwerk

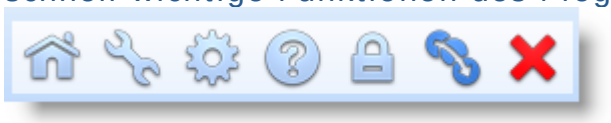
Klicken Sie auf ein Element der folgenden Grafik, um weitere Informationen zu erhalten.

Die Home-Seite bietet nachfolgend genannte Möglichkeiten:

- Öffnen und Schließen von Laufwerken
- Erstellen neuer Laufwerke
- Zusätzliche Werkzeuge für Live Laufwerke
- Werkzeuge für das geöffnete Laufwerk
- Einstellungen
- Favoriten

Menüleiste

Die Menüleiste wird in verschiedenen Kategorien am oberen rechten Rand von ArchiCrypt Live angezeigt. Sie erlaubt es, schnell wichtige Funktionen des Programms aufzurufen.



Bedeutung der Symbole von links nach rechts:

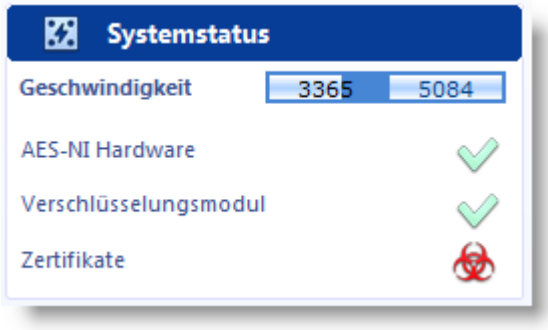
- Home-Seite
- Werkzeuge für Live Laufwerke
- Einstellungen
- Hilfe und Informationen
- Schützen
- Ruhen
- Beenden

Laufwerk-Fabrik

Durch Klick auf die Schaltfläche **Erstelle ein Laufwerk...** rufen Sie den Assistenten für das Erstellen eines Live Laufwerks auf. Sie können direkt in der Fabrik eine bestimmte Art von Laufwerk voreinstellen. Im Expertenmodus haben Sie die komplette Vielfalt an Einstellungsmöglichkeiten.

Systemstatus

Der Systemstatus gibt auf einen Blick Informationen über Leistung und Zustand des Systems an. Fahren Sie mit der Maus über eines der Elemente um mehr darüber zu erfahren.
Unter Geschwindigkeit sehen Sie je nach Hardwareausstattung zwei Säulen. Hier erfahren Sie jeweils, welchen maximalen Datendurchsatz das System mit und ohne Hardwareunterstützung zum Zeitpunkt des Starts geleistet hat.
Bei AES-NI Hardware sehen Sie, ob Ihr System mit entsprechender Hardware ausgestattet ist und ob diese Möglichkeit in ArchiCrypt Live verwendet wird.



Bei Verschlüsselungsmodul und Zertifikate dürfen niemals rote Symbole erscheinen. Sobald hier kein grünes Häkchen zu sehen ist, ist die Software manipuliert und unsicher!

Beenden von ArchiCrypt Live

Wichtiger Hinweis

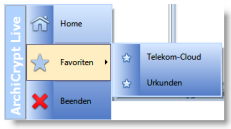
ArchiCrypt Live sollte NICHT geschlossen werden, wenn Sie noch Laufwerke geöffnet haben! Laufwerke können nur über die Anwendung ArchiCrypt Live geschlossen werden. Auch die Funktionen zur automatischen Passwortabfrage bei Einlegen eines Wechselmediums mit Live Laufwerk und die Funktion zum Schließen der Laufwerke im Falle von Inaktivität, benötigen ArchiCrypt Live. Statt ArchiCrypt Live zu beenden, versetzen Sie die Software möglichst in den Ruhemodus (Ruhen)!

Ruhen von ArchiCrypt Live

Mit Ruhen wird ArchiCrypt Live minimiert. Falls Sie s.g. Hotkeys/Tastaturkürzel festgelegt haben, können Sie die Funktionen über eine Tastenkombinationen aufrufen. Ansonsten genügt ein Klick auf das Sternsymbol im s.g. Traybereich um die Anwendung zu minimieren bzw. maximieren.

Kontextmenü im Traybereich

Mit einem Klick der rechten Maustaste über dem Sternsymbol rufen Sie ein Kontextmenü auf, mit dem Sie einzelne Funktionen von ArchiCrypt Live aufrufen können.



Mit diesem Menü können Sie zur Home-Seite in ArchiCrypt Live springen, die Favoriten bedienen oder das Programm beenden. Die Farbe der Sterne gibt dabei den Zustand des Laufwerks an.

Blaue Sterne = Nicht geladene Laufwerke

Grüne Sterne = Geladene Laufwerke mit Lese- und Schreibzugriff

Rote Sterne = Geladene Laufwerke mit Lesezugriff

Klick auf nicht geladene Favoriten lädt diese, klick auf geladene Laufwerke schließt sie.

Ruhen und schützen

Bevor ArchiCrypt Live in den Ruhezustand versetzt wird, wird ein Passwort abgefragt, welches man zum Reaktivieren benötigt. Der Zugriff auf alle Funktionen der Anwendung ist erst nach einem Neustart von ArchiCrypt Live möglich oder nach der Eingabe des Schutzpasswortes.

ACHTUNG: Alle eventuell geöffneten Laufwerke bleiben geöffnet und können weiterhin vollkommen transparent genutzt werden. Um zu verhindern, dass Unbefugte Zugriff auf die Laufwerke haben, müssen Sie die Laufwerke schließen!

Hilfe

Sie können an jeder Stelle im Programm die F1 Taste betätigen, um kontextbezogen Hilfe zu erhalten. Alternativ betätigen Sie die Hilfe-Schaltfläche.

Statusleiste

ArchiCrypt Live besteht aus mehreren Anteilen. Der Anwendung, mit der Sie Laufwerke laden, entladen und verwalten (*sichtbarer Anteil*) und zwei unsichtbaren Anteilen, dem Echtzeit-Verschlüsselungstreiber und dem Filtertreiber, der Umleitungen und Programm-Zugriffsrechte verwaltet.

Links in der Statusleiste finden Sie die Versionsnummer der Anwendung. In der Mitte die Versionsnummer des Verschlüsselungstreibers und des Filtertreibers.

Lernvideothek

Bilder sagen mehr als Worte. Entsprechend finden Sie hier zahlreiche Videos, in denen spezielle Themen in Form von Videos besprochen werden.

Weiter zu Erstellen >>

10.3 Videothek

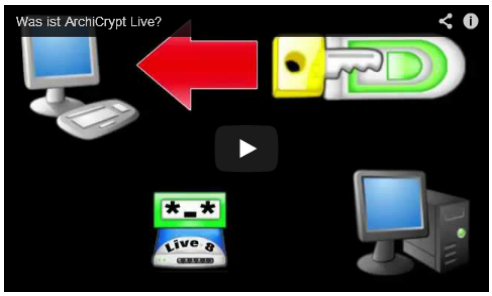
Sollten sich die nachfolgenden Videos im Browser nicht anzeigen lassen, so können Sie die Videos alternativ direkt in Youtube auf unserem ArchiCrypt Kanal ansehen.

Video - Neues in Version 8

Wie unterscheidet sich Version 8 von der Vorversion?

Video - Einleitung

Ist Verschlüsselung nicht zu kompliziert und wozu brauche ich als Normalsterblicher überhaupt Verschlüsselung?



Video - Was ist ArchiCrypt

Wie funktioniert ArchiCrypt Live und was kann es?

Video - 60 Sekunden Demo

In 60 Sekunden wird ein neues 700 Megabyte großes

Live Laufwerk erstellt. Anschließend wird es geöffnet, eine Datei wird darauf gespeichert und das Laufwerk wieder sicher verschlossen.

Video - Live Laufwerk

Schritt für Schritt wird mit dem Assistenten eine neues ArchiCrypt Live Laufwerk erstellt.

Video - Steganografisches

ArchiCrypt Live kann verschlüsselte Laufwerke in anderen Daten verstecken. Dies nennt man Steganografie. Der Clou: Die Datei, Musikstück, Video, Anwendung etc. kann weiter normal genutzt werden. Nur ArchiCrypt Live kann die Datei zusätzlich mit Hilfe des korrekten Passwortes als Laufwerk laden.

Video - mobiler Datensafe

ArchiCrypt Live kann eine Anwendung erzeugen, die sich selbst an jedem Windows Rechner nach Eingabe des Passwortes als Laufwerk laden kann. Ideal zum

Video - Live Partition

ArchiCrypt Live kann Datenpartitionen komplett verschlüsseln.

sicheren Transport von Daten und zum sicheren Austausch sensibler Daten.

Video - Geheimfach

ArchiCrypt Live kann in einem verschlüsselten Laufwerk einen weiteren geheimen Bereich erstellen, auf den man nur mit Hilfe eines speziellen Passwortes zugreifen kann. Ohne dieses Passwort ist nicht einmal nachweisbar, dass es ein solches Geheimfach überhaupt gibt.

Video - Umleitung nutzen

ArchiCrypt Live kann Dateien von einem ganz normalen Verzeichnis, unbemerkt von Anwender und Anwendung einfach auf ein verschlüsseltes Laufwerk umleiten.

Video -

Gerade im Zusammenhang mit sensiblen Daten ist selbst Misstrauen gegenüber den Anwendungen auf dem eigenen Rechner angebracht. Oft finden im Hintergrund scans statt, die Daten indexieren, katalogisieren,

Video - Passwort zu

ArchiCrypt bietet neben dem klassischen Passwort weitere Möglichkeiten, den Zugriff auf das verschlüsselte Live Laufwerk zu schützen. Eine Schlüsseldatei, die ebenfalls mit Passwort geschützt werden kann, entspricht

kopieren und inzwischen nicht selten in die Cloud laden. Die Anwendungskontrolle erlaubt, explizit festzulegen, welche Anwendungen die Inhalte von Live Laufwerken sehen dürfen.

dabei einem Passwort, welches aus 100 Zeichen besteht.

Video - Anderen Zugriff

Video - X509 Zertifikat

Gelegentlich möchte man anderen Zugriff auf sein Live Laufwerk gewähren. Nicht immer will man das eigene Passwort, welches man unter Umständen an anderer Stelle ebenfalls nutzt, weitergeben. Auch soll der Gast vielleicht nur Daten lesen, nicht aber ändern können. Mit den Gastzugängen bei ArchiCrypt Live lässt sich genau das realisieren.

Möchte man sensible Daten sicher weitergeben, hat aber keine Möglichkeit, das Passwort sicher weiterzugeben, hat man ein Problem. Mit Zertifikaten kann man Live Laufwerke mit anderen Austauschen, ohne dabei das eigentliche Passwort auszutauschen. Zudem kann man Live Laufwerke signieren und dem Empfänger verlässlich die Authentizität und Integrität der Daten vermitteln. Das Erstellen s.g. self-signed Zertifikaten ist dabei Bestandteil von ArchiCrypt Live.

Video - Favoriten

ArchiCrypt Live bietet mit Hilfe so genannter Favoriten die Möglichkeit, rasch auf häufig genutzte Live Laufwerke zuzugreifen. Dabei können bereits spezielle Eigenschaften festgelegt werden, die beim Laden zu berücksichtigen sind.

10.4 Funktionen

10.4.1 Erstellen

Sollten sich die nachfolgenden Videos im Browser nicht anzeigen lassen, so können Sie die Videos alternativ direkt in Youtube auf unserem ArchiCrypt Kanal ansehen.

Video - Live Laufwerk

Video - 60 Sekunden Demo

Video - Steganografisches

Video - mobiler Datensafe

Video - Live Partition

Video - Geheimfach

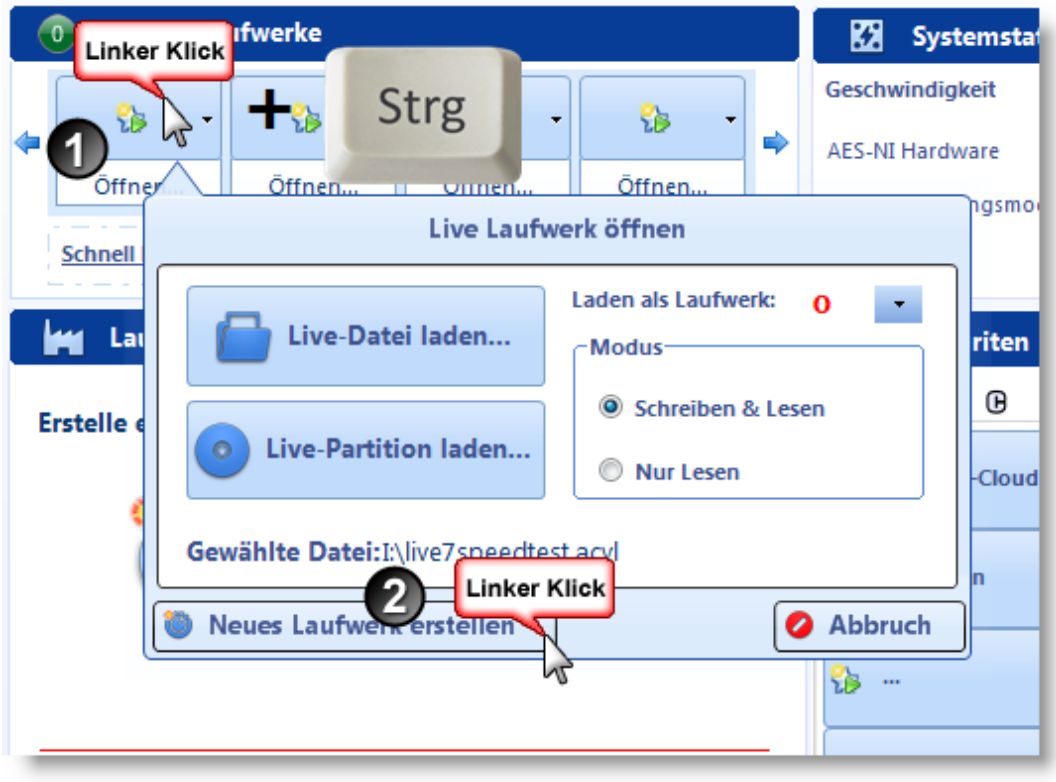
siehe auch: Wichtige Begriffe - Begriffserläuterungen
Partition

Erstellen eines ArchiCrypt Live Laufwerks Schritt für Schritt

So rufen Sie den Assistenten zum Erstellen neuer Laufwerke auf:

Möglichkeit 1:
Aufruf über die Home-Seite Laufwerk-Fabrik durch Klick auf die Schaltfläche **Erstelle ein neues Laufwerk...**

Möglichkeit 2:
Aufruf durch Linksklick bei betätigter Strg-Taste auf einen leeren Speicherplatz (*Slot*) bei **Aktive Laufwerke**.



Der Assistent zum Erstellen neuer Laufwerke wird gestartet. Dabei werden die nachfolgenden Schritte durchlaufen.

➡Wenn Sie ein Geheimfach erstellen möchten, lesen Sie bitte zunächst das gleichnamige Kapitel!

➡Wenn Sie eine Live Partition erstellen möchten, lesen Sie bitte zunächst das Kapitel Live Partition!

1 Welche Art Laufwerk soll erstellt werden?

Ein normales Live Laufwerk oder ein Geheimfach erstellen

1. Möglichkeit, ein dateibasiertes Live Laufwerk zu erstellen.

Alle Daten und Inhalte des Laufwerks werden in einer Datei, der s.g. Trägerdatei gespeichert.

Vorteil:
Leicht kopierbar, verschiebbar und zu sichern. Kann auf nahezu beliebigen Datenträgern abgelegt werden. Zusammen mit ArchiCrypt Live Mobile können Sie das Laufwerk auf jedem Windows XP (SP3), 2003, Vista oder Windows 7/8 System laden.

Nachteil:
Anfällig gegen versehentliches Löschen.

2. Möglichkeit eine Live-Partition zu erstellen. Dabei wird eine Partition einer Festplatte, intern oder extern komplett in ein Medium umgewandelt, welches ArchiCrypt Live in Ihr System als Laufwerk einbinden kann.

Vorteil:
Partition muss nicht zwingend aktiv geschaltet sein, um Sie mit ArchiCrypt Live laden zu können. Nach außen hin wirkt das Speichermedium wie ein unformatiertes Medium. Kann auf externe Speichermedien wie USB-Laufwerke, -Sticks und Speicherkarten angewendet werden.

Nachteil:
Schwer zu sichern (siehe Partitionssicherung)
Sehr anfällig gegenüber Änderungen am Betriebssystems
Sehr anfällig gegenüber Systemsoftware (*Backup-,Recoverysoftware; Partitionierungswerkzeuge*)
Ausschließlich für versierte Anwender

siehe Partition

3. Geheimfach:

Setzt voraus, dass bereits ein Live Laufwerk (*dateibasiert oder Live Partition*) existiert. siehe Geheimfach

Mobiles Live Laufwerk

Möglichkeit einen s.g. mobilen Datensafe zu erstellen. Dabei ist die Datei Anwendung und Laufwerk zugleich. Die Anwendung kann sich selbst als Laufwerk laden. Alle Inhalte des Laufwerks können dabei nicht nur gelesen, sondern nach belieben geändert werden. Alle Daten werden direkt in das mobile Laufwerk gespeichert, also nicht etwa zunächst unverschlüsselt zwischengespeichert. Sie können die Datei sofort nach getaner

Arbeit mit zum nächsten Rechner nehmen und dort mit geänderten Daten weiter arbeiten. Ideal sind mobile Datensafes auch, um mit Dritten Daten sicher auszutauschen. Der Empfänger benötigt keine eigene ArchiCrypt Live Lizenz, sondern nur das Passwort. Da er Lese- und Schreibzugriff hat, kann er Ihnen selbst ebenfalls sicher Daten senden.

Wenn Sie ein mobiles Live Laufwerk aus einem bestehenden Live Laufwerk erstellen möchten, erfolgt dabei keine direkte Umwandlung! Das dateibasierte Live Laufwerk bleibt im Original erhalten.

Vorteil:
Ideal geeignet, um sensible Daten zwischen verschiedenen Rechnern sicher zu transportieren oder mit anderen Personen auszutauschen. Diese benötigen keine Live Lizenz, können jedoch uneingeschränkt auf die Daten im Laufwerk zugreifen. Leicht kopierbar, verschiebbar und zu sichern. Kann auf nahezu beliebigen Datenträgern abgelegt werden.

Nachteil:
Laufwerk inklusive enthaltenem Starter (*Anteil, der die Echtzeit-Verschlüsselung übernimmt*) dürfen höchstens 4 Gigabyte groß sein! Alternativ bietet sich die Nutzung von ArchiCrypt Live Mobile an. Der frei Verfügbare "Lader" für ArchiCrypt Live Laufwerke kennt keine solche Größenbeschränkung und ist ebenfalls kostenlos verfügbar. Allerdings muss man hier mit mehreren Dateien leben, die nur zusammen funktionieren.

siehe Steganografische Laufwerke und mobile Live Laufwerke

Steganografisches Live Laufwerk

Möglichkeit, ein s.g. Steganografisches Laufwerk zu erstellen, bei dem eine normale Datei (*meist Anwendung oder Multimediadatei*) mit einem Live Laufwerk vermischt wird. Die Datei kann nach dem Erstellen sowohl im ursprünglichen Sinne (*z.B. als Video/Musikstück*) als auch als Live Laufwerk genutzt werden. Bitte beachten Sie, dass beim Vermischen eines dateibasierten Live Laufwerks mit einer Anwendung (*meist Dateiendung exe*) das entstehende Steganografische Laufwerk maximal 4 Gigabyte groß sein darf. Windows verweigert ansonsten das Starten der Anwendung und gibt eine Fehlermeldung aus. Für spezielle Datentypen können ähnliche Beschränkungen gelten.

Es erfolgt keine direkte Umwandlung! Das dateibasierte Live

Laufwerk bleibt im Original erhalten.

Vorteil:
Sehr unauffällig, da die Datei die ursprünglichen Eigenschaften behält. Leicht kopierbar, verschiebbar und zu sichern. Kann auf nahezu beliebigen Datenträgern abgelegt werden.

Nachteil:
Steganografisches Laufwerk wird zerstört, sobald man die Datei (*Video, Bild, Musikstück*), die mit einem Live-Laufwerk vermischt wurde, ändert und abspeichert. Anfällig gegen versehentliches Löschen.

siehe Steganografische Laufwerke und mobile Live Laufwerke

Cloud Live Laufwerk

Sofern ArchiCrypt Live beim Start einen unterstützten Cloud-Dienst (*Dropbox, Google Drive, OneDrive, Telekom-Cloud und Strato HiDrive*) findet, wird Ihnen diese Möglichkeit auf der Home-Seite im Bereich Laufwerk-Fabrik und im Assistenten angezeigt. ArchiCrypt Live kann ein Laufwerk in der Cloud erstellen. Alle Daten, die Sie in dieses Laufwerk speichern, werden vor der Übertragung in die Cloud in Echtzeit verschlüsselt.

Sie müssen darauf achten, dass Sie mit dem Live Laufwerk nicht die maximale Kapazität Ihres Cloud-Speichers

Vorteil:
Sensible Daten sind so auch im Cloud-Speicher absolut sicher. Werden die Daten beim Dienst entwendet, können die Datendiebe mit den Dateien ohne Kenntnis Ihres Passwortes nichts anfangen.

Nachteil:
Ein kleiner Nachteil ergibt sich im Zusammenhang mit Arbeitsgruppen, die auf Daten in der Cloud zugreifen. Cloud-Dienste sperren die Daten nicht, wenn diese geöffnet sind. Die Unterstützung von Arbeitsgruppen ist für Live Laufwerke, die in einer Cloud liegen, nicht zu 100% sichergestellt.

Wo soll das neue Laufwerk erstellt werden?

Zu Hause

Wenn Sie ein Laufwerk aus der Rubrik "**Zu Hause**" gewählt haben, erscheint der folgende Dialog:

Zum Erstellen eines dateibasierten Laufwerks betätigen Sie bitte die Schaltfläche Verzeichnis. Wechseln Sie in das Verzeichnis, in dem Sie das neue Laufwerk erstellen möchten und geben Sie einen Namen für das neue Laufwerk ein. Wenn Sie hier ein bestehendes ArchiCrypt Live Laufwerk (*Datei oder Partition*) wählen, haben Sie die Möglichkeit, ein Geheimfach zu erstellen. Dazu müssen bestimmte Voraussetzungen erfüllt sein.

Das Erstellen einer Live Partition wird wegen der Risiken nur erfahrenen Nutzern empfohlen. Zudem bieten Live Partitionen nur in speziellen Fällen Vorteile gegenüber den dateibasierten Live Laufwerken. Falls Sie eine Partition umwandeln möchten, rufen Sie den Dialog zur Auswahl einer Partition auf und lesen Sie zuvor sorgfältig das Kapitel Live Partition durch.

Bestätigen Sie die Schaltfläche **Weiter >>>** um zum nächsten Schritt zu gelangen

➡ ACHTUNG Windows Vista und höher! *Windows Vista startet Programme so, dass diese mit möglichst wenig Rechten laufen. Es spielt dabei keine Rolle, ob Sie selbst Administratorrechte besitzen! Um Partitionen umwandeln zu können, benötigt ArchiCrypt Live zwingend*

Administratorrechte. Es genügt also kein einfacher Start von ArchiCrypt Live.

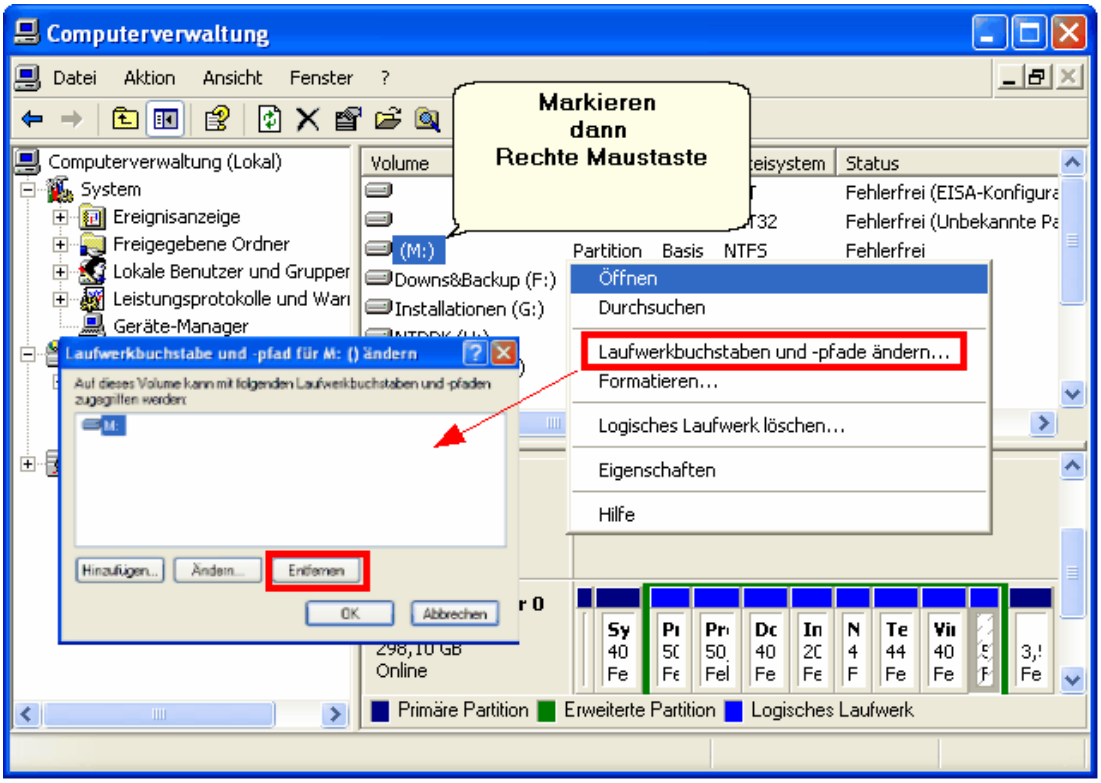
So starten Sie ArchiCrypt Live unter Vista und höher mit Administratorrechten:
Klicken Sie entweder auf die Schaltfläche Partition.*damit ArchiCrypt Live sich selbst mit entsprechenden Rechten startet oder starten Sie ArchiCrypt Live direkt wie folgt: Klicken Sie mit der rechten Maustaste auf die ArchiCrypt Live (NET) Anwendung und wählen Sie* **"Als Administrator ausführen"**

➡ ACHTUNG: ***Falls Sie im Dialog ein bereits bestehendes Live Laufwerk auswählen, wird gefragt, ob Sie das Laufwerk überschreiben möchten, oder ein Geheimfach erstellen möchten. Falls Sie ein Geheimfach erstellen wird Ihnen eine Warnung angezeigt, die auffordert, sich das Kapitel Geheimfach genau durchzulesen. Nachdem Sie die Frage mit Ja beantwortet haben, wird der aktuelle Laufwerk-Administrator-Schlüssel abgefragt. ArchiCrypt Live öffnet damit das Laufwerk und ermittelt, wie viel Platz für ein Geheimfach theoretisch verfügbar ist. Bevor Sie die Größe für den Geheim-Container festlegen können, wird das Laufwerk wieder geschlossen.***

 ***Der Name des Laufwerkes und die Dateiendung können beliebig gewählt werden. Falls Sie ein Laufwerk jedoch per Doppelklick öffnen möchten oder die Funktion zur automatischen Passwortabfrage bei Einlegen eines Datenträgers mit Live Laufwerk nutzen wollen, sollten Sie die Dateiendung .acl belassen. Wählen Sie eine Dateiendung wie z.B. bmp oder mp3. Dadurch wird das ArchiCrypt Laufwerk schwer auszumachen!***

 TIPP: Wenn Sie eine Partition in eine Live Partition umgewandelt haben, sollten Sie in der Datenträgerverwaltung von Windows (**Start-Systemsteuerung-Verwaltung-Computerverwaltung-Datenträgerverwaltung**) einen ggf. zugewiesenen Laufwerksbuchstaben entfernen. Damit entfällt der lästige Hinweis des Windows Explorers, dass das Laufwerk nicht formatiert sei (*Windows kann die verschlüsselten Inhalte nicht interpretieren*). Wenn die Live Partition als Live Laufwerk geladen ist, haben Sie

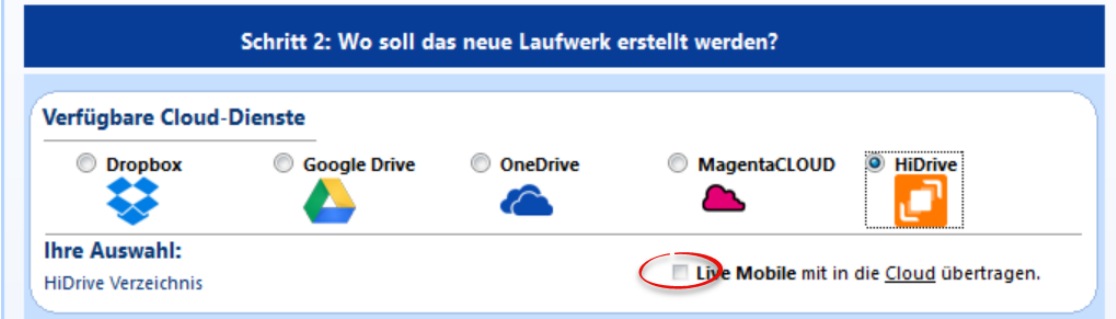
zudem nur noch einen Laufwerksbuchstaben über den Sie auf die Inhalte des Laufwerks zugreifen können.



Entfernen Sie den Laufwerksbuchstaben einer Live Partition

CLOUD

Falls Sie ein Cloud Laufwerk erstellen, können Sie markieren Sie als Ziel bitte einfach den entsprechenden Cloud Dienst. Sie können nur die Dienste anwählen, die zum Zeitpunkt des Programmstarts bei Ihnen installiert waren.



ArchiCrypt Live erstellt im jeweiligen Cloud Verzeichnis ein Unterverzeichnis namens ArchiCryptLive. Je nach gewähltem Cloud Dienst wird eine Datei erstellt, die einen für den Cloud Dienst eindeutigen Namen trägt.

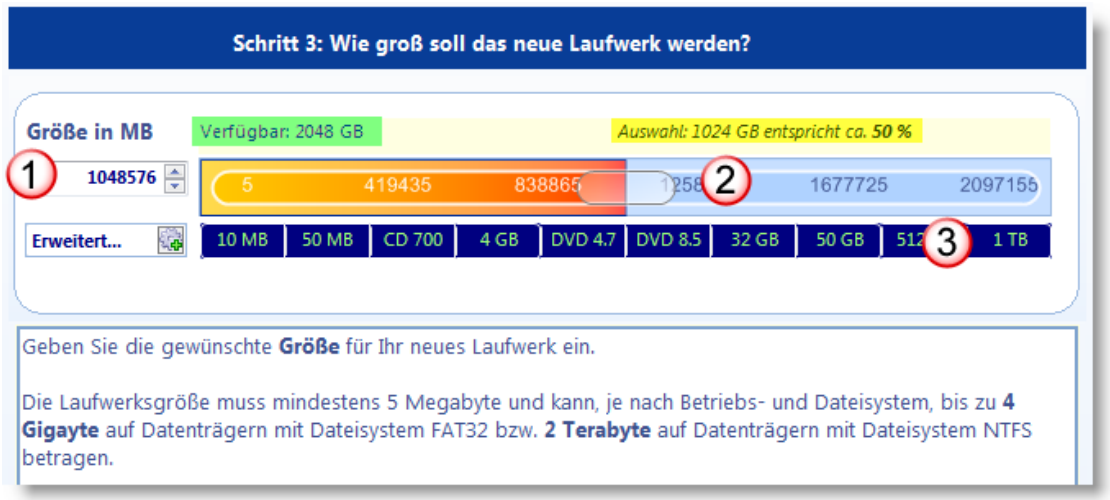
- Dropbox: **Dropbox.acyl**
- GoogleDrive: **GoogleDrive.acyl**
- OneDrive: **OneDrive.acyl**
- Telekom-Cloud / MagentaCLOUD: **TelekomCloud.acyl**
- Strato HiDrive: **HiDrive.acyl**

➡ WICHTIG: Wenn Sie mit Hilfe des Assistenten ein Live Laufwerk für einen Dienst erstellt haben und den Assistenten noch einmal für diesen Dienst durchlaufen, merkt ArchiCrypt Live, dass ein solches Laufwerk bereits existiert und bietet Ihnen an, ein Geheimfach zu erstellen oder das vorhandene Laufwerk zu überschreiben.

Im Umkehrschluss bedeutet dies, dass man für jeden Cloud Dienst nur ein Live Laufwerk mit Hilfe des Assistenten erstellen kann. Es stellt jedoch kein Problem dar, manuell weitere Laufwerke in die Cloud zu legen. Wählen Sie als Art einfach die Option "*Zu Hause*" aus und geben Sie als Verzeichnis einfach das entsprechende Cloud-Verzeichnis als Ziel an. ArchiCrypt Live erkennt, wenn ein Laufwerk in einem Cloud-Verzeichnis liegt.

Falls Sie von anderen Windows Rechnern auf Ihr Cloud Live Laufwerk zugreifen möchten und für diesen Rechner keine Lizenz für ArchiCrypt Live vorhanden ist, wählen Sie die Option **Live Mobile mit in die Cloud übertragen**. In diesem Fall wird die Anwendung ACLiveMobile.exe in der Cloud abgelegt. Wenn Sie diese Anwendung an einem anderen Windows Rechner starten, können Sie dort nach Eingabe des Passwortes das Cloud Live Laufwerk laden und Daten Lesen und beliebig ändern. Die mobile Variante unterstützt jedoch keine Arbeitsgruppen.


Wie groß soll das neue Laufwerk werden?



Legen Sie hier die Größe Ihres neuen Live Laufwerks in Megabyte fest. Dazu können Sie die gewünschte Größe in das Eingabefeld eingeben, oder durch das Betätigen einer der Schaltflächen festlegen. Falls Sie eine Live Partition erstellen, wird der komplette verfügbare Platz der Partition genutzt.

➡ ACHTUNG: ***Bedenken Sie bei der Festlegung der Laufwerksgröße, dass zum verantwortungsvollen Umgang mit wichtigen Daten eine regelmäßige Datensicherung gehört (am besten täglich und oder vor jedem Eingriff in das System). Große Laufwerke sind dabei schwer handhabbar! Falls Sie eine Live Partition erstellen, sollten Sie eine Komplettsicherung Ihres Systems durchführen, da die Gefahr eines Datenverlustes durch falsche Partitionswahl hoch ist.***

Bei einem Cloud Laufwerk müssen SIE darauf achten, dass Sie die maximale Datenmenge Ihres Cloud-Speichers nicht überschreiten!

Bei 1 können Sie die Größe direkt in Megabyte festlegen. Mit dem Schieberegler bei 2 können Sie schnell eine bestimmte Größe einstellen und bei 3 bieten Ihnen verschiedene Schaltflächen die Möglichkeit, rasch vordefinierte Größen zu aktivieren.

Die Größe eines Laufwerks wird durch folgende Faktoren begrenzt:

- Verfügbarer Speicherplatz
- Größe einer bestehenden Trägerdatei/Partition (*wenn Sie zum Beispiel ein Geheimfach erstellen*)

- Ca. 4 Gigabyte sofern ein dateibasiertes ArchiCrypt Live Laufwerk auf einem Datenträger abgelegt wird, der mit dem FAT32 Dateisystem formatiert ist.
- Ca. 2 Terabyte sofern Windows XP/Vista/Windows 7/8 als Betriebssystem dient und die Trägerdatei/Partition auf einem Datenträger abgelegt wird, der mit dem Dateisystem NTFS formatiert ist.

Sonderfunktionen

Wenn Sie mit der linken Maustaste auf **Erweitert...** klicken, können Sie die speziellen Einstellungen **Ultraschnelles Erstellen** und **Wachsendes Laufwerk** auswählen.

Lesen Sie sich hierzu bitte unbedingt das Kapitel Wachsende Laufwerke und Ultraschnelles Erstellen durch. Hier werden Vor- und Nachteile aufgeführt und Fallstricke im Umgang mit solchen Laufwerken erläutert.

ArchiCrypt Live wählt als Vorgabe immer ca. 50% des Verfügbaren freien Speichers

Um zum nächsten Schritt zu gelangen, betätigen Sie die Schaltfläche **Weiter >>>**.

➡ WICHTIG: ***Sofern Sie einen Geheim-Container erstellen, zieht ArchiCrypt Live von der Größe des Laufwerks (Dateigröße) ca. 5% ab. Bitte beachten Sie, dass die Daten im Normalbereich möglicherweise deutlich mehr Platz benötigen. Beachten Sie daher die Hinweise unter Geheimfach***

4 Wie soll das Laufwerk geschützt werden?

Schutz

Sie haben hier die Möglichkeit, festzulegen, ob Sie Ihr Laufwerk konventionell mittels Passwort (siehe Passwortdialog), mit Hilfe einer Schlüsseldatei, einer speziellen ArchiCrypt Card oder einem Security-Token schützen möchten. Schlüsseldatei und ArchiCrypt Card ersparen Ihnen die lästige Eingabe eines komplizierten Passwortes.
(Siehe Schlüsseldatei erstellen und Schlüsseldatei einlesen --- ArchiCrypt Card einlesen und ArchiCrypt Card personalisieren und Schlüssel von Token nutzen).

Der beim Erstellen eines Laufwerks angegebene Schlüssel wird auch als Laufwerk-Administrator-Schlüssel bezeichnet. Es kann sich um ein normales Passwort, eine Schlüsseldatei oder um einen Schlüssel von der ArchiCrypt Card oder einem Security-Token handeln.
siehe auch: Laufwerk-Administrator-Schlüssel

Verschlüsselungsmethode

Legen Sie die Methode fest, mit der Ihre Daten verschlüsselt werden sollen. Beide Verfahren haben in zahlreichen Tests durch die besten Kryptanalytiker der Welt unter Beweis gestellt, dass der Verschlüsselungsmechanismus auf absehbare Zeit nicht zu brechen ist. AES (*Advanced Encryption Standard; im XEX Modus*) ist der Nachfolger des bekannten DES (*Data Encryption Standard*). Die in ArchiCrypt Live eingesetzten Verfahren sind in der besonders sicheren Variante mit 256 BIT großem Schlüssel im s.g. XEX Modus implementiert. Die Verschlüsselungsroutinen stammen aus einer Referenzimplementierung die frei verfügbar ist (siehe auch Eingesetzte Verfahren). Sofern auf Ihr

Prozessor den erweiterten Befehlssatz AES-NI unterstützt, müssen Sie dieses Verfahren wählen, um von den Geschwindigkeitsvorteilen zu profitieren.

Dateisystem

Hier können Sie, sofern Sie ArchiCrypt Live mit Administratorrechten gestartet haben das neue Live Laufwerk im Rahmen des Erstellvorgangs im Dateisystem NTFS formatieren lassen.
Lassen Sie das Häkchen weg und ArchiCrypt Live erzeugt das neue Laufwerk automatisch mit dem Dateisystem FAT.


TECHNIK *Das ArchiCrypt Live Laufwerk besitzt, wie eine normale Festplatte, ein s.g. Dateisystem. Ein Dateisystem legt die Art fest, wie die binären Daten auf dem Datenträger organisiert und interpretiert werden. Unter Windows werden die Dateisysteme FAT (FAT12, FAT16, FAT32 und exFAT) und NTFS eingesetzt. Beim Erstellen kann ArchiCrypt Live ohne Hilfe des Betriebssystems die FAT Dateisysteme (Ausnahme exFAT) erstellen. Unter Zuhilfenahme des Betriebssystems kann ArchiCrypt Live seine Laufwerke auch als NTFS Laufwerk formatieren. FAT32 ist am meisten verbreitet und hinsichtlich der Kompatibilität eine sichere Bank. Wenn es jedoch darum geht, große Dateien zu speichern, hat FAT sein Limit bei 4 Gigabyte. Diese Beschränkung kennt das NTFS Dateisystem nicht.*

Vorteile FAT Dateisystem:

- FAT Laufwerke können auf allen durch ArchiCrypt Live unterstützten Windows Systemen auch im Nur-Lesen-Modus geladen werden. Dies ist insbesondere dann wichtig, wenn Sie Ihre ArchiCrypt Live Laufwerke zum Beispiel auf CD oder DVD sichern und von dort laden wollen.
- Auf ArchiCrypt Live Laufwerken, die das FAT Dateisystem aufweisen, können Sie ein s.g. Geheimfach einrichten.
- ArchiCrypt Live ToGo (*separat erhältliches Zusatzprogramm*) kann auf FAT Dateisysteme zugreifen und ermöglicht dadurch den Zugriff auf Inhalte eines ArchiCrypt Live Laufwerks ohne jegliche Installation und ohne besondere Nutzerrechte. Zudem kann ArchiCrypt Live ToGo solche Live Laufwerke über das Internet (*von einer ganz normalen Internetseite*) lokal als Laufwerk einbinden.

Nachteile FAT Dateisystem:
- Dateien, die man auf dem Live Laufwerk ablegt, dürfen maximal 4 Gigabyte groß sein

Vorteile NTFS Dateisystem:
- Erlaubt das Speichern riesiger Dateien.

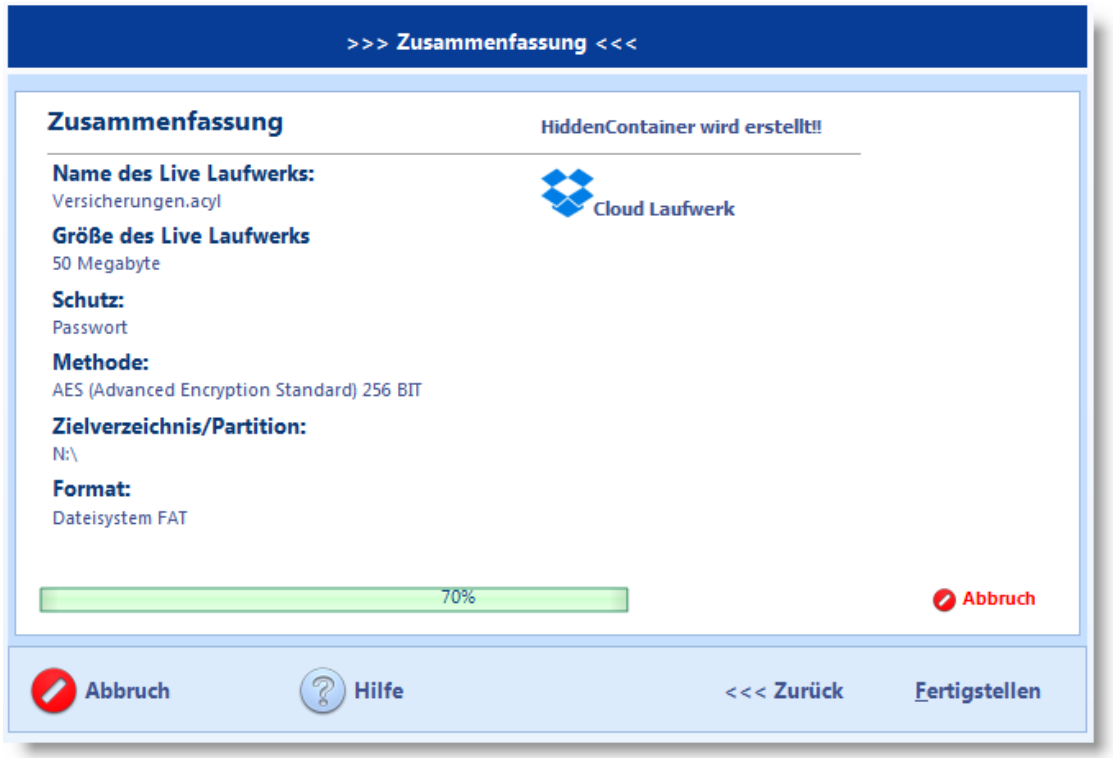
Nachteile NTFS Dateisystem:
- ArchiCrypt Live ToGo (*separat erhältliches Zusatzprogramm*) kann auf NTFS Laufwerke nicht zugreifen.
- In einem NTFS formatierten Live Laufwerk können Sie später kein Geheimfach erzeugen.
- Sollte ArchiCrypt Live einmal auf andere Plattformen portiert werden, ist dort nicht sichergestellt, dass NTFS unterstützt wird. FAT hingegen ist auf allen gängigen Plattformen vorhanden.


TIPP*Das NTFS Dateisystem wird meist gewählt, wenn man große Dateien (> 4 Gigabyte; wie z.B. Videos oder Backups) auf dem Laufwerk speichern möchte. Wenn Sie ein Geheimfach erzeugen und große Dateien nutzen wollen, erstellen Sie das ArchiCrypt Live Laufwerk zunächst als FAT Laufwerk. Wenn Sie jetzt ein Geheimfach erzeugen, lassen Sie diesen als NTFS Laufwerk formatieren. Jetzt können Sie im Geheimfach auch Dateien größer 4 Gigabyte speichern.*

Durch das Betätigen der Schaltfläche **Weiter >>>** wird der Passwortdialog (siehe Passwortdialog) bzw. der Dialog zum Einlesen/Erzeugen einer Schlüsseldatei bzw. Einlesen der ArchiCrypt Card oder Auswahl eines Schlüssels auf einem Token aufgerufen.

(Siehe Schlüsseldatei erstellen und Schlüsseldatei einlesen --- ArchiCrypt Card einlesen und ArchiCrypt Card personalisieren und Schlüssel von Token nutzen).

Zusammenfassung



Sie haben alle notwendigen Angaben gemacht. ArchiCrypt Live zeigt Ihnen auf einer Seite eine Zusammenfassung. Falls Sie eine der Angaben ändern möchten, können Sie durch das Betätigen der Schaltfläche **<<< Zurück** zu jedem vorangegangenen Schritt navigieren.

Durch einen Klick auf die Schaltfläche Fertigstellen, starten Sie den Erstellvorgang des ArchiCrypt Live Laufwerks. Den Erstellvorgang können Sie durch das Betätigen der Schaltfläche Abbruch neben der Fortschrittsanzeige abbrechen.

ACHTUNG. ***Falls Sie ein sehr großes ArchiCrypt Live Laufwerk erstellen, kann der Erstellvorgang sehr lange dauern! Das Erstellen eines Laufwerks mit der Option "Ultraschnelles Erstellen" oder "Als Wachsendes Laufwerk erstellen" geht hingegen sehr schnell vonstatten.***

Ergebnis des Erstellens

Nachdem der Erstellvorgang abgeschlossen wurde können Sie anhand der Meldung feststellen, ob das Erstellen fehlerfrei durchgeführt werden konnte. Um das Laufwerk sofort zu nutzen, Betätigen Sie die Schaltfläche Öffnen.
Sofern Sie nach ca. 5 Sekunden nicht auf die Schaltfläche Öffnen betätigen, wird die Schaltfläche deaktiviert und das Passwort

aus dem Speicher entfernt. Zum Öffnen müssen Sie das Passwort neu eingeben.

Sie haben zudem die Möglichkeit, das gerade erstellte Laufwerk als Favorit zu übernehmen.

Öffnen des neuen Laufwerkes

Nachdem Sie die Schaltfläche Öffnen betätigt haben, erscheint der Dialog zum Öffnen/Schließen von Laufwerken, das Laufwerk ist jetzt geöffnet!

Weiter zu Öffnen / Schließen >>

10.4.2 Öffnen/Schließen

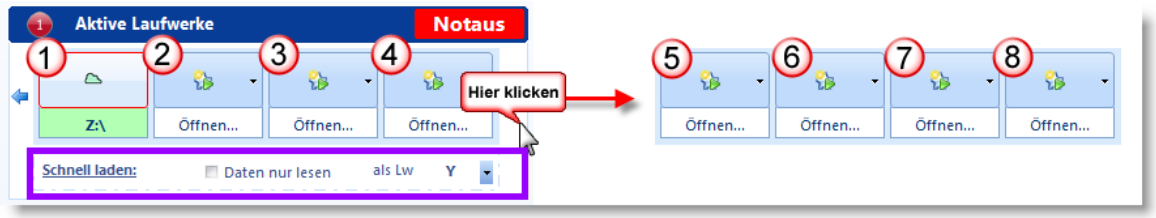
siehe auch: Wichtige Begriffe - Begriffserläuterungen
Favoriten

ACHTUNG: Laufwerke, die mit Version 5 oder älter erstellt wurden sollten ausschließlich mit Lesezugriff geöffnet werden!!! Sie sollten jedes Schreiben auf das Laufwerk vermeiden! Falls Sie zwingend

schreibenden Zugriff benötigen, deaktivieren Sie die Option Auf Laufwerke älteren Typs nur lesend zugreifen.

So öffnen und schließen Sie die verschlüsselten Laufwerke

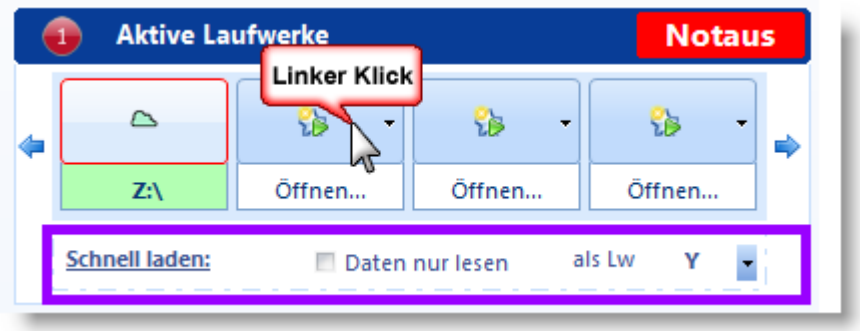
Auf der Home-Seite von ArchiCrypt Live finden Sie unter Aktive Laufwerke ACHT Speicherplätze (Slots) für Live Laufwerke. Dies entspricht der maximalen Anzahl an Laufwerken, die ArchiCrypt Live gleichzeitig laden und verwalten kann.



Über diese Speicherplätze können Sie Live Laufwerke laden und entladen. Dauerhaften Komfort bieten die so genannten Favoriten.

- Öffnen eines ArchiCrypt Live Laufwerks
- Automatisches Laden mit Schlüsseldatei
- WERKZEUGE
- Schließen
- Notaus
- Alle schließen
- Inhalt ansehen
- Autostart festlegen
- Autostart löschen
- Umleitung einrichten
- Anwendungskontrolle

Öffnen eines ArchiCrypt Live Laufwerks



ArchiCrypt Live wählt vom Ende des Alphabets den ersten freien Laufwerksbuchstaben und stellt diesen als Vorgabe ein.

Ein Linksklick auf einen freien Speicherplatz öffnet jetzt den Dateidialog, in dem Sie die Live-Laufwerksdatei wählen können. Nach Eingabe des Passwortes steht das Laufwerk dann unter dem angegebenen Buchstaben bereit. Sie können hier selbstverständlich auch einen anderen Buchstaben voreinstellen.

Mit Strg + Linksklick auf einen freien Speicherplatzrufen Sie einen erweiterten Dialog auf.

TIPP: Wenn Sie in den Einstellungen die Option Verlauf - Zuletzt geöffnete Live Laufwerke merken aktiviert haben, sehen Sie bei den freien Speicherplätzen einen kleinen Pfeil. Wenn Sie diesen betätigen, erscheint ein Menü in dem Sie ein zuletzt geöffnetes Laufwerk wählen können.

➡Falls Sie Anwendungen auf den ArchiCrypt Laufwerken installiert haben, sollten Sie das Laufwerk möglichst immer mit dem gleichen Laufwerksbuchstaben laden. Legen Sie das Laufwerk als Favorit an, dort können Sie dies als Vorgabe dauerhaft speichern.

Modus

Wählen Sie aus, ob Sie das Laufwerk im Lesemodus "Nur Lesen" (*Laufwerksinhalte können gelesen, nicht aber geändert werden; ähnlich wie CD/oder DVD*) oder im Schreibmodus

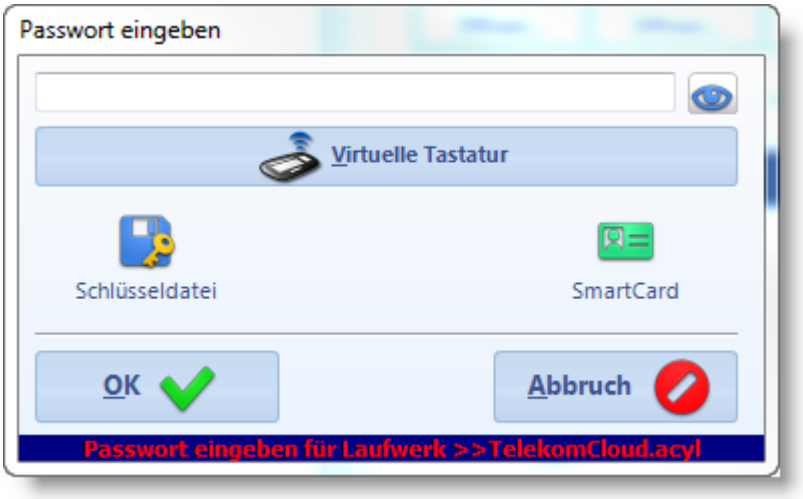
"Schreiben & Lesen" (*Daten können geändert und gelöscht werden*) öffnen möchten.

Betätigen Sie die Schaltfläche Live-Datei um ein dateibasiertes Live Laufwerk (*Trägerdatei*) auszuwählen, bzw. Live-Partition um eine Live Partition zu wählen.

➡ HINWEIS: Der Modus Schreiben und Lesen ist nur dann wirksam, wenn der eingegebene Schlüssel eine entsprechende Berechtigung hat (*Laufwerk-Administrator-,Geheimfach-, Gast Lesen Schreiben-Schlüssel*).

Es erscheint der Windows-Dialog zur Auswahl einer Datei!

Geben Sie im nachfolgenden Dialog das Passwort für das Laufwerk ein, Betätigen die Schaltfläche Schlüsseldatei, Token oder SmartCard, um den Schlüssel von einer Datei, einer ArchiCrypt Card oder einem Security-Token einzulesen. Zur Eingabe des Passwortes können Sie die s.g. Virtuelle Tastatur nutzen.



Falls Sie das Passwort korrekt eingegeben, die richtige Schlüsseldatei oder ArchiCrypt Card eingelegt oder den korrekten Schlüssel vom Token eingelesen haben, wird das Laufwerk geöffnet und steht jetzt in Ihrem System unter dem angegebenen Laufwerksbuchstaben zur Verfügung. Den Erfolg erkennen Sie an dem (grünen - Lese-Schreibzugriff/roten-Lesezugriff) Symbol auf dem zum Laufwerk gehörenden Speicherplatz. Ein in Cloud Laufwerk hat Symbol eine kleine Wolke.

TIPP: Unterhalb des Speicherplatzes finden Sie bei einem geladenen Live-Laufwerk den Laufwerksbuchstaben. Wenn Sie darauf Linksklicken, wird der Dateimanager geöffnet und der Inhalt des Live-Laufwerks angezeigt.

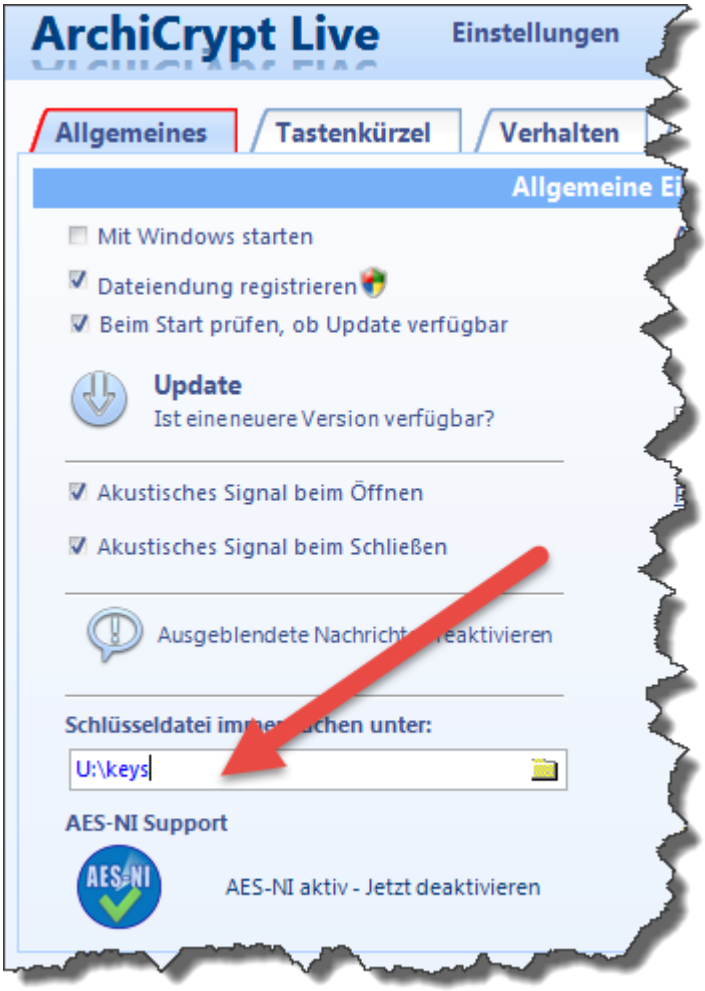
Schlüsseldatei für automatisches Laden einsetzen

Sie können in den Einstellungen von ArchiCrypt Live einen Pfad angeben, in dem nach Schlüsseldateien gesucht werden soll. Also zum Beispiel den Pfad zu einem Wechselmedium, welches Sie am Rechner immer dann anschließen, wenn Sie Live Laufwerke laden. Auf diesem Datenträger speichern Sie dann im angegeben Pfad dann die zu einem Laufwerk gehörende Schlüsseldatei.
Die Schlüsseldatei muss vom Typ unverschlüsselt sein.

Benennen Sie die Schlüsseldatei wir die Live Laufwerksdatei, wobei die Endung ack sein muss.

Beispiel:

Sie haben einen USB-Stick, der auf Ihrem Rechner unter dem Laufwerksbuchstaben U:\ geladen wird. Auf diesem Stick gibt es ein Verzeichnis U:\keys in welchem Sie die Schlüsseldateien ablegen möchten.
Tragen Sie diesen Pfad in den Einstellungen ein.



Sie haben jetzt ein Live Laufwerk (F:\Dokumente\LiveUrkunden.acyl erstellt und mit einer UNVERSCHLÜSSELTEN Schlüsseldatei abgesichert. Benennen Sie die Schlüsseldatei jetzt um in LiveUrkunden.ack und legen Sie sie unter U:\keys ab. Beim Öffnen eines ive Laufwerks sieht Live jetzt immer zuerst unter diesem Verzeichnis nach, ob eine passende Schlüsseldatei existiert. Falls ja, wird diese zum Laden verwendet.

TIPP: Wenn Sie mehrere Laufwerke mit der gleichen Schlüsseldatei abgesichert haben, dann kopieren Sie die Schlüsseldatei einfach und benennen sie jeweils nach dem oben beschriebenen Schema.

WARNUNG: Denken Sie daran, dass es Sie den USB-Stick oder Datenträger nach dem Laden ggf. wieder vom Rechner entfernen, sofern die Gefahr besteht, dass unbefugt auf die Schlüsseldateien zugegriffen werden könnte.

Werkzeuge für das Live Laufwerk

Wenn Sie auf einen Speicherplatz mit geladenem Laufwerk linksklicken, werden Ihnen Informationen zum Laufwerk und spezielle Werkzeuge angezeigt. Der ausgewählte Speicherplatz wird ROT umrahmt. Um zur normalen Home-Ansicht zurückzukehren, linksklicken Sie auf den rot umrandeten Speicherplatz.

Neben der Kapazität, dem belegten und noch freien Speicherplatz des Live Laufwerks, sehen Sie den Namen der zugehörigen Datei. Oberhalb der Kapazitätsanzeige finden Sie Werkzeuge für das aktuelle Laufwerk.

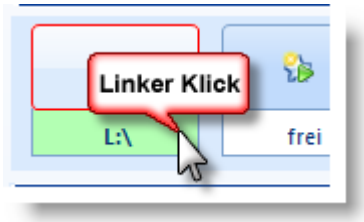
Inhalt ansehen...

Jedes geladene Live Laufwerk können Sie vollkommen transparent aus jeder Anwendung heraus ansprechen. Den

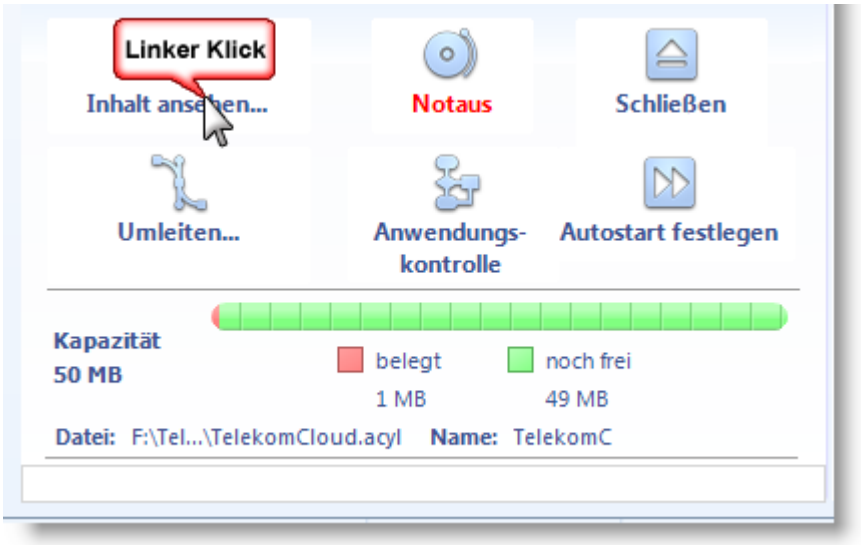
Inhalt können Sie sich über den Windows Explorer anzeigen lassen.

Aus ArchiCrypt Live heraus gibt es mehrere Möglichkeiten, sich den Inhalt direkt im Dateimanager anzeigen zu lassen:

1. Klicken Sie bei dem Speicherplatz, der das entsprechende Laufwerk beheimatet einfach auf den Laufwerksbuchstaben.

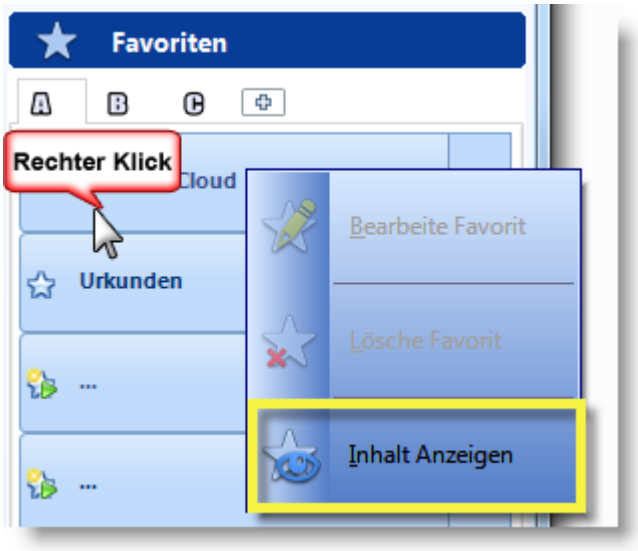


2. Klicken Sie bei den Werkzeugen auf die Schaltfläche Inhalt ansehen...



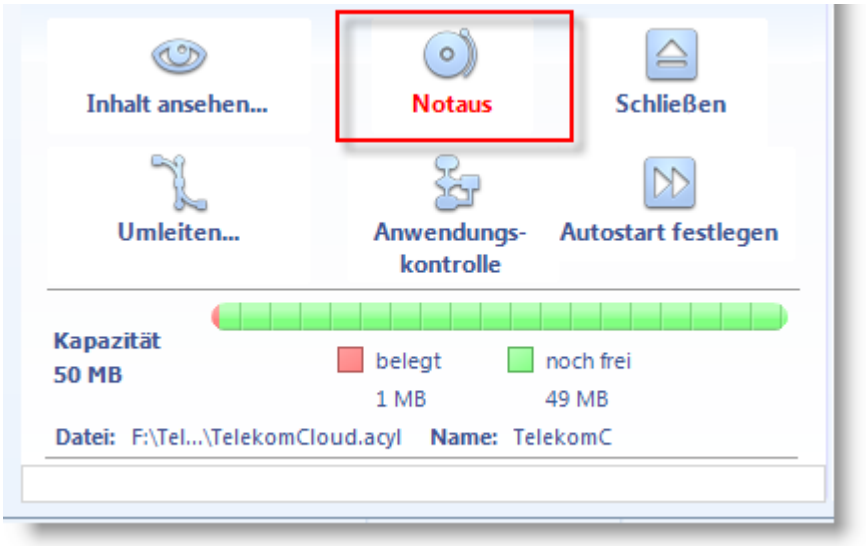
3. Falls Sie in den Einstellungen Tastenkürzel für das Anzeigen des Inhalts festgelegt haben, genügt der Aufruf per Tastenkombination.

4. Sollten Sie das Laufwerk als Favorit angelegt haben, können Sie über dem Favoriten-Speicherplatz die rechte Maustaste betätigen und im Kontextmenü den Punkt Inhalt anzeigen



Notaus

Das Laufwerk wird geschlossen, auch wenn noch auf Dateien des Laufwerks zugegriffen wird. Dieses Notaus bezieht sich ausschließlich auf das aktuell ausgewählte Laufwerk.

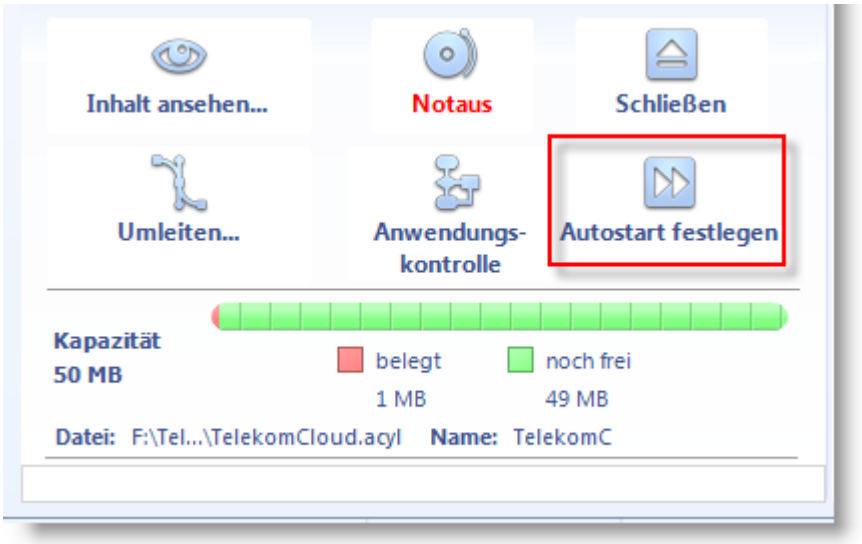


➡ WARNUNG! Ihr System kann dadurch instabil werden, im schlimmsten Fall kann es zu Datenverlust kommen.

HINWEIS: Sollte sich ein ArchiCrypt Live Laufwerk einmal nicht schließen lassen, starten Sie den Rechner neu. Beim Herunterfahren werden offene Laufwerke grundsätzlich geschlossen. Die Inhalte des Laufwerks liegen zu jedem Zeitpunkt verschlüsselt auf dem Datenträger.

Autostart festlegen

Hier können Sie eine Datei oder Anwendung festlegen, die geöffnet bzw. gestartet werden soll, sobald dieses Laufwerk geöffnet wird.



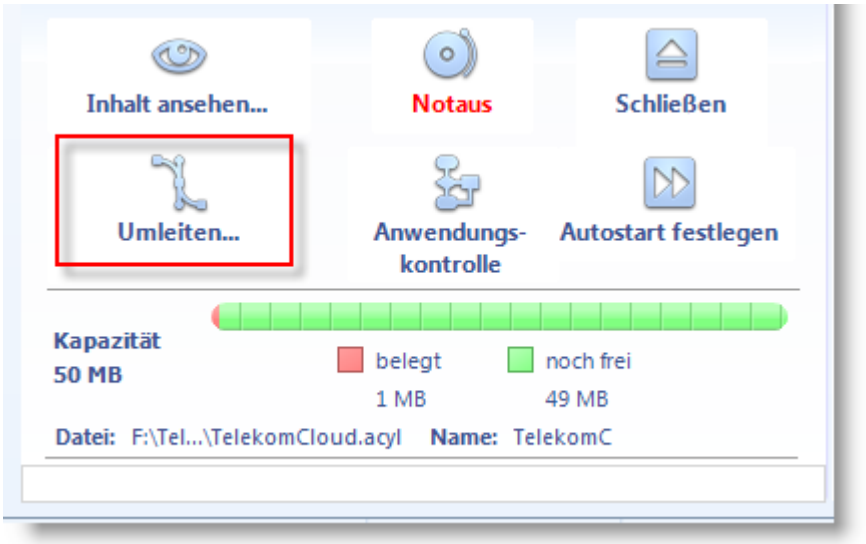
TIPP: Die Datei oder Anwendung muss nicht auf dem ArchiCrypt Live Laufwerk abgelegt sein! Sie können so zum Beispiel Microsoft Word starten, um Dateien auf Ihrem Live Laufwerk damit bearbeiten zu können.

Autostart löschen

Die Autostartfunktion wird zurückgesetzt. Beim Öffnen des Laufwerks wird keine Datei geöffnet oder gestartet.

Umleitung einrichten

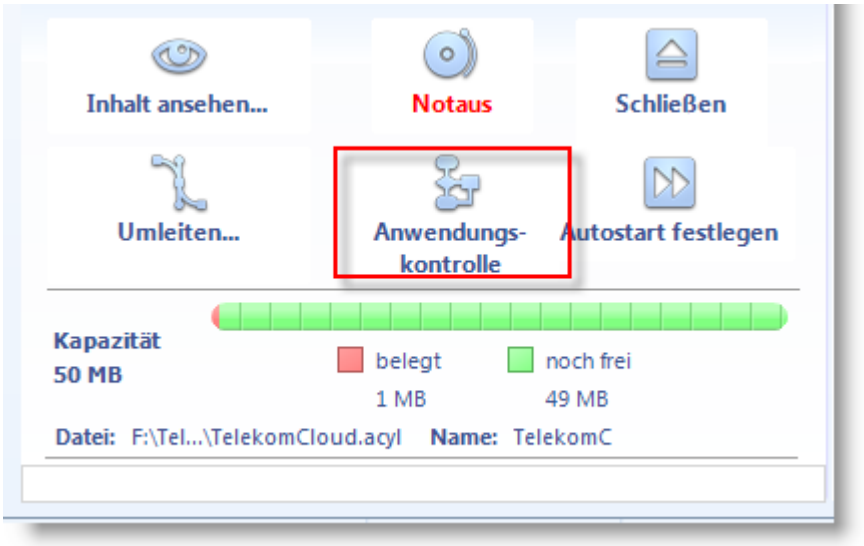
Mit Umleitungen können Sie bequem Dateioperationen von einem Verzeichnis auf ein Live-Laufwerk umleiten. Eine detaillierte Beschreibung finden Sie im Kapitel Umleitung.



Anwendungskontrolle - Zugriff durch Programme

Wenn Sie ein Live Laufwerk geladen haben, können Sie vollkommen transparent auf die Daten darauf zugreifen. Gerade bei hoch sensiblen Daten ist dies nicht immer gewünscht. Es kann durchaus sinnvoll sein, nur wenigen Anwendungen zu erlauben, auf Daten des Live Laufwerks zuzugreifen. Insbesondere ist es vielleicht nicht erwünscht, dass Internet Explorer, Firefox, Chrome und deren Erweiterungen uneingeschränkten Zugriff auf Laufwerksinhalte haben. Hier hilft die Anwendungskontrolle - Zugriff durch Programme. Detaillierte Informationen erhalten Sie im Kapitel Anwendungskontrolle - Zugriff durch Programme.

Eine detaillierte Beschreibung finden Sie im Kapitel Anwendungskontrolle.

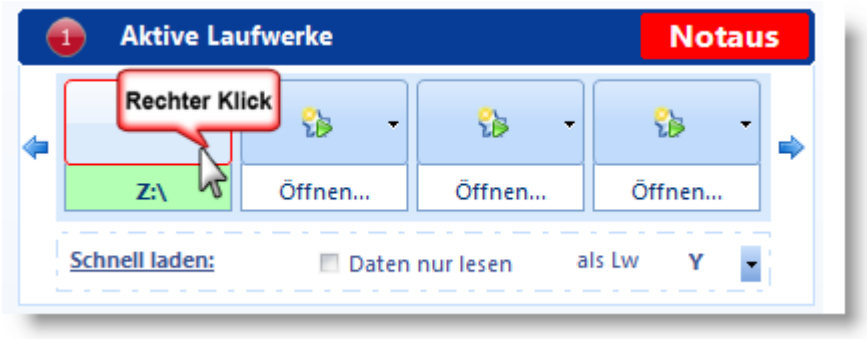


So schließen Sie ein ArchiCrypt Live Laufwerk:

Es gibt verschiedene Möglichkeiten, ein Laufwerk zu schließen. Grundsätzlich kann man dabei zwischen dem s.g. Notaus und dem normalen Schließen unterscheiden. Während die Notaus Variante keine Rücksicht auf Programme nimmt, die eventuell noch auf Daten des Laufwerks zugreifen, prüft das normale Schließen zunächst, ob Anwendungen
auf Dateien zugreifen und bricht das Schließen ggf. ab.

Einzelne Laufwerke schließen

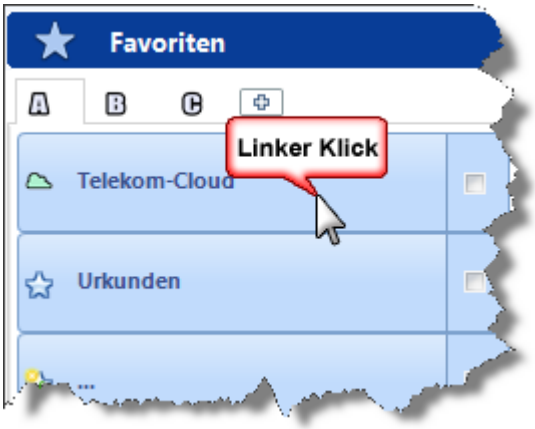
Die schnellste Möglichkeit besteht darin, auf den entsprechenden Speicherplatz rechtszuklicken.



➡ Sollte das Laufwerk nicht geschlossen werden können, liegt dies meist daran, dass sein Inhalt im Dateimanager angezeigt wird oder andere Anwendungen auf Inhalte zugreifen.

HINWEIS: Beim Herunterfahren werden offene Laufwerke grundsätzlich geschlossen. Die Inhalte des Laufwerks liegen zu jedem Zeitpunkt verschlüsselt auf dem Datenträger.

Wenn Sie ein Laufwerk als Favorit eingerichtet haben, können Sie auf den zugehörigen Favoriten linksklicken.

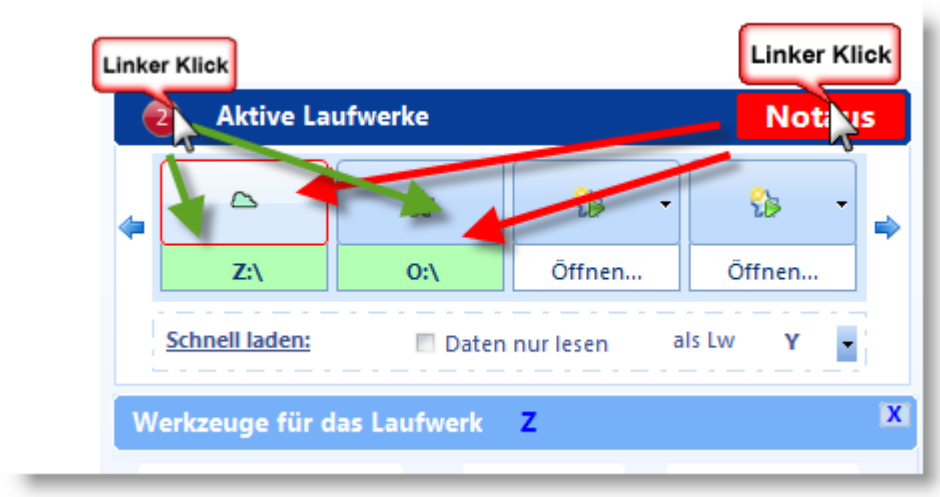


Bei einem Favoriten gibt es noch weitere Möglichkeiten, das Laufwerk zu schließen. Zum Beispiel durch das Entfernen der ArchiCrypt Card oder der Eingabe des Magic Word.

Mehrere Laufwerke schließen

Auch hier kann man wieder zwischen dem Notaus (*Schließen ohne Rücksicht*) und dem normalen Schließen unterscheiden.

Die Notaus Schaltfläche bei Aktive Laufwerke schließt alle zur Zeit aktiven Laufwerke ohne Rücksicht darauf, ob Anwendungen noch auf Dateien dieses Laufwerks zugreifen. Linksklick auf die Zahl 2 prüft zunächst, ob noch Anwendungen auf das Laufwerk zugreifen und bricht das Schließen ggf. ab.



In den Einstellungen können Sie ein Tastaturkürzel festlegen, mit dem alle Laufwerke geschlossen werden.

Wenn die geladenen Laufwerke als Favorit eingerichtet sind, können Sie die zu schließenden Laufwerke mit einem Häkchen markieren und die Schließen Schaltfläche betätigen.

10.4.3 Live Partition

Sollten sich die nachfolgenden Videos im Browser nicht anzeigen lassen, so können Sie die Videos alternativ direkt in Youtube auf unserem ArchiCrypt Kanal ansehen.

Video - Live Partition

siehe auch: Wichtige Begriffe - Begriffserläuterungen
Dialog zur Auswahl einer Partition

Das Erstellen einer Live Partition wird nur erfahrenen Nutzern empfohlen

Was ist eine Live Partition?

Eine Live Partition ist eine Partition, die so umgewandelt wurde, dass ArchiCrypt Live die komplette Partition direkt als Laufwerk mit Echtzeitverschlüsselung laden kann. Die Umwandlung der Systempartition (*Partition auf dem sich das Betriebssystem befindet*) ist nicht möglich.

Der Erstellprozess ist im Wesentlichen identisch mit dem Vorgehen, wie Sie es vom Erstellen eines Live Laufwerks (*dateibasiert*) als Trägerdatei her kennen. Neben einer Beschreibung und Auflistung der Vor- und Nachteile verschiedener Laufwerksarten ist das Verfahren zum Erstellen einer Live Partition auch im Kapitel Erstellen erläutert.

Grundsätzlich bietet eine komplett verschlüsselte Partition keine unschlagbaren Vorteile gegenüber den sehr flexiblen, dateibasierten Live Laufwerken (*Trägerdateien*). In Einzelfällen kann es jedoch von Vorteil sein, eine ganze Datenpartition umzuwandeln. So ist eine Live Partition nicht einfach zu löschen, wohingegen dateibasierte Laufwerke auch versehentlich gelöscht werden könnten.

Was ist beim Erstellen einer Live Partition zu beachten?

- Daten, die sich auf der umzuwandelnden Partition befinden, werden beim Erstellprozess überschrieben und sind unwiederbringlich verloren. Sichern Sie ggf. die Daten die sich auf der Partition befinden.
- Um Verwirrung zu vermeiden, sollten Sie einen der Partition zugeordneten Laufwerksbuchstaben in der Datenträgerverwaltung des Betriebssystem entfernen. Tun Sie dies nicht, erscheint beim Zugriff über diesen Laufwerksbuchstaben die Meldung, dass es sich um eine nicht formatierte Partition handelt. Gleichzeitig wird angeboten, die Partition zu formatieren. Windows kann die verschlüsselten Daten nicht interpretieren, daher geht es von einem unformatierten Datenträger aus. Ein Formatieren würde natürlich die Live Partition zerstören. Wie Sie den Laufwerksbuchstaben entfernen ist im Kapitel Erstellen beschrieben.

Sie können alternativ die Hilfe des Betriebssystems aufrufen und dort den Suchbegriff Datenträgerverwaltung eingeben.

➡ACHTUNG: Drohender Datenverlust!! ***Bevor Sie z.B. durch falsche Auswahl einer Partition Datenverlust erleiden, sollten Sie Ihr komplettes System mit einer geeigneten Backup-Software sichern!***

Definition Partition:

Als Partition bezeichnet man im Allgemeinen eine Unterteilung eines Ganzen in mehrere Teile. Übertragen auf die Welt des Computers bedeutet Partition, die Einteilung eines Datenträgers in mehrere Teile (Partitionen/Laufwerke). So kann in Ihrem Rechner z.B. eine einzige Festplatte installiert sein, die jedoch in mehrere Partitionen unterteilt ist. Diese Partitionen können dann in Ihrem Rechner als verschiedene Laufwerke auftauchen. Z.B. Laufwerk C und Laufwerk D. Partitionen können aktiv und damit direkt sichtbar sein, oder aber inaktiv.
Die Partitionen tragen in Ihrem Rechner eindeutige Bezeichnungen, die Sie in der Form nie zu Gesicht bekommen. So tragen Partitionen s.g. Devicenamen (*Gerätenamen*) wie
\Device\Harddisk0\Partition1 oder
\Device\Harddisk1\Partition3
Damit Sie sich nicht mit diesen unhandlichen Namen herumschlagen müssen, gibt es die Laufwerksbuchstaben wie C:\, D:\ usw. Diese Laufwerksbuchstaben sind jedoch nicht eindeutig und können beliebig geändert werden. ArchiCrypt Live greift daher auf die eindeutige Bezeichnung zurück, gibt Ihnen jedoch genau an, unter welchem Laufwerksbuchstaben das Laufwerk in Ihrem System gerade verfügbar ist (*sofern die Partition aktiv ist*)!

10.4.4 Geheimfach

Sollten sich die nachfolgenden Videos im Browser nicht anzeigen lassen, so können Sie die Videos alternativ direkt in Youtube auf unserem ArchiCrypt Kanal ansehen.

Video - Geheimfach

siehe auch: Wichtige Begriffe - Begriffserläuterungen

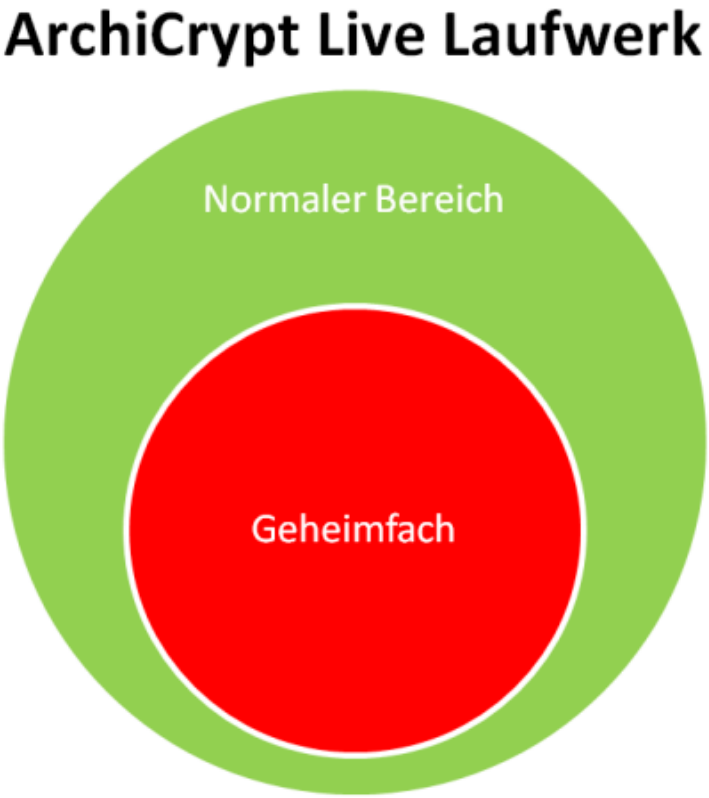
Was ist ein Geheimfach?

Bei einem Geheimfach handelt es sich um einen Bereich in einem ArchiCrypt Live Laufwerk, der nur mit Hilfe eines speziellen Schlüssels dem s.g. Geheimfach Schlüssel zugänglich ist. Werden Sie gezwungen, den Schlüssel herauszugeben, teilen Sie eines der Passwörter für den "Normalen Bereich" mit. Die tatsächlich geheimen Daten liegen sicher versteckt im Geheimfach, auf das man mit dem normalen Passwort nicht zugreifen kann.

Öffnet man ein Live-Laufwerk mit dem Laufwerk-Administrator-Schlüssel (*der Schlüssel der beim Erstellen angegeben wurde*) oder einem Gast-Schlüssel, erhält man Zugang zu den "normalen" Inhalten. Wenn das Geheimfach Passwort eingegeben wird, erhält man Zugriff auf den geheimen Inhalt.

Das Besondere an einem Geheimfach ist der Umstand, dass man seine Existenz nicht nachweisen kann.

siehe Plausibles Verleugnen



Normaler Bereich

Der normale Bereich ist sichtbar, wenn man das Passwort eingibt, welches man beim Erstellen des Laufwerks festgelegt hat. (Natürlich werden spätere Änderungen des Passwortes berücksichtigt). Gäste haben ebenfalls nur auf den normalen Bereich Zugriff. Der Bereich, in dem das Geheimfach untergebracht ist, stellt sich als nicht interpretierbare Ansammlung von Datenmüll dar und ist als freier Speicher im normalen Bereich verfügbar. Das "normale" Laufwerk weiß also nichts um die Existenz des Geheimfachs. Auf der einen Seite ist diese Eigenschaft wunderbar, da sie uns garantiert, dass jemand der Zugang zum normalen Bereich hat, weder auf Inhalte im Geheimfach zugreifen kann, noch die Existenz nachweisen kann. Auf die der anderen Seite besteht jedoch die Gefahr, dass man Daten im Geheimfach durch Speichern von Daten im normalen Laufwerk versehentlich überschreibt. Das Geheimfach wird durch eine solche Aktion zerstört!

Geheimfach

Der Bereich ist nur sichtbar, wenn man das Geheimfach-Passwort eingibt. Öffnet man das Live Laufwerk mit einem anderen Passwort, wird der normale Bereich sichtbar, in dem die Daten des Geheimfachs nicht sichtbar und nicht nachweisbar sind.

Was muss man beim Erstellen eines Geheimfachs beachten?

Um ein Geheimfach erstellen zu können, müssen Sie über ein bereits bestehendes Live Laufwerk verfügen, zu dem Sie den Laufwerk-Administrator-Schlüssel (*Schlüssel, der beim Erstellen angeben wurde*) besitzen.

Denken Sie beim Festlegen der Größe für das komplette Live Laufwerk daran, genug Platz für die "normalen" Daten und das Geheimfach zu reservieren.

Welche Voraussetzungen müssen erfüllt sein, damit Sie in einem bestehenden ArchiCrypt Live Laufwerk ein Geheimfach erzeugen können?

1. Das ArchiCrypt Live Laufwerk (*nicht verwechseln mit dem Laufwerk, auf dem die Live Laufwerksdatei liegt*), in dem Sie ein Geheimfach erzeugen wollen, darf nicht im Dateisystem NTFS formatiert sein. Das Geheimfach selbst darf gerne im Dateisystem NTFS erzeugt werden.

 TECHNIK*Das ArchiCrypt Live Laufwerk besitzt, wie eine normale Festplatte, ein s.g. Dateisystem. Ein Dateisystem legt die Art fest, wie die binären Daten auf dem Datenträger organisiert und interpretiert werden. Unter Windows werden die Dateisysteme FAT (FAT12, FAT16, FAT32 und exFAT) und NTFS eingesetzt. Beim Erstellen kann ArchiCrypt Live ohne Hilfe des Betriebssystems die FAT Dateisysteme (Ausnahme exFAT) erstellen. Unter Zuhilfenahme des Betriebssystems kann ArchiCrypt Live seine Laufwerke auch als NTFS Laufwerk formatieren.*

2. Sie dürfen das Laufwerk nicht mit einer der beiden Optionen "Ultraschnelles Erstellen" oder Als "Wachsendes Laufwerk" erstellen erzeugt haben.

siehe auch: Dateisystem
Wachsende Laufwerke und Ultraschnelles Erstellen

Welche Gefahren bestehen beim Umgang mit einem Geheimfach?

Es bestehen grundsätzlich 2 Gefahren:

1. Beim Erstellen eines Geheimfachs können im ungünstigsten Fall Daten, die sich bereits auf dem Live Laufwerk im Normalbereich befinden überschrieben und zerstört werden. Dies ist eher unwahrscheinlich.
2. Schreiben Sie Daten in den Normalbereich, nachdem ein Geheimfach erstellt wurde, kann dabei das Geheimfach zerstört werden! Da der Normalbereich nicht weiß, ob oder wo ein Geheimfach existiert, stellt er beim Öffnen den Bereich mit den Daten des Geheimfachs als freien Speicher dar.

Wie soll man beim Erstellen eines Geheimfachs vorgehen?

1. Überlegen Sie sich zunächst, wie viel Platz Sie für die Daten benötigen, die Sie im Normalbereich unterbringen möchten und wie viel Platz notwendig ist, um die tatsächlich geheimen Daten zu speichern.
2. Zählen Sie diese beiden Werte zusammen und schlagen Sie ca. 20% auf diesen Wert.
3. Erstellen Sie ein ArchiCrypt Live Laufwerk in dieser Größe.
4. Öffnen Sie dann das Laufwerk und legen Sie die Daten im Normalbereich ab (*Daten die Sie im Notfall preisgeben möchten/können*).
5. Schließen Sie jetzt das Laufwerk.
6. Rufen Sie die Funktion **Neues Live Laufwerk ...** auf und aktivieren dort die Option **"Ein neues Live Laufwerk oder Geheimfach".** Im nächsten Schritt wählen Sie das soeben geschlossene ArchiCrypt Live Laufwerk aus.
7. Führen Sie die Schritte zum Erstellen des Laufwerks aus. ArchiCrypt Live ermittelt den maximal möglichen Platz, der für das Geheimfach verfügbar ist.
8. Nach dem Erstellen öffnen Sie den Normalbereich im Nur-Lesen Modus und prüfen, ob die Daten lesbar sind. Sollte dies nicht möglich sein, schlagen Sie bei der Größenberechnung 30% oder mehr auf und durchlaufen den Erstellprozess erneut (Punkt 1).
9. Ab diesem Zeitpunkt sollten Sie generell nur noch mit dem Geheimfach arbeiten. Sie können dort beliebig Daten hinzufügen, ändern, löschen etc. Beim Arbeiten mit dem Geheimfach wird der Normalbereich nie angetastet oder zerstört. Das Öffnen des Normalbereichs im Nur-Lese Modus ist ebenso unkritisch.

Beispiel:

Sie haben unverfängliche Daten die ca. 20 Megabyte umfassen und

etwas weniger als 30 Megabyte hoch-geheime Daten. Zusammen benötigen diese Dateien also ca. 50 Megabyte. Mit dem Sicherheitszuschlag von 20% ergibt sich die Größe des zu erstellenden Live Laufwerks zu ca. 60 Megabyte. Nach dem Erstellen des 60 MB großen Live Laufwerks öffnen wir das Laufwerk mit dem gerade beim Erstellen angegebenen Laufwerk-Administrator-Schlüssel. Jetzt kopieren wir die 20 MB unverfängliche Daten auf das Laufwerk und schließen es. Wir rufen erneut die Funktion zum Erstellen eines ArchiCrypt Live Laufwerkes auf und wählen unter Schritt 2 das soeben erstellte Live Laufwerk/die zugehörige Trägerdatei oder Live Partition aus. In Schritt 3 legen wir die Größe mit 30 MB fest und setzen den Erstellprozess wie gewohnt fort. Das hier eingegebene Passwort ist das Geheimfach Passwort. Nachdem das Erstellen erfolgreich beendet ist, verfügen wir über ein Live Laufwerk, welches je nach eingegebenem Passwort Zugriff auf den Normalbereich oder das Geheimfach erlaubt.

Wie soll ich mit einem Laufwerk, welches ein Geheimfach beinhaltet, umgehen?

Beim Erstellen des Geheimfachs kann es zum Verlust der bereits im Live Laufwerk vorhandenen Daten kommen. Wenn ein Geheimfach erfolgreich erstellt wurde, sollten Sie den Normalbereich nicht mehr mit Schreibzugriff (Modus Schreiben & Lesen) öffnen. Wenn Sie ihn dennoch mit Schreibzugriff öffnen müssen und Daten speichern, wird das Geheimfach unter Umständen zerstört!

Sind die Daten des Geheimfachs mit Spezialprogrammen einsehbar wenn der Normalbereich geöffnet ist?

Da der Normalbereich nichts von der Existenz des Geheimfachs weiß, sind keinerlei Inhalte (*Dateiinhalte, Programm-/Verzeichnisnamen, etc.*) oder Verweise auf die Daten vorhanden. Spezialprogramme sehen nur Datenmüll. Der Datenmüll wird beim Erstellen eines Live Laufwerks (*außer mit aktivierter Option "Ultraschnelles Erstellen" oder Als "Wachsendes Laufwerk";* siehe dazu: *Wachsende Laufwerke und Ultraschnelles Erstellen*) automatisch in den Datenbereich des neuen Laufwerks geschrieben und zwar immer. Untersucht man also mit einem Spezialprogramm den Normalbereich sieht man immer eine Ansammlung nicht interpretierbaren Datenmülls.

Der Bereich in dem das Geheimfach untergebracht ist, wird im Normalbereich als frei gekennzeichnet, wodurch die Gefahr des Überschreibens der Geheimdaten beim Schreiben von Daten im Normalbereich resultiert!

 TECHNIK*Aktivieren Sie beim Erstellen eines neuen Live Laufwerks eine der beiden Optionen* ***"Ultraschnelles Erstellen" oder Als "Wachsendes Laufwerk", resultieren die Geschwindigkeits- und Platzvorteile zumindest teilweise gerade aus dem Umstand heraus, dass ArchiCrypt Live das Laufwerk nicht mit Zufallsdaten vorbelegt. Würde man in einem solchen Laufwerk mit nicht vorbelegten Strukturen ein Geheimfach erstellen, wäre dieser bei geöffnetem Normalbereich nachweisbar (nicht einsehbar).*** Siehe***: Plausible Verleugnung***

Plausible Deniability (plausible Verweigerung, Leugnung)

Da in jedem ArchiCrypt Live Laufwerk, welches ohne die Optionen "Ultraschnelles Erstellen" oder Als "Wachsendes Laufwerk" erstellen erzeugt wurde, Zufallsdaten existieren (*bei der Erstellung werden diese bereits geschrieben*) und sich die Daten des Geheimfachs beim Öffnen des Normalbereichs ebenfalls nur als Ansammlung von Zufallsdaten darstellen, kann es sich bei diesen Daten um Zufallsdaten oder um ein Geheimfach handeln. Damit ist die Existenz eines solchen Geheim-Containers nicht beweisbar und damit plausibel zu leugnen. *siehe auch: Wachsende Laufwerke und Ultraschnelles Erstellen*)

10.4.5 Wachsende Laufwerke und Ultraschnelles Erstellen

Wenn Sie ein neues Laufwerk erstellen, haben Sie die Möglichkeit, eine der beiden Sonderfunktionen

"Ultraschnelles Erstellen" oder Als "Wachsendes Laufwerk" erstellen zu wählen.

Wachsendes Laufwerk und Ultraschnelles Erstellen

Voraussetzung:

Die beiden Sonderfunktionen stehen Ihnen nur dann zur Verfügung, wenn folgende Voraussetzungen erfüllt sind:

- Der Datenträger muss lokal verfügbar sein. Es darf sich also nicht um eine Netzwerk-Ressource (*z.B. Netzlaufwerk*) handeln.
- Um die Funktion Wachsendes Laufwerk nutzen zu können, muss der Datenträger, auf dem Sie das ArchiCrypt Live Laufwerk erzeugen möchten, im Dateisystem NTFS formatiert sein.

Nutzen:

Ultraschnelles Erstellen:

Erhebliche Ersparnis an Zeit beim Erstellen eines neuen Laufwerks

Beispiel:

ArchiCrypt Live benötigt für das Erstellen eine neuen Live Laufwerks der Größe 1 Terabyte (*Dateisystem FAT*) auf einer externen USB-Festplatte ohne die Option ca. 9 Stunden. Mit aktivierter Option lediglich 20 Sekunden.

Wachsendes Laufwerk:

Erhebliche Ersparnis an Zeit und Platz beim Erstellen und der Datensicherung

Wachsende Laufwerke werden grundsätzlich Ultraschnell erstellt und wachsen nach Bedarf bis zu einer Maximalgröße an.

Beispiel:

Ein Live Laufwerk mit einer Maximalkapazität von 512 Gigabyte (=524288 Megabyte) belegt nach dem Erstellen lediglich 144 Megabyte (*entspricht ca. 0,03%*).

Besonderheiten solcher Laufwerken

Bei den mit Sonderfunktionen erstellten Laufwerken gilt es, folgende Besonderheiten im Umgang zu berücksichtigen:

- Laufwerke arbeiten langsamer, als Laufwerke die ohne Sonderfunktion erzeugt wurden.
- Auf Laufwerken, die mit Sonderfunktionen erzeugt wurden, können keine Geheimfächer erzeugt werden.

Zusätzlich sind bei Wachsenden Laufwerken die folgenden Punkte wichtig

In der Cloud verliert die Datei Ihre Eigenschaft! Partitionen können nicht als wachsendes Laufwerk erzeugt werden. Es wird immer der komplette Partitionsplatz genutzt.
Die im Windows Explorer angezeigte Größe eines Wachsenden Laufwerks entspricht der von Ihnen als Maximum angegebenen Laufwerksgröße. Erst wenn Sie die Eigenschaften der Trägerdatei im Windows Explorer anzeigen lassen, können Sie den tatsächlich belegten Platz ersehen.

Beim Kopieren und Verschieben von Wachsenden Laufwerken mit Betriebssystemmitteln, verliert das ArchiCrypt Live Laufwerk für immer seine Eigenschaft. Es belegt dann also den vollen Platz. Verwenden Sie daher für diese Aktionen grundsätzlich das in ArchiCrypt Live angebotene Hilfsmittel unter Verwalten-Wachsende Laufwerke.

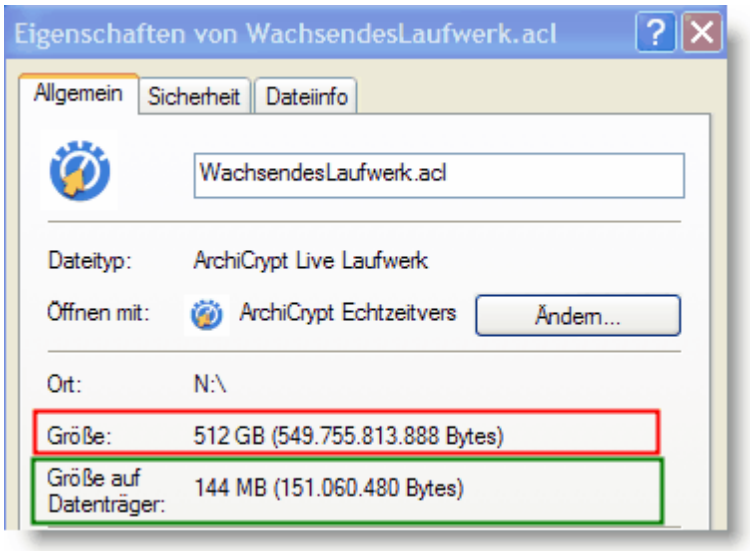
Wichtiger Hinweis

Hier droht Datenverlust!!!!
Angenommen, Sie haben einen Datenträger mit einer Kapazität von 512 Gigabyte. Jetzt erstellen Sie ein Wachsendes Live Laufwerk mit Maximalgröße von 512 Gigabyte. Anschließend kopieren Sie Daten auf den gleichen Datenträger auf dem auch Ihr

wachsendes Live Laufwerk liegt. Dies ist durchaus möglich, schließlich belegt das Wachsende Laufwerk zunächst nur Bruchteile der Maximalgröße. Wenn Sie jetzt jedoch Daten auf Ihr Live Laufwerk kopieren, die zusammen mit den Daten außerhalb des Live Laufwerks größer sind, als die Kapazität des Datenträgers es zulässt, kommt es unweigerlich zum Datenverlust. Das Betriebssystem meldet diesen Datenverlust und erzeugt Einträge für die Windows eigene Ereignisanzeige. ArchiCrypt Live ist hier machtlos, da das Betriebssystem ihm den entsprechenden Platz zusichert!!!

So ermitteln Sie die tatsächliche Größe eines Wachsenden Laufwerks auf dem Datenträger:

Im Dateimanager (*z.B. Windows Explorer*) die Trägerdatei auswählen und rechte Maustaste betätigen. Menüpunkt Eigenschaften aufrufen.



Grün umrahmt sehen Sie den tatsächlich belegten Platz (*im Beispiel* 144 Megabyte), rot umrahmt die Größe, bis zu der das Laufwerk anwachsen kann (*im Beispiel* 512 Gigabyte).

10.4.6 Steganografische Laufwerke und mobile Live Laufwerke

Sollten sich die nachfolgenden Videos im Browser nicht anzeigen lassen, so können Sie die Videos alternativ direkt in Youtube auf unserem ArchiCrypt Kanal ansehen.

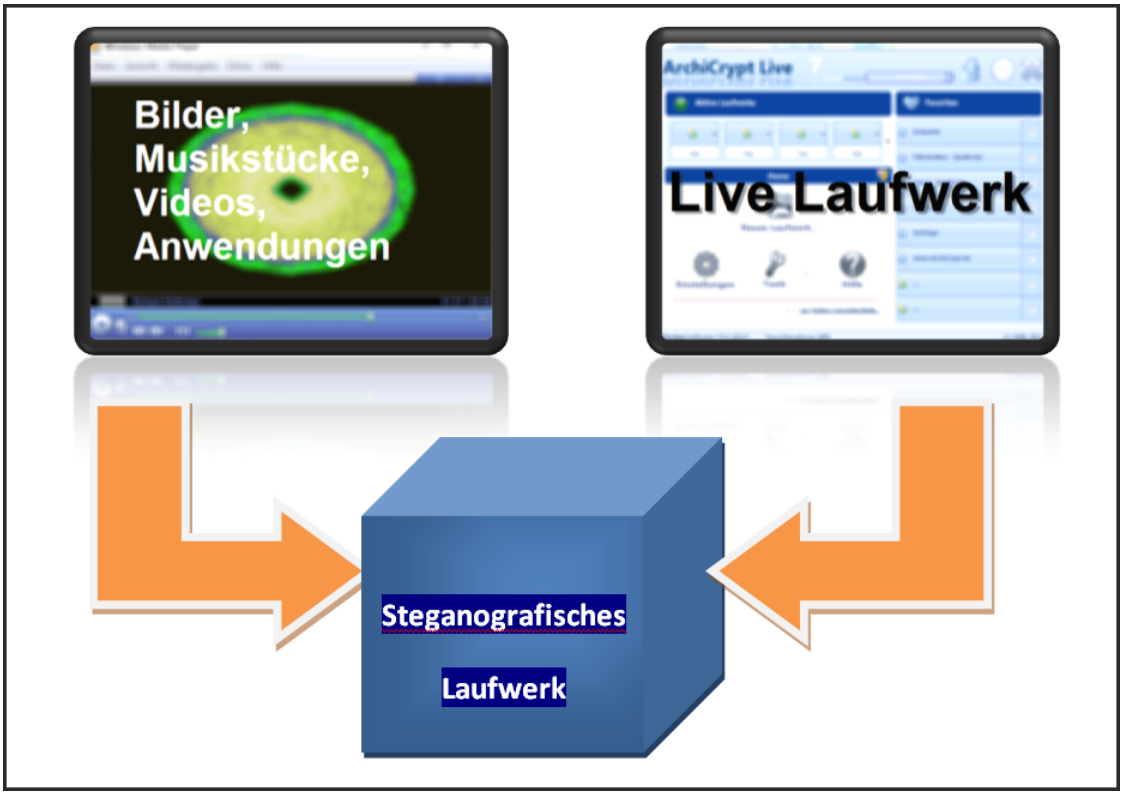
Video - Steganografisches

Video - mobiler Datensafe

siehe auch: Wichtige Begriffe - Begriffserläuterungen
ArchiCrypt Live Mobile

Was sind Steganografische Laufwerke?

Steganografische Laufwerke gehören ebenfalls zu den dateibasierten Laufwerken. D.h. alle Daten und Laufwerksinhalte befinden sich in einer Datei (s.g. Trägerdatei). Steganografische Laufwerke werden erstellt, indem man ein dateibasiertes Live Laufwerk mit einer zweiten Datei vermischt.



Zum Vermischen mit einem Live Laufwerk sind besonders Anwendungen (*Dateien mit Endung exe*) und zahlreiche Multimediadaten (*Videos, Musikstücke, viele Grafikformate*) geeignet. Sie sollten etwas experimentieren. Beim Erstellen eines Steganografischen Laufwerks werden die Originaldateien (*Live Laufwerk und Datendatei*) nicht angetastet!

Die aus dem Erstellprozess hervorgehende steganografische Datei hat die unglaubliche Eigenschaft, dass sie auf der einen Seite unverändert im ursprünglichen Sinne genutzt werden kann (*als Video, Grafik betrachtet, als Musikstück angehört, als Anwendung normal gestartet und genutzt*), man sie auf der anderen Seite jedoch auch als normales Live Laufwerk mit Lese-/Schreibzugriff laden kann.
Der Vorteil einer solchen steganografischen Datei liegt auf der Hand. Steganografische Dateien sind unverfänglich, nur Eingeweihte wissen, dass sich in der Datei ein Live Laufwerk verbirgt.

➡ WARNUNG: ***Ändern Sie niemals die Datei, die mit dem Live Laufwerk vermischt wurde und speichern die Änderungen ab. Dies würde Ihr Live Laufwerk zerstören, die Daten im Laufwerk wären verloren.***
Beispiel: Sie haben ein Live Laufwerk mit einem Bild vermischt. Sie laden das Laufwerk in ein Grafikprogramm und nehmen Änderungen vor

(geringste Änderungen genügen). Wenn Sie diese Änderungen jetzt speichern, sind die Laufwerksdaten verschwunden.

Was sind mobile Datensafes (mobile Live Laufwerke)?

Ein mobiler Datensafe ist Anwendung und Laufwerk in einem. Die Datei ist in der Lage, sich selbst (*korrektes Passwort vorausgesetzt*) als Laufwerk mit vollem Schreib-Lesezugriff zu laden. Sie sollten entweder die ArchiCrypt Live Mobile Engine installiert haben oder als Administrator eingeloggt sein!

Ein mobiler Datensafe ist daher ideal geeignet, um sensible Daten zu transportieren und an verschiedenen Rechnern mit den Daten zu arbeiten. Die Weitergabe der Laufwerke ist ebenfalls gestattet. Der Empfänger der Daten benötigt keine spezielle ArchiCrypt Live Lizenz! Er kann die Inhalte des Laufwerks nach belieben ändern und Ihnen das Ergebnis wieder zukommen lassen. Sicherer Datenaustausch und nur einer benötigt eine Lizenz!

ACHTUNG Mobile Datensafes dürfen höchstens 4 Gigabyte groß sein! Falls Sie ein Laufwerk > 4 Gigabyte als mobiles Laufwerk nutzen möchten, finden Sie mit ArchiCrypt Live Mobile die richtige Lösung! Die Begrenzung ist keine Begrenzung von ArchiCrypt Live, sondern eine des Betriebssystems. Das Windows System ist nicht in der Lage Anwendungen zu starten, die größer als 4 Gigabyte sind.

➔WICHTIG:

Mobile Datensafes setzen als Betriebssystem Windows XP, Windows Vista oder Windows 7/8 voraus. Um das Laufwerk direkt laden zu können müssen Sie als lokaler Administrator angemeldet sein. Sie können den mobilen Datensafe als lokaler Administrator jedoch mit dem Parameter /i von der Kommandozeile aus aufrufen und die Live Mobile Engine dauerhaft für alle Nutzer installieren. Anschließend kann jeder Nutzer die mobilen Live Laufwerke laden!

Die mobilen Live Laufwerke unterstützen verschiedene Parameter/Kommandozeilenschalter:

Parameter können Sie zum Beispiel von der Kommandozeile oder einer Batch-Datei aus übergeben. Selbstverständlich können Sie die Schalter auch in eine Autorun-Datei (*autorun.inf*) aufnehmen.
siehe ArchiCrypt Live Mobile

/ i
Sorgt bei Vorliegen eines Klebe-Laufwerks dafür, dass dem Administrator permanente Installation der Mobile Engine angeboten wird.

/ r
Laufwerk wird im Nur-Lese-Modus geöffnet.

/ f
Laufwerk wird als Lokales Laufwerk geladen.
Anm.: Fehlt der Schalter, wird das Laufwerk als Wechsellaufwerk geladen.

/ d
Übergeben Sie hier den Laufwerksbuchstabe, unter dem Ihr Live Laufwerk geladen werden soll. Die Angabe hat in der Form -d=LW
Beispiel: -d=Y

/ k
Hier können Sie einen Pfad zu einer Textdatei angeben, in der der Schlüssel für das Laufwerk zu finden ist. Angabe hat in der Form -k="Dateiname" zu erfolgen.
Beispiel: -k="C:\Live\Keys\MobileKey.txt"

Anm.: Die Textdatei ist nicht mit den Schlüsseldateien zu verwechseln. Es handelt sich vielmehr um reine Textdateien, die das Passwort für ein Laufwerk als Klartext enthalten.


TIPP: ***Wozu dieser Schalter? Angenommen Sie pendeln mit sensiblen Daten zwischen verschiedenen Rechnern. An den Rechnern selbst besteht für die Daten keine Gefahr, der Transport der sensiblen Daten hingegen ist kritisch. Da das Passwort nur auf den Rechnern, nicht jedoch zusammen mit dem Mobilen Laufwerk gespeichert ist, sind die Daten beim Transport nicht gefährdet. Beim Laden der Laufwerke an den Rechnern entfällt die lästige Passworteingabe. Achten Sie darauf, dass die Passwortdatei auf allen Rechnern unter dem selben Pfad mit identischem Namen abgelegt ist.***

siehe dazu auch ArchiCrypt Live Mobile

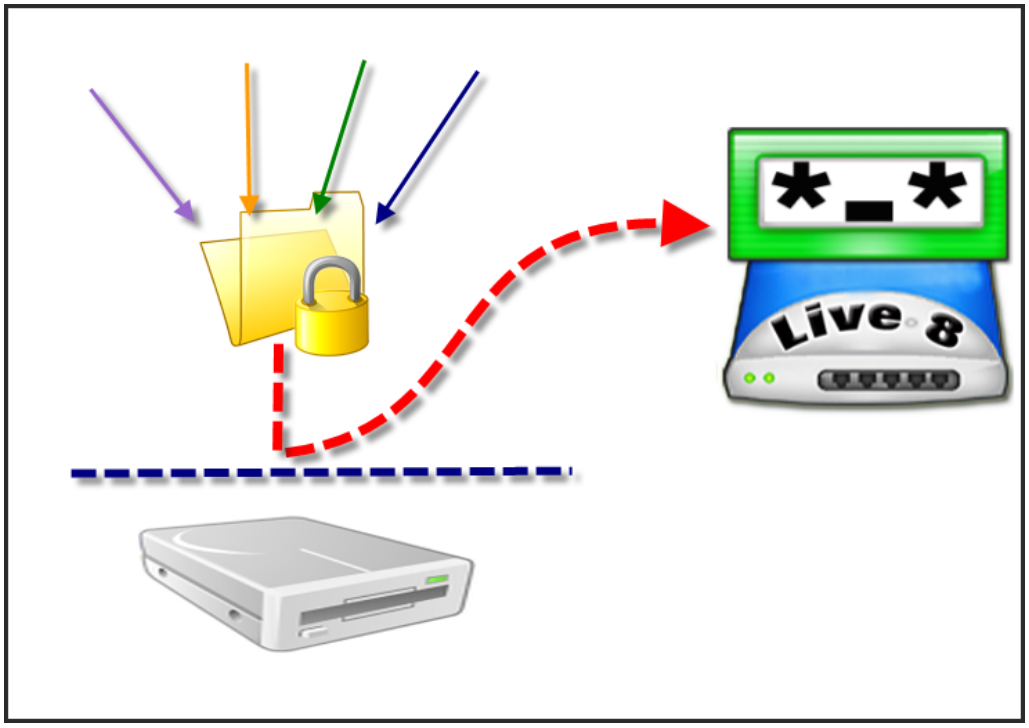
10.4.7 Umleitung

Sollten sich die nachfolgenden Videos im Browser nicht anzeigen lassen, so können Sie die Videos alternativ direkt in Youtube auf unserem ArchiCrypt Kanal ansehen.

Video - Umleitung nutzen

siehe auch: Einstellungen - Umleitung für ArchiCrypt Live Laufwerke

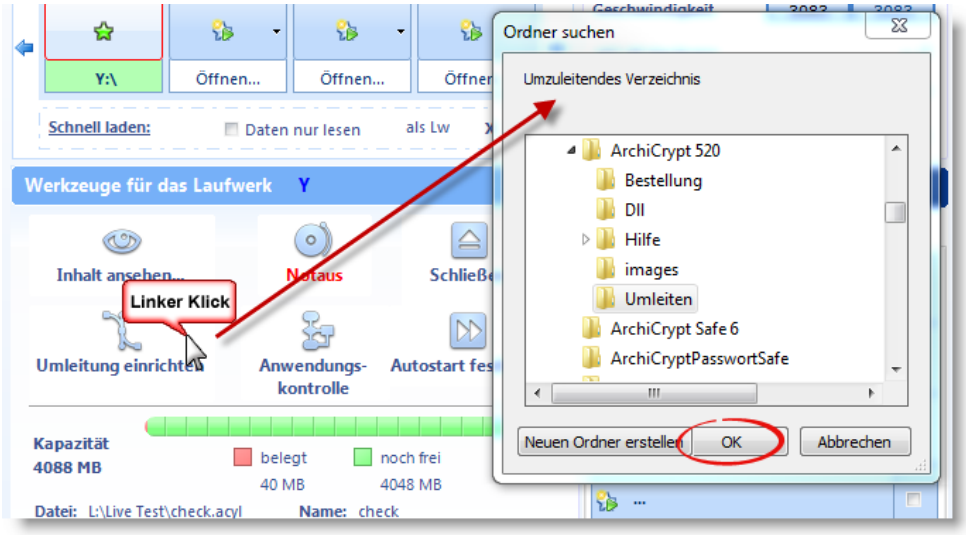
Mit Umleitungen können Sie Dateioperationen von einem Verzeichnis auf ein Live Laufwerk umleiten. Dabei muss das Verzeichnis, für welches Sie eine Umleitung einrichten möchten zu Beginn LEER sein.



Gelegentlich ist es nicht einfach bzw. teilweise sogar unmöglich, einer Anwendung beizubringen, Daten an einem bestimmten Speicherort abzulegen. Im besten Falle muss man sich durch zahlreiche Menüpunkte und Einstellungen quälen. Einfacher ist es, wenn die Anwendung gar nichts davon mitbekommt, dass die Daten nicht im Verzeichnis XY abgelegt sind, sondern auf einem verschlüsselten Live Laufwerk.

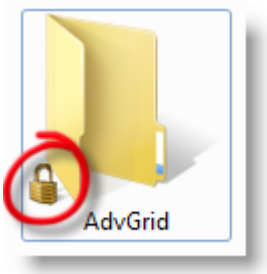
So richten Sie eine Umleitung ein

Laden Sie das Live Laufwerk und linksklicken Sie auf den Speicherplatz um ggf. die Werkzeuge für das Laufwerk anzuzeigen. Bei den Werkzeugen rufen Sie Umleitung einrichten auf.

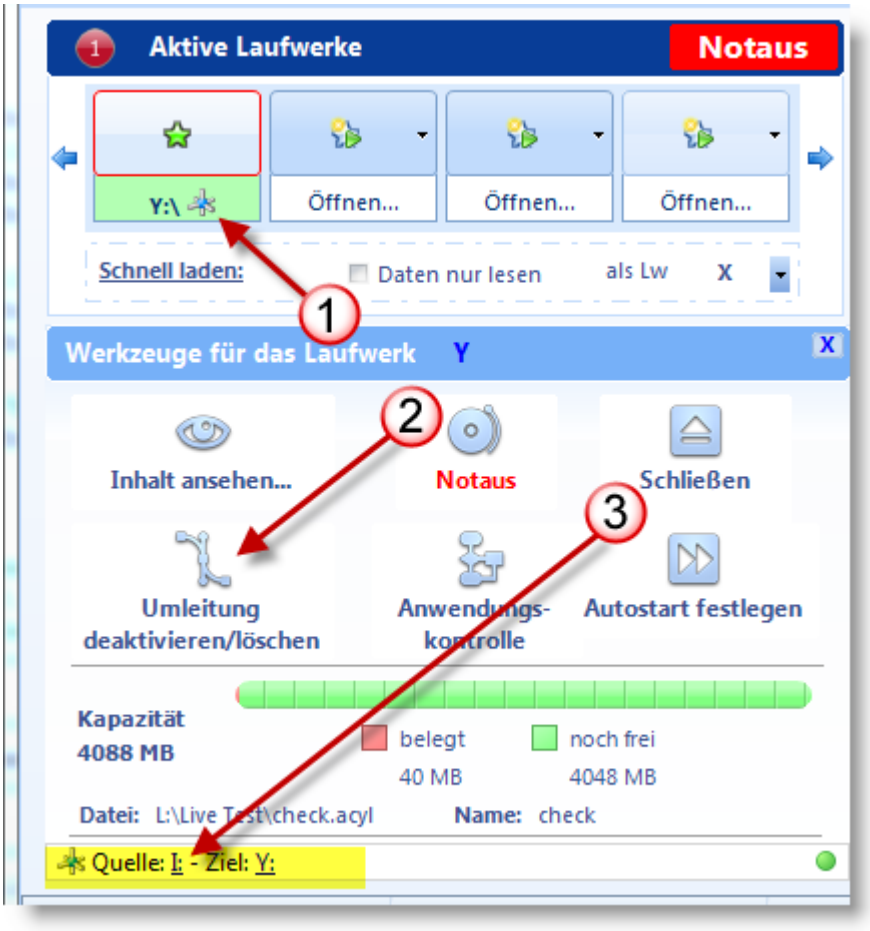


➡ WICHTIG: Das umzuleitende Verzeichnis muss beim Einrichten der Umleitung LEER sein. Wenn das zugehörige Live Laufwerk geschlossen ist, werden im umgeleiteten Verzeichnis keine Daten mehr angezeigt. Sie dürfen hier auch keine Daten mehr ablegen, sofern Sie die Umleitung später wieder aktivieren möchten.

Nachdem Sie das Verzeichnis ausgewählt haben, dessen Inhalte umgeleitet werden sollen, ändert sich das Symbol des Verzeichnisses (*nicht unter allen Betriebssystemen!*). Es wird ein kleines Schlosssymbol angezeigt.



In ArchiCrypt Live können Sie jetzt an mehreren Stellen sehen, dass eine Umleitung aktiv ist.



Bei aktiven Laufwerken wird ein Umleitungssymbol  auf dem zugehörigen Speicherplatz (1) angezeigt. Die Schaltfläche ändert die Beschriftung zu Umleitung deaktivieren/entfernen (2). In der Statusleiste (3) der Werkzeuge sehen Sie, welche Umleitung aktiv ist. Quelle ist dabei das Verzeichnis, welches umgeleitet wird, Ziel ist das Verzeichnis, in dem die Dateioperationen tatsächlich stattfinden. Die grüne LED in der Statusleiste rechts zeigt an, dass die Umleitung aktiv ist. Wenn Sie auf den Schriftzug für Quelle bzw. Ziel linksklicken, wird der Dateimanager geöffnet und der Inhalt angezeigt.

Wenn Sie jetzt damit beginnen, Dateien in das Quellverzeichnis zu kopieren, dort zu erstellen, zu löschen, etc., dann werden alle Änderungen auch im Quellverzeichnis (*im Beispiel oben I:\Project6\AdvGrid)* angezeigt. In Wahrheit aber finden alle Änderungen ausschließlich auf dem Live Laufwerk (*Ziel - im Beispiel oben L:\Project6\AdvGrid*)

statt. Wenn Sie das Live Laufwerk schließen oder die Umleitung deaktivieren, ist das Quellverzeichnis leer. Die Daten liegen im Zielverzeichnis.

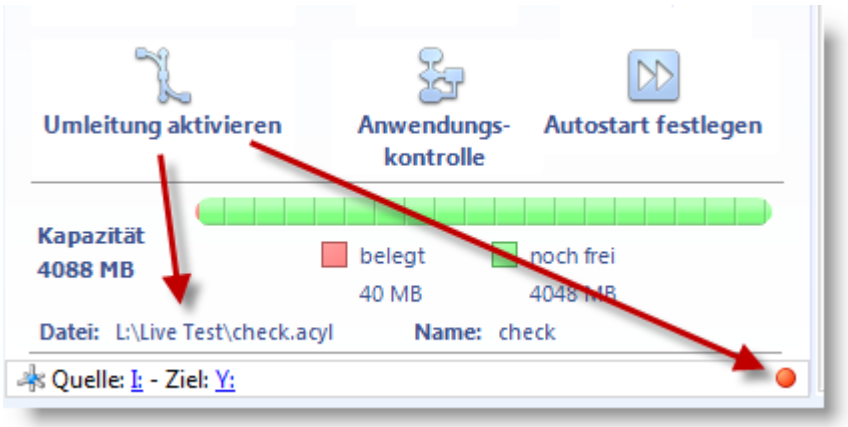
HINWEIS: Daten, die Sie direkt im Zielverzeichnis, also auf dem Live Laufwerk ändern, werden ebenfalls in das Quellverzeichnis gespiegelt.

Sofern Sie in den Einstellungen die Option Umleitung automatisch einrichten aktiviert haben, wird eine aktive Umleitung eingerichtet, sobald Sie das Laufwerk laden. Das Schließen eines Laufwerks löscht gleichzeitig die Umleitung.

So deaktivieren Sie eine Umleitung

Aktivieren Sie ggf. die Werkzeugansicht des Laufwerks indem Sie auf den zugehörigen Speicherplatz linksklicken.

Indem Sie mit der linken Maustaste auf die Schaltfläche klicken, deaktivieren Sie die Umleitung. Die Informationen über die Umleitung bleibt erhalten, ein erneuter Linksklick aktiviert die Umleitung wieder.



In der Statusleiste sehen Sie in diesem Fall, dass Informationen über eine Umleitung vorliegen, diese jedoch inaktiv ist (*rote LED*).

Möchten Sie die Umleitung deaktivieren und die Informationen darüber komplett löschen, weil Sie zum Beispiel eine neue Umleitung einrichten möchten, halten Sie die Strg-Taste (*gelegentlich CTRL*) gedrückt, während Sie mit links auf die Schaltfläche klicken.

➡ WARNUNG: Deaktivieren Sie eine Umleitung erst, wenn keine Daten mehr in das Verzeichnis geschrieben werden. Wenn Sie die

Umleitung deaktivieren, werden die Daten tatsächlich in das Verzeichnis (nicht mehr auf das Live Laufwerk) geschrieben. Ein erneutes Aktivieren der Umleitung ist nicht möglich, da eine Umleitung immer ein leeres Quellverzeichnis voraussetzt.

10.4.8 Anwendungskontrolle - Zugriff durch Programme

Sollten sich die nachfolgenden Videos im Browser nicht anzeigen lassen, so können Sie die Videos alternativ direkt in YouTube auf unserem ArchiCrypt Kanal ansehen.

Video - Anwendungskontrolle

Die Vollverschlüsselung eines Betriebssystems ist eine gute Sache, wenn es rein darum geht, den sorgfältig heruntergefahrenen Rechner zu schützen. Bei Verlust oder Diebstahl sind die Daten sicher. Ist das System gebootet, kann jede Anwendungen vollkommen ungehindert auf alle Daten zugreifen. Auch Unbefugte können dann Daten mit Schadprogrammen, Trojanern oder über ein Netzwerk abgreifen. Wird man im Ausland zur Herausgabe des Passwortes gezwungen, ist der ungeschützte Vollzugriff auf die Daten ebenfalls möglich.

Mit Live Laufwerken, die man dynamisch (*im laufenden Betrieb*) öffnen und schließen, mit unterschiedlichen Passwörtern versehen und auf anderen Datenträgern ablegen kann, ist man hier bereits flexibler. Verwendet man dann noch ein Geheimfach, ist man nahezu für jeden Fall abgesichert.

Insbesondere bei hochbrisanten Daten kann es jedoch sein, dass man selbst Anwendungen auf dem eigenen Rechner misstraut. Denken Sie nur an die unzähligen Bild- und Videoprogramme, die

automatisch beim Anschließen von Laufwerken, Einlegen von Speicherkarten etc. den Datenträger scannen, Bilder katalogisieren, kopieren und im ungünstigsten Fall sogar ungeschützt in die Cloud laden. Auch Office Programme bieten ähnliche Funktionen. Was im Alltag durchaus arbeitserleichternd sein kann, ist bei sensiblen Daten absolut unerwünscht.
Fragwürdig sind oft auch Programme, die pseudo nützliche Funktionen im Zusammenhang mit dem Internet bieten. Neben den eigentlichen Browsern gibt es hier s.g. Plug-Ins, die die Funktionalität der Browser vermeintlich erweitern, in Wahrheit den Browser jedoch nicht selten in eine Datenschleuder verwandeln.

ArchiCrypt Live bietetdie Möglichkeit, einzelne Live Laufwerke mittels Whitelisting zusätzlich abzusichern.

Was ist Whitelisting?

Es gibt zwei Arten von Programmen. Gute und böse Programme. Um welche Art von Programm es sich handelt, kann durchaus vom Kontext abhängen. Während Viren und Trojaner sicher grundsätzlich böser Natur sind, ist dies bei anderen Programmen, siehe Einleitung, von den äußeren Umständen abhängig.
Man kann jetzt Listen aufstellen, auf denen man entweder notiert, wer zu den Guten gehört, oder man listet alle bösen Programme auf. Am meisten Verbreitung hat das s.g. Blacklisting, bei dem man die Bösen auflistet und diesen den Zugriff auf bestimmte Dinge verwehrt. Hersteller von Betriebssystemen bieten diese Version bevorzugt an, weil Anwender damit am wenigsten Probleme haben. Allerdings ist dieses Verfahren recht unsicher, da Programmen erst dann der Zugriff auf bestimmte Informationen untersagt wird, wenn man sie explizit als böse einstuft.
Daraus kann man jetzt bereits ableiten, was Whitelisting ist. Hier werden die Guten aufgelistet. Nur wer als gut auf einer Liste steht, kommt an die speziell abgesicherten Daten.

Hier treten mehr Probleme auf der Anwenderseite auf. Man installiert ein neues Grafikprogramm und möchte damit auf die mit Whitelisting geschützten Daten zugreifen. Dies funktioniert jedoch erst dann, wenn man das Programm auf die Whitelist genommen hat.

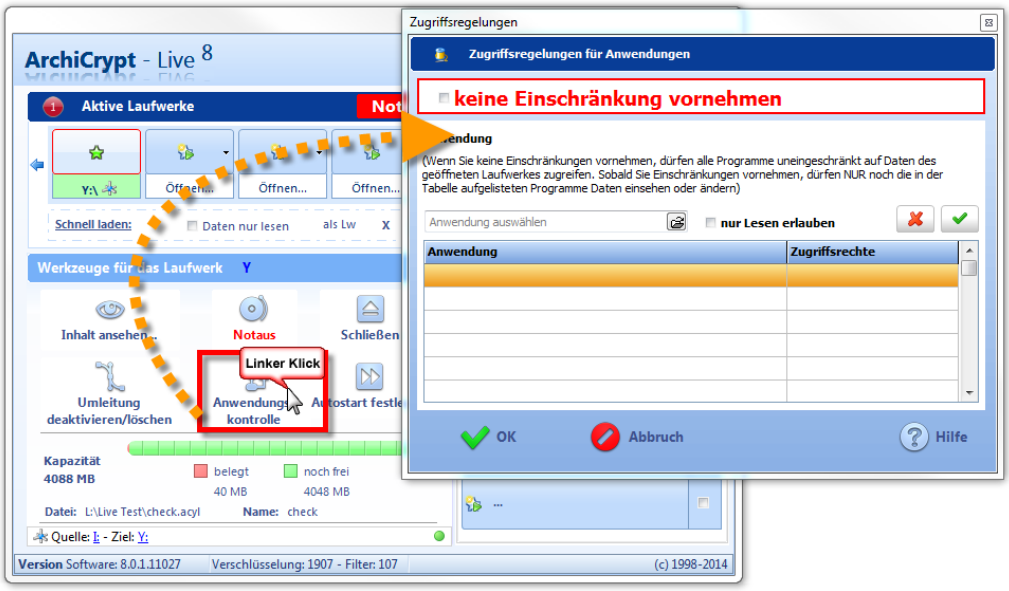
Für die Umsetzung in ArchiCrypt Live geht Sicherheit vor absoluter Bequemlichkeit. Die Natur der Daten auf einem Live Laufwerk ist zudem eher dazu geeignet, den Zugriff auf eine kleine Anzahl an Programmen zu beschränken, die ungehindert Zugriff auf die Daten haben sollen.

So beschränken Sie den Zugriff auf Live Laufwerke auf bestimmte Anwendungen

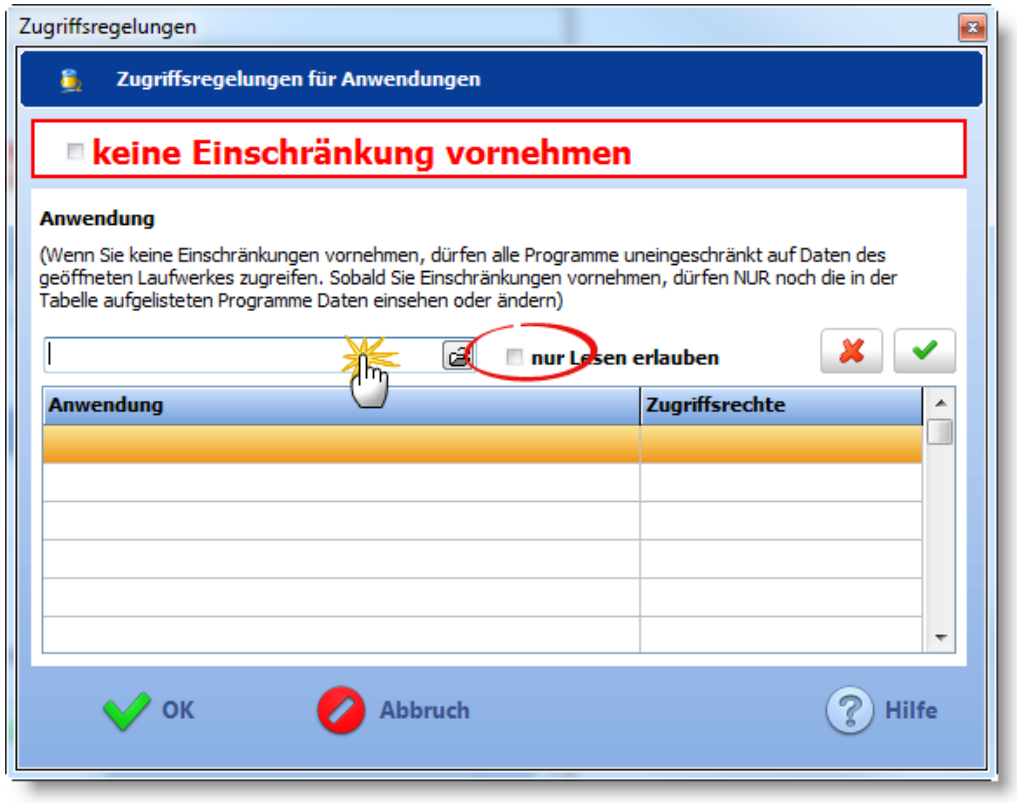
Rufen Sie ggf. die Werkzeuge für ein Live Laufwerk auf, indem Sie auf den zugehörigen Speicherplatz links-klicken. Klicken Sie jetzt mit der linken Maustaste auf die Schaltfläche Anwendungskontrolle.

In der Voreinstellung sehen Sie, dass es keine Einschränkungen gibt, also alle Anwendungen auf die Daten des geöffneten Laufwerks zugreifen dürfen.

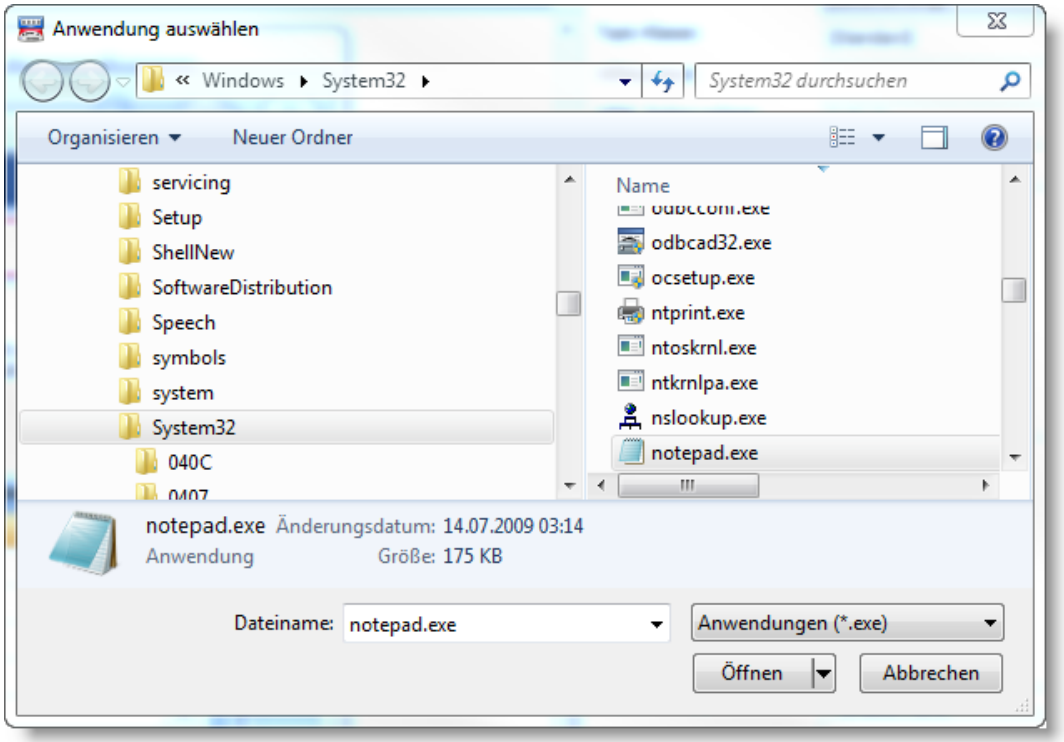
Entfernen Sie das Häkchen bei keine Einschränkungen vornehmen.



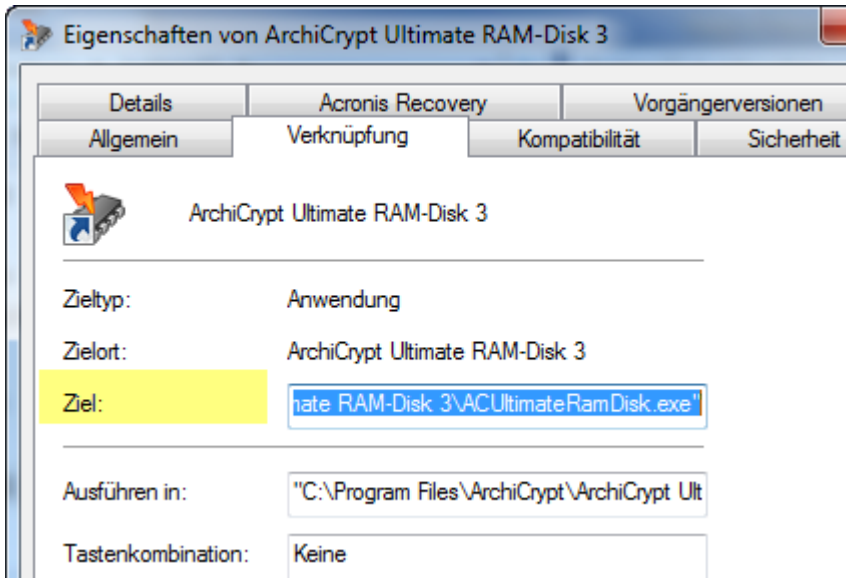
Klicken Sie auf das Ordnersymbol, um den Windows-Dialog zur Auswahl einer Anwendung aufzurufen.



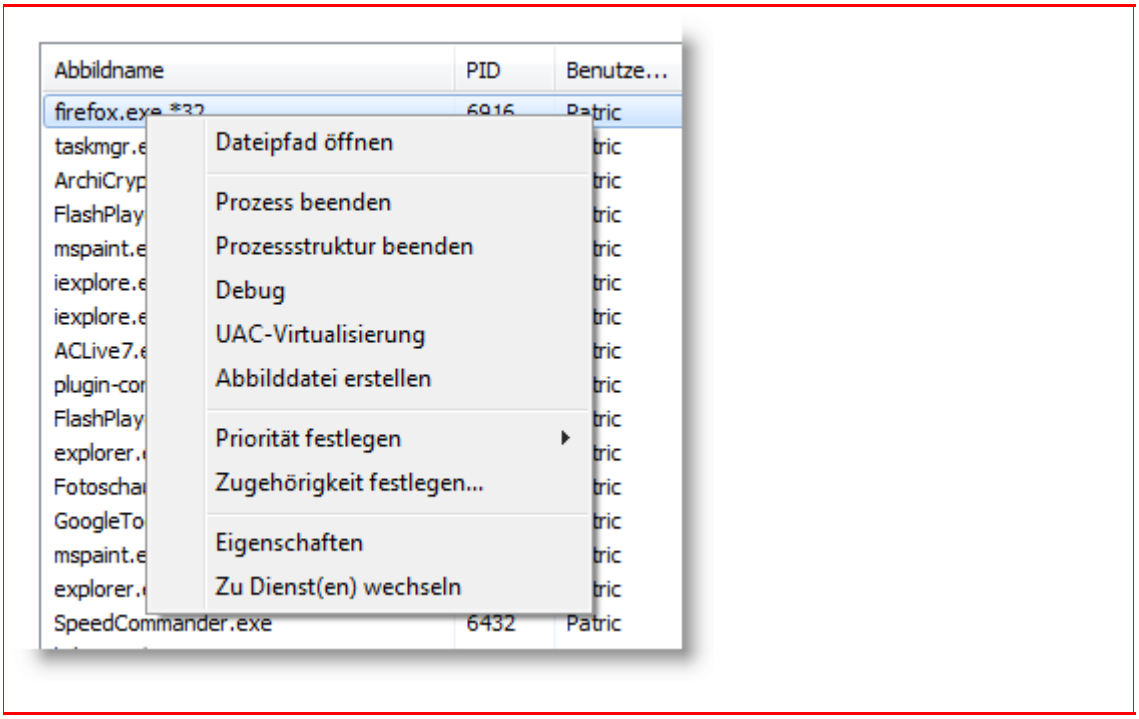
Navigieren Sie zur entsprechenden Anwendung und "öffnen" Sie diese.

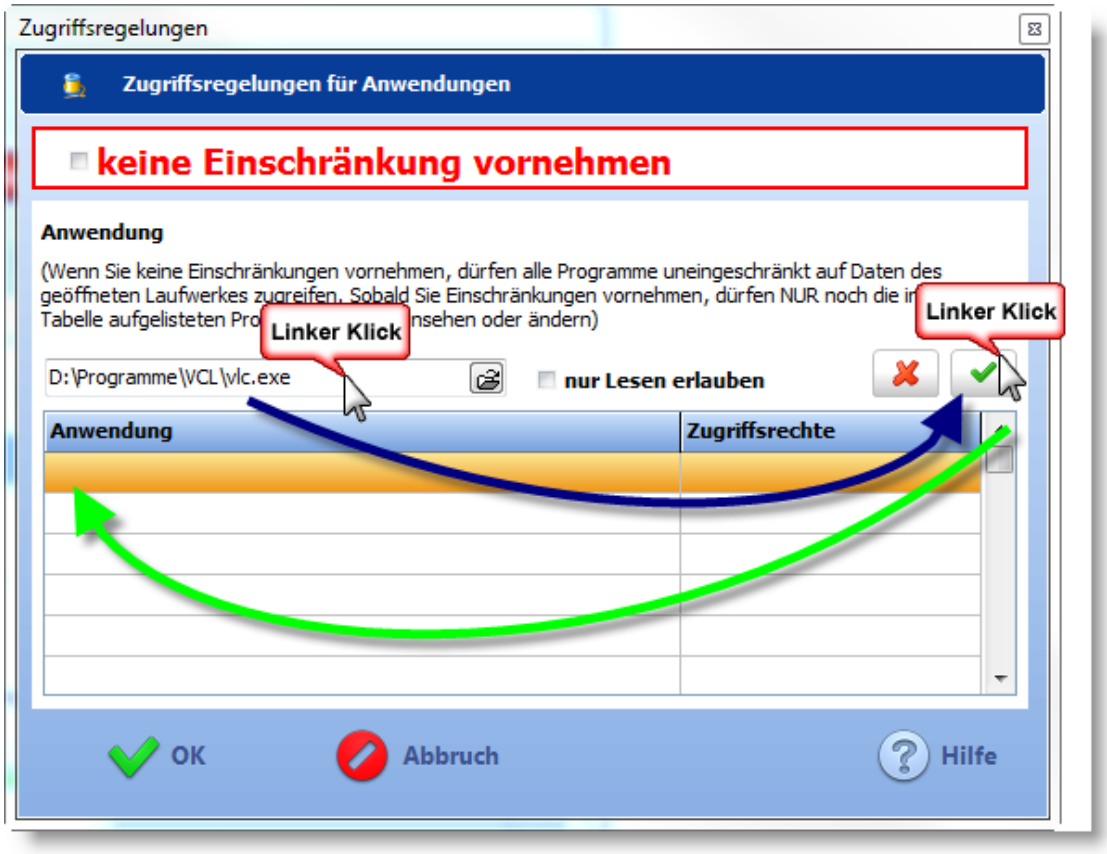


TIPP: Wenn Sie nicht wissen, wo eine bestimmte Anwendung gespeichert ist, können Sie meist das Symbol der Anwendung mit der rechten Maustaste anklicken und im Kontextmenü den Punkt Eigenschaften aufrufen. Auf der Registerseite Verknüpfung sehen Sie im Feld Ziel den Speicherort.



Wenn Sie den Taskmanager aufrufen (Strg+Alt+Entf) können Sie in auf der Registerseite Prozesse eine Prozess mit der rechten Maustaste anklicken und im Kontextmenü den Punkt Dateipfad öffnen auswählen.





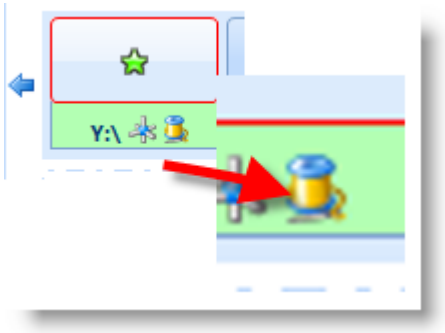
Um die Anwendung in die Liste zu übernehmen, links-klicken Sie auf das Häkchen.

Zum Löschen eines Eintrags aus der Liste, selektieren Sie diesen in der Tabelle und klicken auf das Kreuzsymbol. Der Eintrag wird aus der Liste entfernt. Wenn die Liste keinen Eintrag enthält, haben automatisch alle Anwendungen Zugriff (*entsprecht aktivierter Option* keine Einschränkung vornehmen)

Wenn Sie alle gewünschten Anwendungen in die Liste übertragen haben, bestätigen Sie dies durch Klick auf die OK Schaltfläche.

➡HINWEIS: Sie können pro Laufwerk maximal 8 Anwendungen festlegen. Vorsicht bei komplexen Programmen. Hier ruft oft ein Hauptpogramm zahlreiche Untermodule auf. Diese müssen zwingend ebenfalls die Zugriffserlaubnis besitzen. Festzustellen, welche Programme dies sind, ist oft nicht trivial. Man benötigt ggf. Spezialprogramme. Oft hilft es jedoch bereits, im Verzeichnis der Anwendung die dort aufgeführten weiteren Programme aufzunehmen.

Ist die Anwendungskontrolle für ein Laufwerk aktiv, können Sie dies am Kontrollsymbol im Speicherplatz des Laufwerks erkennen.



Anwendungskontrolle temporär deaktivieren

Die Anwendungskontrolle können Sie deaktivieren, indem Sie den Dialog durch Klick auf Anwendungskontrolle aufrufen und das Häkchen bei keine Einschränkung vornehmen setzen. Die Liste mit festgelegten Anwendungen bleibt erhalten.

Wichtiger Hinweis: Die Anwendungskontrolle ersetzt in keiner Weise ein Antiviren-Programm. Die Funktion versteht sich als Schutz vor regulären Programmen, die im Zusammenhang mit sensiblen Daten jedoch ungeeignete Funktionen wie Indexierung, Katalogisierung, Kopieren, etc. ausführen.

Anwendungskontrolle beim Öffnen eines Laufwerks automatisch aktivieren
Oft ist es sinnvoll, die Anwendungskontrolle beim Laden des Live Laufwerks zu aktivieren. In den Einstellungen finden Sie dazu die Option Anwendungskontrolle automatisch einrichten.

10.4.9 Tipps zum Umgang mit der ArchiCrypt Card

Auch Smartcards können zerstört werden oder verloren gehen. Solche Vorkommnisse sind selten, aber überaus dramatisch in ihren Folgen. Ohne Schlüssel ist MIT KEINEM Mittel ein Zugriff auf die Daten in einem Live Laufwerk möglich. Arbeiten Sie daher stets mit der Kopie eines Schlüssels. Planen Sie beim Einsatz von Smartcards für jeden Nutzer 2-3 Karten ein. Wenn Sie PIN oder Master PIN einsetzen, dann merken Sie sich diese Daten.

Master PIN

Beim Einsatz einer ArchiCrypt Card können Sie diese mit einer PIN zusätzlich absichern. Wird die PIN 4 Mal falsch eingegeben, wird die Karte gesperrt. Die Sperre (*PIN Fehler zurücksetzen*) kann im Personalisieren Dialog zurückgesetzt werden. Wenn Sie die Karte zusätzlich mit einer Master PIN abgesichert haben, dann ist für bestimmte Operationen die Master PIN einzugeben.

Wird die Master PIN 3 Mal falsch eingegeben, wird die komplette ArchiCrypt Card unbrauchbar. Es kann also auch kein PIN Fehler zurückgesetzt werden, wodurch Sie in der Folge eventuell keinen Zugriff mehr auf Laufwerksinhalte haben, sofern Sie keine Maßnahmen im Vorfeld ergriffen haben.!

Also PIN und MASTER PIN MERKEN

Sie können im Vorfeld folgende Maßnahmen ergreifen:

1. Fertigen Sie nach dem Erzeugen des Schlüssels auf der ArchiCrypt Card einen Klon an. Diesen Klon können Sie bei Verlust oder dann, wenn Sie PIN/Master PIN vergessen haben, nochmals verwenden. Verwahren Sie diese Karte an einem sicheren Ort.

2. Sie können die Laufwerke zunächst mit einem klassischen (*sehr langen Passwort absichern*). Dieses Passwort notieren Sie und verwahren es an einem sicheren Ort. Anschließend fertigen Sie eine

Schlüsselsicherung durch Verwaltung - Key-Sicherung. Jetzt ändern Sie den Zugang auf SmartCard. Geht die SmartCard verloren oder Sie vergessen die PIN/Master PIN, können Sie die Schlüsselsicherung zurückspielen und mit dem Passwort auf das Laufwerk zugreifen. Achten Sie darauf, dass Sie dies für ein normales Live Laufwerk ebenso durchführen müssen, wie für das Geheimfach.

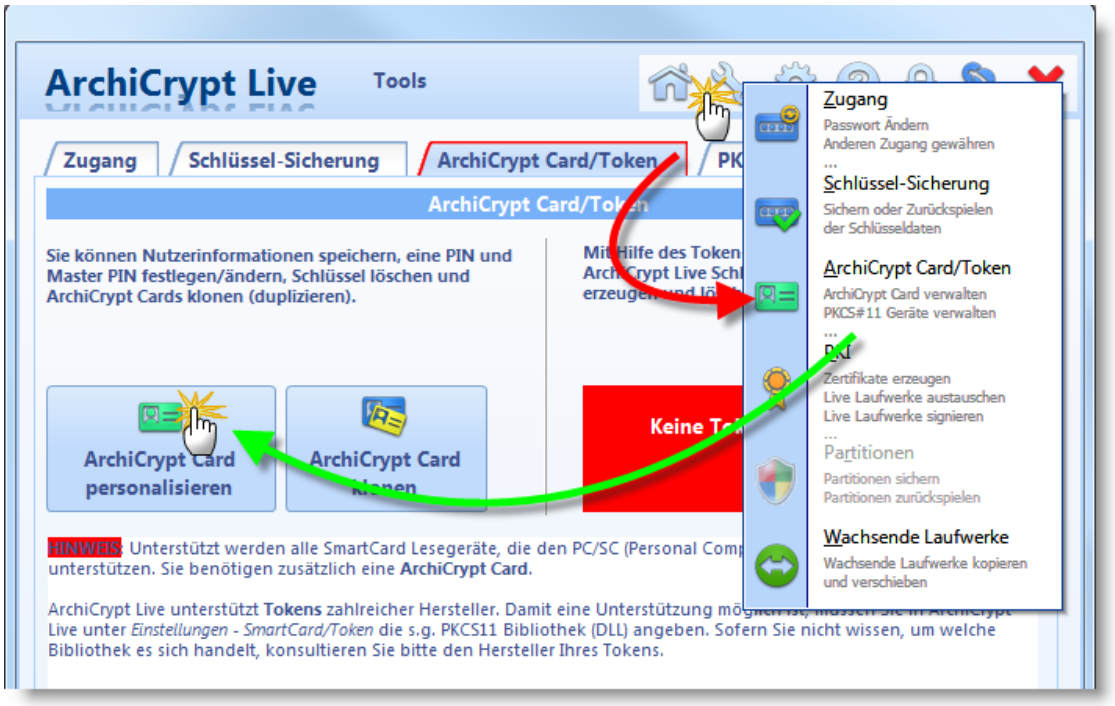
Richten Sie nach dem Erstellen einen Gastzugang ein

Sie können für ein Laufwerk direkt nach dem Erstellen einen Gastzugang einrichten, den Sie alternativ zum Beispiel mit einem "normalen" Passwort absichern. So haben Sie selbst dann noch Zugriff zu Ihrem Laufwerk, wenn Schlüsseldatei, Smartcard oder Token zerstört sind. Das funktioniert nicht für das Geheimfach, da es hier nur einen Zugang gibt! Hier müssen Sie eine Schlüsselsicherung mit normalem Passwort wie oben beschrieben ausführen.
siehe: Verwaltung - Zugang

Wie richte ich ArchiCrypt Live ein, damit die ArchiCrypt Card genutzt wird?

Starten Sie ArchiCrypt Live und wählen Sie unter Einstellungen SmartCard/Token den SmartCard Reader aus, mit dem ArchiCrypt zusammenarbeiten soll.
(siehe Einstellungen - SmartCard Reader wählen) Nach der Auswahl muss ArchiCrypt Live neu gestartet werden (siehe Installationshinweise)

Wechseln Sie jetzt zu den Werkzeugen -ArchiCrypt Card/Token und betätigen Sie die Schaltfläche ArchiCrypt Card personalisieren.



ArchiCrypt Live sollte Ihren Kartenleser erkannt haben und Sie auffordern, die ArchiCrypt Card einzulegen (Bitte Karte einlegen...). Wenn Sie die Karte einlegen und ArchiCrypt Live die Karte erkennt, erscheint die Meldung Karte verfügbar. Sofern Sie wünschen, können Sie persönliche Daten eingeben und speichern.

ArchiCrypt Live ist jetzt so eingerichtet, dass er die ArchiCrypt Card erkennt.

Wie erstelle ich einen Schlüssel auf der ArchiCrypt Card?

Sobald Sie einen Schlüssel benötigen, generiert die ArchiCrypt Card mit Hilfe des eingebauten Hardware Zufallszahlengenerators automatisch einen hochsicheren Schlüssel. Dieser Schlüssel wird bei einer neuen ArchiCrypt Card generiert, sobald Sie damit ein neues Laufwerk erstellen oder den Zugangsschutz eines Laufwerks ändern. Sie bekommen von diesem Vorgang nichts mit.

Wie kann ich die Vorteile der ArchiCrypt Card voll nutzen?

- Erstellen Sie neue Laufwerke mit dem Schutz ArchiCrypt Card

- Ändern Sie den Zugangsschutz bestehender Laufwerke hin zu ArchiCrypt Card (siehe Passwörter und Schlüssel ändern und anlegen)
- Schalten Sie in den Einstellungen SmartCard / Token die Option Schlüssel zuerst auf ArchiCrypt Card suchen? ein
- Richten Sie sich Favoriten ein und schalten Sie die Optionen Entfernen der ArchiCrypt Card schließt Laufwerk und Einlegen einer ArchiCrypt Card öffnet Laufwerk ein.

Sie haben dadurch die folgenden Vorteile:

- Beim Einlegen einer ArchiCrypt Card werden alle Laufwerke die als Favorit eingerichtet sind und bei denen die entsprechende Option aktiviert ist, automatisch geöffnet. Entfernen Sie die ArchiCrypt Card aus dem Leser, wird versucht, die Laufwerke zu schließen.
- Beim Öffnen von Laufwerken wird zunächst nach einer ArchiCrypt Card gesucht. Befindet sich eine ArchiCrypt Card im Leser, wird der Schlüssel automatisch genutzt um das Laufwerk zu öffnen.

Muss ich die Nutzerinformationen auf der ArchiCrypt Card speichern?

Die ArchiCrypt Card benötigt diese Informationen nicht. Zusammen mit der Master PIN können Sie jedoch diese Daten auf der ArchiCrypt Card speichern und vor Veränderung schützen. Dadurch ist es einem Fremden ohne Wissen der Master PIN nicht möglich, diese Nutzerdaten zu ändern.

Wozu dienen die Nutzerdaten?

Nutzerdaten sind nützlich, um eine ArchiCrypt Card einer bestimmten Person zuzuordnen. Die Nutzerdaten können mit einer Master PIN gegen Änderung geschützt werden. Interessant sind die Nutzerdaten besonders für Firmen, die Informationen zum jeweiligen Nutzer auf der Karte abspeichern möchten.

Wozu dient die Master PIN?

Die Master PIN kann dazu genutzt werden, die Nutzerdaten gegen Veränderung zu schützen. Gleichzeitig kann mit der Master PIN der Schlüssel auf der ArchiCrypt Card gegen löschen geschützt werden. Ist die Master PIN gesetzt und sind die Nutzerdaten mit der Master PIN geschützt, kann man nur nach Eingabe der Master PIN Nutzerdaten ändern und den Schlüssel auf der ArchiCrypt Card löschen. Für die "normale" Nutzung der Karte ist die Master PIN ohne Belang! Die Master PIN arbeitet unabhängig von der PIN. Ein Administrator kann daher Nutzerdaten ändern/erstellen und Nutzerinformationen und Schlüssel gegen Änderung schützen, ohne die PIN zu kennen. Umgekehrt kann jeder Nutzer ohne Kenntnis der Master PIN die ArchiCrypt Card nutzen.

Die Master PIN ist ebenfalls nötig, um einen Zähler in der ArchiCrypt Card zurückzusetzen, der die fehlerhafte Angabe der PIN protokolliert.

Wozu dient die PIN?

Eine PIN (Persönliche IdentifikationsNummer) ist nicht vergleichbar mit der PIN Ihrer Kreditkarte oder Ihrem Handy. Im Sinne von ArchiCrypt handelt es sich bei der PIN um einen bis zu 800 Bit langen Schlüssel, der benötigt wird um Funktionen aufzurufen, die mit dem auf der Karte gespeicherten Schlüssel arbeiten. Die PIN schützt also den auf der Karte abgelegten Schlüssel.

Muss ich die PIN nutzen?

Generell ist die PIN für den Betrieb der ArchiCrypt Card nicht notwendig.
Wenn Sie die PIN nicht nutzen, genügt der Besitz der ArchiCrypt Card um an die sensiblen Daten zu gelangen. Der Schutz basiert also auf dem Besitz einer bestimmten Sache, ähnlich wie der Besitz Ihres Autoschlüssels den Zugang zu Ihrem Fahrzeug regelt. Ein normales Passwort arbeitet nach dem Prinzip Wissen. Wer das Passwort weiß, kommt an die sensiblen Daten. Eine mit PIN geschützte ArchiCrypt Card kombiniert beide Prinzipien. Man muss die ArchiCrypt Card besitzen und das Passwort (PIN) wissen. Es hängt nun konkret von der Bedrohung für Ihre sensiblen Daten ab. Möchten Sie zum Beispiel verhindern, dass auf Ihre sensiblen Daten zugegriffen werden kann, so lange Sie im Internet sind, ist die ArchiCrypt Card ohne PIN die erste Wahl. Wenn Sie jedoch Angst haben müssen, dass die ArchiCrypt Card in die Hände einer unautorisierten Person gelangen könnte, müssen Sie zwingend eine PIN nutzen oder mit Argusaugen über die ArchiCrypt Card wachen.

Welche Nachteile habe ich durch den Einsatz einer PIN?

Der Einsatz einer PIN erhöht die Sicherheit der ArchiCrypt Card erheblich. Nur in besonderen Ausnahmen sollten Sie auf die PIN verzichten.
Der einzige Nachteil besteht darin, dass Sie die PIN 1 Mal bei jedem Einführen der ArchiCrypt Card in den Kartenleser eingeben müssen. Sie können die ArchiCrypt Card bequem so lange im Kartenlesen belassen, wie Sie mit ArchiCrypt Live arbeiten um nicht bei jedem Öffnen eines Laufwerks die PIN erneut eingeben zu müssen.

Was geschieht, wenn die PIN mehrfach falsch eingegeben wird?

Die ArchiCrypt Card besitzt einen internen Zähler, der bei jeder Falscheingabe erhöht wird. Wird die PIN 5 Mal falsch eingegeben, gibt die ArchiCrypt Card bei jedem Aufruf einer geschützten Funktion einen Fehler zurück. Dieser Zähler kann nur mit Hilfe der

Funktion PIN -Fehler zurücksetzen auf Null gestellt werden. Um diese Funktion aufzurufen, ist eine ggf. vorhandene Master PIN nötig.

Durch diese Maßnahme ist sichergestellt, dass die PIN nicht geknackt werden kann. Ein programmgesteuerter Test möglicher PINs ist nicht durchführbar. Bitte beachten Sie auch, dass die PIN nicht nur aus einem 10000 Schlüssel umfassenden Bereich stammen kann (Zahlen 0000 - 9999), sonder aus dem unvorstellbar riesigen Schlüsselraum von 2 ^ 800 Schlüsseln = 6,668014432879854274079851790721 3e+240. Zum Vergleich: Unsere Erde besteht aus etwa 6e+49 Atomen, das Universum besteht aus ca. 1e+78 Atomen. Die Anzahl möglicher Schlüssel ist also um gigantische Ausmaße größer als die Anzahl aller Atome im Universum.

Wie entsperre ich die Karte, wenn die PIN mehrfach falsch eingegeben wurde?

Rufen Sie den Dialog zum Personalisieren der ArchiCrypt Card auf. Geben Sie, sofern nötig, die Master PIN ein. Wechseln Sie zu den Masterfunktionen und rufen Sie die Funkion PIN-Fehler zurücksetzen auf.

Was tun, wenn ich meine ArchiCrypt Card verloren habe?

Sie müssen auf jeden Fall vorsorgen um zu vermeiden, dass Sie im Falle eines Verlusts oder der mechanischen Zerstörung der ArchiCrypt Card nicht mehr an Ihre Laufwerksinhalte kommen.

Der einfachste Weg besteht darin, dass Sie sich eine 2te ArchiCrypt Card besorgen und Ihre Hauptkarte mit der Funktion ArchiCrypt Card klonen, duplizieren. Der günstigere Weg besteht darin, sich einen Gastzugang für sein Laufwerk zu erstellen, den man mit einfachem Passwort oder mit einer Schlüsseldatei absichert.

Was tun, wenn die ArchiCrypt Card defekt ist?

Die ArchiCrypt Card ist ähnlich wie Ihre EC Karte sehr robust und verträgt einiges. Wenn es trotz dieser Robustheit zur Beschädigung der Karte kommt, müssen Sie bereits vorgesorgt haben. Siehe dazu auch Was tun, wenn ich meine ArchiCrypt Card verloren habe?

Wie kann ich mein Geheimfach mit der ArchiCrypt Card absichern?

Um die ArchiCrypt Card zum Öffnen des Geheimfachs zu nutzen, müssen Sie beim Erstellen des Laufwerks die Schutzmethode Passwort oder Schlüsseldatei auswählen. Erst beim Erstellen des Geheimfachs dürfen Sie die ArchiCrypt Card nutzen!

Ich bin Administrator und soll mehreren Personen Zugang zu bestimmten Laufwerken verschaffen

Erstellen Sie mit Hilfe einer neuen ArchiCrypt Card zunächst ein Dummylaufwerk. Bei diesem Vorgang wird auf der Karte ein neuer Schlüssel erzeugt. Diese Karte können Sie jetzt mit Hilfe der Funktion ArchiCrypt Card klonen beliebig oft kopieren (*Schlüsselkopien*). Mit der Funktion ArchiCrypt Card personalisieren können Sie anschließend für jeden Nutzer individuelle Daten vergeben und ggf. eine Master PIN festlegen.

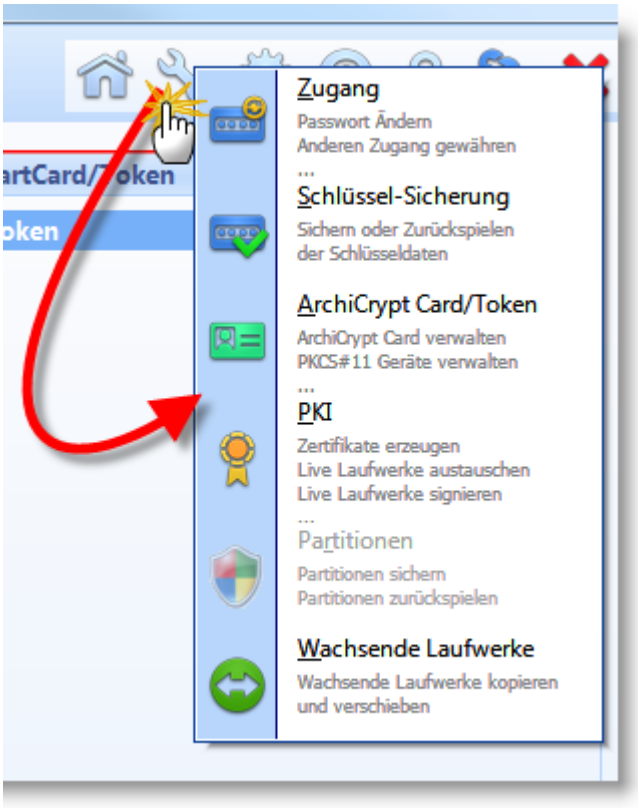
Wie kann ich verhindern, dass beim Einführen und Entfernen der ArchiCrypt Card Laufwerke geöffnet oder geschlossen werden?

Sie können dies verhindern, indem Sie die <Strg> - Taste gedrückt halten während Sie die Karte einführen oder entfernen.

10.4.10 Werkzeuge

Werkzeuge für Live Laufwerke

Hinter der Bezeichnung Werkzeuge verbergen sich zahlreiche Funktionen, die die Laufwerke betreffen.



siehe auch: Wichtige Begriffe - Begriffserläuterungen

- Zugang - Passwörter und Schlüssel ändern und anlegen

- Schlüssel Sicherung (Key Backup and Recovery)
- ArchiCrypt Card / Token
- PKI - Public-Key
- Partitionen - Sicherung und Wiederherstellung
- Wachsende Laufwerke

10.4.10.1 Zugang - Passwörter und Schlüssel ändern und anlegen

Sollten sich die nachfolgenden Videos im Browser nicht anzeigen lassen, so können Sie die Videos alternativ direkt in Youtube auf unserem ArchiCrypt Kanal ansehen.

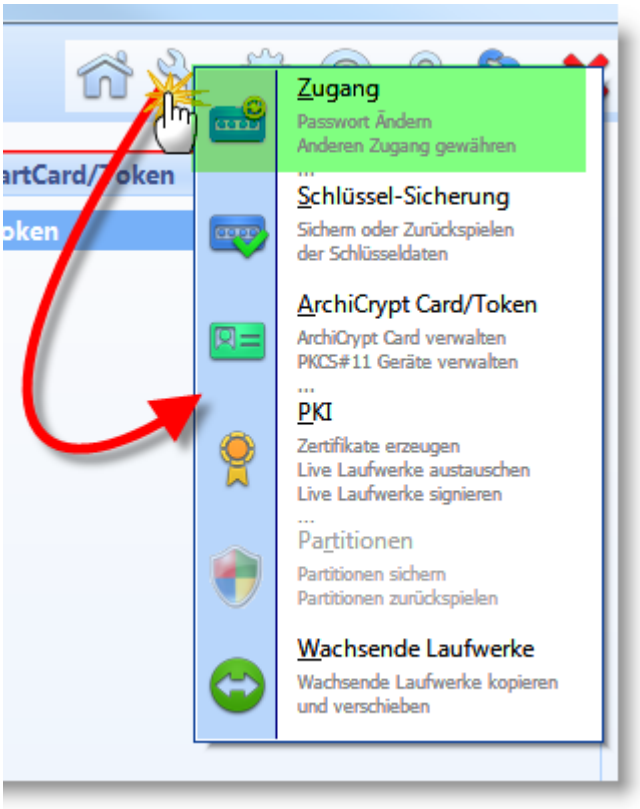
Video - Passwort zu

Video - Anderen Zugriff

siehe auch: Wichtige Begriffe - Begriffserläuterungen

So Ändern Sie den Zugang für ein Laufwerk

- Ändern eines bestehenden Zugangs
- Anlegen eines Gastzugangs



Mit dieser Funktion können Sie bestehende Zugänge oder Zugangsarten ändern oder anlegen.

Aufgabe: Ändern eines bestehenden Zugangs

Haben Sie den Zugang zum verschlüsselten Laufwerk aktuell mit einem Passwort abgesichert, können Sie dies hier so ändern, dass Sie künftig das Laufwerk zum Beispiel mit einer Schlüsseldatei öffnen können. Selbstverständlich können Sie auch ein bestehendes Passwort ändern.

Anm.: ***Man kann sich den Vorgang so verdeutlichen. Ein Live Laufwerk hat ein oder mehrere Schlösser. Beim Erstellen eines Laufwerks wir immer das s.g. Administratorschloss eingebaut. Sie legen dabei fest, wie dieses Administratorschloss (Laufwerk-Administrator-Schlüssel) zu öffnen ist. In jedes dieser Schlösser passt genau ein Schlüssel. Dieser Schlüssel kann als Passwort, als Schlüsseldatei, ArchiCrypt Card oder Security Token vorliegen. Ändern wir einen Zugang, tauschen wir quasi ein Schloss gegen ein anderes aus. Während das aktuelle Schloss sich zum Beispiel mit einem Passwort öffnen lässt, wird das neue Schloss mit einer Schlüsseldatei geöffnet.***

Gehen Sie entsprechend der Nummerierung in der Anwendung vor.

1. Wählen Sie zunächst das Live Laufwerk aus, für welches Sie das Schloss austauschen möchten.
2. Wählen Sie jetzt den Zugang (das Schloss) aus, welches Sie austauschen wollen.
3. Legen Sie fest, wie man das Schloss künftig öffnen soll
4. Geben Sie jetzt an, wie der Laufwerk-Administrator sein Administratorschloss öffnet.

Betätigen Sie jetzt die Schaltfläche "Schlüssel ändern/erstellen" und folgen Sie den Anweisungen.

 Hinweis: ***Sie benötigen zur Änderung jedes Schlüssels den aktuellen Schlüssel des Laufwerk-Administrators! Wenn Sie den Zugang zum Geheimfach ändern möchten, benötigen Sie neben dem Laufwerk-Administrator-Schlüssel zusätzlich den aktuellen Geheimfach Schlüssel.***

➡ACHTUNG: ***Das Vorbereiten für den Versand setzt keinen Laufwerk-Administrator-Schlüssel voraus, da diese Methode weder ein Passwort ändert, noch einen weiteren Zugang schafft. Das Vorbereiten für den Versand entspricht der sicheren Weitergabe eines bereits eingerichteten Passwortes!***

Aufgabe: Anlegen eines Gastzugangs

Mit einem Gastzugang schaffen Sie eine weitere Möglichkeit, auf die Inhalte eines Live Laufwerkes zuzugreifen. Sie können so anderen Personen, ohne IHR Passwort weiterzugeben, den Zugriff auf Inhalte ermöglichen oder sich zum Beispiel eine Art Notzugang für den Fall schaffen, dass Ihre ArchiCrypt Card oder ein Security-Token beschädigt wird oder verloren geht.

 Anm.: ***Man kann sich den Vorgang so verdeutlichen. Ein Live Laufwerk hat nach dem Erstellen genau ein Schloss, über welches man Zugang zu den Laufwerksinhalten erhält. Das beim Erstellen eingerichtete Schloss wird als Administratorschloss bezeichnet. Der zum Öffnen benötigte Schlüssel als Laufwerk-Administrator-Schlüssel. Beim Einrichten eines Gastzugangs wird ein neues Schloss eingebaut (Gastschloss), welches sich mit dem festgelegten Gastschlüssel öffnen lässt. Je nachdem, welche Art Gastschloss Sie eingebaut haben, kann der Gast nur eingeschränkt (zum Beispiel nur Daten lesend) auf die Daten in dem entsprechenden Laufwerk zugreifen.***

Gehen Sie entsprechend der Nummerierung vor.

1. Wählen Sie zunächst das Live Laufwerk aus, für welches Sie ein neues Gastschloss einbauen möchten.

2. Wählen Sie jetzt die Art des Gastschlosses aus. (Gast 1 nur Lesen, Gast 2 nur Lesen oder Gast 3 Lesen/Schreiben)
3. Legen Sie fest, wie man das neue Schloss öffnen soll
4. Geben Sie jetzt an, wie der Laufwerk-Administrator sein Administratorschloss öffnet.
Betätigen Sie jetzt die Schaltfläche "Schlüssel ändern/erstellen" und folgen Sie den Anweisungen.

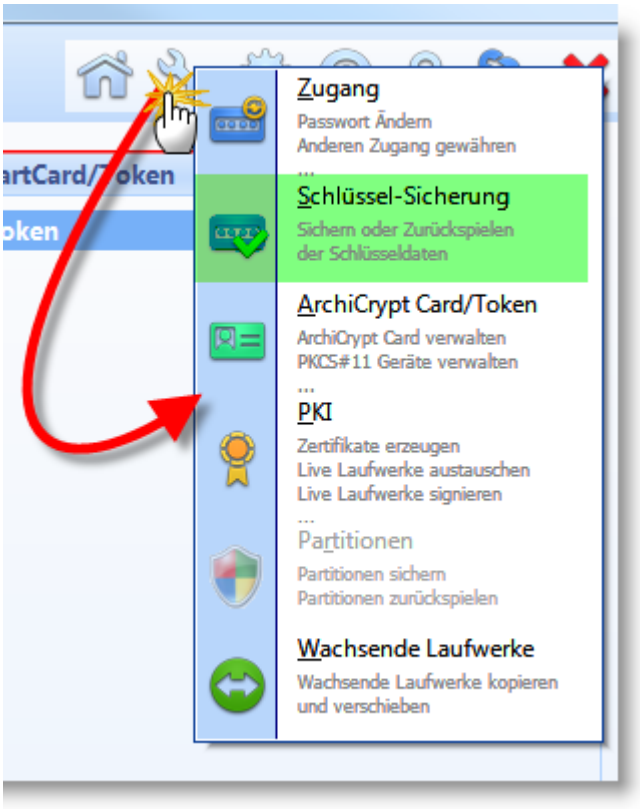
➡ACHTUNG***: Das ArchiCrypt Live Laufwerk für welches die Zugangsregelung geändert werden soll, darf nicht als Laufwerk geöffnet sein! Falls es sich um ein dataibasiertes Live Laufwerk handelt, darf die Datei nicht schreibgeschützt sein.***

Auch wenn Sie den Gast mit Lese-/Schreibrechten einrichten, hat dieser kein Recht, Laufwerksschlüssel zu ändern oder Gastzugänge zu erstellen. Hierzu wird immer der Laufwerk-Administrator-Schlüssel benötigt.
Unbedingt darauf achten, dass der neue Schlüssel nicht mit einem bereits bestehenden übereinstimmt!

10.4.10.2 Schlüssel-Sicherung

siehe auch: Wichtige Begriffe - Begriffserläuterungen
Datensicherung - Schlüssel-Backup und -Recovery

Sicherung und Wiederherstellung von Laufwerksschlüsseln



Warum sollten Sie eine Schlüsselsicherung durchführen?

Laufwerk defekt ...

Sie können sich so eine Art Rückversicherung für den schlimmen und in der Praxis äußerst seltenen Fall schaffen, dass der lebenswichtige Bereich Ihres Live Laufwerks beschädigt wird. Mit Hilfe der Schlüsselsicherung können Sie ggf. wieder auf die Inhalte Ihres Live Laufwerks zugreifen.

Mitarbeiter vergisst sein Passwort ...

Mit Hilfe einer Sicherung können Sie dafür sorgen, dass Live Laufwerke in Ihrem Unternehmen auch dann noch genutzt werden können, wenn ein Mitarbeiter die Firma inkl. dem aktuellen Schlüssel verlässt. Sie können Live Laufwerke zum Beispiel von einer zentralen Instanz erstellen lassen. Nach dem Erstellen wird die Schlüsselsicherung durchgeführt. Das Laufwerk wird jetzt an den/die entsprechenden Mitarbeiter weitergegeben. Diese können nach belieben Schlüssel ändern. Verlässt der Mitarbeiter die Firma inkl. Schlüssel, können Sie die Schlüsselsicherung zurück spielen und mit dem Schlüssel, der beim Erstellen verwendet wurde, auf die Laufwerksinhalte zugreifen.

Sicherung der Laufwerksschlüssel

Wählen Sie das Live Laufwerk aus und geben Sie einen Namen für die zu erstellende Schlüsselsicherung ein. Betätigen Sie anschließend die Schaltfläche Backup.

➡ WARNUNG: Bei der erstellten Schlüsselsicherung wird lediglich der Anteil Ihres Laufwerks gesichert, welcher Informationen über Schlüssel (nicht die Schlüssel selbst) enthält. Die eigentlichen Daten in Ihrem Laufwerk müssen mit einem normalen Backup-Programm gesichert werden.

Bitte beachten Sie, dass insbesondere der Zugang zum Geheimfach ungültig wird, sobald ein neues Geheimfach erstellt oder das Geheimfach durch unsachgemäßen Umgang (Schreiben in den Normalbereich) beschädigt wurde! In diesen Fällen nutzt ein Zurückspielen der Schlüsselsicherung nichts!

Wiederherstellen der Laufwerksschlüssel

Wählen Sie das Live Laufwerk und die zugehörige Sicherungsdatei. Betätigen Sie anschließend die Schaltfläche Restore.

➡ HINWEIS: ***Live Laufwerke,*** welche mit ArchiCrypt Live 4 oder höher erstellt wurden, enthalten eine eindeutige ID. Anhand dieser ID stellt die Restorefunktion fest, ob die Schlüsselsicherung zu der ausgewählten Trägerdatei passt. Es wird ebenfalls verhindert, dass Sie eine nicht kompatible Schlüsselsicherung nutzen.

Die ID schließt die Gefahr, ein Restore mit unpassender Schlüsseldatei auszuführen, nahezu aus. Bei Live Laufwerken älteren Typs besteht keine derartige Rückversicherung. Unabhängig vom Schutz durch eine ID sollten Sie die komplette Trägerdatei vor einem Restoreversuch sichern!

Bricht ArchiCrypt Live den Restorevorgang aufgrund eines ID- oder Versionsfehlers ab, können Sie, sofern Sie sich sicher sind, dass die Schlüsselsicherung zum ausgewählten Live Laufwerk gehört, die Option "Versions- und ID-Fehler ignorieren?" auswählen. Hier gilt ganz besonders der Hinweis auf Datensicherung vor der Restoreoperation!

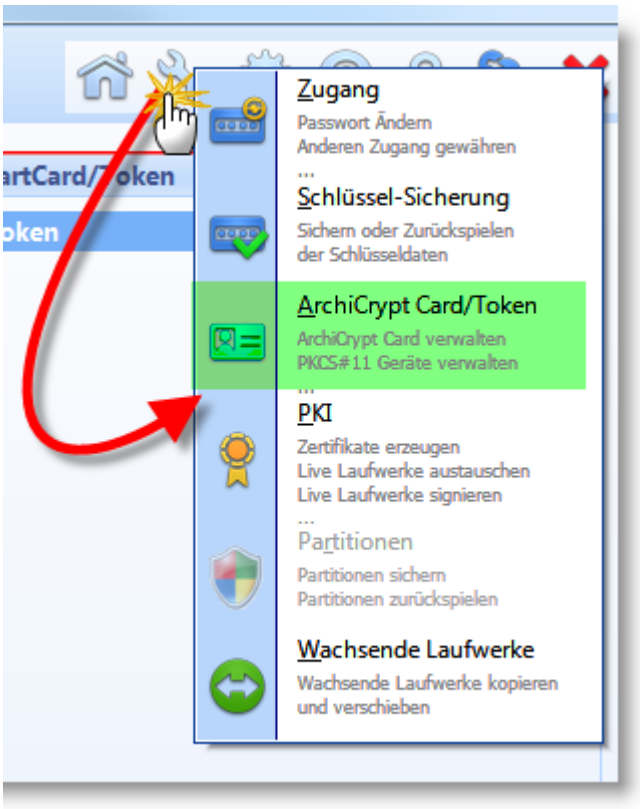
Siehe unbedingt Datensicherung

TIPP: ***Falls Sie mit einer Schlüsseldatei, einer ArchiCrypt Card oder einem Security Token arbeiten, können Sie sich einen Gastzugang anlegen, den Sie durch ein "normales" Passwort absichern. Falls Sie Ihre***

Schlüsseldatei, ArchiCrypt Card oder Token verlieren, haben Sie immer noch die Möglichkeit, an die Daten in Ihrem Laufwerk zu gelangen.

10.4.10.3 ArchiCrypt Card/Token

siehe auch: Wichtige Begriffe - Begriffserläuterungen
ArchiCrypt Card personalisieren
ArchiCrypt Card klonen
ArchiCrypt Token Manager



ArchiCrypt Card

Eine ArchiCrypt Card ist eine Smartcard, die besondere kryptografische Funktionen zur Verfügung stellt (siehe ArchiCrypt Card Info). Sie können die spezielle Smartcard als Schlüssel für ArchiCrypt Live Laufwerke nutzen. Insbesondere im Zusammenspiel mit den Favoriten ergeben sich enorme Vorteile gegenüber der Absicherung mit normalem Passwort. Grundsätzlich ist die ArchiCrypt Card dem konventionellen Passwort hinsichtlich der Sicherheit überlegen. Sie erhalten die ArchiCrypt Card in unserem Online Shop unter http://shop.ArchiCrypt.de

➡ ACHTUNG: Beachten Sie die Systemvoraussetzungen

Security Token

Bei einem Security Token handelt es sich um eine Hardware mit speziellen kryptografischen Funktionen. Der Token kann von ArchiCrypt Live genutzt werden, um darauf Schlüssel für ArchiCrypt Live Laufwerke abzulegen. Sie können ArchiCrypt Live Laufwerke also mit dem Token öffnen. Im Zusammenspiel mit den Favoriten erhöht sich der Komfort beim Umgang mit Live Laufwerken. Die Nutzbarkeit des Tokens setzt voraus, dass er den s.g. PKCS#11 Standard erfüllt.

➡ ACHTUNG: Beachten Sie die Systemvoraussetzungen

Klicken Sie auf ein Element der folgenden Grafik, um weitere Informationen zu erhalten.

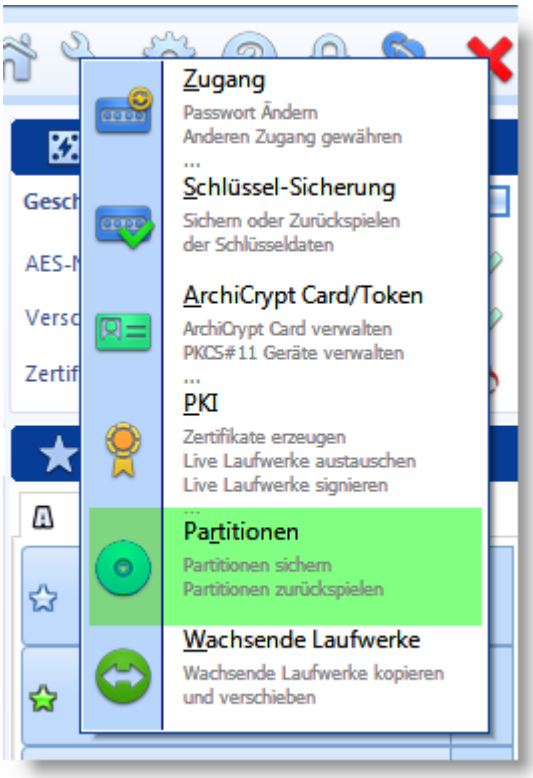
Siehe ArchiCrypt Card personalisieren
ArchiCrypt Card klonen
ArchiCrypt Token Manager

10.4.10.4 Partitionen Sicherung und Wiederherstellung

siehe auch: Wichtige Begriffe - Begriffserläuterungen
Datensicherung

Sicherung und Wiederherstellung von Partitionen

- Sichern
- Wiederherstellen



➔ Wichtig: ***Live Partitionen nutzen Ihre Hardware auf unterster Ebene. ArchiCrypt Live greift direkt auf das jeweilige Laufwerk zu. Sie haben es bei Live Partitionen nicht mit Dateien zu tun, sondern mit einem Teil eines Datenträgers. Partitionen sind mit einigen Backup-Programmen gut zu sichern. Prüfen Sie bitte, ob Ihr Backup-Programm in der Lage ist, Live Partitionen zu sichern. Falls dies der Fall ist, nutzen Sie Ihr Backup-Programm. Die Funktionen zur Sicherung von Partitionen in ArchiCrypt Live sind als*** Notlösung ***zu verstehen!***

Ebenso wie zum Erstellen einer Live Partition, benötigen Sie zur Sicherung und Wiederherstellung Administratorrechte! Partitionen müssen exklusiv geöffnet werden können. Das Medium auf welches die Sicherung gespeichert werden soll, muss ausreichend Speicherkapazität bieten. Falls Sie Partitionen sichern, die größer als 4 Gigabyte sind. Muss

dass Medium, auf welches die Sicherung gespeichert wird solche Dateigrößen unterstützen (NTFS empfohlen).

➔ ACHTUNG Windows Vista und höher: ***Windows startet Programme so, dass diese mit möglichst wenig Rechten laufen. Es spielt dabei keine Rolle, ob Sie selbst Administratorrechte besitzen! Um Partitionen zu bearbeiten, benötigt ArchiCrypt Live zwingend Administratorrechte. Es genügt also kein einfacher Start. Klicken Sie mit der rechten Maustaste auf die ArchiCrypt Live. Anwendung und wählen Sie "Als Administrator ausführen". Jetzt haben Sie Zugriff auf Funktionen, die Partitionen behandeln.***

In der Laufwerk-Fabrik finden Sie ein Schildsymbol. Durch Klick auf dieses Schild startet sich ArchiCrypt Live selbst mit höheren Rechten.

TIPP: ***1. Sie können auch "Nicht-Live-" Partitionen sichern und wiederherstellen. Erstellen Sie z.B. USB-Stick Images***
2.Gesicherte Live Partitionen können sofort als dateibasiertes Live Laufwerk (Trägerdatei) geladen und genutzt werden.

Sichern einer Partition

1. Wählen Sie die Partition aus, die gesichert werden soll.
2. Legen Sie fest, wo die Sicherung abgelegt werden soll.

Starten Sie dann die Abbilderstellung mit Partition als Datei sichern

siehe auch Partitionsauswahldialog

Wiederherstellen einer Partition

1. Wählen Sie die Partition aus, die wieder hergestellt werden soll.
2. Geben Sie an, wo sich die Sicherung befindet.

Starten Sie dann die Wiederherstellung mit Datei nach Partition schreiben

siehe auch Partitionsauswahldialog

➔ Warnung: ***Bei diesem Vorgang werden alle aktuellen Inhalte der ausgewählten Partition überschrieben. Auch falls der Vorgang abgebrochen wird ist die ursprüngliche Partition zerstört.***

10.4.10.5 PKI Public Key Funktion

Sollten sich die nachfolgenden Videos im Browser nicht anzeigen lassen, so können Sie die Videos alternativ direkt in Youtube auf unserem ArchiCrypt Kanal ansehen.

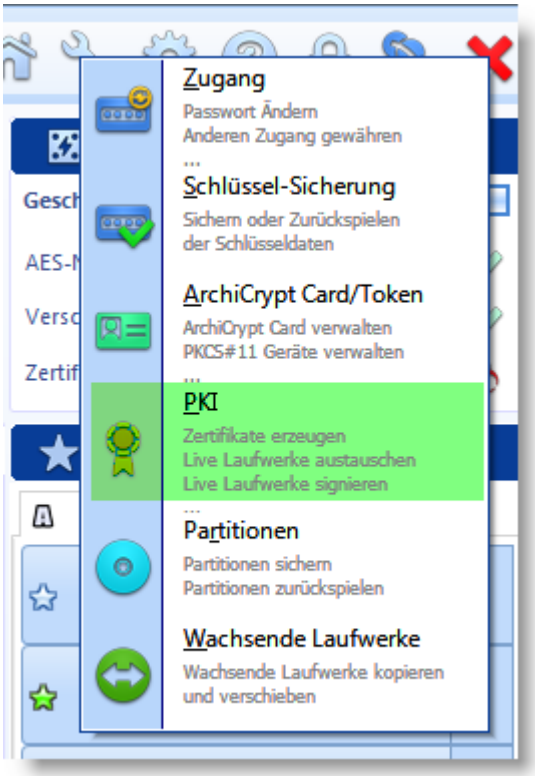
Video - X509 Zertifikat

siehe dazu: Was sind Zertifikate

Public-Key Funktionen

Eine wesentliche Rolle für die Funktionen der Kategorie Public-Key bilden

Zertifikat, Privater Schlüssel und Öffentlicher Schlüssel



Hinter dem Begriff Public-Key verbergen sich eine ganze Reihe von Funktionen, die folgende Zwecke erfüllen.

Sicherheit bei der Übermittlung
Weitergabe von Live Laufwerken ohne Übermittlung des Laufwerkspasswortes.

Authentizität
Sicherstellen, dass das Laufwerk von einem bestimmten Absender stammt.

Integrität
Sicherstellen, dass das Laufwerk auf dem Weg zum Empfänger nicht verändert wurde

- Überblick über die Nutzung von Zertifikaten in ArchiCrypt Live
- Erstellen eines Zertifikats
- Laufwerk signieren
- Signatur prüfen
- Versand mit Öffentlichem Schlüssel
- Empfang mit Privatem Schlüssel
- Zertifikat weitergeben
- Zertifikate laden
- Zertifikate von Zertifizierungsstelle nutzen

10.4.10.5.1 Zertifikate in ArchiCrypt Live

Sollten sich die nachfolgenden Videos im Browser nicht anzeigen lassen, so können Sie die Videos alternativ direkt in Youtube auf unserem ArchiCrypt Kanal ansehen.

Video - X509 Zertifikat

Zertifikate

Zertifikate ermöglichen es, nachzuweisen, dass ein bestimmter öffentlicher Schlüssel eines asymmetrischen Verschlüsselungsverfahrens zu der vorgeblichen Person oder Institution gehört.

ArchiCrypt Live nutzt das Zertifikat dazu, einen öffentlichen Schlüssel auf standardisierte Weise zu speichern. Sobald Sie eine Aktion durchführen, die ein Zertifikat erfordert, bietet Ihnen ArchiCrypt Live an, ein s.g. self-signed Zertifikat (*selbst signiertes*) zu erstellen.

Bei diesem Vorgang werden der Öffentliche Schlüssel und der Private Schlüssel (*Schlüsselpaar*) generiert und in einem Zertifikat im Windows-eigenen Systemzertifikatspeicher abgelegt. Da Sie das Zertifikat selbst signiert (*selbst unterzeichnet*) haben, ist für einen Empfänger dieser Nachricht nicht zu 100% sichergestellt, dass der Öffentliche Schlüssel tatsächlich zu Ihnen gehört. Wenn Sie der Person Ihren Öffentlichen Schlüssel jedoch so weitergegeben haben, dass dieser sicher sein kann, dass das Zertifikat zu Ihnen gehört, genügen selfsigned Zertifikate völlig!

Im geschäftlichen Umfeld macht es Sinn, auf Zertifikate zurückzugreifen, die von einer s.g. Zertifizierungsstelle ausgestellt wurden. Diese zumeist kostenpflichtigen Zertifikate verlangen, dass Sie sich als Zertifikatnutzer gegenüber der Zertifizierungsstelle ausweisen. Erst nachdem Sie authentifiziert sind, erhalten Sie Ihr Zertifikat. Der Umfang des Verfahrens wird maßgeblich durch die Art des Zertifikats bestimmt.

Dieses "Fremdzertifikat" können Sie in ArchiCrypt Live statt des selbst signierten nutzen. Damit geben Sie dem Nutzer Ihres Öffentlichen Schlüssels die Gewissheit, dass nur Sie in der Lage

sind, Daten zu entschlüsseln, die mit Ihrem öffentlichen Schlüssel verschlüsselt wurden und, dass Daten, die Sie mit Ihrem Privaten Schlüssel signiert haben, tatsächlich von Ihnen signiert (*unterzeichnet*) wurden.

(siehe Zertifikate von Zertifizierungsstelle nutzen)

10.4.10.5.2 Erstellen eines Zertifikats

Sollten sich die nachfolgenden Videos im Browser nicht anzeigen lassen, so können Sie die Videos alternativ direkt in Youtube auf unserem ArchiCrypt Kanal ansehen.

Video - X509 Zertifikat

siehe auch: Zertifikate in ArchiCrypt Live
Zertifikate von Zertifizierungsstelle nutzen

Ein eigenes Zertifikat erstellen

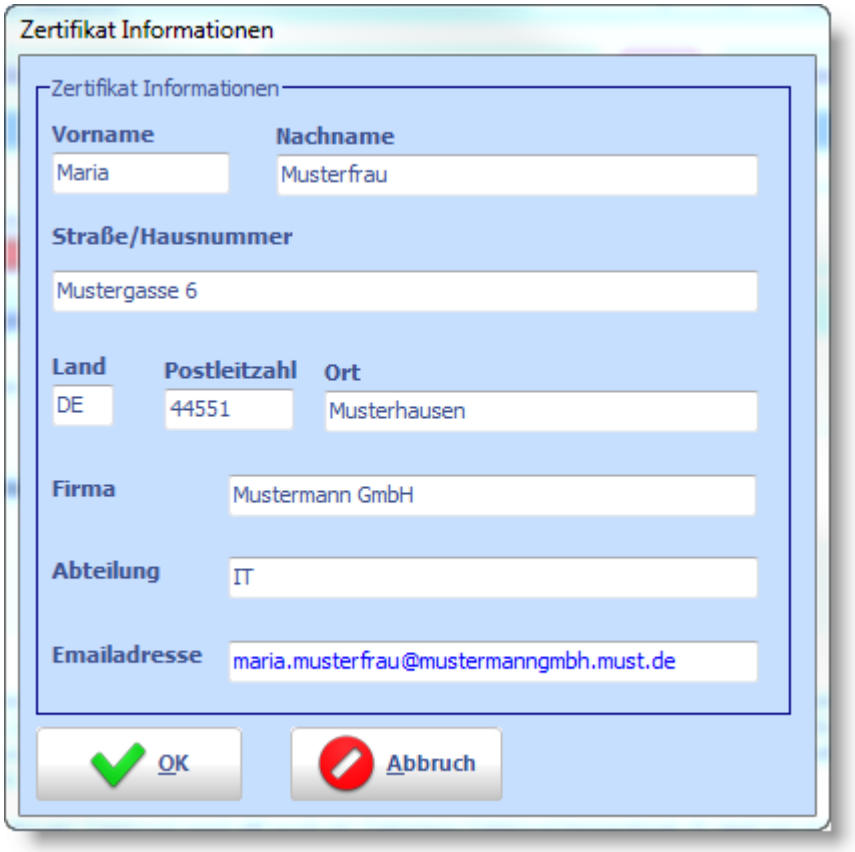
Um die Funktionen der Rubrik Public-Key nutzen zu können, benötigen Sie ein Zertifikat. ArchiCrypt Live ist in der Lage, ein Zertifikat zu erstellen.

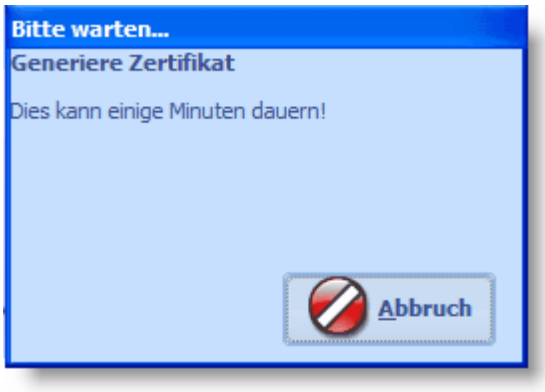
Schritt 1:

Betätigen Sie die Schaltfläche Zertifikat erstellen

Schritt 2:

➡ ACHTUNG: ***Füllen Sie die entsprechenden Felder bitte korrekt aus! Einmal erstellt, können Sie das Zertifikat nur über den Windows Zertifikatmanager löschen!***





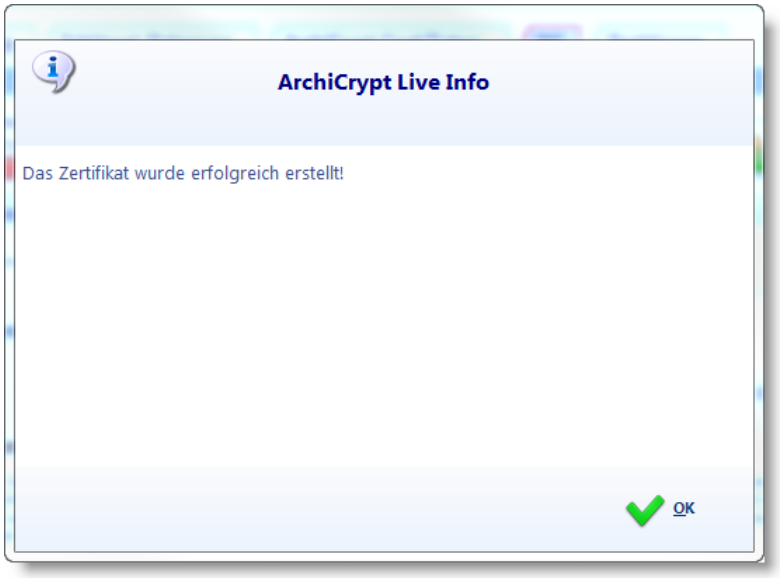
Bitte beachten Sie, dass auch beim Abbrechen des Vorgangs einige Zeit verstreicht, bis ArchiCrypt Live wieder zur Verfügung steht.

Schritt 3:

Nach dem Erstellen wird das Zertifikat inkl. des Privaten (*geheimen*) Schlüssels als geschütztes Objekt in Windows abgelegt. Die nachfolgenden Dialoge und Funktionen sind Bestandteil des Betriebssystems und nicht Gegenstand von ArchiCrypt Live.

Da es sich bei dem Privaten Schlüssel um eine hochsensible Information handelt, sollten Sie die Sicherheitsstufe auf HOCH stellen. Dazu bitte die Schaltfläche Sicherheitsstufe... betätigen.

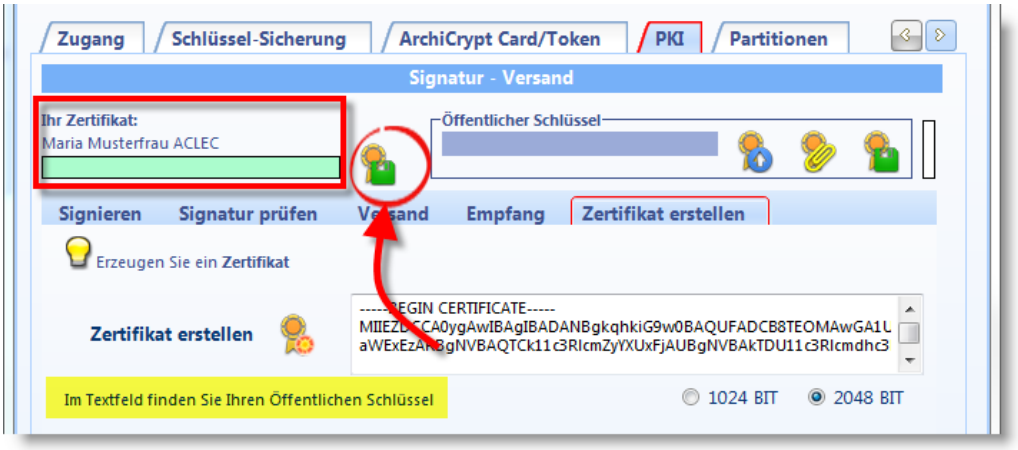
Geben Sie jetzt ggf. einen Bezeichner und ein Passwort ein (*Sie sollten mindestens 12 Zeichen, Groß-/Kleinbuchstaben Ziffern und Sonderzeichen*) eingeben.



Tritt ein Fehler auf, beachten Sie bitte die Hinweise weiter unten!

Weitergabe des Öffentlichen Schlüssels (*Public Key*)

Nach dem Erstellen wird der Öffentliche Schlüssel im Textfeld angezeigt. Diesen können Sie zum Beispiel per Email versenden oder auf Ihrer Internetseite bekannt geben. Sie können alternativ jeden Öffentlichen Schlüssel als Textdatei über die Funktion Speichern exportieren.



➡WICHTIG: ***Das erstellte Zertifikat hat einen Öffentlichen Schlüssel 2024 BIT (RSA). Bitte beachten Sie, dass Sie alle aktuellen Service Packs eingespielt haben müssen, um diese Schlüssellänge zu unterstützen. Sollte Ihnen das Einspielen von Service Packs nicht möglich sein, können Sie ArchiCrypt Live dazu veranlassen, Zertifikate mit Schlüssellängen von 1024 BIT (RSA) zu erzeugen. Treffen Sie dazu die Auswahl 1024 BIT***

Zur Unterstützung der Schlüssellängen 1024 und 2048 ist insbesondere der Internet Explorer von Bedeutung. Es sollte mindestens Version 5.5 mit SP 1 installiert sein.

10.4.10.5.3 Ein Laufwerk signieren

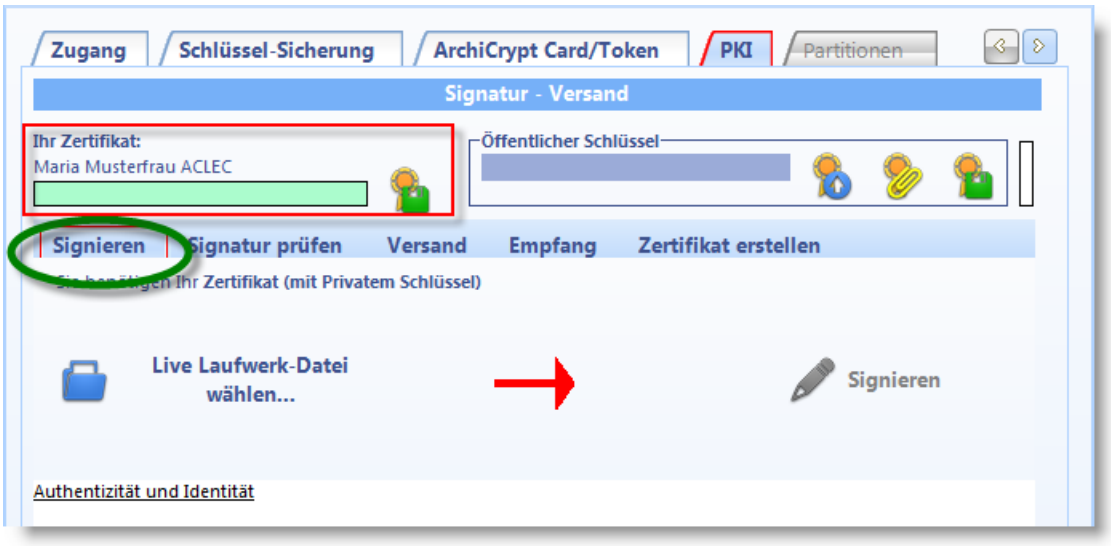
siehe auch: Wichtige Begriffe - Begriffserläuterungen

Signieren eines Laufwerks

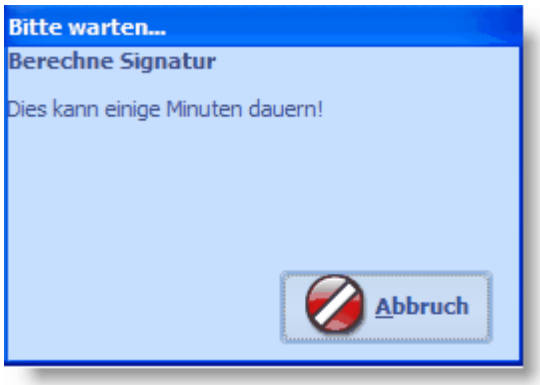
Das Signieren kann man mit dem Unterzeichnen eines Schriftstücks gleichsetzen. Eine Signatur entspricht quasi einer Unterschrift und wird oft auch als Digitale Unterschrift bezeichnet. Das Signieren erfüllt zwei wichtige Aufgaben.
1. Es teilt dem Empfänger eines Live Laufwerks mit, dass das Laufwerk auch tatsächlich von Ihnen stammt (Authentizität).
2. Die Signatur stellt sicher, dass das Laufwerk seit dem Zeitpunkt des Signierens nicht geändert wurde (Integrität).

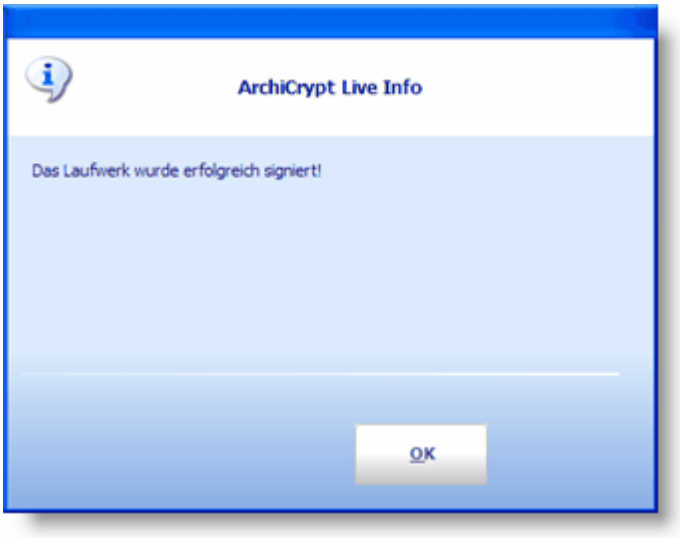
Um ein Laufwerk zu signieren, benötigen Sie

Ihr Zertifikat mit Privatem Schlüssel. siehe dazu ggf. Erstellen eines Zertifikats

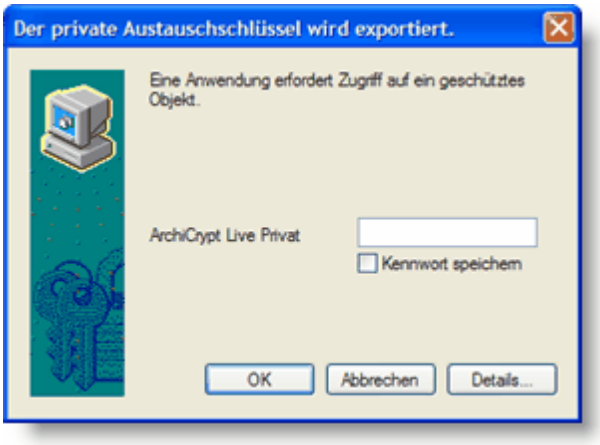


Laden Sie das dateibasierte Live Laufwerk (Live Laufwerk-Datei wählen ...), welches Sie signieren möchten. Das Laufwerk darf nicht geladen sein! Betätigen Sie jetzt die Schaltfläche Signieren.





➡ACHTUNG***: Sofern Sie unserem Ratschlag gefolgt sind, bei der Ablage Ihres Privaten Schlüssels im Zertifikatspeicher von Windows die Sicherheitsstufe HOCH zu wählen, werden Sie jetzt durch das Betriebssystem aufgefordert, das Schutzpasswort einzugeben. (siehe Erstellen eines Zertifikats)***



HINWEIS: Bitte beachten Sie, dass die Signatur nur so lange gültig ist, bis die Daten des Laufwerks geändert wurden. Wird das Laufwerk verändert, ist auch die Unterschrift ungültig! Gelegentlich genügt es schon, das Laufwerk nach dem Signieren zu öffnen, um die Signatur ungültig zu machen. Es können ausschließlich dateibasierte Laufwerke signiert werden. Das Signieren von Partitionen ist nicht möglich!

10.4.10.5.4 Signatur Prüfen

siehe auch: Wichtige Begriffe - Begriffserläuterungen

Signatur prüfen

Durch das Prüfen der Signatur werden zwei Fragen beantwortet:
1. "Stammen die Daten tatsächlich vom vorgeblichen Absender?" (Authentizität)
2. "Wurden die Daten seit der Signierung geändert?" (Integrität).

Ist die Signatur in Ordnung, bestätigt ArchiCrypt Live die Authentizität (Laufwerk stammt vom Absender) und die Integrität (Daten sind seit der Signierung nicht geändert worden). Bitte beachten Sie die Hinweise zu Zertifikaten im Kapitel Fremde Zertifikate laden. Insbesondere bei selbst signierten Zertifikaten müssen Sie selbst sicher sein, aus welcher Quelle das Zertifikat stammt!

Um eine Signatur zu prüfen benötigen Sie

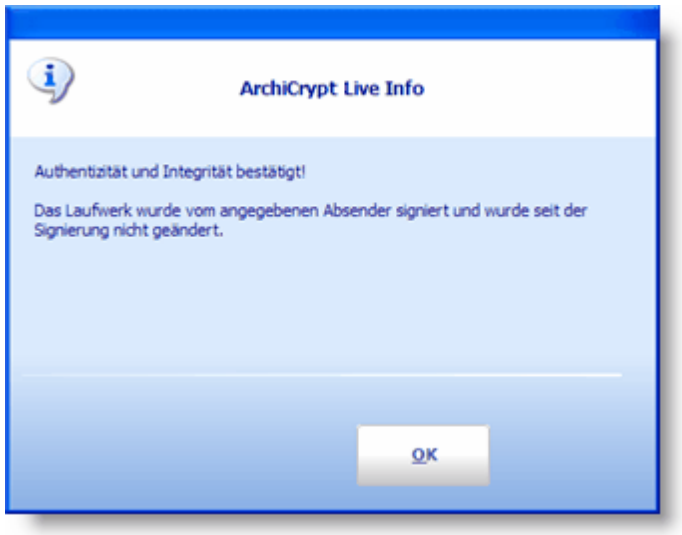
Das Zertifikat (mit Öffentlichem Schlüssel) des Absenders.

Laden Sie, sofern noch nicht geschehen, den Öffentlichen Schlüssel des Absenders (siehe Fremde Zertifikate laden).

Laden Sie das dateibasierte Live Laufwerk (Live Laufwerk-Datei wählen ...), deren Signatur Sie prüfen möchten. Stellen Sie sicher, dass der Öffentliche Schlüssel des Absenders geladen ist. Betätigen Sie jetzt die Schaltfläche Signatur prüfen.

Falls die Signatur nicht in Ordnung ist, wird die Integrität und Authentizität nicht bestätigt. Dies bedeutet, dass entweder das Laufwerk nicht von diesem Absender stammt, oder dass die Inhalte des Laufwerks seit der Unterzeichnung geändert wurden.

Ist die Signatur in Ordnung (*Laufwerk stammt vom vorgeblichen Absender und Inhalt wurde seit dem Signieren nicht geändert*), bestätigt ArchiCrypt Live Authentizität und Integrität.



HINWEIS: Es können ausschließlich dateibasierte Live Laufwerke (Trägerdateien) geprüft werden.

10.4.10.5.5 Versand mit Öffentlichem Schlüssel

siehe auch: Wichtige Begriffe - Begriffserläuterungen

Versand mit Öffentlichem Schlüssel

Technisch ausgedrückt, hat man es mit folgendem Problem zu tun: Wie kann man vertrauliche Daten sicher über unsichere Kommunikationskanäle übertragen. Unsere vertraulichen und sensiblen Daten befinden sich geschützt in einem ArchiCrypt Live Laufwerk. Das Laufwerk und damit die sensiblen Daten können ohne Gefahr an einen Empfänger übertragen werden. Jedoch kann der Empfänger ohne ein Passwort nichts mit unserem Laufwerk anfangen. Die Gefahr, dass ein Unbefugter das Passwort in Erfahrung bringt, ist dann besonders groß, wenn man dieses Passwort über einen so genannten unsicheren Kommunikationskanal an jemanden übermitteln muss.

Ein unsicherer Kommunikationskanal wäre z.B.

- Übersenden des unverschlüsselten Passwortes per Email
- Übersenden des Passwortes per Post
- Mitteilen des Passwortes per Telefon
- Mitteilen des Passwortes in einer Umgebung in der andere mithören könnten.

Hier kommen der Öffentliche Schlüssel und der Private Schlüssel mit ihren besonderen Eingenschaften zum Einsatz. Mit Hilfe des frei verfügbaren Öffentlichen Schlüssels des Empfängers, verschlüsseln wir ein Zugangspasswort.

Das mit dem Öffentlichen Schlüssel des Empfängers verschlüsselte Zugangspasswort kann bekanntlich nur durch den Besitzer des zugehörigen Privaten Schlüssels entschlüsselt werden. Somit können wir das Laufwerk sicher über einen unsicheren Kommunikationskanal übertragen.

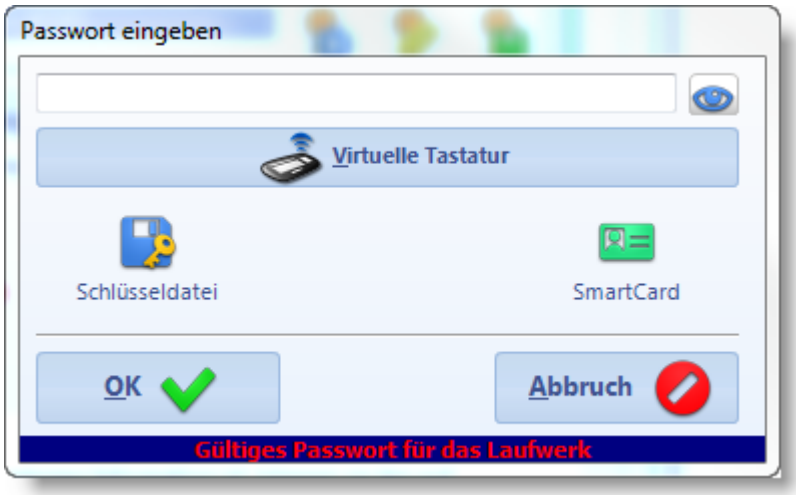
Um ein Laufwerk für den Versand vorzubereiten benötigen Sie

Das Zertifikat (mit Öffentlichen Schlüssel) des Empfängers.

(siehe Fremde Zertifikate laden).

Laden Sie das dateibasierte Live Laufwerk (Live Laufwerk wählen ...), die Sie versenden möchten. Stellen Sie sicher, dass das Zertifikat mit Öffentlichem Schlüssel des Empfängers geladen ist. Betätigen Sie jetzt die Schaltfläche Verschlüsseln.

Sie werden zur Eingabe eines Passwortes aufgefordert, welches sicher weitergegeben werden soll.
➡WICHTIG: ***Es muss sich um einen bestehenden Schlüssel/bestehendes Passwort handeln!***



Für den Empfänger spielt es keine Rolle, welchen Zugangsschutz (*Passwort, Schlüsseldatei, Token, SmartCard*) Sie nutzen. Der Empfänger benötigt nur seinen Privaten Schlüssel!

➡ACHTUNG***: Die*** Rechte ***die mit diesem Schlüssel verbunden sind,*** gehen ***auch*** an den Empfänger über***. Wenn Sie hier den Laufwerk-Administrator-Schlüssel weitergeben, hat der Empfänger vollen Zugriff auf***

alle Laufwerkfunktionen, wenn Sie ein Gastpasswort mit reiner Leseberechtigung weitergeben, hat der Empfänger nur Leserechte. Der Empfänger kann das Laufwerk ebenfalls für den Versand vorbereiten, dabei kann er (entsprechend der Rechte seines Zugangs) höchstens die Rechte weitergeben, die er selbst hat.

➡ACHTUNG: ***Das Vorbereiten für den Versand setzt keinen Laufwerk-Administrator-Schlüssel voraus, da diese Methode weder einen Schlüssel ändert, noch einen weiteren Zugang schafft. Das Vorbereiten für den Versand entspricht der sicheren Weitergabe eines bereits eingerichteten Passwortes!***
Nach dem Vorbereiten dürfen Sie keinesfalls das Passwort ändern, welches Sie bei der Vorbereitung für den Versand eingegeben haben. Der Empfänger kann sonst das Laufwerk nicht öffnen.

 HINWEIS: Es können ausschließlich dateibasierte Live Laufwerke versandt werden.

10.4.10.5.6 Empfang mit Privatem Schlüssel

siehe auch: Wichtige Begriffe - Begriffserläuterungen

Empfang mit Privatem Schlüssel

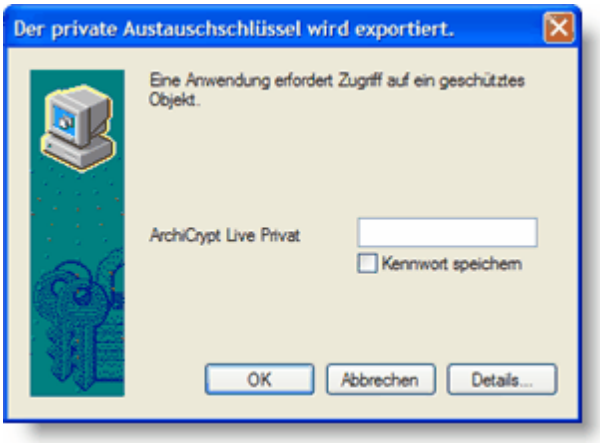
Haben Sie ein Laufwerk empfangen, welches speziell für den Versand vorbereitet wurde, können Sie mit Ihrem Privaten Schlüssel Ihres Zertifikats Zugang zum Laufwerk erhalten.

Um ein Laufwerk welches für den "Empfang durch Sie" vorbereiten wurde, zu öffnen, benötigen Sie

Ihr Zertifikat (mit Privatem Schlüssel).

Laden Sie das dateibasierte Live Laufwerk (Live Laufwerk-Datei wählen ...), welches speziell für den "Empfang durch Sie" vorbereitet wurde. Betätigen Sie jetzt die Schaltfläche Schlüssel auslesen.

➡ACHTUNG***: Sofern Sie unserem Ratschlag gefolgt sind, bei der Ablage Ihres Privaten Schlüssels im Zertifikatspeicher von Windows die Sicherheitsstufe HOCH zu wählen, werden Sie jetzt durch das Betriebssystem aufgefordert, das Schutzpasswort für Ihren Privaten Schlüssel einzugeben. (siehe Erstellen eines Zertifikats)***



Sie werden jetzt gefragt, ob Sie den übermittelten Zugang als Schlüsseldatei ablegen möchten.

Es wird empfohlen dies zu tun, da Sie ansonsten das erhaltene Laufwerk ausschließlich über die Funktion Empfang mit Privaten Schlüssel öffnen können. Speichern Sie den Schlüssel hingegen in einer Datei ab, können Sie über die normale Öffnen/Schließen Funktion Zugang zum Laufwerk erhalten. Sofern Sie den Schlüssel als Schlüsseldatei gespeichert haben, wird Ihnen angeboten, den Zugang mit Privatem Schlüssel zu löschen. Dies wird empfohlen!

Zuletzt werden Sie danach gefragt, ob Sie das Laufwerk laden möchten.

➡HINWEIS: Ihre Rechte (Lesen/Schreiben, Ändern von Schlüsseln, Erstellen von Gastzugängen) hängen davon ab, welche Rechte Ihnen der Absender des Laufwerks zugedacht hat.

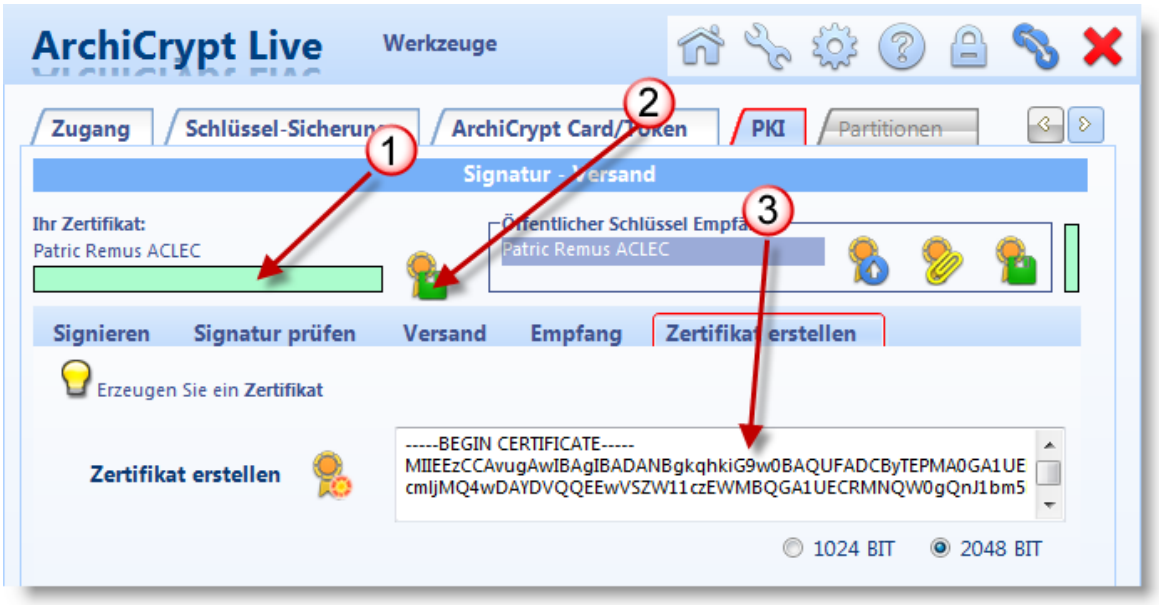
10.4.10.5.7 Das eigene Zertifikat weitergeben

siehe auch: Wichtige Begriffe - Begriffserläuterungen

Weitergabe des Öffentlichen Schlüssels

Damit andere Ihnen Daten zusenden können die nur Sie entschlüsseln können oder andere Ihre Signatur prüfen können, benötigen diese Ihren Öffentlichen Schlüssel. Der Öffentlich Schlüssel ist neben einigen weiteren Daten Bestandteil eines Zertifikats.

Sofern Sie bereits ein Zertifikat erstellt haben, finden Sie Ihren Öffentlichen Schlüssel immer unter Werkzeuge-PKI-Zertifikat erstellen



Falls Sie Informationen über Ihr Zertifikat wünschen, doppelklicken Sie auf den Namen des Zertifikats (bei 1).

Weitergabe Ihres Öffentlichen Schlüssels als Datei

Sie können das Zertifikat in einer Datei speichern um es weiterzugeben. Dabei wird selbstverständlich nur Ihr Öffentlicher Schlüssel weitergegeben. Betätigen Sie zum Speichern des Zertifikats die Schaltfläche (bei 2). Dabei stehen Ihnen bestimmte Formate zur Verfügung, die die standardisierte Weitergabe von Schlüsseln erlauben.

Die Datei können Sie auf beliebigem Wege weitergeben; Sie ist nicht schützenswert.

Weitergabe Ihres Öffentlichen Schlüssels als Text

Sobald Ihr Zertifikat geladen ist, erscheint es im markierten Bereich (3). Sie können diesen Text markieren und in die Zwischenablage kopieren (Strg+C oder rechte Maustaste + kopieren). Aus der Zwischenablage können Sie das Zertifikat in jeden Text einfügen. Zum Beispiel an jede E-Mail anhängen oder auf der WEB-Seite veröffentlichen!

Damit der Empfänger den Öffentlichen Schlüssel nutzen kann, achten Sie bitte darauf immer auch die umschließenden Zeilen (-----BEGIN CERTIFICATE-----
und -----END CERTIFICATE-----) mit weiterzugeben. Fügen Sie keine zusätzlichen Zeichen oder Leerzeilen ein!

Der Schlüssel sieht dann etwa so aus:

-----BEGIN CERTIFICATE-----
MIIEUTCCAzmgAwIBAgIBADANBgkqhkiG9w0BAQUFADCB6DEOMAwG
A1UEKhMFQmVy
bmQxEzARBgNVBAQTCk11c3Rlcm1hbm4xFjAUBgNVBAkTDU11c3Rlc
mdhc3NlIDUx
CzAJBgNVBAYTAkRFMQ4wDAYDVQQREwUxMDAwMDEVMBMGA1UEB
xMMTXVzdGVyaGF1
c2VuMRIwEAYDVQQKEwlNdXN0ZXJiYXUxDDAKBgNVBAsTA0VEVjEyM
DAGCSqGSIb3
DQEJARMjQmVybmRATXVzdGVybWFubkluTXVzdGVyaGF1c2VuLmluZ
m8xHzAdBgNV
BAMTFkJlcm5kIE11c3Rlcm1hbm4gQUNMRUMwIBcNMDQxMDA1MTIzN
zEyWhgPMjEw
NDA5MTExMjM3MTJaMIHoMQ4wDAYDVQQqEwVCZXJuZDETMBEGA1
UEBBMKTXVzdGVy
bWFubjEWMBQGA1UECRMNTXVzdGVyZ2Fzc2UgNTELMAkGA1UEBhM
CREUxDjAMBgNV
BBETBTEwMDAwMRUwEwYDVQQHEwxNdXN0ZXJoYXVzZW4xEjAQBg
NVBAoTCU11c3Rl
cmJhdTEMMAoGA1UECxMDRURWMTIwMAYJKoZIhvcNAQkBEyNCZXJu
ZEBNdXN0ZXJt
YW5uSW5NdXN0ZXJoYXVzZW4uaW5mbzEfMB0GA1UEAxMWQmVyb
mQgTXVzdGVybWFu

biBBQ0xFQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEA
DkiKf6z2P8Jw
MIxiOnU5M/Lx6CqFqa69HSNAk7j1wVUrYtJ5m3ejnM01dJKV4lsm7e5p
sKcUQLID
4CWPtgeJMtAOfOB8UPvOWV5UxKhbumFwoOcr/s4lO6PHx9g3p1khdE
5YJ3g9jjS9
mdkdJOZ2eWv97Qvs1sOg83c5Xp/JStq65t8V+lzAAO3RsLF8XSOKV7
VHmIjYbqWe
NV6DAE+b97FtXWbyZqR+A+KrXffmONYDGIhKly3shKk2kIcFYK9HtQ
IAQlVlmvm4
4vmiZomu3iKpnJWu5hcduR/VxSAs8n24Q1A5Pe54xgVvZ99MRg1+L+
OwTdWWMGFH
H7CVvcosuQIEAAEAAaMCMAAwDQYJKoZIhvcNAQEFBQADggEBAA4x
eRq0Tfe9oBN5
LlYPmAOZ1ajaeZsgLq/J7xObPJqAV71gX7ABcV9VFcAxU5sVYEfm4Htk
Ci49BEP+
wVNN6snPEzGHoO2iV5x2io8sZq9UtG8qap1qKE4G5n9qVO9KAQ3p0s
5ZplKs/j6v
5dqtUuynfhRqkCCFy7aREZ5KsfOgzk2VTIaAS4XjxvyHIHq+frYpzrb8g
AMjPnYs
E/Ibg3p1rL3pQmsffrlNPoY+h1ee/buFNSsXmBASOEv5oBgPdcMA4Qc7
4mhCyntv
0BLsnNZjk0xhNgLbmqS+t2E12lurqklwvaPTEJCky9cWUaKLPYWrIZsd
cedXdiF4
y4ECiXA=
-----END CERTIFICATE-----

10.4.10.5.8 Fremde Zertifikate laden

Laden von Öffentlichen Schlüsseln

Falls Sie jemandem verschlüsselte Daten senden möchten, benötigen Sie dessen Zertifikat mit Öffentlichem Schlüssel. (siehe Das eigene Zertifikat weitergeben). Das Gleiche gilt beim Empfang von signierten Daten. Sie benötigen zur Prüfung den Öffentlichen Schlüssel des Absenders.

Laden eines Öffentlichen Schlüssels aus einer Datei

Sie können Zertifikate in Form einer Datei oder in Form von Text (*eingebettet in ein Dokument wie Internetseite, Email etc.*) erhalten.

Sofern Sie eine Datei erhalten haben, können Sie diese laden (1).

Laden des Öffentlichen Schlüssels aus Text

Eventuell ist das Zertifikat auch in einen Text eingebettet. Markieren Sie zum Laden diesen Text mit der Maus und kopieren ihn dann in die Zwischenablage (*Strg+C oder Kontextmenü+kopieren*). Betätigen Sie dann in ArchiCrypt Live die Schaltfläche bei (2).

➡HINWEIS*:*
Konnte das Zertifikat importiert werden, werden Ihnen Zertifikatinformationen angezeigt. Gleichzeitig wird das Zertifikat validiert. D.h. es wird geprüft, ob die Echtheit des Zertifikats durch eine Zertifizierungsstelle bestätigt wird. (siehe auch Zertifikate von Zertifizierungsstelle nutzen). Dazu nutzt ArchiCrypt Live den Zertifikatspeicher von Windows.

Falls es sich um ein Zertifikat handelt, welches von keiner Zertifizierungsstelle ausgestellt wurde, wird der Hinweis
Zertifikat ist vom Typ SelfSigned (vom Besitzer selbst unterschrieben). Bitte vergewissern Sie sich, dass das Zertifikat echt ist!
ausgegeben. Sofern Sie sich über die Herkunft des Zertifikats im Klaren sind, spielt dies keine Rolle.

Umwandeln des Zertifikatformats

Sofern Sie ein Zertifikat als Text erhalten haben und dies aus der Zwischenablage importiert wurde (2), möchten Sie das Zertifikat evtl. als Datei speichern. Betätigen Sie die Schaltfläche (3) und speichern das Zertifikat im gewünschten Format.

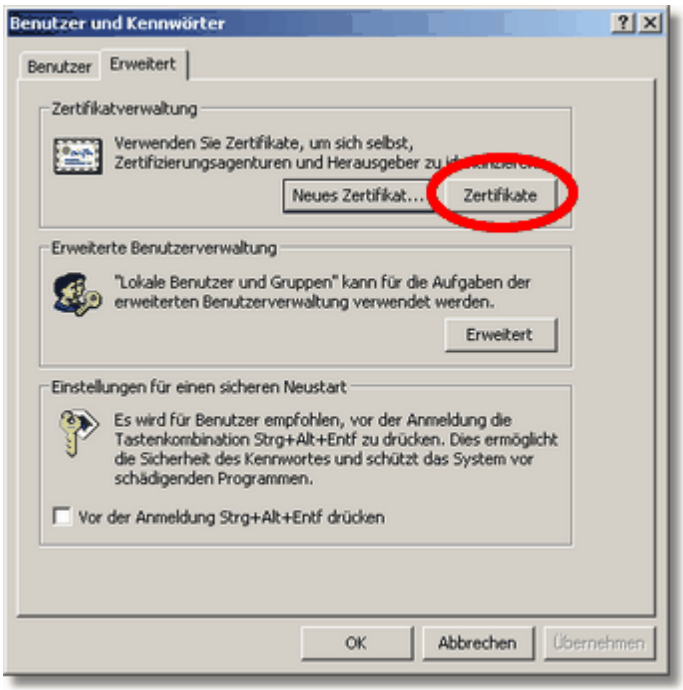
10.4.10.5.9 Zertifikate von Zertifizierungsstelle nutzen

Um ArchiCrypt Live zu veranlassen, ein Zertifikat zu nutzen, welches nicht von ArchiCrypt Live generiert wurde, müssen Sie das Zertifikat zunächst in Windows importieren. Sobald Sie das Zertifikat erhalten haben, können Sie das Zertifikat, per Doppelklick auf die Datei, installieren. Bitte beachten Sie, dass Sie das Zertifikat inkl. Privatem Schlüssel importieren müssen! ArchiCrypt Live setzt als Signaturalgorithmus SHA1RSA und als Fingerabdruckalgorithmus SHA1 voraus.

➡ACHTUNG***: Nachfolgend beschriebene Funktionen und Dialoge entstammen dem Betriebssystem und sind nicht Bestandteil von ArchiCrypt Live!***

Schritt 1: Öffnen Sie jetzt die Zertifikatverwaltung von Windows

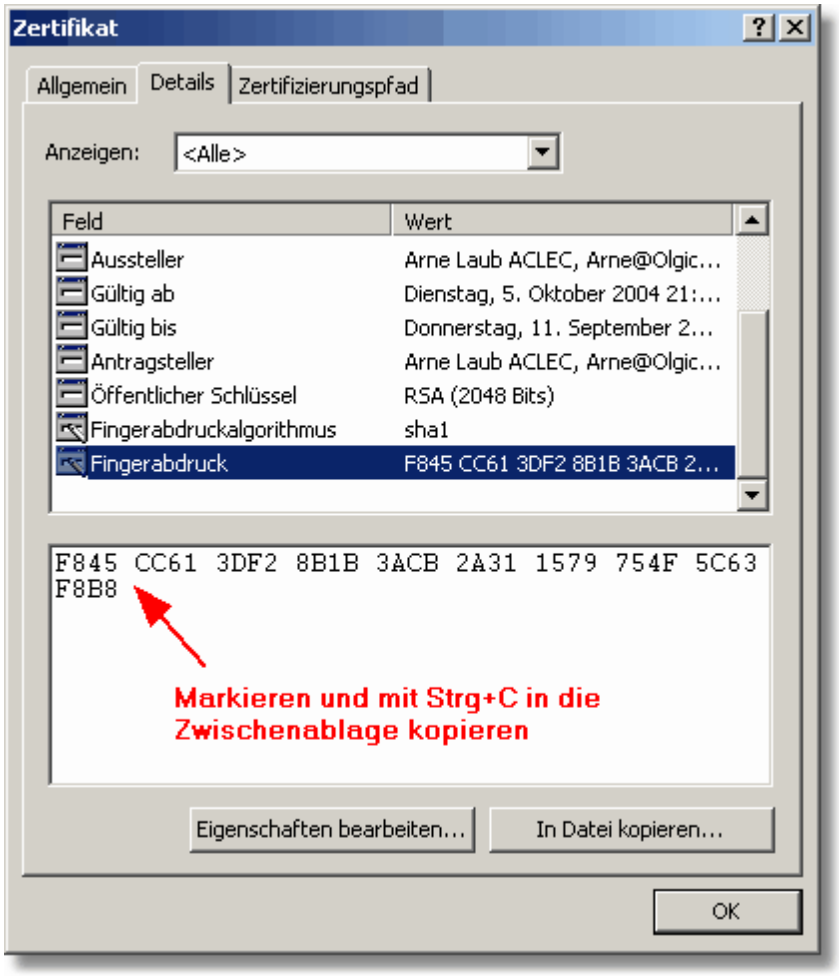
In Windows 2000 rufen Sie dazu die Systemsteuerung und dort die Funktion Benutzer und Kennwörter auf. Wechseln Sie auf die Registerseite Erweitert und betätigen Sie die Schaltfläche Zertifikate



Unter Windows XP, Windows 2003 und Vista / W7 und W8 rufen Sie die Systemsteuerung und dort die Funktion Netzwerk- und Internetverbindungen auf. Dort wählen Sie bitte Internetoptionen aus.
Auf der Registerseite Inhalte finden Sie die Schaltfläche Zertifikate.

Schritt 2: Wählen Sie im Dialog Zertifikate das Zertifikat aus, welches Sie in ArchiCrypt Live nutzen möchten.

Betätigen Sie die Schaltfläche Anzeigen. Wechseln Sie in der Zertifikatansicht zur Seite Details.



Schritt 3: Suchen Sie den Eintrag Fingerabdruck und kopieren Sie diesen in die Zwischenablage.

Stellen Sie sicher, dass ArchiCrypt Live beendet ist.

Schritt 4: Öffnen Sie die Initialisierungsdatei ACLive8.ini mit einem Texteditor. Sie finden diese Datei unter

Windows 2000/XP/2003/Vista
C:\Dokumente und Einstellungen\<Ihr Nutzername>\Anwendungsdaten\ACLive5
Windows 7/8
C:\Users\<Ihr Nutzername>\AppData\Roaming\ACLive5

Schritt 5: Suchen Sie den Abschnitt [Certificate].

Hinter Fingerprint= tragen Sie bitte den soeben kopierten Fingerabdruck des Zertifikats ein.
Im Beispiel F845 CC61 3DF2 8B1B 3ACB 2A31 1579 754F 5C63 F8B8. Löschen Sie alle Leerzeichen und wandeln Sie Groß- in Kleinbuchstaben um. Gegebenenfalls enthaltene Sonderzeichen wie z.B. ? sind ebenfalls zu entfernen!
Es sollte sich also anschließend der Eintrag wie folgt darstellen:
[Certificate]
Fingerprint=f845cc613df28b1b3acb2a311579754f5c63f8b8

Falls kein entsprechender Eintrag existiert, erstellen Sie bitte einen. Beim nächsten Start nutzt ArchiCrypt Live das entsprechende Zertifikat.

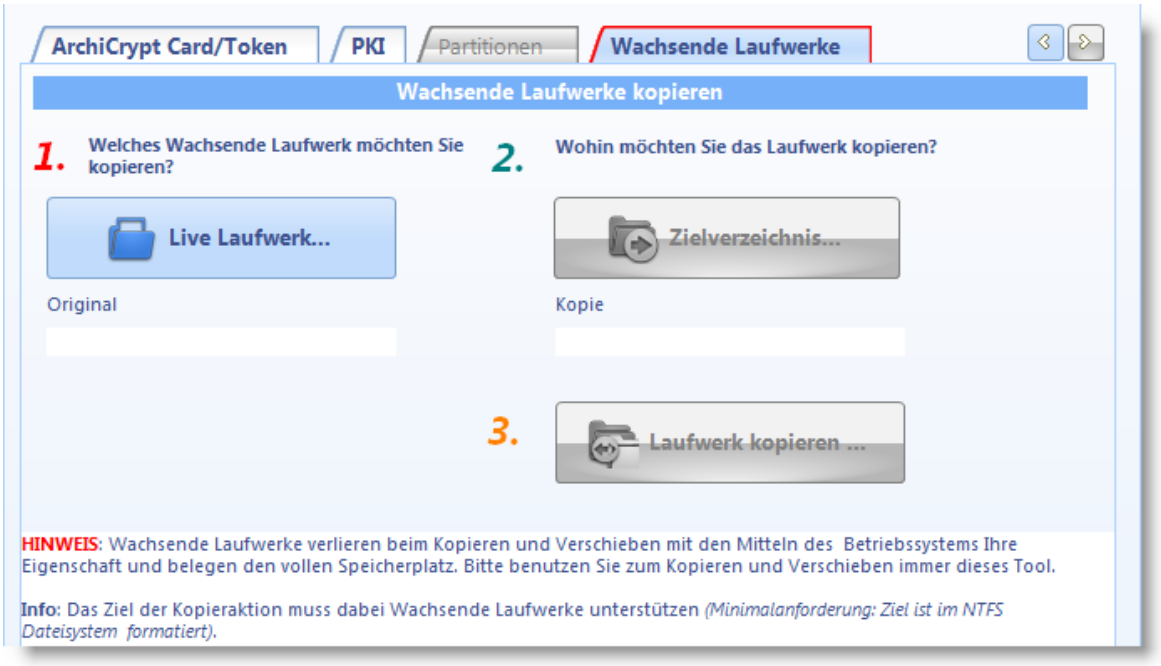
10.4.10.6 Wachsende Laufwerke

siehe auch: Wichtige Begriffe - Begriffserläuterungen
Wachsende Laufwerke und Ultraschnelles Erstellen

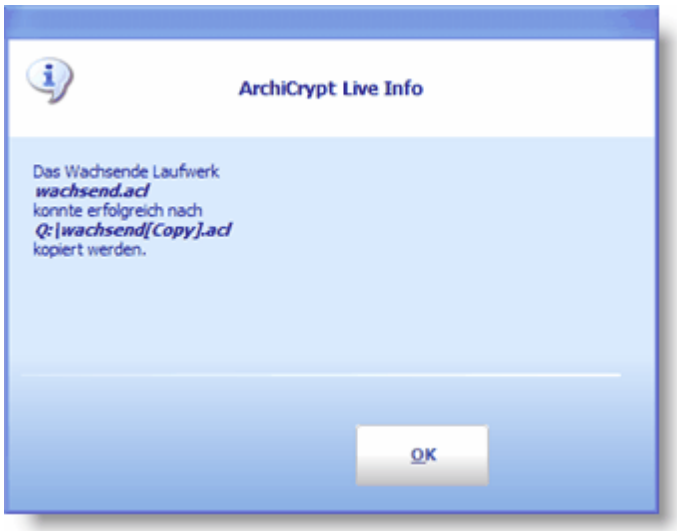
So kopieren und verschieben Sie Wachsende Laufwerke

Wenn Sie mit Betriebssystemmitteln ein Wachsendes Laufwerk kopieren oder verschieben gehen die angenehmen Eigenschaften verloren. Die Kopie belegt den als Maximum angegebenen Speicherplatz auf dem Datenträger.

ArchiCrypt Live bringt ein Werkzeug mit, mit dem Sie Wachsende Laufwerke so kopieren können, dass die Eigenschaften erhalten bleiben. Voraussetzung ist, dass das Ziel des Kopiervorgangs Wachsende Laufwerke unterstützt. (siehe Voraussetzung Wachsende Laufwerke.)



1. Wählen Sie zunächst das Wachsende Laufwerk (bei 1)
2. Wählen Sie das Zielverzeichnis der Kopieroperation (bei 2)
3. Starten Sie den Kopiervorgang (bei 3)



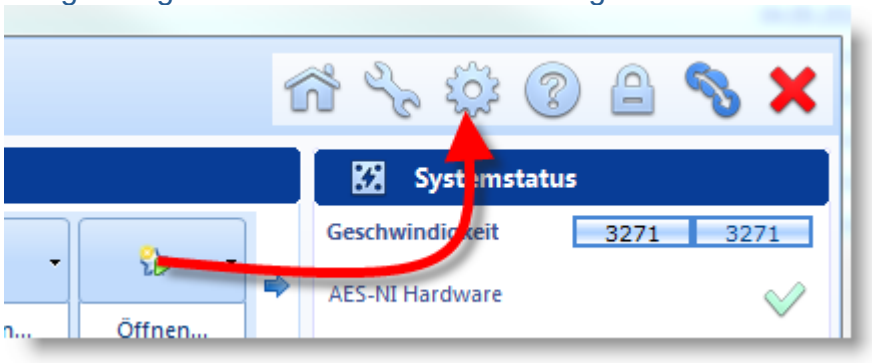
Wenn Sie das Wachsende Laufwerk verschieben wollten, löschen Sie jetzt das Original.

10.4.11 Einstellungen

Einstellungen

Hinter dem Begriff Einstellungen verbergen sich Funktionen und Optionen, die das Verhalten von ArchiCrypt Live festlegen. Neben allgemeinen Funktionen können Hotkeys festgelegt werden.

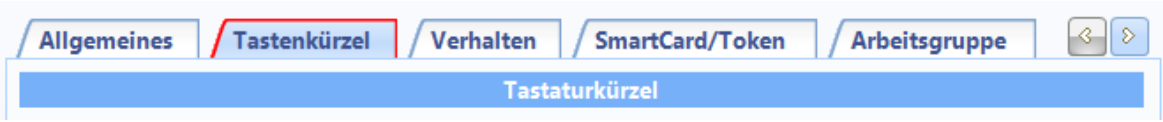
So gelangen Sie zu den Einstellungen



Allgemeines

- Mit Windows starten
- Dateiendung registrieren
- Beim Start prüfen, ob Update verfügbar
- Update
- Ausgeblendete Nachrichten reaktivieren
- Akustisches Signal beim Öffnen / Akustisches Signal beim Schließen
- Schlüsseldatei immer suchen unter
- AES-NI Support
- Alternativer Dateimanager
- Favoriten - Alphabetisch sortieren
- Verlauf - Zuletzt geöffnete Laufwerke merken
- Live Filter-Modul aktivieren / deaktivieren

Tastaturkürzel

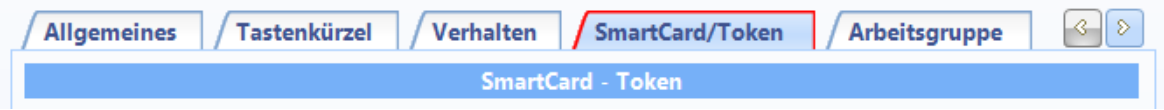


- Alle Laufwerke schließen
- Laufwerksinhalt anzeigen
- ArchiCrypt Live beenden

Verhalten

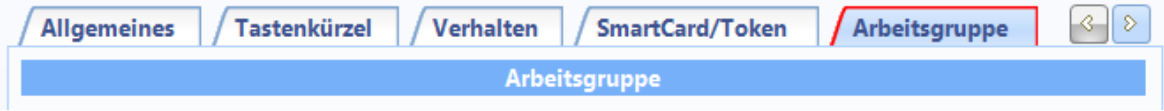
- ArchiCrypt Live nach dem Start minimieren
- Beim Beenden Zuletzt verwendete Dokumente löschen
- Auslagerungsdatei beim Herunterfahren des Rechners überschreiben
- Notaus bei Alle schließen
- Laufwerke automatisch schließen, wenn der Computer nicht benutzt wurde für ... Minuten
- Autostart für ArchiCrypt Live Laufwerke
- Beim Einlegen eines Datenträgers mit einem Live Laufwerk nach dem Passwort fragen
- Notaus bei Schließen mit ArchiCrypt Card/Token
- Beim Öffnen auf Signatur prüfen
- Beim Öffnen auf Schlüsselübermittlung prüfen
- Live Laufwerk als "Lokales Laufwerk" laden
- Laufwerke beim Erstellen automatisch als NTFS Laufwerk erzeugen
- Passwort merken bei Autostart mit Favorit
- Prozesssperre für ArchiCrypt Laufwerke
- Umleitung für ArchiCrypt Live Laufwerke
- Auf Laufwerke älteren Typs nur lesend zugreifen
- Laufwerke beim Beenden von ArchiCrypt Live automatisch schließen

SmartCard/Token



- SmartCard Lesegerät wählen
- Schlüssel zuerst auf ArchiCrypt Card suchen
- PKCS11 Unterstützung aktivieren
- PKCS11 Bibliothek

Arbeitsgruppe



- Arbeitsgruppen-Optionen verwenden
- Anwenderkonto

Einstellungen - Allgemeines

Mit Windows starten

Wählen Sie diese Option aus, wenn ArchiCrypt Live beim Anmelden des Benutzers automatisch gestartet werden soll. Diese Funktion ist im Zusammenhang mit den Favoriten (*Beim Start von ArchiCrypt Live automatisch laden*) nützlich, da Sie so beim Rechnerstart bestimmte ArchiCrypt Live Laufwerke automatisch nach Angabe der Zugangsdaten öffnen können.

Dateiendung registrieren

ArchiCrypt Live Laufwerke (*die Trägerdateien*) tragen die Dateiendung acyl *(ältere Versionen acl)* . Bei eingeschalteter Option wird dem System bekannt gemacht, dass ArchiCrypt Live für Dateien mit der Endung acyl und acl zuständig ist. Dadurch ist es möglich, eine Trägerdatei im Windows-Explorer per Doppelklick auszuwählen und damit ArchiCrypt Live zu aktivieren. Die Dateien erhalten zudem das Symbol von ArchiCrypt Live.

Beim Start prüfen, ob Update verfügbar

Besteht während des Starts von ArchiCrypt Live eine Internetverbindung, wird geprüft ob eventuell eine neuere Version verfügbar ist. Findet ArchiCrypt Live eine neuere Version, können Sie die neue Version über einen Link, der dann auf der Hauptseite erscheint laden.

Update

Hier können Sie manuell prüfen, ob es eine neuere Version von ArchiCrypt Live gibt.

Akustisches Signal beim Öffnen
Akustisches Signal beim Schließen

Bei jeweils eingeschalteter Option wird das Öffnen und Schließen mit einem akustischen Signal begleitet.

Ausgeblendete Nachrichten reaktivieren

Bei bestimmten Meldungen bietet ArchiCrypt Live an, sie künftig nicht mehr anzuzeigen. Die so ausgeblendeten Nachrichten können durch Betätigen der Schaltfläche wieder aktiviert werden.

Schlüsseldatei immer suchen unter

Nicht immer muss eine s.g. Schlüsseldiskette zur Aufnahme einer Schlüsseldatei dienen. Die Schlüsseldatei kann durchaus auch auf einem USB / Memory-Stick oder einem anderen Wechselmedium untergebracht sein. Das Wechselmedium kann dabei unterschiedliche Laufwerks- und Verzeichnisnamen aufweisen. Um Ihnen die ständige Suche nach der Schlüsseldatei zu ersparen, können Sie einen festen Pfad vorgeben, unter dem dann beim Einlesen einer Schlüsseldatei zuerst gesucht wird.

AES-NI Support

Sofern der Prozessor Ihres Rechners den erweiterten AES-NI Befehlssatz unterstützt, können Sie hier für ArchiCrypt Live festlegen, ob bei Live Laufwerken mit AES Verschlüsselung auf die Hardware zurückgegriffen werden soll. AES-NI lässt sich deaktivieren und wieder reaktivieren. Andere Software auf dem System wird von diesen Einstellungen nicht betroffen. Um die Einstellungsänderung wirksam werden zu lassen, muss der Rechner neu gestartet werden.

Alternativer Dateimanager

Nach dem Laden eines Laufwerks können Sie sich dessen Inhalt anzeigen lassen. siehe Öffnen/Schließen Dazu wird der Windows Explorer gestartet. Sofern Sie einen anderen Dateimanager nutzen, können Sie ArchiCrypt Live anweisen, den Inhalt mit diesem anzuzeigen. Werfen Sie einen Blick in die Dokumentation des Dateimanager um herauszufinden, welche Kommandozeilenparameter das Programm unterstützt.

In Name der ausführbaren Datei tragen Sie bitte den Pfad und den Dateinamen des Dateimanagers ein. Der Dateimanager muss wissen, welches Laufwerk er anzeigen soll. Dies teilen Sie ihm über die s.g. Parameter mit.

Beispiel:
SpeedCommander
Sie können SpeedCommander aufrufen und als Parameter das anzuzeigende Laufwerk übergeben.

/ l: % lw %
% lw % ist hierbei ein Platzhalter, den ArchiCrypt Live durch den Laufwerksbuchstaben des anzuzeigenden Laufwerks ersetzt.

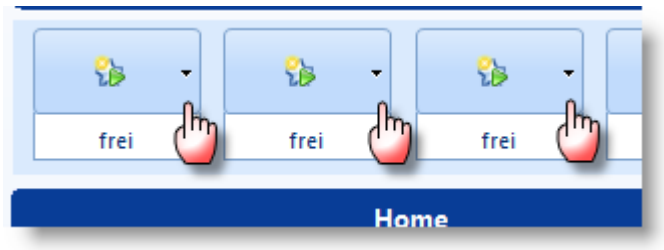
Tragen Sie diesen Parameter in das Feld Parameter [optional] ein.

Favoriten - Alphabetisch sortieren

Bei aktivierter Option werden Favoriten alphabetisch gelistet.

Verlauf - Zuletzt geöffnete Laufwerke merken

Bei aktivierter Option werden die Dateinamen der zuletzt genutzten 10 Live Laufwerke gemerkt. Diese stehen als Menü auf der Home-Seite bereit. Die Liste kann durch Klick auf den Pfeil bei einem der freien Speicherplätze aufgerufen werden.



Live Filter-Modul aktivieren / deaktivieren

ArchiCrypt Live bietet mittels eines speziellen Moduls (Filtertreiber) die Möglichkeit, Verzeichnisse umzuleiten und zu kontrollieren, welche Anwendungen auf Dateien in einem Laufwerk zugreifen dürfen. Da dieser Filter tief in das System eingreift, kann es durchaus vorkommen, dass sehr systemnahe Software mit diesen Funktionen nicht zurecht kommt.
Aus diesem Grund haben Sie hier die Möglichkeit, dass Filtermodul von ArchiCrypt Live bei Verdacht auf Inkompatibilität gesondert zu deaktivieren bzw. zu reaktivieren.

Einstellungen - Tastenkürzel

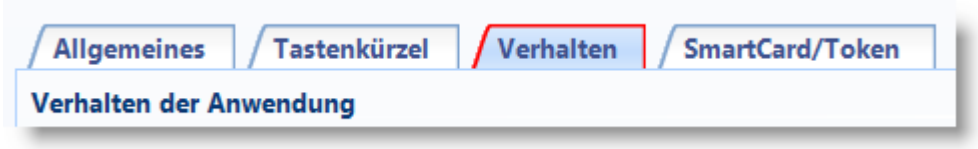
Alle Laufwerke Schließen
Laufwerksinhalt anzeigen
ArchiCrypt Live beenden

Diese Optionen bieten Ihnen die Möglichkeit, s.g. systemweite HOTKEYS (*Tastenkombinationen*) zu definieren. Systemweit bedeutet dabei, dass Sie, gleichgültig in welcher Anwendung Sie sich aktuell befinden, über diese Tastenkombinationen die zugehörigen Funktionen von ArchiCrypt Live aufrufen können.

Setzen Sie den Eingabecursor in das entsprechende Eingabefeld und betätigen Sie die Tastenkombination zum Auslösen des Ereignisses. Das Auswahlfeld aktivieren prüft, ob die Tastenkombination noch frei ist und aktiviert diese.

Eine Ausnahme sind die Tastenkombinationen zur Inhaltsanzeige von Laufwerken. Es wird zunächst untersucht ob die Kombinationen STRG+ 1..8 frei sind, anschließend ALT+1..8 und zuletzt STRG+ALT+1..8.
Die aktiven Tastenkombinationen werden Ihnen angezeigt.

Einstellungen - Verhalten



ArchiCrypt Live nach dem Start minimieren

ArchiCrypt Live wird nach dem Start sofort in den Infobereich (*Systemtray*) verkleinert.

Beim Beenden Zuletzt verwendete Dokumente löschen

Löscht Spuren in Zuletzt verwendete Dokumente Einstellungen von Windows

Notaus bei Alle schließen

Die Funktion Alle schließen wird ausgeführt, auch wenn auf den Laufwerken Dateiaktivitäten stattfinden. Die Schaltfläche Notaus auf der Home-Seite schließt die Laufwerke grundsätzlich ohne Rücksicht auf andere Anwendungen.

➡ WARNUNG! Ihr System kann dadurch instabil werden, im schlimmsten Fall kann es zu Datenverlust kommen.

siehe Öffnen/Schließen

Laufwerke automatisch schließen, wenn der Computer nicht benutzt wurde für ... Minuten

Wenn Sie Ihren Computer verlassen und vergessen haben, die Laufwerke zu schließen, übernimmt dies ArchiCrypt Live automatisch. Wird festgestellt, dass für die vorgegebene Zeit weder Tastatureingaben noch Mausbewegungen erfolgten, werden noch offene Laufwerke geschlossen.

Auslagerungsdatei beim Herunterfahren des Rechners überschreiben

Wird der Speicher (Hauptspeicher/RAM) knapp und wird eine Anwendung gerade nicht verwendet, kann Windows bestimmte Daten dieser Anwendung in die so genannte Auslagerungsdatei auf der Festplatte schreiben. Holen Sie diese Anwendung wieder in den Vordergrund und arbeiten weiter, lädt Windows die Daten neu in den Speicher und verschiebt ggf. Daten einer anderen Anwendung in die Auslagerungsdatei. Dies kann den unangenehmen Effekt haben, dass Daten, die Sie zum Beispiel mit einem Office Programm aus einem geöffneten Live Laufwerk laden, in Fragmenten in dieser Auslagerungsdatei landen. Äußerst schwer aufzuspüren, schwer zu rekonstruieren, aber durchaus kritisch. Bei aktivierter Funktion sorgt ArchiCrypt Live dafür, dass die in der Auslagerungsdatei abgelegten Daten sicher mit Nullen überschrieben werden.

➡ ACHTUNG *Das Herunterfahren Ihres Rechners wird dadurch ggf. verlangsamt!*

Autostart für ArchiCrypt Live Laufwerke

Falls Autostart aktiv ist, wird beim Öffnen eines Laufwerkes die mit Autostart festlegen festgelegte Datei automatisch gestartet.
(siehe Öffnen/Schließen)

Passwort merken bei Autostart mit Favorit

Sie können beim Festlegen von Favoriten definieren, dass ein Laufwerk beim Start automatisch geladen wird. Dabei erfolgt eine Passwortabfrage für jedes Laufwerk. Wurden mehrere Laufwerke mit gleichem Passwort/Schlüssel geschützt, erfolgt dennoch jedes mal eine Abfrage. Sofern Sie diese Option aktivieren, wird der Schlüssel nur 1 Mal abgefragt. Befindet sich jedoch ein Laufwerk mit anderem Passwort unter den Autostart-Favoriten, bricht das automatische Laden ab und das Passwort wird abgefragt.

Anwendungskontrolle automatisch einrichten

Hier können Sie zentral festlegen, ob beim Öffnen von ArchiCrypt Laufwerken automatisch die Liste mit Zugriffsregeln für Programme abgearbeitet wird.

Umleitung automatisch einrichten

Hier können Sie zentral festlegen, ob beim Öffnen von ArchiCrypt Laufwerken automatisch zuvor festgelegte Umleitungen aktiviert werden sollen.

Beim Einlegen eines Datenträgers mit einem Live Laufwerk automatisch nach dem Passwort fragen

ArchiCrypt Live ist nicht zuletzt deshalb so flexibel, weil man die s.g. Trägerdateien, die die eigentlichen Laufwerksdaten beinhalten auf beliebigen Medien ablegen kann. Sofern Sie diese Option ausgewählt haben, erkennt ArchiCrypt Live, wenn Sie einen Datenträger (*USB-Laufwerk, USB-Stick, CD, DVD*) einlegen, auf dem sich ein ArchiCrypt Live Laufwerk befindet. Automatisch wird nach dem zugehörigen Passwort gefragt und nach dessen korrekter Eingabe das Laufwerk geladen.

➡ACHTUNG: ***Es werden nur solchen Laufwerke erkannt, die die Dateiendung ACL Tragen! Die Trägerdatei muss sich auf dem Medium im Hauptverzeichnis (*nicht in einem Unterverzeichnis*) befinden!***

Notaus bei Schließen mit ArchiCrypt Card/Token

Beim Entfernen einer ArchiCrypt Card oder eines Security-Token werden geöffnete Laufwerke ohne Rücksicht auf geöffnete Dateien geschlossen.

➡ WARNUNG! Ihr System kann dadurch instabil werden, im schlimmsten Fall kann es zu Datenverlust kommen.

Beim Öffnen auf Signatur prüfen

ArchiCrypt Live prüft vor dem Laden einer Datei, ob diese digital signiert ist. Falls eine Signatur gefunden wird, besteht die Möglichkeit, diese zu verifizieren. Bitte beachten Sie, dass das Zertifikat mit öffentlichem Schlüssel des Absenders geladen sein muss!

siehe dazu: Signatur Prüfen

➡ACHTUNG: ***Diese Funktion wird nicht ausgeführt, wenn Sie ein Live Laufwerk per Doppelklick laden, die Auto-Ladeliste oder den Schnellzugriff nutzen!***

Beim Öffnen auf Schlüsselübermittlung prüfen

ArchiCrypt Live prüft vor dem Laden, ob die Datei mit Ihrem Öffentlichen Schlüssel abgesichert wurde. Sie können das ArchiCrypt Live Laufwerk dann mit Ihrem Privaten Schlüssel öffnen.

siehe dazu: Empfang mit Privatem Schlüssel

Live Laufwerk als "Lokales Laufwerk" laden

Wenn Sie Live Laufwerke als Lokales Laufwerk laden, wird das Live Laufwerk in etwa wie eine interne Festplatte behandelt. Das Laden als Lokales Laufwerk empfiehlt sich, wenn man eine Anwendungen auf einem Live Laufwerk installieren möchte, die sich nicht auf einem Wechsellaufwerk installieren lässt. Nachteil beim Laden als Lokales Laufwerk: Windows legt einen Papierkorb für das Laufwerk an. Dies äußerst sich nur optisch bei der Anzeige des Laufwerks im Dateimanager. Gelöschte Daten bleiben auf dem Live Laufwerk und landen nicht etwa außerhalb!!

Laufwerke beim Erstellen automatisch als NTFS Laufwerk erzeugen

ArchiCrypt Live Laufwerke stellen sich in Ihrem Computer wie ganz normale Laufwerke dar. Auch ArchiCrypt Live Laufwerke können formatiert werden und haben dann die normalen Eigenschaften, wie sie durch das Dateisystem vorgegeben sind. Eine Gegenüberstellung der verschiedenen Formate und Ihrer Vor- und Nachteile finden Sie unter Dateisysteme.

Bei aktivierter Funktion zeigt ArchiCrypt Live im Rahmen des Erstellvorgangs die Option Laufwerk als NTFS Laufwerk formatieren an. Die Auswahl ist bereits aktiv. Sie haben die Möglichkeit, die Auswahl zurückzunehmen und das Laufwerk im Dateisystem FAT erzeugen zu lassen.

Im Zusammenhang mit dieser Option gibt es folgende Besonderheiten zu beachten:

1. Um das Laufwerk im Dateisystem NTFS zu formatieren, benötigt ArchiCrypt Live Administratorrechte.
2. Ist die Option aktiviert und ArchiCrypt Live besitzt keine Administratorrechte, haben Sie beim Start des Erstellvorgangs die Möglichkeit zu wählen, ob Sie ArchiCrypt Live mit Administratorrechten neu starten zu lassen, oder das Laufwerk im Dateisystem FAT erzeugen zu lassen.

siehe auch: Dateisysteme

Auf Laufwerke älteren Typs nur lesend zugreifen

Diese Einstellung sorgt dafür, dass auf Laufwerk, die mit Version 5 oder älter erstellt wurden, im Nur-Lesen Modus geöffnet werden. Sie können also keine weiteren Daten auf das alte Laufwerk kopieren. Sie sollten Ihre Daten die sich auf Laufwerken befinden, die mit Version 5 oder älter erstellt wurden, grundsätzlich auf ein Laufwerk neuen Typs kopieren.

Laufwerke beim Beenden von ArchiCrypt Live automatisch schließen?

Sobald ArchiCrypt Live beendet wird, versucht ArchiCrypt Live geöffnete Laufwerke zu schließen.

Laufwerke beim Übergang in den Ruhe- oder Energiesparmodus automatisch schließen.

WICHTIGE INFORMATIONEN ZUM Ruhezustand und Energie sparen

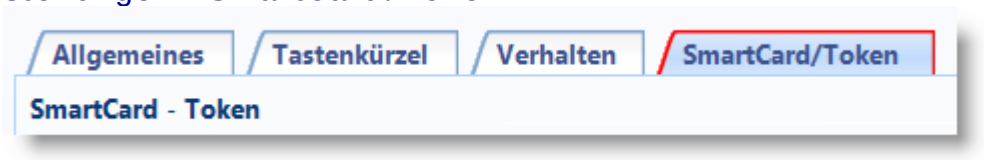
Wenn Sie Windows nicht herunterfahren, sondern den PC in den Ruhe- oder einen Energiesparmodus versetzen, wird der aktuelle Inhalt des Hauptspeichers auf dem Datenträger (*meist Festplatte C*) UNGESCHÜTZT abgelegt. Haben Sie beim Übergang in den Ruhe- oder Energiesparmodus ein Live Laufwerk geöffnet kann ein Angreifer mit direktem Zugang zu Ihrem Rechner mit speziellen Werkzeugen theoretisch Schlüsseldaten auslesen und mit diesen später Zugriff auf ein Live Laufwerk erhalten.

Sie sollten daher möglichst die Energiesparmodi vermeiden und den Rechner komplett herunterfahren oder zumindest die Laufwerke beim Übergang in den Ruhe- oder Energiesparmodus automatisch schließen lassen.

Wenn Sie diese Option aktivieren, dann wird versucht, geöffnete Live Laufwerke unter allen Umständen zu schließen und jegliche Schlüsselinformationen aus dem Speicher zu löschen. Die Gefahr, dass Windows Schlüsselmaterial ungesichert auf die Festplatte auslagert wird dadurch nahezu ausgeschlossen. Vermeiden können Sie dies generell, indem Sie den Rechner immer komplett herunterfahren. Ganz nebenbei sparen Sie hier die meiste Energie, da in diesem Fall der Rechner komplett ausgeschaltet ist.

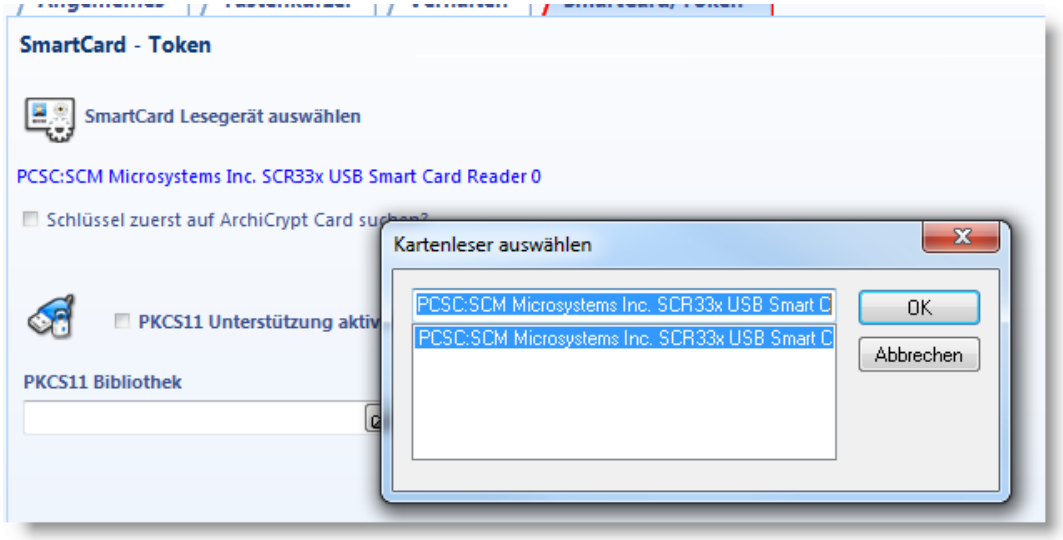
Siehe auch: Energiespar-Funktionen

Einstellungen - SmartCard/Token



SmartCard Lesegerät auswählen

Sie können den SmartCard Reader wählen, mit dem ArchiCrypt Live zusammenarbeiten soll.



➡ACHTUNG: ***Wählen Sie bitte keine Einträge die mit Debug beginnen!!!***

Schlüssel zuerst auf ArchiCrypt Card suchen

Falls Sie ein Laufwerk laden, wird bei eingeschalteter Option immer zuerst geprüft, ob sich eine ArchiCrypt Card mit einem Schlüssel im SmartCard Leser befindet. Wird ein Schlüssel gefunden, versucht ArchiCrypt Live das Laufwerk mit diesem Schlüssel zu öffnen.

PKCS11 Unterstützung aktivieren

Wenn Sie eine gültige PKCS11 Bibliothek angegeben haben, können Sie ArchiCrypt Live Laufwerke mit s.g. Security-Tokens schützen und Live Laufwerke automatisch beim Anschließen

oder Entfernen eines Token öffnen bzw. schließen lassen. Ihre Token Hardware muss zwingend den PKCS#11 Standard erfüllen Die bei PKCS11 Bibliothek einzutragende Datei entnehmen Sie bitte der Dokumentation Ihres Token oder erfragen sie beim Hersteller der Token Hardware. Die Namen einiger Bibliotheken haben wir Ihnen in einer Liste bereitgestellt.

Ob die von Ihnen ausgewählte Datei dem Standard entspricht, können Sie durch Klick auf die Schaltfläche Prüfen feststellen.

siehe auch: ArchiCrypt Card / Token
Liste mit Token Bibliotheken

Arbeitsgruppe

Arbeitsgruppen-Optionen verwenden

Sobald LAN Kommunikation oder Cloud Kommunikation aktiviert wurden, wird beim Zugriff auf eine Live Laufwerk-Datei eine Datei im Verzeichnis der Laufwerk-Datei angelegt. Diese Datei trägt den Namen der Laufwerkdatei und hat die Dateiendung acn (ACN Datei). Diese Datei ist nötig, damit verschiedene Anwender sich über Blockierung und Freigabe von Live Laufwerken austauschen können. Die Datei kann, sofern das zugehörige Live Laufwerk auf allen Rechnern entladen ist, ohne jede Gefahr gelöscht werden.

LAN-Kommunikation aktiv

Sofern die Option ausgewählt ist, kann man beim Versuch, ein bereits mit Schreibrechten geöffnetes Live Laufwerk ebenfalls mit Schreibrechten zu öffnen, eine Nachricht an den aktuellen Schreiber senden. Wird das Live Laufwerk von diesem freigegeben, erhält der anfordernde Anwender eine Nachricht, dass das schreibende Laden jetzt möglich ist.

Automatische Aktualisierung

Sofern ein Anwender ein Laufwerk lesend geöffnet hat und ein anderer Anwender Daten schreibt, kann man über diese Funktion eine Aktualisierung der Ansicht auf das

Laufwerk forcieren.

Cloud-Kommunikation aktiv
Sie können mit mehreren Anwendern auf ein Live Laufwerk in der Cloud zugreifen. Allerdings haben Cloud Dienste generell ein gravierendes Problem, welches mit dieser Option in ArchiCrypt Live lediglich abgemildert werden kann. Cloud Dienste blockieren eine Datei (*ein Live Laufwerk ist letztlich auch eine Datei*) nicht, wenn sie
diese schreibend öffnen. Theoretisch können also beliebig viele Anwender ein Live Laufwerk aus der Cloud mit Schreibrechten öffnen und darin Daten ändern. Das Chaos entsteht dann, wenn die Datei wieder gespeichert wird. Plötzlich liegen mehrere Versionen der Datei vor. Die Cloud meldet einen Konflikt. Datenverlust tritt nicht auf, aber man muss mühsam die Daten der verschiedenen Versionen wieder synchronisieren. Dies kann auch bei Live Laufwerken auftreten. ArchiCrypt Live versucht dieses Problem zu lösen, indem es den Zugriff ausschließlich über die ACN Datei (*siehe LAN Kommunikation*) steuert. Dies funktioniert dann gut, wenn nicht zufällig zeitgleich durch mehrere Anwender auf die Clouddaten zugegriffen wird.

Anwenderkonto
Hier werden Informationen aufgelistet, die Sie bei der Kommunikation mit anderen Anwendern eindeutig identifizieren. Die Daten entstammen den Systeminformationen und können in ArchiCrypt Live lediglich gelesen werden!

10.4.12 Kommandozeile

siehe auch: Parameter bei mobilen Live Laufwerken

Kommandozeile / Parameter

Mit Hilfe von Parametern, die Sie beim Start an ArchiCrypt Live übergeben können, ist es möglich, dateibasierte Live Laufwerke automatisch zu laden und zu schließen. Insbesondere fortgeschrittene Nutzer werden die Funktionen zu schätzen wissen. Sehr einfach kann man so in einer Batchdatei zum Beispiel ein Live Laufwerk öffnen, Daten darauf sichern und das Live Laufwerk anschließend wieder schließen. Auch der Aufruf aus anderen Anwendungen heraus ist somit sehr leicht möglich.

Allgemeiner Aufbau der Kommandozeile

<Pfad zu ArchiCrypt Live > <Pfad und Dateiname zur Trägerdatei> [/r] [/d=Laufwerksbuchstabe] [/f] [/u] [/ua] [p=<Passwort>] [k=<Passwortdatei>] [/q] [/qa]

Groß-/Kleinschreibung spielt bei der Übergabe der Parameter (*Ausnahme Passwort*) keine Rolle. /d=x hat die gleiche Wirkung wie /D=X

Schließen Sie Pfad- und Dateinamen immer in Anführungszeichen ("Pfad/Dateiname") ein. Leerzeichen in Pfad- und Dateinamen führen ansonsten zu Fehlern! In den Beispielen finden Sie die korrekte Notation.
Sie können den Pfad zu ArchiCrypt Live in die Path Variable des Systems übernehmen. Sie können ArchiCrypt Live dann aus jedem Verzeichnis heraus nur mit dem Dateinamen alleine aufrufen.

Parameter

➡ACHTUNG: ***Beim Aufruf von ArchiCrypt Live über die Kommandozeile werden ggf. Schnellzugriffe abgearbeitet. Für Schnellzugriffe mit aktivierter Option*** Beim Start von ArchiCrypt Live automatisch laden***, werden ggf. Schlüssel erfragt. Um dies zu vermeiden, verwenden Sie einen der Schalter*** /q ***oder*** /qa***!***

/d=<Laufwerksbuchstabe>

Wenn Sie ein Live Laufwerk laden möchten, müssen Sie einen freien Laufwerksbuchstaben angeben.
Möchten Sie ein bestimmtes Live Laufwerk schließen, übergeben Sie hier den Laufwerksbuchstaben des zu schließenden Live Laufwerks.

Beispiel:
Wir öffnen das Live Laufwerk Q:\123.acl als Wechsellaufwerk und machen es unter dem Laufwerksbuchstaben X im System verfügbar.

```
"C:\Programme\ArchiCrypt Live\ACLive8.exe" "Q:\123.acl" /d=X
```

Wir schließen das gleiche Laufwerk

```
"C:\Programme\ArchiCrypt Live\ACLive8.exe" /d=X /u
```

/r

Das Live Laufwerk wird im Nur Lesen Modus geöffnet. Fehlt der Schalter, wird das Laufwerk im Modus Schreiben & Lesen geöffnet.

Beispiel:
Wir öffnen das Live Laufwerk Q:\123.acl als Wechsellaufwerk im Modus Nur Lesen und machen es unter dem Laufwerksbuchstaben X im System verfügbar.

```
"C:\Programme\ArchiCrypt Live\ACLive8.exe" "Q:
\123.acl" /d=X /r
```

/f

Lädt das Laufwerk als lokales Laufwerk. Fehlt der Schalter, wird das Laufwerk als Wechsellaufwerk geladen.

Beispiel:
Wir öffnen das Live Laufwerk Q:\123.acl als lokales Laufwerk und machen es unter dem Laufwerksbuchstaben X im System verfügbar.

```
"C:\Programme\ArchiCrypt Live\ACLive8.exe" "Q:
\123.acl" /D=X /ef
```

/u

Schließen eines Laufwerks die Angabe des Parameters */d=<Laufwerksbuchstabe>* ist zwingend!

Beispiel:
Wir schließen das Laufwerk, welches aktuell unter dem Laufwerksbuchstaben X geladen ist.

```
"C:\Programme\ArchiCrypt Live\ACLive8.exe" /d=X /u
```

/ua

Schließt alle geladenen Laufwerke

Beispiel:
Wir schließen alle zur Zeit geöffneten Laufwerke.

```
"C:\Programme\ArchiCrypt Live\ACLive8.exe" /ua
```

/p=[Passwort]

Nutze das in der Kommandozeile übergebene Passwort zum Öffnen des Laufwerks

Beispiel:
Wir öffnen das Live Laufwerk Q:\123.acl als Wechsellaufwerk und machen es unter dem Laufwerksbuchstaben X im System verfügbar.
Dazu soll ArchiCrypt Live das Passwort 123 nutzen.

```
"C:\Programme\ArchiCrypt Live\ACLive8.exe" "Q:
\123.acl" /d=X /p=123
```

/k=<Passwortdatei>

Hier können Sie einen Pfad zu einer Textdatei (*nicht Schlüsseldatei!!!*) angeben, in der der Schlüssel für das Laufwerk zu finden ist. Angabe hat in der Form -k="Dateiname" zu erfolgen.

Beispiel:
Wir öffnen das Live Laufwerk Q:\123.acl als Wechsellaufwerk und machen es unter dem Laufwerksbuchstaben X im System verfügbar.
Dazu soll ArchiCrypt Live das Passwort aus der Datei "O:\Pass.txt" nutzen.

```
"C:\Programme\ArchiCrypt Live\ACLive8.exe" "Q:
\123.acl" /d=X /k="O:\Pass.txt"
```

/q

Schließt ArchiCrypt Live (*die Instanz der wir den Parameter übergeben*) nach dem Öffnen des angegebenen Laufwerks. Eine eventuell durch den Nutzer bereits gestartete Instanz bleibt geöffnet.

Beispiel:
Wir öffnen das Live Laufwerk Q:\123.acl als Wechsellaufwerk und machen es unter dem Laufwerksbuchstaben X im System verfügbar.
ArchiCrypt Live (die Instanz, der wir den Parameter übergeben) soll nach dem Laden geschlossen werden. Zum Öffnen soll das Passwort 123 genutzt werden.

```
"C:\Programme\ArchiCrypt Live\ACLive8.exe" "Q:
\123.acl" /d=X /p=123 /q
```

/qa

Schließt auch eine bereits aktive ArchiCrypt Live Instanz nach Abschluss der Aktion (*Öffnen/Schließen*).

Beispiel:
Wir öffnen das Live Laufwerk Q:\123.acl als Wechsellaufwerk und machen es unter dem Laufwerksbuchstaben X im System verfügbar.
Alle ArchiCrypt Live Instanzen (auch eine eventuell bereits aktives ArchiCrypt Live des Benutzers) sollen nach dem Laden geschlossen werden. Zum Öffnen soll das Passwort 123 genutzt werden.

```
"C:\Programme\ArchiCrypt Live\ACLive8.exe" "Q:
\123.acl" /d=X /p=123 /qa
```

10.4.13 Favoriten

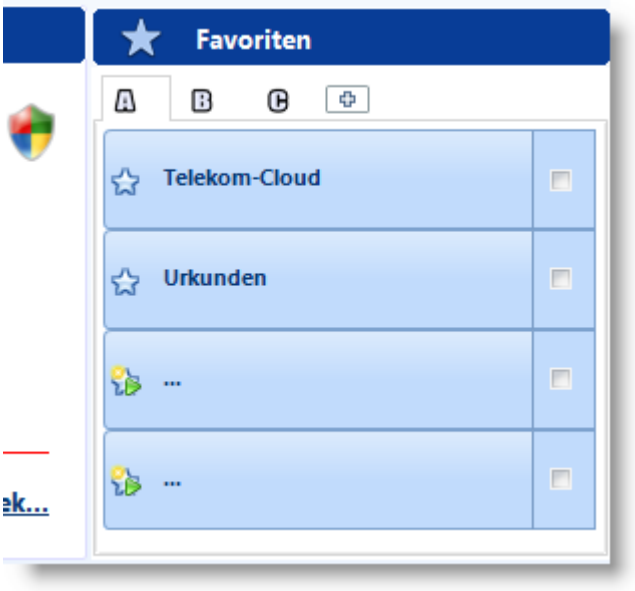
Sollten sich die nachfolgenden Videos im Browser nicht anzeigen lassen, so können Sie die Videos alternativ direkt in Youtube auf unserem ArchiCrypt Kanal ansehen.

Video - Favoriten

siehe auch: Aktive Laufwerke

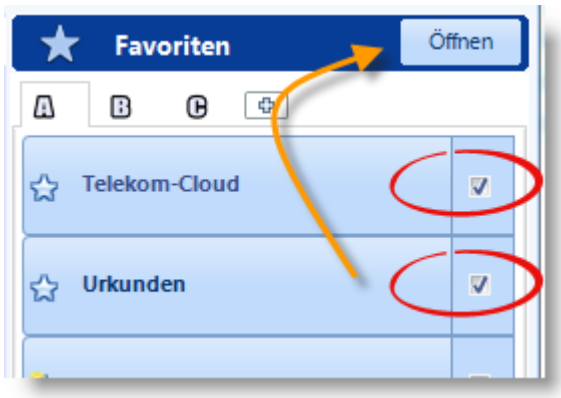
Schneller Zugriff auf häufig genutzte Laufwerke

Mit Hilfe der Favoriten lässt sich der Umgang mit häufig verwendeten ArchiCrypt Live Laufwerken extrem komfortabel gestalten. Unabhängig von den Dateinamen können Sie jedem Favoriten einen "Sprechenden Namen" zuordnen. Über Favoriten können Sie ArchiCrypt Live auch anweisen, bestimmte Laufwerke beim Start zu laden, auf Einfügen und Entfernen von ArchiCrypt Card oder Security-Token zu reagieren oder Laufwerke nach Eingabe eines Magic Word (*magische Zeichenfolge*) in beliebiger Anwendung, zu laden oder zu schließen. Für fortgeschrittene Nutzer bieten die Favoriten die Möglichkeit, Kommandos festzulegen, die vor/nach dem Öffnen oder cor/nach dem ausgeführt werden sollen.



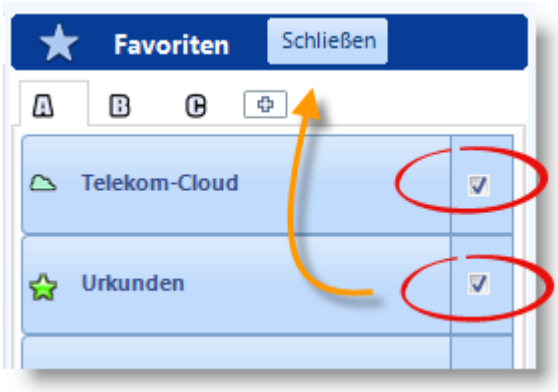
So laden bzw. schließen Sie mehrere Favoriten gleichzeitig

Neben den Favoriten befinden sich Auswahlkästchen. Wenn Sie ein Häkchen neben einem nicht aktivierten Laufwerk setzen, erscheint eine Schaltfläche Öffnen im Titel der Favoriten.



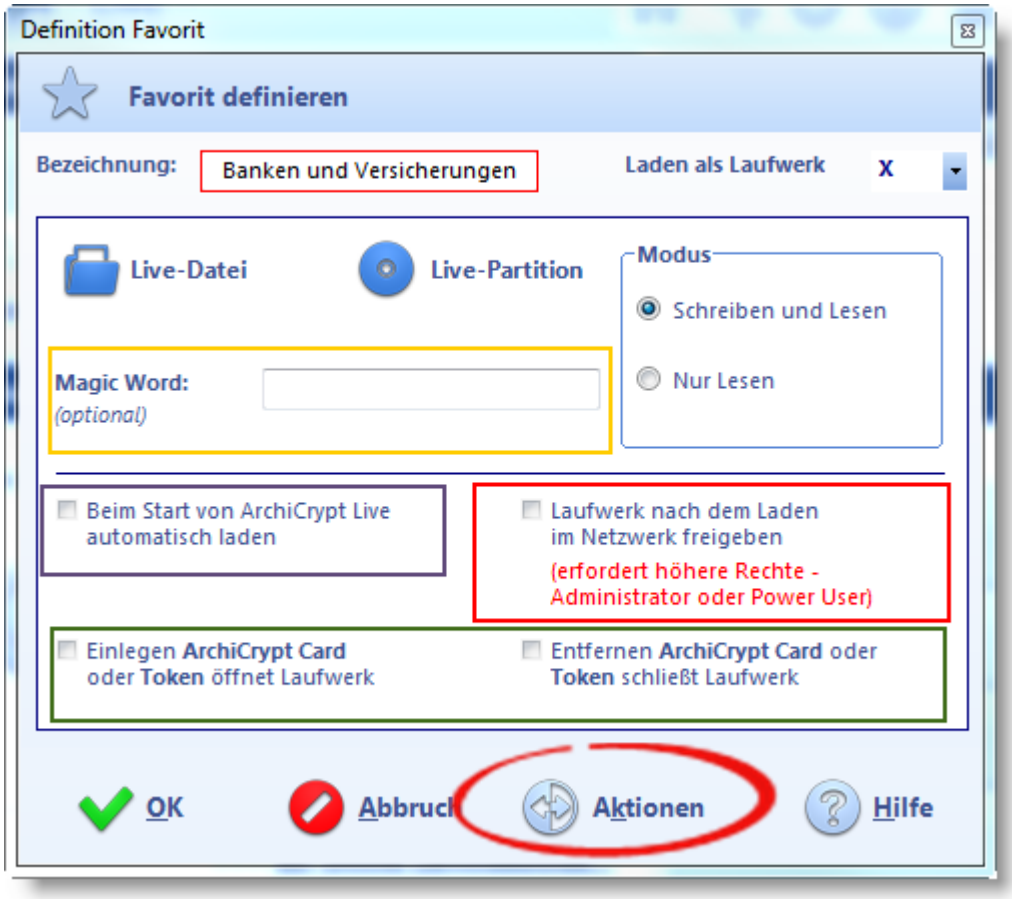
Haben Sie für die ausgewählten Favoriten das selbe Passwort gewählt, wird das Passwort nur ein Mal abgefragt.

Zum Schließen können Sie ein Häkchen neben geladene Favoriten setzen und dann die Schaltfläche Schließen betätigen.



So erstellen Sie einen Favoriten

Ein noch nicht belegter Favoritenplatz trägt keine Bezeichnung. Sobald Sie auf den freien Platz klicken, öffnet sich der Dialog zur Definition des Favoriten.



Tragen Sie unter Bezeichnung einen sprechenden Namen ein. Legen Sie dann bei Laden als Laufwerk den Laufwerksbuchstaben fest, unter dem das ArchiCrypt Live Laufwerk nach dem Laden im System erreichbar sein soll. Wählen Sie jetzt die "Live Datei" (dateibasiertes Live Laufwerk) oder die "Partition" (Live Partition) aus und legen Sie bei Modus fest, ob das Laufwerk mit Nur Lesezugriff oder mit Lese-/Schreibrecht geöffnet werden soll. Mehr Angaben sind nicht nötig, Sie können den Favoriten durch Klick auf die OK Schaltfläche übernehmen.

➡ACHTUNG: Der Modus wird auch durch die Art des Passwortes/Schlüssels bestimmt. Auch wenn Sie hier Modus Schreiben und Lesen wählen, können Sie mit einem "Gast Nur-Lesen-Schlüssel" nicht schreibend auf das Laufwerk zugreifen!

Beim Start von ArchiCrypt Live automatisch laden

Wird ArchiCrypt Live gestartet, wird automatisch auch dieses Laufwerk geladen. Kombinieren Sie diese Option mit "Mit Windows starten" unter Einstellungen Allgemeines, um Laufwerke direkt beim Start von Windows zu laden.

Ausnahme: Wird ArchiCrypt Live über Kommandozeile mit dem Parameter /q oder /qa aufgerufen, werden keine Favoriten abgearbeitet.

Automatisch nach dem Öffnen Inhalt im Windows Explorer anzeigen

Ä: Version 8.8.6

Sie können bei den Favoriten festlegen, dass nach dem Öffnen automatisch ein Explorer Fenster geöffnet wird, welches den Inhalt des Live Laufwerks anzeigt.

Laufwerk nach dem Laden im Netzwerk freigeben

Ist die Option aktiviert, versucht ArchiCrypt Live das neu geladene Laufwerk im Netzwerk freizugeben. Die Freigabe erfolgt für alle mit Vollzugriff. Wird das Laufwerk über den Favoriten geschlossen, wird vor dem Schließen versucht, die Freigabe aufzuheben.

Der Datenverkehr im Netzwerk ist dabei nicht abgesichert. Die Daten werden unverschlüsselt übertragen. Um Daten verschlüsselt im Netzwerk übertragen zu können, nutzen Sie die Arbeitsgruppen-Option. Sie müssen die Live Laufwerk-Datei an einem Ort abspeichern, der durch die Anwender erreichbar ist, die mit der Datei arbeiten sollen.

➡ACHTUNG: ***Die Option Netzwerkfreigabe wirkt sich nur aus, wenn ArchiCrypt Live mit Administratorrechten gestartet ist!***

ArchiCrypt Card / Token

Diese Funktionen stehen nur dann zur Verfügung, wenn Sie einen SmartCard Leser bzw. den Security Token installiert haben. Der SmartCard Leser muss den PC/SC Standard erfüllt, der Token den PKCS#11 Standard. Die Hardware muss in ArchiCrypt Live entsprechend eingerichtet sein.
Sie benötigen ggf. eine ArchiCrypt Card.

siehe dazu: Einstellungen-SmartCard/Token

Einlegen ArchiCrypt Card oder Token öffnet Laufwerk

Erkennt ArchiCrypt Live, dass eine ArchiCrypt Card oder ein Security Token angeschlossen wurde, versucht es, die Laufwerke mit aktivierter Funktion im Schnellzugriff zu laden. Ist die ArchiCrypt Card mit einer PIN geschützt, muss die PIN 1 Mal eingegeben werden. ArchiCrypt Live merkt sich die PIN bis zum Beenden.

Beim Anschließen eines Token wird immer zur Eingabe der PIN aufgefordert. siehe dazu: Schlüssel von Token nutzen

Möchten Sie nicht, dass beim Anschließen der ArchiCrypt Card /Token Laufwerke geladen werden, halten Sie die CTRL- bzw Strg-Taste gedrückt.

Entfernen der ArchiCrypt Card schließt Laufwerk

Erkennt ArchiCrypt Live, dass eine ArchiCrypt Card oder ein Token entfernt wurde, versucht es, die Laufwerke mit aktivierter Funktion im Schnellzugriff zu schließen.

Möchten Sie nicht, dass beim Entfernen der ArchiCrypt Card /des Token Laufwerke geschlossen werden, halten Sie beim Entfernen die CTRL- bzw. Strg-Taste gedrückt.

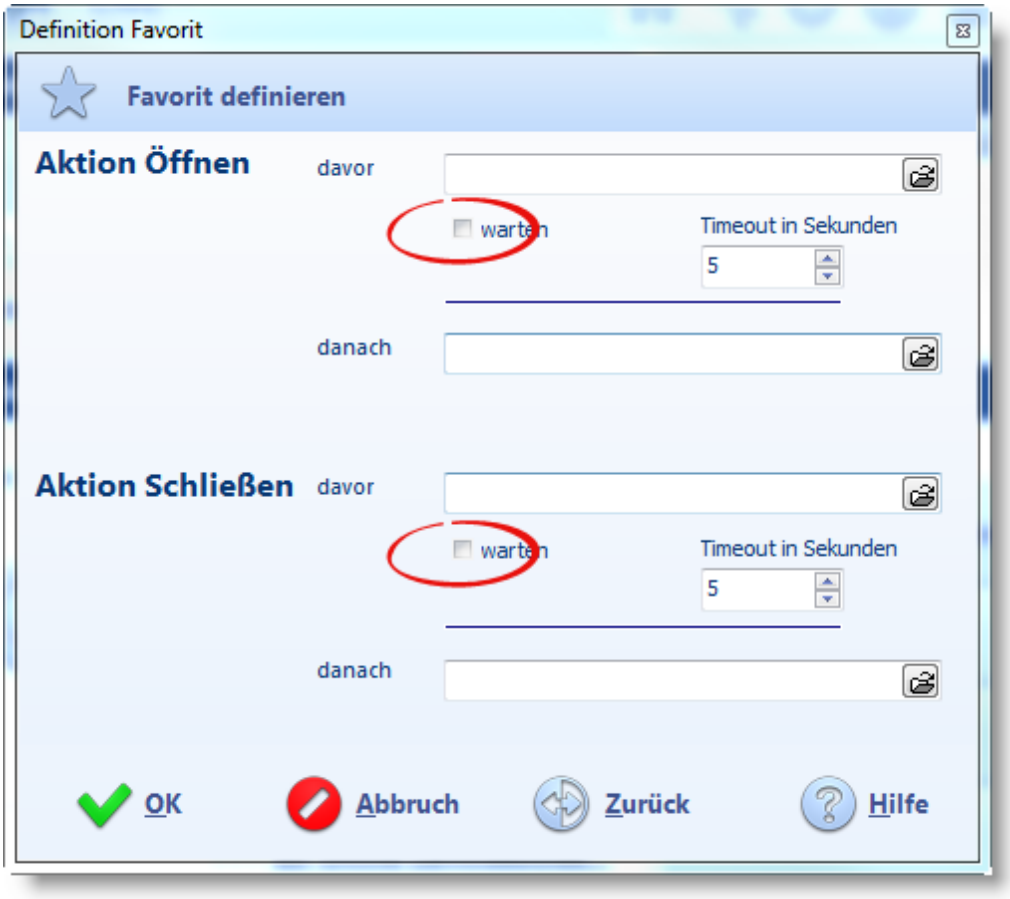
Magic Word

Ein Magic Word ist eine "magische" Zeichenfolge. Wird diese Zeichenfolge in einer beliebigen Anwendung eingegeben, erfragt ArchiCrypt Live das Passwort für das zugeordnete Laufwerk und öffnet es. Ist das zugeordnete Live Laufwerk geöffnet, wird es bei Eingabe des Magic Word wieder geschlossen.

Das Magic Word kann auch ins "Leere" (*einfach auf der Tastatur eintippen*) eingegeben werden. Die Zeichenfolge muss also nicht als Text zu sehen sein! Es empfiehlt sich, eine Zeichenfolge zu wählen, die so als Wort nicht vorkommt (Beispiel #sesam). Sie können Laufwerke gruppieren, indem Sie ihnen das gleiche Magic Word zuordnen.

Aktionen festlegen

Mit den Favoriten können Sie Aktionen festlegen, die vor/nach dem Laden oder vor/nach dem Schließen ausgeführt werden sollen. Für versierte Nutzer bieten sich hier zahlreiche Möglichkeiten. Sie können Pfade zu Programmen festlegen oder zu selbst geschriebenen Script-, Batch- oder cmd-Dateien.



Falls Sie Aktionen vor dem Öffnen oder Schließen ausführen, können Sie ArchiCrypt Live Anweisen, auf die Beendigung dieser Aktion zu warten. Falls die Aktion nach der in Timeout in Sekunden angegebenen Zeit nicht beendet ist, fährt ArchiCrypt

Live fort. Achten Sie darauf, dass das Warten ArchiCrypt Live blockiert und während dieser Zeit keine anderen Aktionen ausgeführt werden können (*dies betrifft nicht die Verfügbarkeit und Ansprechbarkeit der geladenen Live Laufwerke*).

Sie können durch Klick auf das kleine Verzeichnissymbol im Windows-Dialog eine Datei auswählen oder manuell in das jeweilige Feld eingeben.

Sie können einer Anwendung (*.exe) bestimmte Schlüsselwörter voranstellen um diese zu beenden! Es genügt dann die Angabe des Dateinamens der Anwendung (*z.B. firefox.exe*).

Terminate
Beendet die Anwendung ohne Rücksicht darauf, ob diese noch aktiv ist und gegebenenfalls nicht abgespeicherte Daten hat.

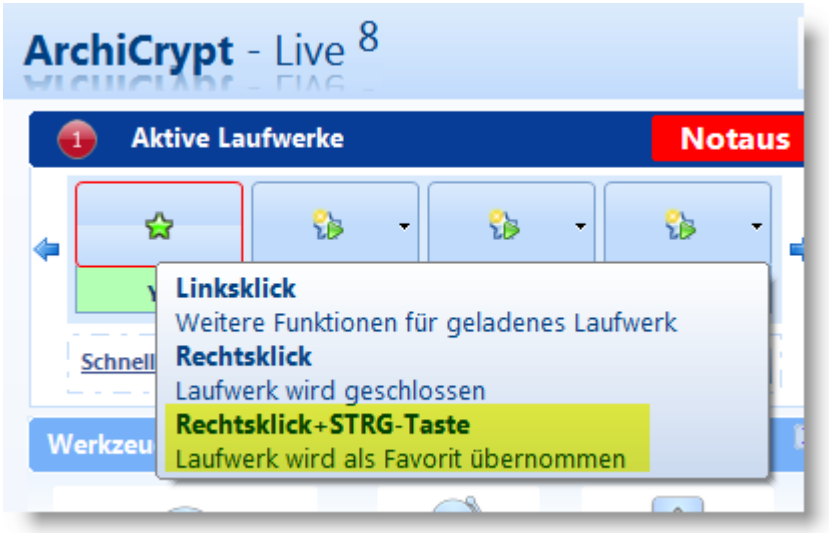
Close oder Quit
Versucht die Anwendung regulär zu beenden. Dabei kann es sein, dass die Anwendung einen Dialog zum Speichern oder andere Dialoge anzeigt, die Sie manuell schließen müssen!

Falls Firefox aktiv ist, wird die Anwendung unter allen Umständen geschlossen. Dabei wartet ArchiCrypt Live maximal 20 Sekunden, bis mit den Schließen fortgefahren wird.

Weitere Möglichkeiten zum Anlegen eines Favoriten

1. Wenn Sie ein neues ArchiCrypt Live Laufwerk erstellen, können Sie das gerade erzeugte Laufwerk als Favorit übernehmen.

2. Wenn Sie ein Live Laufwerk geladen haben, dann halten Sie die Steuerungstaste (*Strg oder Ctrl*) gedrückt und betätigen über dem Speicherplatz die RECHTE Maustaste.



Der Dateiname und der aktuelle Laufwerksbuchstabe werden im Favoritendialog vorbelegt.

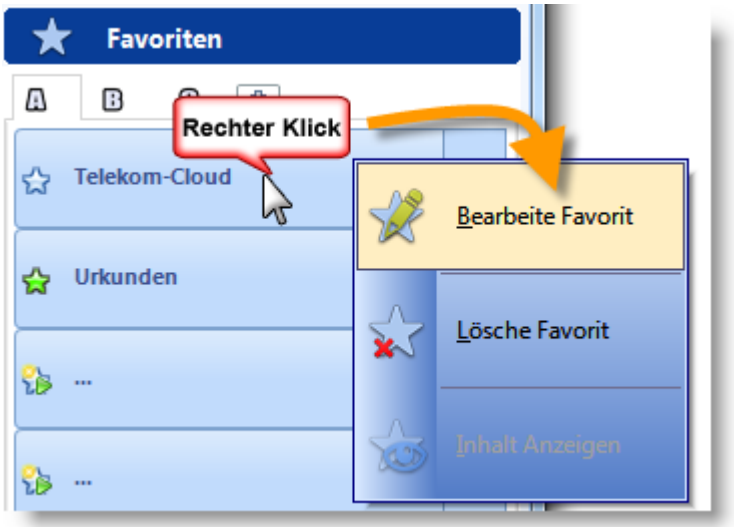
So löschen Sie einen Favoriten

Um einen Favoriten freizugeben, bewegen Sie den Mauszeiger über den Speicherplatz, betätigen die rechte Maustaste und rufen im Kontextmenü den Befehl Lösche Favorit auf.

➡HINWEIS: Sie werden zusätzlich gefragt, ob Sie die zugehörige Datei löschen möchten. Sofern Sie dies wünschen, wird die Datei gelöscht und alle Inhalte des verschlüsselten Live Laufwerks sind unwiederbringlich gelöscht.

So bearbeiten Sie einen Favoriten

Klicken Sie mit der rechten Maustaste auf den Favorit, den Sie bearbeiten möchten. Wählen Sie im Kontextmenü den Eintrag Bearbeite Favorit.



So laden Sie einen Favoriten

Linksklicken Sie auf den Speicherplatz des ungeladenen Favoriten. Sie werden nach dem Schlüssel gefragt. Anschließend wird das Laufwerk geladen.

Der Favorit wird mit grünem Stern dargestellt, wenn das Laufwerk mit Schreibrechten geöffnet wurde und mit rotem Stern, wenn es schreibgeschützt (Daten können nicht geändert werden) geladen wurde.

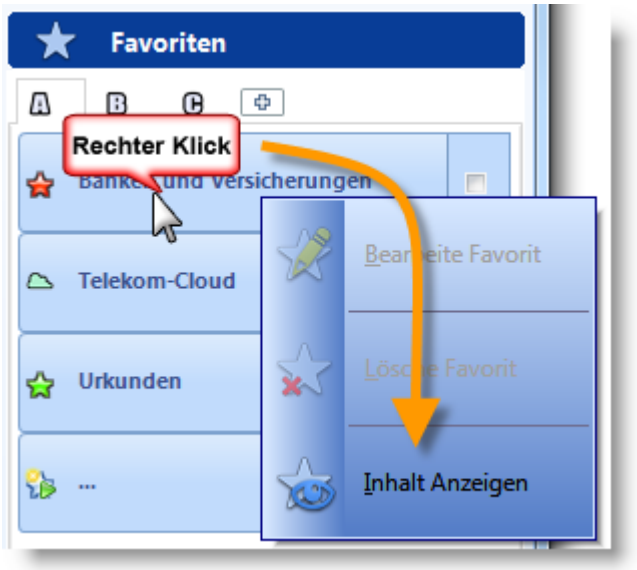
ist kein Laufwerk geladen, wird ein blauer Stern angezeigt.

So schließen Sie den Favoriten

Ist das Laufwerk, welches mit dem Schnellzugriff verknüpft ist, geladen (grüner oder roter Stern/Wolke als Symbol), genügt ein Linksklick auf den Speicherplatz. Sie können das Laufwerk auch durch Linksklick auf die zugehörige Schaltfläche bei den aktiven Laufwerken schließen.

So lassen Sie sich den Inhalt eines Favoriten anzeigen

Sofern das Laufwerk geladen wurde (grüner oder roter Stern als Symbol), können Sie im Kontextmenü (rechte Maustaste über dem entsprechenden Speicherplatz betätigen) den Punkt Inhalt anzeigen aufrufen.



siehe auch: Aktive Laufwerke

10.5 Dialoge

10.5.1 Passwortdialog

Passworteingabe - Schlüsseldatei - SmartCard - Token

Es gibt zwei verschiedene Dialoge. Den Dialog zur Eingabe eines vorhandenen Passworts, und den Dialog zur Festlegung eines neuen Passworts. Beachten Sie bitte das gesonderte Kapitel über Passwörter im technischen Teil. ArchiCrypt Live bietet einige Besonderheiten an, um Ihre Daten umfassend zu sichern.

Eine sehr lästige Gefahr geht von s.g. Trojanern (*Bezeichnung für ein Programm, das die Benutzeroberfläche eines anderen Programms nachahmt, oder vorgibt, eine bestimmte Funktion zu haben, tatsächlich jedoch Daten ausspioniert*) aus. Diese Programme protokollieren jeden Einzelnen Buchstaben den Sie eingeben und können so jedes Passwort, welches über Tastatur eingegeben wird, weiterleiten. Programme mit diesen Eigenschaften werden auch Keylogger genannt.

Die Keylogger haben bei ArchiCrypt keinen Erfolg, wenn Sie die s.g. Virtuelle Tastatur nutzen.

Eingabe eines Schlüssels (Abfrage)

Geben Sie in das Eingabefeld Direkteingabe das notwendige Passwort ein, betätigen Sie anschließend die <Eingabe> Taste oder die Schaltfläche OK. Wenn Sie das Passwort im Klartext sehen möchten, betätigen Sie die Schaltfläche *. Deutlich sicherer ist hingegen die Eingabe mit Hilfe der virtuellen Tastatur. Hier haben Keylogger keine Chance.

Handelt es sich um einen Schutz mit einer Schlüsseldatei, können Sie über die Schaltfläche Schlüsseldatei , den Dialog zum Einlesen einer Schlüsseldatei aufrufen, falls Sie eine ArchiCrypt Card nutzen betätigen Sie die Schaltfläche SmartCard, bei Einsatz eines Security-Token die Schaltfläche Token.

siehe dazu ArchiCrypt Card einlesen
Schlüssel von Token nutzen
Virtuelle Tastatur

Eingabe eines neuen Passwortes (Festlegen)

Geben Sie Ihr Passwort ein. Um sicherzustellen, dass Sie sich bei der Eingabe nicht vertippt haben, geben Sie das Passwort bei Passwort (Wiederholung) nochmals ein. ArchiCrypt Live bewertet Ihr Passwort nach einem ausgeklügelten Verfahren. Unter anderem wird Ihr Passwort daraufhin untersucht, ob es in einem von Hackern verwendeten Wörterbuch vorkommt.

Über die Schaltfläche  können Sie das Passwort sichtbar machen bzw. bei nochmaligem Betätigen, verbergen.

Nachdem Sie in die beiden Passworteingabefelder das gleiche Passwort eingegeben haben, können Sie durch Betätigen der Schaltfläche Übernehmen den Dialog beenden.

Sie können Ihr Passwort zur Sicherheit auch über die Virtuelle Tastatur eingeben.

Technik: *Für Datendiebe gibt es im Internet vorgefertigte Wörterbücher in denen Begriffe aus den wichtigsten Sprachen der Welt zusammengestellt sind. Ebenfalls enthalten sind sehr häufig verwendete Passwörter wie qwertz, LAKERS, 123456, arschloch, schatz, nadine, monkey etc. Mit Hilfe dieser Wörterbücher greifen Datendiebe Seiten im Internet an und versuchen so an geschützte Zugänge bei eBay, PayPal, Postbank, Volksbank und Co. zu gelangen. Auch*

verschlüsselte Dateien auf Ihrem Rechner werden damit angegriffen. ArchiCrypt Live nutzt Wörterbücher, die um die gesamte deutsche Wikipedia ergänzt sind und testet Ihr Passwort in Echtzeit gegen fast 27 Millionen Einträge. Sie erfahren direkt, ob ein Angreifer Ihren Zugang innerhalb von wenigen Augenblicken knacken kann.

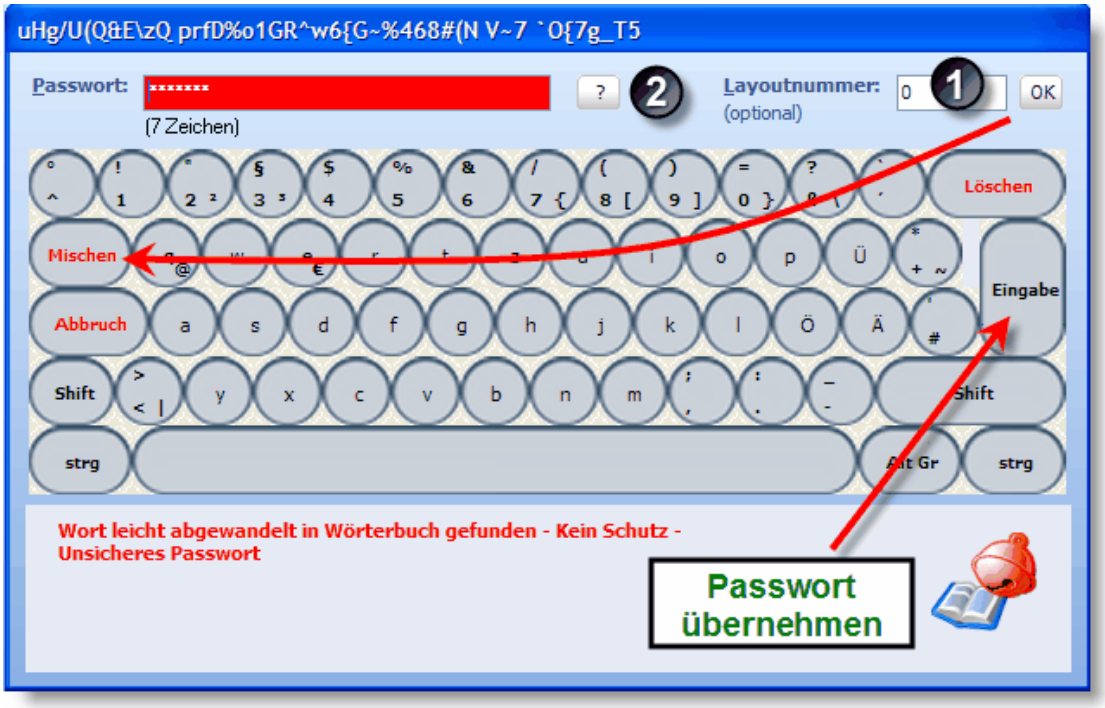
siehe auch Virtuelle Tastatur

10.5.2 Virtuelle Tastatur

siehe auch Passwortdialog

Virtuelle Tastatur zur Eingabe eines Passwortes

Die virtuelle Tastatur ist ein wirksames Mittel gegen s.g. Key-Logger, die jede Eingabe in eine normale Tastatur protokollieren können.



Hinweise:
Die Titelleiste trägt bewusst eine zufällige und unsinnige Bezeichnung. Dies hindert Spionageprogramme daran, das Fenster anhand des Titels zu identifizieren.

Bedienung:

Wenn Sie bei 1 eine Layoutnummer (*Werte von 0 .. 65565*) eingeben, werden die Zeichen auf der Tastatur an anderen Positionen angezeigt. Dies erschwert zusätzlich das Ausspähen von Mausbewegungen.

Mit der Taste Eingabe übernehmen Sie das angegebene Passwort, Löschen löscht das Passwort. Mischen hat die gleiche Wirkung wie die OK Schaltfläche bei 1, zeigt also nur Wirkung, wenn Sie eine neue Layoutnummer eingeben. Mit Abbruch, brechen Sie die Eingabe des Passwortes ab.

Über ? bei 2, können Sie sich das eingegebene Passwort in einem Dialog anzeigen lassen.

Im Feld Passwort (*oben links*) sehen Sie nur die Länge des von Ihnen eingegebenen Passwortes, nicht das Passwort selbst.

10.5.3 Schlüsseldatei erstellen

Sollten sich die nachfolgenden Videos im Browser nicht anzeigen lassen, so können Sie die Videos alternativ direkt in Youtube auf unserem ArchiCrypt Kanal ansehen.

Video - Passwort zu Schlüsseldatei

siehe auch: Schlüsseldatei laden

Erstellen einer Schlüsseldatei

Es gibt zwei verschiedene Arten von Schlüsseldateien.

1. Schlüsseldatei, die den Schlüssel offen, also unverschlüsselt enthält

und

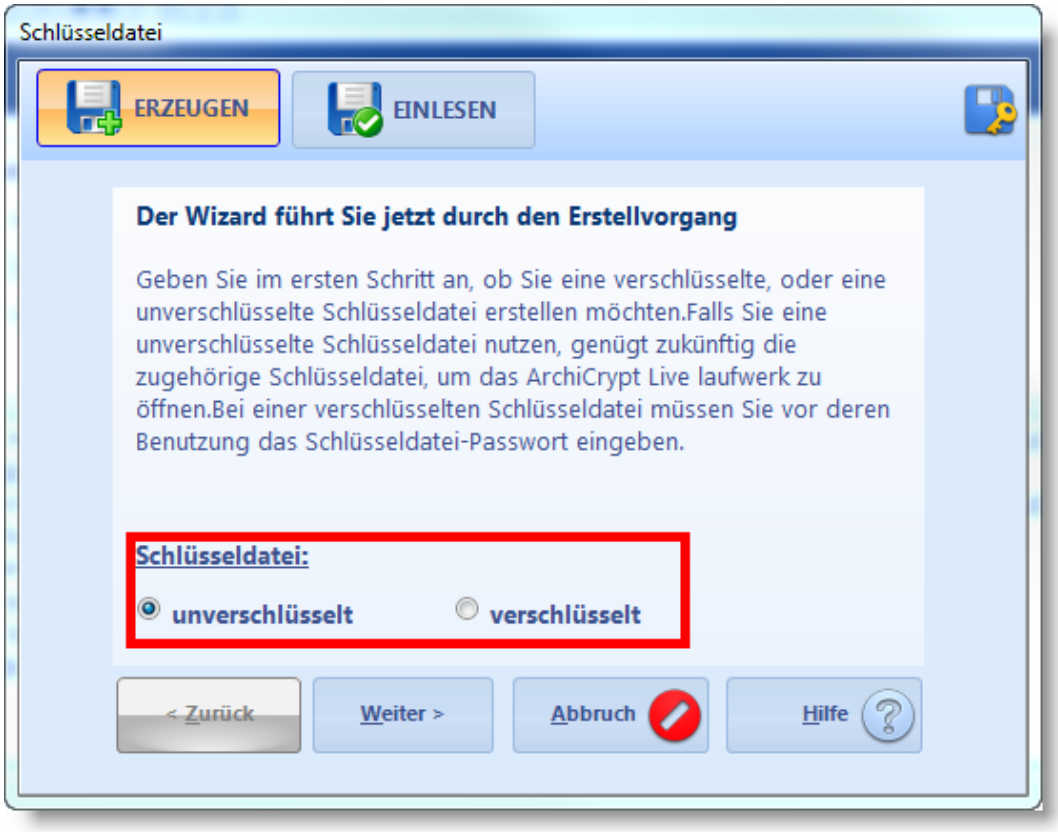
2. Verschlüsselte Schlüsseldatei. Das heißt zum Ver- und Entschlüsseln von Daten benötigen Sie die Schlüsseldatei und das zugehörige Passwort.

Einige Hinweise über den Umgang mit Schlüsseldateien erhalten Sie im technischen Anteil.

➡ WARNUNG! Wenn Sie mit einer Schlüsseldatei arbeiten, stellen Sie immer sicher, dass Sie eine funktionstüchtige Kopie an einem sicheren Ort verwahren. Insbesondere dann, wenn Sie die Datei auf einer Diskette oder einem USB-Stick abgelegt haben. Diese Datenträger sind allgemein sehr anfällig. Ist der Schlüssel zerstört, gibt es keine Möglichkeit mehr, an die Daten im ArchiCrypt Live Laufwerk zu kommen.

So erstellen Sie sich eine Schlüsseldatei

Schritt 1: Art der Schlüsseldatei festlegen (*gilt für beide Schlüsseldateiarten*)



Wählen Sie hier aus, welche Art von Schlüsseldatei Sie erstellen möchten. Betätigen Sie anschließend die Weiter > Schaltfläche.

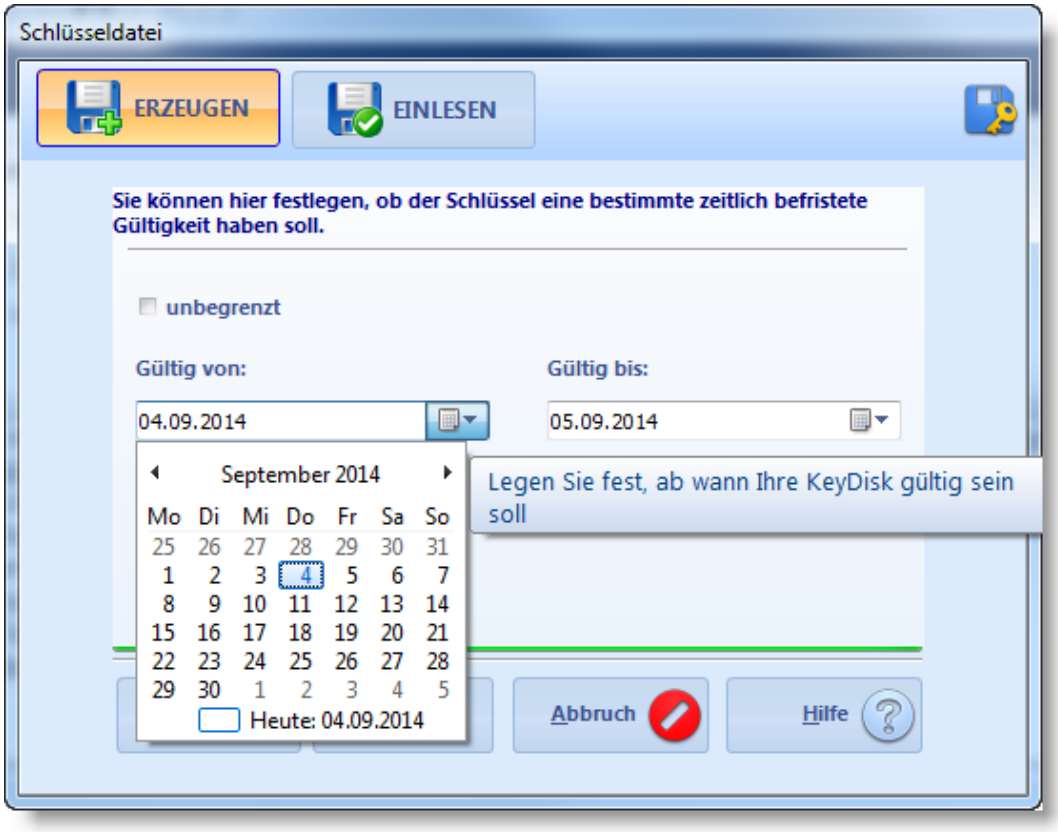
Schritt 2: Zufallsdaten sammeln (*gilt für beide Schlüsseldateiarten*)

Zur Generierung des Schlüssels werden Zufallsdaten benötigt. Bewegen Sie den Mauszeiger über dem Dialogfenster.

Schritt 3: Passwort festlegen (*gilt nur für verschlüsselte Schlüsseldatei*)

Nachdem genügend Zufallsdaten gesammelt wurden, erscheint automatisch der Dialog zur Passworteingabe.

Schritt 4: Zeitliche Gültigkeit festlegen (*gilt nur für verschlüsselte Schlüsseldatei*)



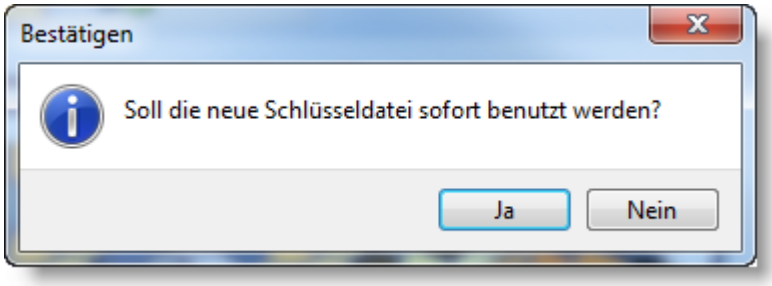
In diesem Schritt können Sie angeben, ob der Schlüssel unbegrenzt, oder innerhalb zeitlicher Grenzen gültig ist. Beachten Sie bitte, dass es sich hierbei nicht um einen tatsächlichen Schutz handelt. ArchiCrypt Live muss zur Ermittlung des Datums auf das Betriebssystem zugreifen. Ist dort ein falsches Datum eingestellt, erkennt ArchiCrypt Live dies nicht. Diese Option macht lediglich dann Sinn, wenn man sich oder andere vertrauenswürdige Personen daran erinnern möchten, von Zeit zu Zeit den Schlüssel zu wechseln.

Schritt 5: Schlüsseldatei speichern (*gilt für beide Schlüsseldateiarten*)

Der Dialog zum Speichern der Schlüsseldatei wird aufgerufen. Obwohl es möglich ist, sollten Sie auf keinen Fall die Schlüsseldatei auf einer Ihrer Festplatten speichern. Nutzen Sie einen USB Stick oder ein anderes Wechselmedium.

Schritt 6: Nutzen der Schlüsseldatei (*gilt für beide Schlüsseldateiarten*)

Nachdem Sie die Schlüsseldatei gesichert haben erscheint der Dialog:



Beantworten Sie die Frage mit Ja, wird der Schlüssel aus der Schlüsseldatei übernommen.

Die erstellte Schlüsseldatei können Sie jederzeit wie in "Schlüsseldatei einlesen" beschrieben, einlesen und nutzen.

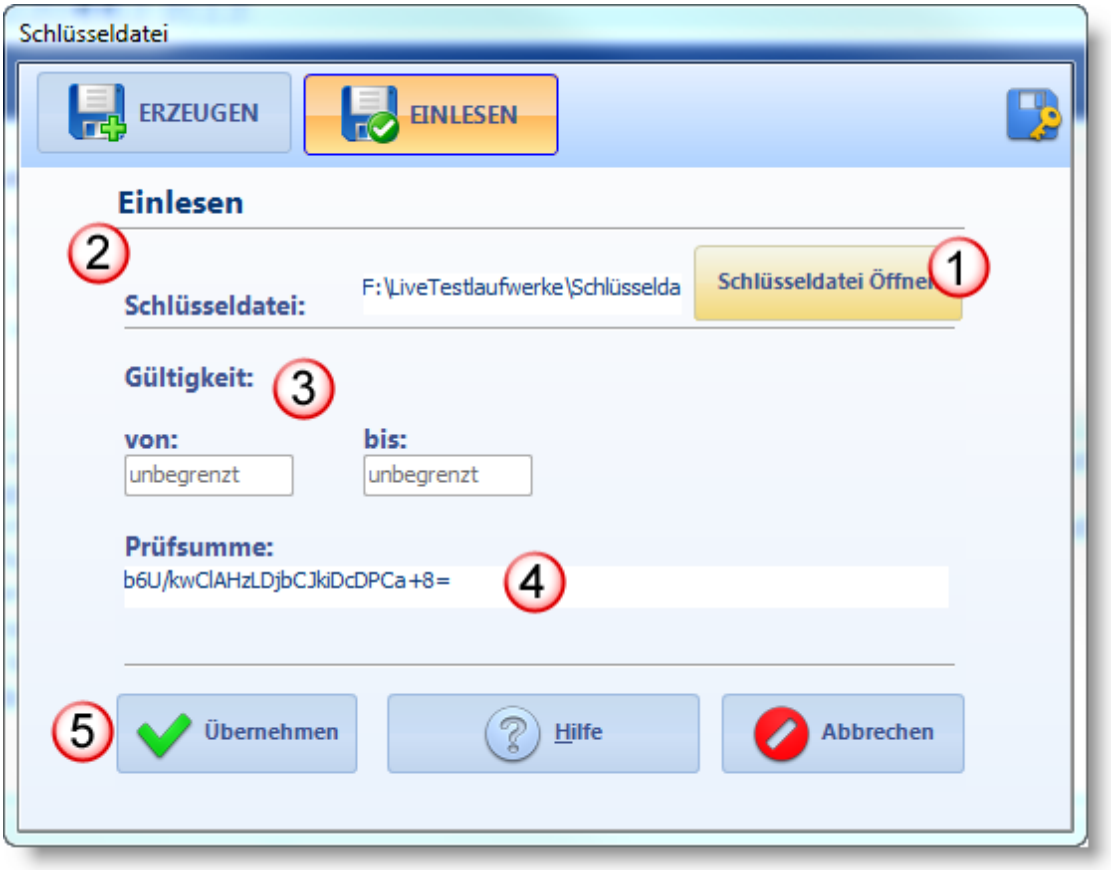
10.5.4 Schlüsseldatei einlesen

siehe auch Schlüsseldatei erstellen

So lesen Sie eine Schlüsseldatei ein

Mit dieser Funktion können Sie Schlüsseldateien laden und in ArchiCrypt Live verwenden.

Klicken Sie im Dialog ggf. am oberen Rand auf die Schaltfläche Einlesen.



Mit der Schaltfläche Schlüsseldatei Öffnen (*bei 1*) erreichen Sie den Dialog zur Auswahl einer Schlüsseldatei. Wählen Sie im Dialogfenster die Schlüsseldatei aus und bestätigen Sie Ihre Wahl durch das Betätigen der Schaltfläche Öffnen.

Die Schlüsseldatei (*Name wird bei 2 angezeigt*) wird jetzt geladen und auf Gültigkeit überprüft. Falls es sich um eine kennwortgeschützte Schlüsseldatei (siehe Schlüsseldatei erstellen) handelt, wird zunächst das Passwort abgefragt (siehe Passwortdialog). Wenn das Passwort gültig ist wird geprüft, ob eventuell eine Gültigkeitsdauer eingegeben wurde. Die Gültigkeit wird bei 3 angezeigt. Falls die Schlüsseldatei ungültig ist, wird sie nicht geladen.

Die Prüfsumme, angezeigt bei 4, ist eine Zahl, die die Schlüsseldatei eindeutig identifiziert. D.h. anhand dieser Zahl können Sie die Schlüsseldatei identifizieren, auch wenn die Schlüsseldatei umbenannt wurde. Die Zahl lässt allerdings keinerlei Rückschlüsse auf den eigentlichen Schlüssel oder ein eventuell verwendetes Passwort zu.

Nachdem der Schlüssel geladen wurde, können Sie diesen durch betätigen der Schaltfläche Übernehmen (*bei 5*) zum aktuellen Schlüssel für ArchiCrypt Live machen.

10.5.5 ArchiCrypt Card einlesen

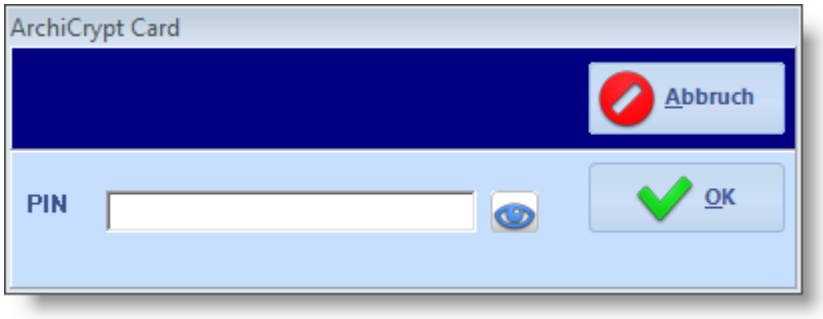
siehe auch Passwortdialog

Einlesen einer ArchiCrypt Card

➡ ACHTUNG: Beachten Sie die Systemvoraussetzungen

Sie können ArchiCrypt Live so einstellen, dass beim Öffnen eines Laufwerks zunächst geprüft wird, ob eine ArchiCrypt Card vorhanden ist. Wird eine Karte gefunden, liest ArchiCrypt Live diesen Schlüssel automatisch ein und versucht damit das Laufwerk zu öffnen. Ist die ArchiCrypt Card mit PIN geschützt und wurde die PIN während der aktuellen Sitzung noch nicht eingegeben, wird zunächst die PIN abgefragt.

siehe Einstellungen - SmartCard/Token



Kann ArchiCrypt Live das Laufwerk nicht mit der aktuellen ArchiCrypt Card öffnen, wird der Standarddialog zur Eingabe des Schlüssels angezeigt.

10.5.6 ArchiCrypt Card personalisieren

siehe auch Tipps zum Umgang mit der ArchiCrypt Card und ArchiCrypt Card klonen

ArchiCrypt Card personalisieren

➡ ACHTUNG: Beachten Sie die Systemvoraussetzungen

Unter Personalisieren versteht man das Speichern von Nutzerdaten und das Einstellen oder Ändern einer PIN oder Master PIN.

Mit den Masterfunktionen können Sie verhindern, dass ein Nutzer Daten (*Schlüssel und Nutzerdaten*) auf der Karte ändern oder löschen kann.
Weiterhin können Sie mit den Masterfunktionen die Karte löschen (*Schlüssel und Nutzerdaten*) und einen Fehlerzähler bei Falscheingabe der PIN zurücksetzen.

Eine ArchiCrypt Card muss nicht zwingend personalisiert werden!

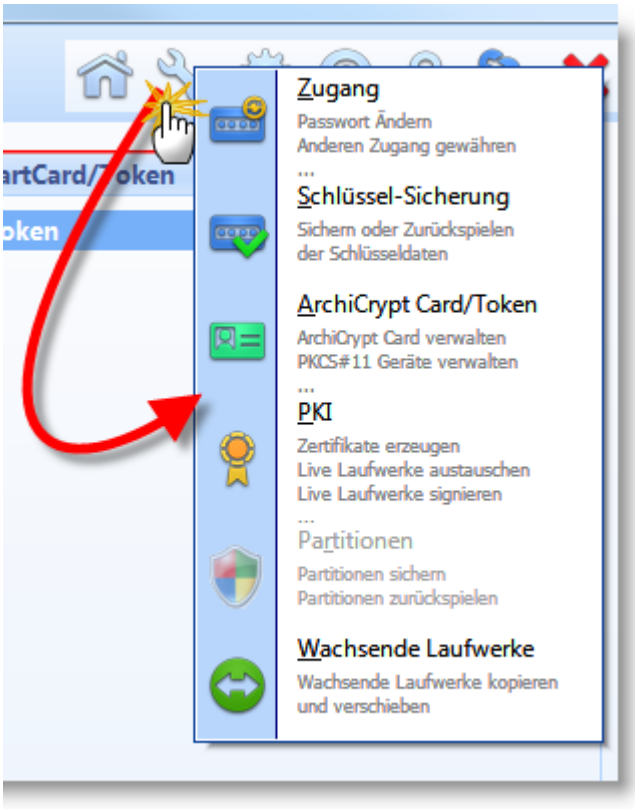
Themen:

- Nutzerinformationen auf der ArchiCrypt Card
- ArchiCrypt Card PIN
- ArchiCrypt Card Master-PIN
- ArchiCrypt Card Masterfunktionen

Aufgaben:

So legen Sie eine PIN für Ihre ArchiCrypt Card fest
So ändern Sie die PIN Ihrer ArchiCrypt Card
So können Sie die PIN Ihrer ArchiCrypt Card entfernen
So geben Sie die ArchiCrypt Card Master PIN ein
So legen Sie eine ArchiCrypt Card Master PIN fest
So ändern Sie eine ArchiCrypt Card Master PIN

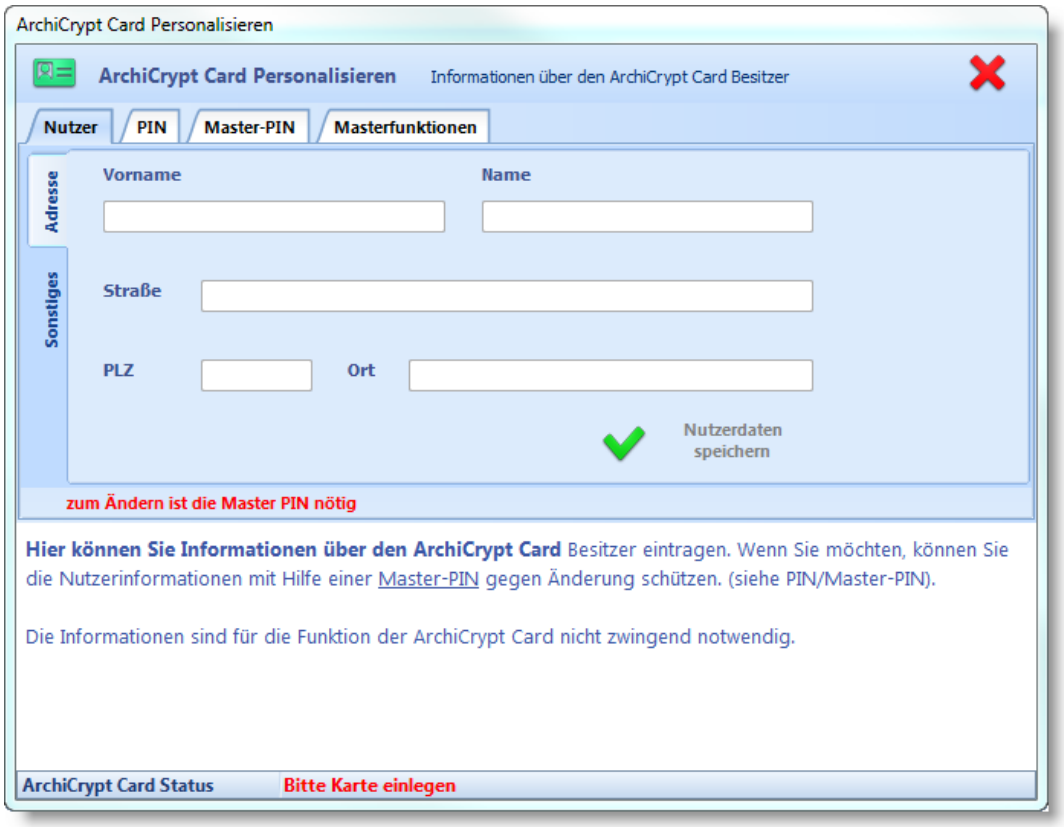
Betätigen Sie unter Werkzeuge ArchiCrypt Card / Token die Schaltfläche ArchiCrypt Card personalisieren.



Nutzerinformationen auf der ArchiCrypt Card

Speichern Sie Persönliche Daten auf der Karte. Sichern Sie die Daten sofern gewünscht mit einer Master PIN (M PIN) gegen Änderung. Dadurch kann niemand ohne Eingabe der Master PIN

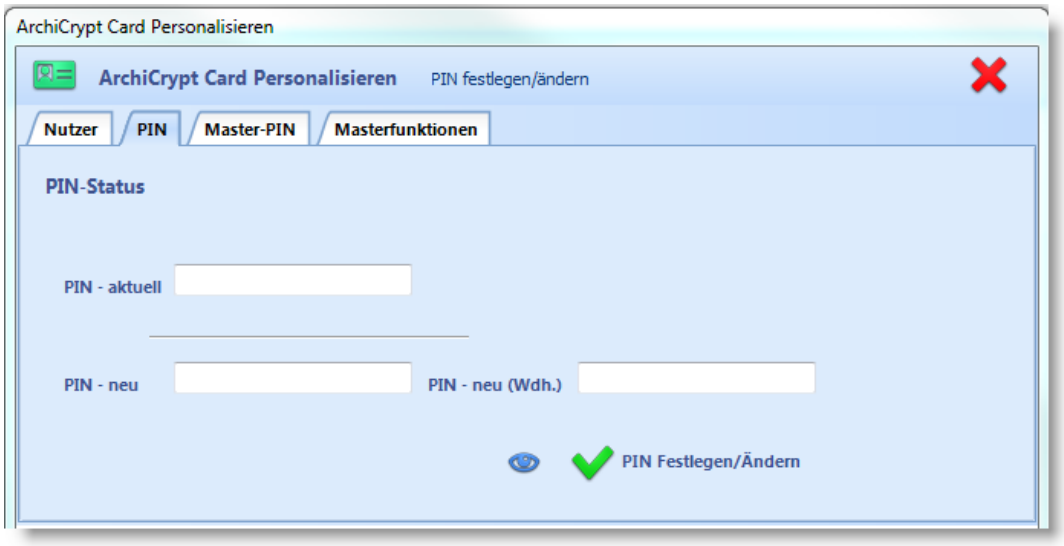
diese Daten ändern. (siehe dazu auch Tipps zum Umgang mit der ArchiCrypt Card)



➡ ACHTUNG: Die Nutzerdaten können von jedem ausgelesen werden! Nutzen Sie die Felder also nicht zum Ablegen von sensiblen Daten.

ArchiCrypt Card PIN

Eine PIN (b*is zu 100 Zeichen langes Passwort*) schützt den auf der ArchiCrypt Card abgelegten Schlüssel. Sie sollten nur in Ausnahmefällen keine PIN vergeben.



So legen Sie eine PIN für Ihre ArchiCrypt Card fest

Falls noch keine PIN festgelegt ist (neben PIN steht deaktiviert), geben Sie bitte in die beiden Eingabefelder neu und neu (Wdh.) die gewünschte PIN ein. Sie müssen die PIN 2 Mal eingeben, um Schreibfehler zu vermeiden. Eine PIN könnte zum Beispiel wie folgt aussehen: "X7h_==Klss"

Um die geänderte PIN zu übernehmen, betätigen Sie bitte die Schaltfläche Festlegen / Ändern

So ändern Sie die PIN Ihrer ArchiCrypt Card

Wurde bereits eine PIN festgelegt (neben PIN steht aktiviert), müssen Sie in das Feld aktuell die aktuelle PIN eingeben. Geben Sie anschließend in die beiden Felder neu und neu (Wdh) die gewünschte neue PIN ein. Um die geänderte PIN zu übernehmen, betätigen Sie bitte die Schaltfläche Festlegen / Ändern

So können Sie die PIN Ihrer ArchiCrypt Card entfernen

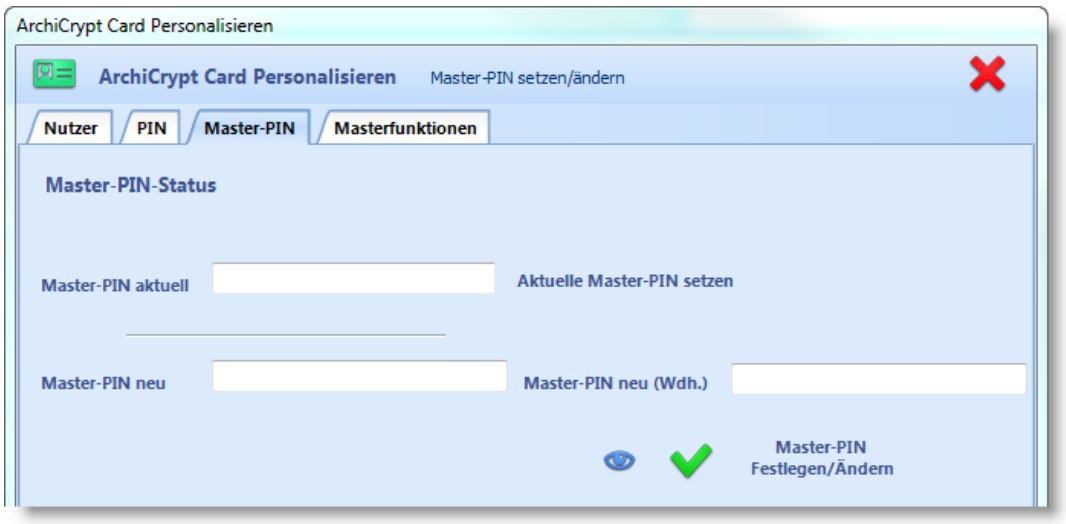
Wurde bereits eine PIN festgelegt (neben PIN steht aktiviert), müssen Sie in das Feld aktuell die aktuelle PIN eingeben. Lassen Sie die beiden Felder neu und neu (Wdh) leer. Betätigen Sie jetzt bitte die Schaltfläche Festlegen / Ändern.

ArchiCrypt Card Master-PIN

Eine Master PIN schützt Nutzerinformationen vor Veränderung, schützt den Schlüssel auf der Karte vor Löschen und dient dazu, bei 5 facher Falscheingabe der PIN, die Sperre aufzuheben. Es wird empfohlen die Master PIN zu nutzen. Merken Sie sich jedoch unbedingt die Master PIN.
Wird die Master PIN 3 Mal falsch eingegeben, wird die Karte unbrauchbar und darauf abgelegte Schlüssel sind nicht mehr verwendbar!

siehe auch Masterfunktionen

TIPP: ***Als Administrator können Sie eine Master PIN festlegen, um zu verhindern, dass wichtige Daten auf der Karte verändert werden. Der Kartennutzer kann davon unabhängig für seinen Schlüssel eine PIN festlegen, ohne die es niemandem möglich ist, auf Funktionen der Karte zuzugreifen!***



So geben Sie die ArchiCrypt Card Master PIN ein

Sie müssen die Master PIN eingeben, sofern bereits eine Master PIN festgelegt ist (neben Master PIN steht aktiviert) und Sie eine der Masterfunktionen nutzen möchten. Geben Sie in das Feld aktuell die aktuelle Master-PIN ein und betätigen Sie die Schallfläche Eingeben. Ist die Master PIN korrekt, erscheint das Wort Master PIN in grüner Farbe. Nach der Eingabe sind die Masterfunktionen verfügbar.

So legen Sie eine ArchiCrypt Card Master PIN fest

Falls noch keine Master PIN festgelegt ist (neben Master PIN steht deaktiviert), geben Sie bitte in die beiden Eingabefelder neu und neu (Wdh.) die gewünschte Master PIN ein. Sie müssen die Master PIN 2 Mal eingeben, um Schreibfehler zu vermeiden. Eine Master PIN könnte zum Beispiel wie folgt aussehen: "Ux8/8h7h_"

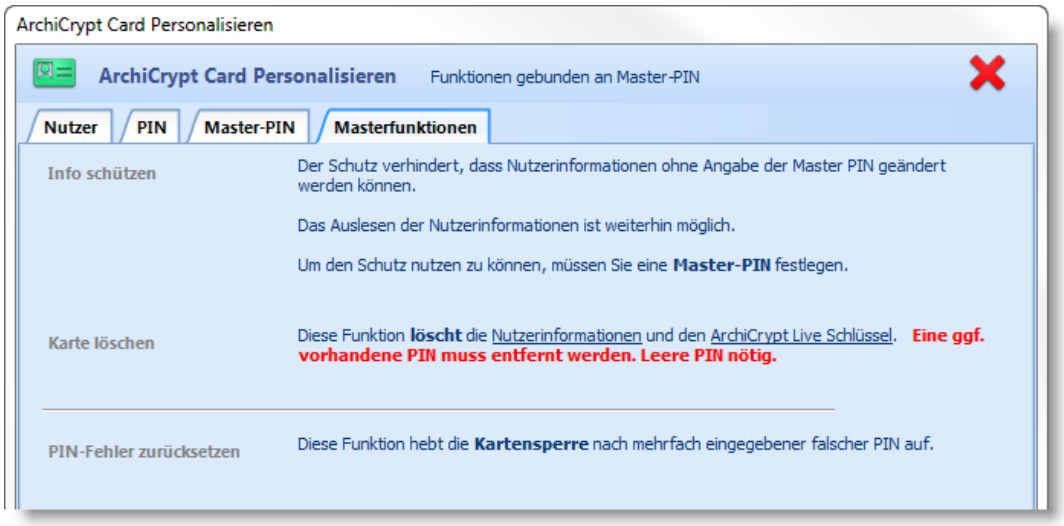
Um die geänderte Master PIN zu übernehmen, betätigen Sie bitte die Schaltfläche Festlegen/Ändern

So ändern Sie eine ArchiCrypt Card Master PIN

Wurde bereits eine Master PIN festgelegt (neben Master PIN steht aktiviert), müssen Sie in das Feld aktuell die aktuelle PIN eingeben. Geben Sie anschließend in die beiden Felder neu und neu (Wdh) die gewünschte neue Master PIN ein. Um die geänderte Master PIN zu übernehmen, betätigen Sie bitte die Schaltfläche Festlegen/Ändern

Masterfunktionen

Die Masterfunktionen verdanken Ihren Namen der Tatsache, dass die Funktionen durch eine ggf. vorhandene Master PIN geschützt sind. D.h. existiert eine Master PIN, muss man vor dem Aufruf einer der Masterfunktionen die Master PIN eingeben. Falls keine Master PIN festgelegt wurde, können die Funktionen ohne weiteres genutzt werden.



Schutz aktivieren

Nutzerinformationen können nur ausgelesen, nicht aber geändert werden. Der Schutz kann aktiviert werden (Schaltfläche trägt Bezeichnung Schutz aktivieren) oder deaktiviert werden (Schaltfläche trägt die Bezeichnung Schutz deaktivieren). Ist der Schutz deaktiviert (Schaltfläche trägt Bezeichnung Schutz aktivieren), können die Nutzerinformationen von jedem geändert werden.

Karte löschen

Diese Funktion löscht einen ggf. auf der Karte gespeicherten Schlüssel und setzt alle Nutzerinformationen zurück.

➡ ACHTUNG: ***Führen Sie diese Operation nur durch, wenn Sie sichergestellt haben, dass kein Laufwerk mehr mit dem Schlüssel auf der Karte geschützt ist. Sie kommen sonst nicht mehr an Ihre Laufwerksinhalte. Die Karte kann aus Sicherheitsgründen nur dann gelöscht werden, wenn Sie die PIN der ArchiCrypt Card zuvor entfernt haben (leere PIN). Zum Entfernen der PIN müssen Sie diese kennen. Eine ArchiCrypt Card, die mit PIN geschützt ist, kann ohne Kenntnis der PIN nicht gelöscht werden!!!***

PIN-Fehler zurücksetzen

ArchiCrypt Card sperrt sich selbst, wenn eine PIN 5 Mal falsch eingegeben wurde. Um die Sperre wieder aufzuheben, muss die Funktion PIN-Fehler zurücksetzen aufgerufen werden. Ist eine Master PIN festgelegt, kann der Fehlerzähler nur nach vorheriger Eingabe der Master PIN zurückgesetzt werden. Diese Maßnahme ist ein Schutz gegen automatisierte Angriffe auf die ArchiCrypt Card. Nachdem Zurücksetzen kann erneut 5 Mal die PIN falsch eingegeben werden.

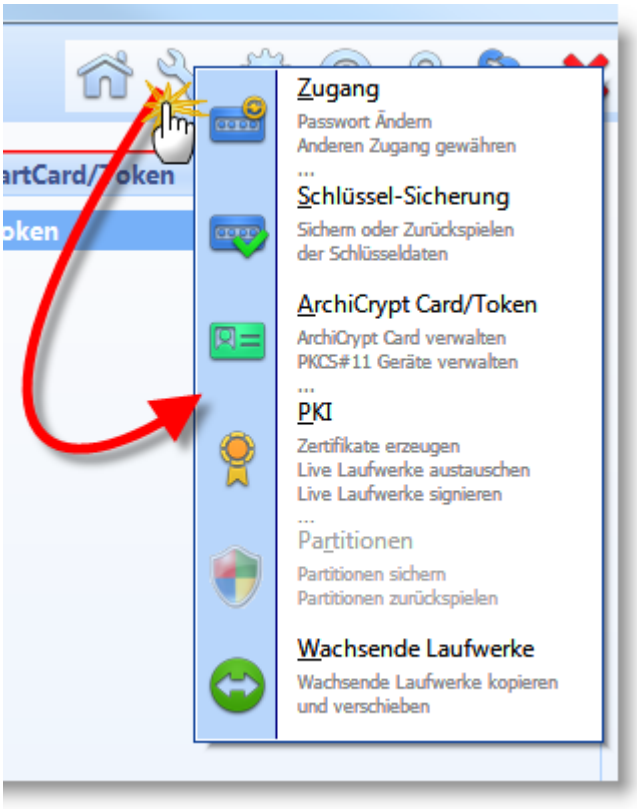
10.5.7 ArchiCrypt Card klonen

siehe auch Tipps zum Umgang mit der ArchiCrypt Card und ArchiCrypt Card personalisieren

Klonen einer ArchiCrypt Card

Mit der Funktion "Klonen einer ArchiCrypt Card" kopieren Sie einen Schlüssel von einer Karte auf eine andere. Sie können damit einem bestimmten Personenkreis Zugang zu den gleichen Laufwerken verschaffen. Jeder Nutzer kann dabei seine eigene ArchiCrypt Card PIN festlegen, für jeden Nutzer können eigene Nutzerdaten angelegt werden.

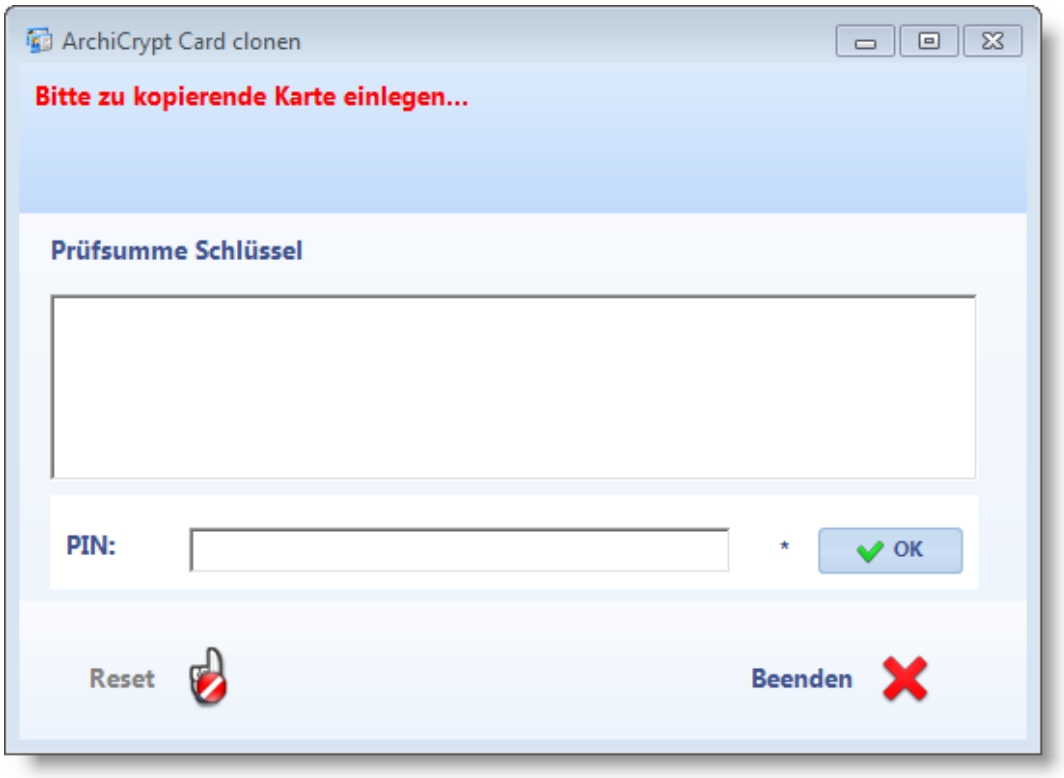
Betätigen Sie unter Werkzeuge ArchiCrypt Card die Schaltfläche ArchiCrypt Card klonen.



Der Vorgang des Klonens ist vollkommen automatisiert. Halten Sie die Karte mit dem zu kopierenden Schlüssel und die leeren ArchiCrypt Cards (*ArchiCrypt Card ohne Schlüssel; entweder neu, oder mit Masterfunktion Karte löschen geleert*) bereit.

ArchiCrypt Live fordert Sie jetzt auf, die Karte mit dem zu kopierenden Schlüssel einzulegen. (Bitte Karte einlegen...).

Nachdem Sie die Karte eingelegt haben, wird im Feld Prüfsumme Schlüssel ein Wert angezeigt, mit dem Sie Schlüssel identifizieren können. Der Wert gibt jedoch keinerlei Auskunft über den Schlüssel selbst!



Sofern Sie eine PIN geschützte ArchiCrypt Card einfügen, wird zunächst die PIN abgefragt.

TIPP: ***Wenn Sie mehrere ArchiCrypt Cards verwalten müssen, speichern Sie die zugehörigen Prüfsummen. Sie können so die verschiedenen Schlüssel leichter Identifizieren. Die Prüfsummen sind nicht schützenswert!***

Sie erhalten den Hinweis, dass der Schlüssel eingelesen wurde und Sie die Karte entnehmen können.
Wenn Sie anhand der Prüfsumme feststellen, dass Sie die falsche ArchiCrypt Card gewählt haben, betätigen Sie die Reset Schaltfläche und führen Sie die korrekte Karte ein.

Jetzt werden Sie aufgefordert, eine leere ArchiCrypt Card einzulegen.

Nach dem Übertragen des Schlüssels können Sie den Schlüssel auf eine beliebige Anzahl weiterer ArchiCrypt Cards übertragen. Führen Sie dazu die jeweils leere ArchiCrypt Card in den Kartenleser ein.

➡ HINWEIS: Nutzerdaten oder PIN und/oder Master PIN werden nicht kopiert.

➡ WARNUNG! Arbeiten Sie mit einer ArchiCrypt Card, stellen Sie immer sicher, dass Sie eine funktionstüchtige Kopie an einem sicheren Ort verwahren. Geht die ArchiCrypt Card verloren oder wird sie beschädigt, gibt es keine Möglichkeit mehr, an die Daten im ArchiCrypt Live Laufwerk zu kommen. ***Alternativ können Sie nach dem Erstellen mit ArchiCrypt Card einen zusätzlichen Zugang zum Laufwerk mit einem Gastpasswort schaffen.***

➡ ACHTUNG: Beachten Sie die Systemvoraussetzungen

10.5.8 Schlüssel von Token nutzen

Wenn ArchiCrypt Live erstmals während einer Sitzung auf einen Security-Token zugreift, müssen Sie die PIN für den Token eingeben.

Die Daten auf Ihrem Token sind mit einer PIN vor unerlaubtem Zugriff geschützt. Sie können die PIN direkt in das entsprechende Eingabefeld eingeben, oder besser, da sicherer, die Sichere Authentifizierung nutzen. Falls Ihre Token-Hardware dies unterstützt, können Sie Ihre PIN zum Beispiel über ein externes PIN Pad eingeben. Ihre Token PIN gelangt so niemals auf den Rechner und kann nicht ausgespäht werden.

Themen:
Token Sitzung öffnen
Token Manager bedienen

Aufgaben:
So erstellen Sie eine neuen ArchiCrypt Live Schlüssel auf Ihrem Token
So nutzen Sie einen ArchiCrypt Live Schlüssel auf Ihrem Token

[So löschen Sie einen ArchiCrypt Live Schlüssel von Ihrem Token]

Token Sitzung öffnen

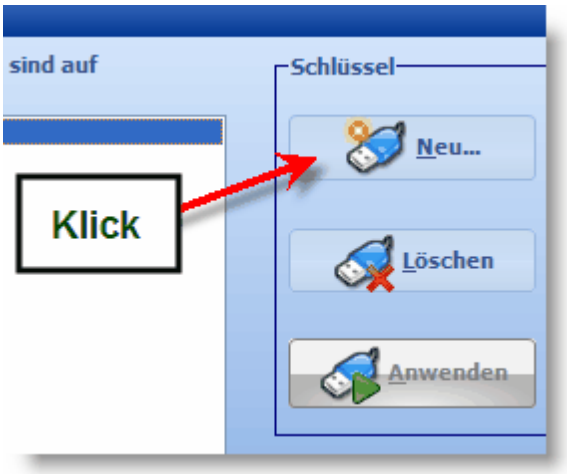
Nachdem Sie Ihre PIN eingegeben haben, erscheint der Token Manager.

Token Manager

Links werden ggf. vorhandene ArchiCrypt Live Schlüssel angezeigt. Rechts stehen Ihnen verschiedene Funktionen zur Verfügung.

So erstellen Sie eine neuen ArchiCrypt Live Schlüssel auf Ihrem Token

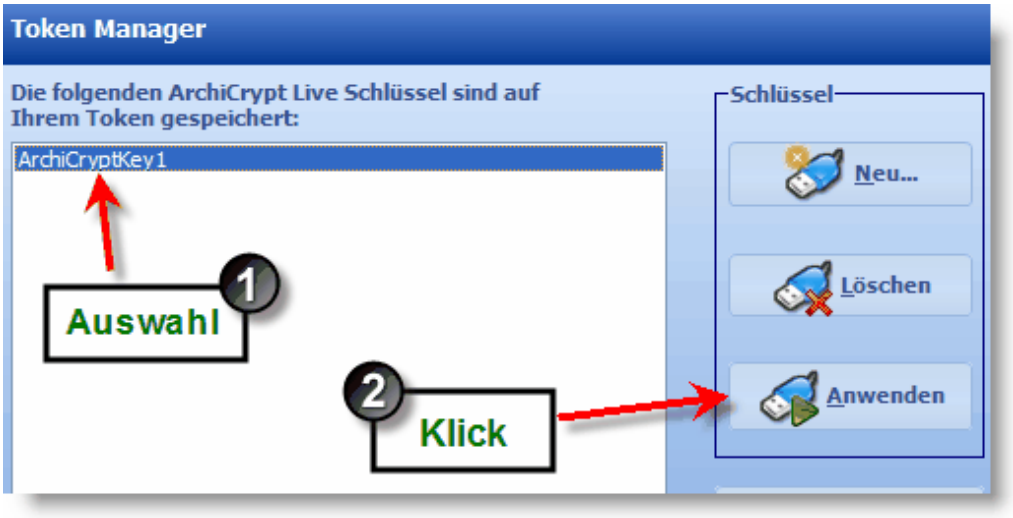
Klicken Sie im Token Manager auf Neu...



Vergeben Sie einen Namen und lassen Sie den Token einen neuen Schlüssel erzeugen.

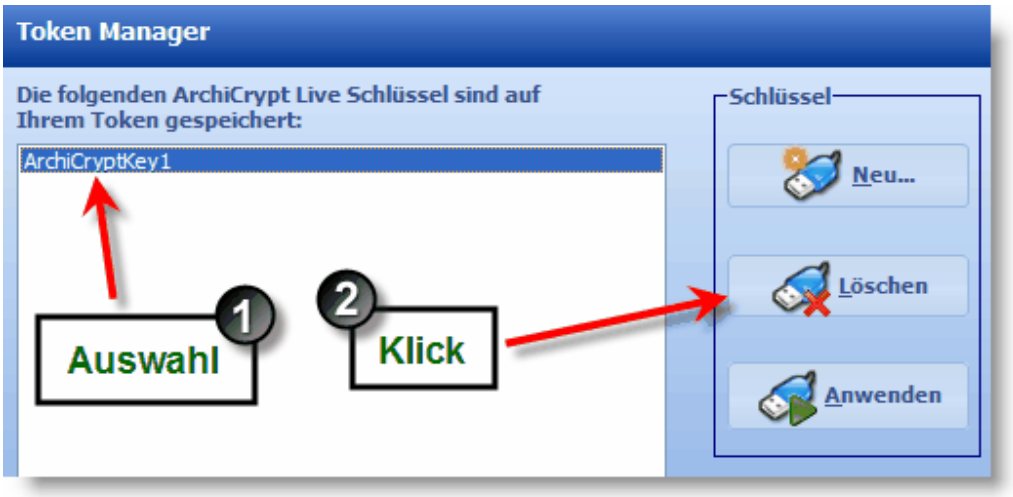
So nutzen Sie einen ArchiCrypt Live Schlüssel auf Ihrem Token

Markieren Sie links den zu verwendenden Schlüssel und betätigen Sie die Schaltfläche Anwenden.



So löschen Sie einen ArchiCrypt Live Schlüssel von Ihrem Token

Markieren Sie links den zu löschenden Schlüssel und betätigen Sie die Schaltfläche Löschen.



10.5.9 Dialog zur Auswahl einer Partition

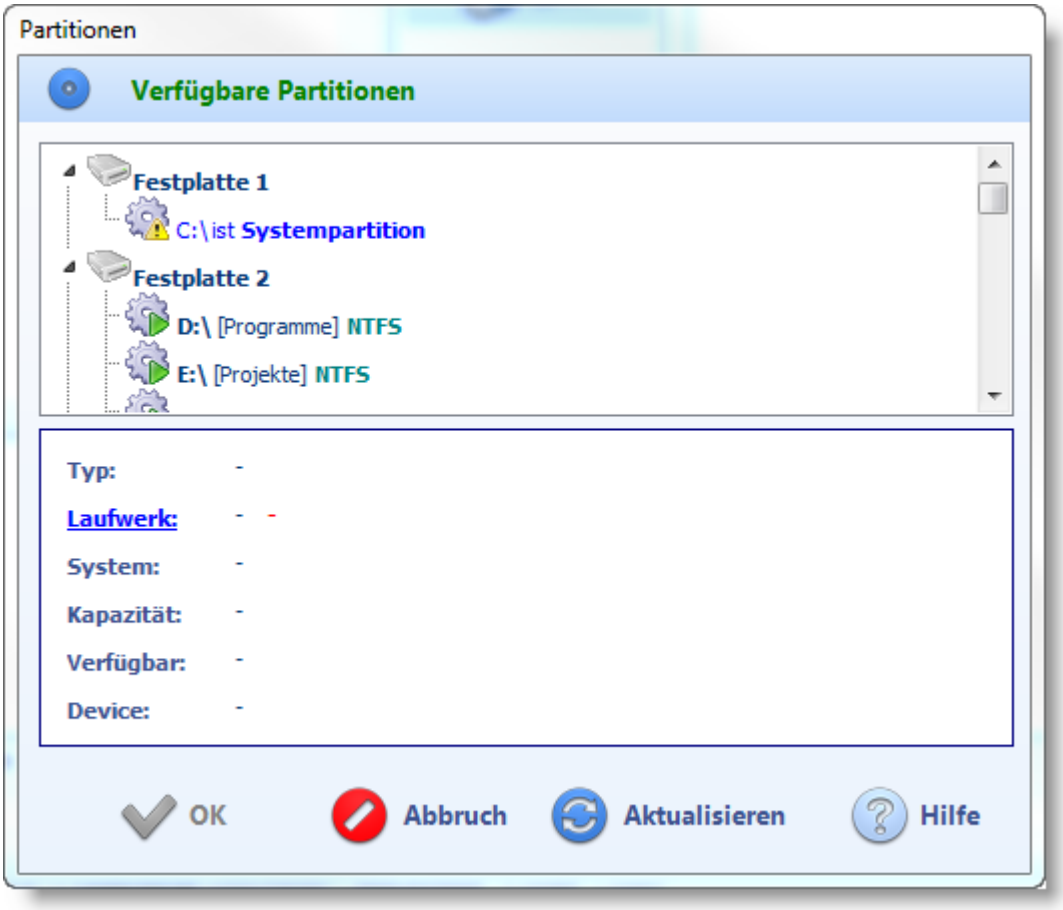
Sollten sich die nachfolgenden Videos im Browser nicht anzeigen lassen, so können Sie die Videos alternativ direkt in Youtube auf unserem ArchiCrypt Kanal ansehen.

Video - Live Partition

siehe auch: Wichtige Begriffe - Begriffserläuterungen

Dialog zur Auswahl einer Partition:

Der Dialog zur Auswahl einer bestimmten Partition kommt an vielen Stellen in ArchiCrypt Live zum Einsatz.



Was der Dialog anzeigt, hängt davon ab, ob

alle Partitionen in Ihrem System angezeigt werden sollen (wie zum Beispiel beim Erstellen einer neuen Live Partition oder zum Sichern einer Partition)

oder

nur bereits bestehende Live Partitionen (wie zum Beispiel beim Laden von Live Partitionen)

Wenn ArchiCrypt Live die Partitionen analysiert, werden so viele Informationen wie möglich gesammelt. Diese Informationen werden Ihnen bei der Auswahl der Partition im Dialog im Informationsfenster angezeigt.

Die Symbole geben zusätzlich Auskunft über die Partition:
(Symbole für Partitionen)

Systempartition. Auf dieser Partition ist das gerade aktive Betriebssystem untergebracht. Sie können diese Partition nicht in ein Live Laufwerk umwandeln!
ACHTUNG. ArchiCrypt Live erkennt nur, auf welcher Partition Ihr aktuell geladenes Betriebssystem untergebracht ist. Haben Sie ein Multiboot-System, erkennt ArchiCrypt Live die weiteren Partitionen nicht als Systempartition. Diese werden wahrscheinlich als inaktiv angezeigt.

Aktive Partition. Auf diese Partition kann mit dem angegebenen Laufwerksbuchstaben zugegriffen werden. Die Partition ist aktiv, ihr wurde in der Datenträgerverwaltung ein Laufwerksbuchstabe zugeordnet.

Live führt bei aktiven Laufwerken auf, welches Dateisystem das Laufwerk besitzt (wird durch die Hardware gemeldet!). Einige Wechsellaufwerke (oft USB-Sticks und Speicherkarten) melden fälschlicherweise, dass Sie unbenutzt seien. Live meldet dann Nicht definiert (VORSICHT). Vorsicht deshalb, weil das Laufwerk ansprechbar ist, ggf. formatiert ist und somit möglicherweise Daten enthält. Wenn der Wert Kapazität deutlich größer als der des Verfügbar-Wertes ist dies ein Indiz hierfür.
Bei aktiven Partitionen, können Sie sich den Inhalt anzeigen lassen, indem Sie auf Laufwerk im Informationsbereich klicken.

Der Inhalt wird nur dann angezeigt, wenn dies möglich ist (Es ist zum Beispiel nicht möglich, den Inhalt unformatierter Partitionen anzuzeigen).

Das Laufwerk ist nicht aktiv. Sie können zur Zeit nicht über einen Laufwerksbuchstaben auf die Partition zugreifen. Auch wenn Sie kein Multiboot System eingerichtet haben, kann es durchaus sein, dass der Hersteller Ihres Rechners Partitionen für bestimmte Zwecke vorgesehen hat. Oft werden Recovery-Programme auf diesen Partitionen untergebracht.

Bei dieser Partition handelt es sich um eine Live Partition die mit ArchiCrypt Live geladen werden kann.

11 Wichtige Begriffe - Begriffserläuterungen

Wichtige Begriffe:

Administrator: Administrator, genauer gesagt der *Laufwerksadministrator* ist derjenige, der das Live Laufwerk erstellt hat und ist nicht mit dem Computer Administrator zu verwechseln! Er hat im Umgang mit den von ihm erstellten Laufwerken besondere Rechte (Änderung Passwort, Erstellen Geheim-Container,etc.).

ArchiCrypt Card: Eine speziell für den Einsatz mit ArchiCrypt Live konzipierte SmartCard. Die SmartCard stellt Funktionen für das Erstellen, Öffnen und Schließen von ArchiCrypt Live Laufwerken bereit. Sie erhalten die ArchiCrypt Card in unserem Online Shop unter http://shop.ArchiCrypt.de

Dateisystem: siehe Dateisystem bei Erstellen

Geheimfach: siehe gleichnamiges Kapitel

Steganografisches Laufwerk: Ein Steganografisches Laufwerk entsteht durch das Vermischen einer - fast - beliebigen Datei (*meist*

Multimedia bzw. Anwendung) mit einer Trägerdatei. Die durch das Vermischen entstehende Datei hat "Zwittereigenschaften". Sie kann im Sinne der beiden beteiligten Dateien weiter genutzt werden. Kann also zum Beispiel als Video betrachtet und als Live Laufwerk geladen werden. siehe auch Kapitel Steganografisches Laufwerke

Laufwerk-Administrator: Der Nutzer, der das Laufwerk erstellt hat. Er legt im Rahmen des Erstellvorgangs den Laufwerk-Administrator-Schlüssel fest. Im Umgang mit dem Laufwerk stehen nur ihm bestimmte Funktionen zur Verfügung. So kann nur er neue Zugänge einrichten oder die Zugangsart ändern.

Laufwerk-Administrator-Schlüssel: Der beim Erstellen eines Laufwerks angegebene Schlüssel. Es kann sich um ein normales Passwort, eine Schlüsseldatei oder um einen Schlüssel von der ArchiCrypt Card oder einem Security-Token handeln.

Laufwerksheader: Bereich des ArchiCrypt Live Laufwerks, in welchem "lebensnotwendige" Informationen abgelegt sind. Ohne diese Daten kann kein ArchiCrypt Live Laufwerk geladen werden.

Live Laufwerk: Oberbegriff für alle Dateiarten und Partitionen, die von ArchiCrypt Live als Laufwerk in Ihr System eingebunden werden können.
Ein ArchiCrypt Live Laufwerk ist eine Datei oder Partition, die durch einen speziellen Mechanismus als Laufwerk in ein System eingebunden werden kann. Die Nutzung entspricht der eines völlig normalen Laufwerks mit dem Unterschied, dass alle Daten beim Speichern sofort verschlüsselt werden und beim Lesen, korrektes Passwort vorausgesetzt, sofort in den Hauptspeicher Ihres Rechners entschlüsselt werden. Um Zugang zu einem solchen Laufwerk zu erhalten, ist ein Schlüssel (*Passwort, Schlüsseldatei, ArchiCrypt Card, Token*) notwendig. Die Echtzeitlösung sorgt dafür, dass selbst bei Stromausfall alle Daten im Live Laufwerk verschlüsselt sind.

Mobile Engine: (*ArchiCrypt Live Mobile Engine*) Ein spezieller Gerätetreiber, der permanent oder temporär auf dem Rechner installiert wird. Mit Hilfe dieses Treibers kann das Betriebssystem ArchiCrypt Live Laufwerke laden und verwalten.

Live Partition: Ihre Laufwerke sind in s.g. Partitionen unterteilt. Als Nutzer sprechen Sie diese Partitionen als Laufwerk (z.B. D:\) an. Live kann eine Partition so umwandeln, dass Sie direkt mit Live als Laufwerk mit Echtzeitverschlüsselung geladen werden kann. Eine solche Partition wird als Live Partition bezeichnet. siehe auch Kapitel Partitionen

Mobiles ArchiCrypt Live Laufwerk (mobiler Datensafe): Bei dieser Datei handelt es sich um einen mobilen Datensafe. Hier wird eine von ArchiCrypt Live bereitgestellte Anwendung mit einer Trägerdatei vermischt. Die entstehende Anwendung ist in der Lage, sich selbst als Laufwerk mit Echtzeitverschlüsselungsfunktionalität und vollem Schreib-/Lesezugriff zu laden. siehe auch Kapitel Steganografisches Laufwerke

Mobiler Datensafe: Synonym für mobiles ArchiCrypt Live -Laufwerk

Security-Token: siehe Token

Schlüssel: Der Schlüssel öffnet das zugehörige "Schloss" und gewährt uns entsprechenden Zugriff auf die Laufwerksinhalte. Die Rechte (*Lesen-/Schreiben etc.*) hängen davon ab, welches Schloss unser Schlüssel geöffnet hat (siehe Zugang). Der Schlüssel kann als Passwort vorliegen, in einer Schlüsseldatei oder auf einer ArchiCrypt Card oder einem Token gespeichert sein.

Schlüsseldatei: Eine Datei, die Schlüsseldaten für ein ArchiCrypt Live Laufwerk enthält. Sie können die Datei ggf. mit einem Passwort schützen und damit den Zugang zu ArchiCrypt Live Laufwerken regeln.

Token: Auch Security-Token genannt, ist eine Hardwarekomponente, die Teil eines Systems zur Identifizierung und Authentifizierung von Benutzern ist. ArchiCrypt Live kann diese Geräte nutzen, um darauf Schlüssel für Live Laufwerke zu erzeugen und abzulegen. Mit Hilfe des Tokens kann man dann den Zugang zu ArchiCrypt Live Laufwerken steuern.

PKCS#11: PKCS ist die Abkürzung von Public Key Cryptography Standard und bezeichnet eine Reihe von kryptographischen Spezifikationen. Die seit 1991 von den RSA-Laboratorien entwickelten Spezifikationen haben das Ziel, die Verbreitung asymmetrischer Kryptosysteme voranzutreiben.
Der PKCS-Standard besteht derzeit aus 13 einzelnen Dokumenten. PKCS#11 kommt in ArchiCrypt Live im Zusammenhang mit der Tokennutzung zum Einsatz. PKCS#11 (Cryptographic Token Interface oder cryptoki) beschreibt eine generische Schnittstelle zu den kryptografischen Funktionen von Token. Programmen wird durch die Erfüllung dieses Standards die Möglichkeit gegeben, Token verschiedenster Bauarten und Hersteller zu unterstützen.

Trägerdatei: Mit ArchiCrypt Live können Sie Laufwerke erstellen, deren gesamter Inhalt in einer Datei abgelegt ist. Eine solche Datei wird als s.g. Trägerdatei bezeichnet. Da die eigentlichen Inhalte des Laufwerks verschlüsselt in einer Datei untergebracht sind, kann man

die Laufwerke auf nahezu beliebigem Speichermedium ablegen und von dort als Live Laufwerk laden.

Zugang: Es gibt verschiedene "Schlösser", die Ihr Laufwerk öffnen. "Betritt" man das Laufwerk, indem man es über ein bestimmtes "Schloss" öffnet, kann man mit unterschiedlichen Rechten auf die Daten im Laufwerk zugreifen.

Zugangsarten:
Man Unterscheidet folgende

- Administrator: Der Administrator kann mit dem Laufwerk und dessen Inhalten anstellen, was er möchte. Er kann allein weitere "Schlösser" einbauen (Zugänge einrichten), über die man dann auf die Laufwerksinhalte Zugreifen kann. Er alleine kann den Zugangsschutz festlegen.
- Geheimfach: Spezieller Bereich in einem Laufwerk, der nur mit einem "Schloss" gesichert werden kann.
- Gast 1/Gast 2 nur Lesen: Laufwerksinhalte können nicht geändert werden. Kein Ändern/Neuerstellen von Zugang oder Zugangsschutz.
- Gast 3 Lesen und Schreiben: Laufwerksinhalte können gelesen und geändert werden. Kein Ändern/Neuerstellen von Zugang oder Zugangsschutz.

Zugangsschutz: Man kann festlegen, wie man einen Zugang ("das Schloss") schützt. ArchiCrypt Live bietet je nach Ausstattung des Rechners verschiedene Schutzarten an. Sie können ein *Passwort* nutzen, eine s.g. *Schlüsseldatei* (die ggf. ebenfalls mit Passwort geschützt ist) einsetzen, oder den Zugang mit Hilfe einer ArchiCrypt Card oder einem Security Token (ggf. mit Passwort/PIN gesichert ist) realisieren.

12 ArchiCrypt Live Mobile

12.1 ArchiCrypt Live Mobile

siehe auch: Wichtige Begriffe - Begriffserläuterungen
Steganografische Laufwerke und mobile Live Laufwerke

Was ist ArchiCrypt Live Mobile?

ArchiCrypt Live Mobile ist ein kostenloses und frei verfügbares Programm, mit dem man dateibasierte ArchiCrypt Live Laufwerke laden kann. Live Mobile kann ein einzelnes Live Laufwerk öffnen. Sofern sich das Laufwerk auf einem wieder-beschreibbaren Medium befindet, können Sie Laufwerksinhalte beliebig ändern. Zum Erstellen von ArchiCrypt Live Laufwerken und zum Ändern von Zugangsdaten benötigen Sie eine kostenpflichtige ArchiCrypt Live Lizenz.

Die mobilen Live Laufwerke bestehen zu einem Teil aus einer speziellen Variante von ArchiCrypt Live Mobile, die mit dem mobil zu nutzenden Live Laufwerk vermischt wird.

Das mobile Live Laufwerk ist ideal geeignet, um ArchiCrypt Live Laufwerke an Personen weiterzugeben, die keine ArchiCrypt Live Lizenz besitzen und, um sensible Daten mit einer einzelnen ArchiCrypt Live Lizenz, bequem auf verschiedenen Rechnern bearbeiten zu können. Sie können sensible Daten sicher an Dritte weitergeben und, da die Inhalte des geschützten Live Laufwerks beliebig änderbar sind, Daten mit anderen austauschen.

Live Mobile können Sie unter Windows XP, Windows Vista und Windows 7/8 nutzen. Die 64 BIT Windows Betriebssysteme werden unterstützt.

Wer kann ArchiCrypt Live Laufwerke mit ArchiCrypt Live Mobile laden?

Sofern die ArchiCrypt Live Mobile Engine permanent installiert ist, kann jeder Nutzer unabhängig von seinen Nutzerrechten ArchiCrypt Live Laufwerke laden. Das Betriebssystem Windows XP, Windows Vista oder Windows 7/8 vorausgesetzt, kann jeder Nutzer der Administratorrechte besitzt ArchiCrypt Live Laufwerke laden. Das Laden von Live Partitionen wird nicht unterstützt.

Wie installiere ich ArchiCrypt Live Mobile permanent?

Unter Windows XP, Windows Vista und Windows 7/8 müssen Sie die folgenden Schritte als Administrator ausführen!

Starten Sie das Programm ACLiveMobile.exe. Das Programm erkennt, dass Sie Administrator sind und bietet im folgenden Dialog an, die ArchiCrypt Mobile Engine dauerhaft zu installieren. Betätigen Sie die Schaltfläche JA um die Installationsroutine für ArchiCrypt Live Mobile zu starten.

Nach der Installation finden Sie in der Systemsteuerung unter Software den Eintrag "ArchiCrypt Live Mobile Encryption" über den Sie die Mobile Engine bei Bedarf wieder deinstallieren können.

Haben Sie einen mobilen Datensafe, starten Sie die Datei mit dem Parameter /i von der Kommandozeile aus um die Möglichkeit zu erhalten, die mobile Engine dauerhaft zu installieren.

Wie erstelle ich eine CD/DVD mit Autostartfunktion?

Erstellen Sie zunächst Ihr ArchiCrypt Live Laufwerk (dateibasiert, Trägerdatei) und achten Sie auf die Kapazität des Mediums, auf dem das Laufwerk gespeichert werden soll.

ACHTUNG: Berücksichtigen Sie, dass ArchiCrypt Mobile auf dem Datenträger ca. 5 Megabyte benötigt.

 TIPP: Mobile Datensafes unterstützen die selben Parameter wie ArchiCrypt Live Mobile und sind einfacher zu nutzen. Ersetzen Sie bei Bedarf den Namen ACLiveMobile.exe durch den Namen Ihres mobilen Datensafes.

Legen Sie jetzt eine Datei mit dem Namen Autorun.inf an. Sie können die Datei mit jedem Texteditor erstellen. Achten Sie beim Speichern der Datei darauf, dass nicht versehentlich mit der Endung txt gespeichert wird. Wenn Sie möchten, dass die CD/DVD nach dem Einlegen im Explorer ein eigenes Icon zeigt, halten Sie eine Icondatei bereit.

Kopieren Sie folgende Zeile in die Textdatei autorun.inf

```
[autorun]
OPEN=
LABEL=Live Mobile
ICON=ACLiveMobile.exe
```

Schreiben Sie jetzt hinter das Gleichheitszeichen bei OPEN

ACLiveMobile.exe

Falls beim Einlegen des Datenträgers ArchiCrypt Live Mobile gestartet werden soll. Sinnvoll, wenn mehrere Live Laufwerke auf der CD/DVD gespeichert sind und man das jeweilige Laufwerk selbst auswählen möchte.

ACLiveMobile.exe /s

Falls beim Einlegen des Datenträgers nur der Dialog zur Auswahl eines Laufwerksbuchstabens und zur Eingabe eines Passworts angezeigt werden soll. Sinnvoll, wenn man nur ein Live Laufwerk auf CD/DVD abgelegt hat und den Laufwerksbuchstaben unter dem das Laufwerk erscheinen soll, selbst festlegen möchte. siehe auch /nw

ACLiveMobile.exe /ts

Falls beim Einlegen des Datenträgers nur der Dialog zur Eingabe des Passwortes erscheinen soll. Sinnvoll, falls nur ein Live Laufwerk auf CD/DVD gespeichert ist und ein Laufwerksbuchstabe automatisch zugeordnet werden soll. Siehe auch /nw

ACHTUNG: Die Schalter /s und /ts funktionieren nur dann korrekt, wenn die ArchiCrypt Live Mobile Engine dauerhaft installiert ist bzw. das Betriebssystem Windows 2003, XP oder Vista vorliegt und der aktuelle Nutzer Administratorrechte besitzt.
Damit die Autorun Funktion arbeitet, muss diese auf dem System aktiviert sein.

Falls Sie möchten, dass das Laufwerk mit entsprechendem Label erscheint, können Sie hinter LABEL= eine eigene Bezeichnung angeben.

Falls Sie dem Datenträger ein eigenes Symbol/Icon zuweisen möchten, können Sie eine Icondatei angeben

ICON=Icondatei.ico

Weitere Parameter für Live Mobile:

Live Mobile besitzt weitere mächtige Kommandozeilenparameter, die im Weiteren erläutert werden.

/i
Sorgt bei Vorliegen eines Self-Glue-Laufwerks dafür, dass dem Administrator permanente Installation der Mobile Engine angeboten wird.

/r
Laufwerk wird im Nur-Lese-Modus geöffnet.

/f
Laufwerk wird als Lokales Laufwerk geladen.
Anm.: Fehlt der Schalter, wird das Laufwerk als Wechsellaufwerk geladen.

/v
Name des zu ladenden Laufwerks. Dabei können Sie den Pfad zur Datei weglassen, sofern sie sich im gleichen Verzeichnis wie Live-Mobile befindet. Bei Self-Glue Laufwerken macht dieser Schalter wenig Sinn.

Die Angabe hat in der Form /v="Dateiname" zu erfolgen. Geben Sie den Dateinamen zwingend in Hochkommata an!

Beispiel:
/v="I:\Live Laufwerke\Version6.acl"

/d
Übergeben Sie hier den Laufwerksbuchstabe, unter dem Ihr Live Laufwerk geladen werden soll. Die Angabe hat in der Form -d=LW
Beispiel: -d=Y

/nw
Falls eine Trägerdatei geöffnet wird, die sich mutmaßlich auf einem Wechseldatenträger befindet (z.B. CD oder DVD) wird davor gewarnt, die das Speichermedium aus dem Laufwerk zu entfernen, bevor ArchiCrypt Live Mobile beendet wurde. Um diese Meldung zu unterdrücken, können Sie den Schalter /nw angeben.

/k
Hier können Sie einen Pfad zu einer Textdatei angeben, in der der Schlüssel für das Laufwerk zu finden ist. Angabe hat in der Form -k="Dateiname" zu erfolgen.
Beispiel: -k="C:\Live\Keys\MobileKey.txt"

Anm.: Die Textdatei ist nicht mit den Schlüsseldateien zu verwechseln. Es handelt sich vielmehr um reine Textdateien, die das Passwort für ein Laufwerk als Klartext enthalten.


TIPP: Wozu dieser Schalter? Angenommen Sie pendeln mit sensiblen Daten zwischen verschiedenen Rechnern. An den Rechnern selbst besteht für die Daten keine Gefahr, der Transport der sensiblen Daten hingegen ist kritisch. Da das Passwort nur auf den Rechnern, nicht jedoch zusammen mit dem Mobilen Laufwerk gespeichert ist, sind die Daten beim Transport nicht gefährdet. Beim Laden der Laufwerke an den Rechnern entfällt die lästige Passworteingabe. Achten Sie darauf, dass die Passwortdatei auf allen Rechnern unter dem selben Pfad mit identischem Namen abgelegt ist.

Sie sollten jetzt folgende Dateien auf CD/DVD brennen, oder auf einem Wechselmedium speichern:

- ACLiveMobile.exe (bzw. mobiles Live Laufwerk)
- ArchiCrypt Live Laufwerk mit Ihren sensiblen Daten (entfällt bei mobilem Live Laufwerken)
- Autorun.inf
- Icondatei.ico (Optional)

Die Autorun.inf Datei und das Icon können Sie für weitere CDs/DVDs nutzen.

Was muss man hinsichtlich der Größe eines ArchiCrypt Live Laufwerks beachten?

siehe dazu auch Dateisysteme

Beachten Sie, dass je nach verwendetem Medium auf welchem Sie das Live Laufwerk für die mobile Nutzung speichern möchten, unterschiedliche Größen möglich sind. DVDs, auf denen Sie Live Laufwerke mit mehr als 2 Gigabyte Größe speichern möchten, sind im UDF Format zu erstellen.

AUSNAHME ist Windows **Vista**, hier können Laufwerke nicht!!! von DVDs geladen werden, die im UDF Format angelegt wurden. Hier müssen Sie beim Erstellen das normale ISO Format (maximale Größe der Trägerdatei 2 GByte) wählen oder die Datei auf einem anderen Medium sichern.

USB Sticks und Laufwerke sind meist im FAT 32 Format formatiert. Dieses Dateisystem unterstützt Dateien bis zu einer Maximalgröße von 4 Gigabyte. Live Laufwerke können folglich nicht größer als 4 Gigabyte sein. Möchten Sie das Live Laufwerk auf einem Medium speichern, welches im NTFS Format vorliegt, kann das Live Laufwerk bis maximal 2 Terabyte groß sein.

Generell darf ein Live Laufwerk (nicht zu verwechseln mit dem Laufwerk, auf welchem die s.g. Trägerdatei abgelegt ist), welches von einem Nur-Lese-Medium (z.B. CD/DVD) geladen wird, nicht im NTFS Format formatiert sein.

13 Datensicherung

13.1 Datensicherung

siehe auch: Wichtige Begriffe - Begriffserläuterungen
Sicherung und Wiederherstellung von Partitionen

Wieso ist Datensicherung wichtig?

Zum verantwortungsvollen Umgang mit wichtigen Daten gehört zwingend ein regelmäßiges Backup dieser Daten. Die Häufigkeit des Backups richtet sich nach der Wichtigkeit der Daten und muss im Extremfall quasi in Echtzeit erfolgen. Beachten Sie bitte auch, dass Ihre Daten ohne zugehörigen Schlüssel (Passwort / Schlüsseldatei / SmartCard / Token) nicht wieder entschlüsselt werden können. Die Daten sind ohne Schlüssel für immer verloren. ArchiCrypt Live bietet mit der Schlüssel-Sicherung die Möglichkeit, ein Reservepasswort oder Notpasswort anzulegen. Mit diesem Notpasswort ist es eventuell möglich ArchiCrypt Live Laufwerke

trotz eines zerstörten Laufwerksheaders (*lebenswichtiger Teil Ihres ArchiCrypt Live Laufwerkes*) zu öffnen. Dennoch können je nach Schweregrad der Laufwerksschädigung erhebliche Datenverluste auftreten.

➡ ACHTUNG: Die Schlüsselsicherung ersetzt auf keinen Fall ein Backup der Trägerdatei/Partition! Diese sollten je nach Wichtigkeit der Daten und Häufigkeit der Datenänderung regelmäßig gesichert werden.

Was kann mit den Trägerdateien/Partitionen geschehen?

Für das Betriebssystem ist ein dateibasiertes Live Laufwerk (Trägerdatei) eine gewöhnliche Datei und eine Live Partition eine gewöhnliche Partition. Als Datei bzw. Partition ist das Live Laufwerk somit allen Gefahren einer gewöhnlichen Datei bzw. Partition ausgesetzt. Die Datei/Partition kann durch Viren, Fehler in Programmen, Betriebssystemkomponenten, durch Hardwarefehler und -ausfälle zerstört und durch böswillige Dritte manipuliert und unbrauchbar gemacht werden. Besonders kritisch ist dabei der Bereich, in dem die Zugangsschlüssel (*selbstverständlich verschlüsselt*) abgelegt sind. Dieser Bereich wird auch als Laufwerksheader bezeichnet.

Wie unterstützt ArchiCrypt Live Sie bei der Datensicherung?

Die "normale Datensicherung" (*Sicherung der Trägerdatei selbst*) können Sie mit Ihrem Standard-Backup Programm durchführen. Da die Inhalte der ArchiCrypt Live Laufwerke verschlüsselt sind, können Sie die Daten ruhigen Gewissens auf Streamer, CDR/CDRW, DVD oder andere Wechsel- und Sicherungsmedien speichern. Beachten Sie jedoch, dass es aufgrund der eingesetzten Verschlüsselung kaum möglich ist, die Daten zu komprimieren! Viele gute Backup Programme bieten auch die Option an, Partitionen zu sichern. Verfügt Ihr Backup Programm über diese Fähigkeit, nutzen Sie Ihr Programm. Falls nicht, können Sie auf die Funktion zur Sicherung und Wiederherstellung von Partitionen in ArchiCrypt Live zurückgreifen. Diese Funktionen bieten jedoch keinerlei Komfort und sind als *Notlösung* zu verstehen.

Die "Sicherung des Laufwerksheaders" können Sie mit Hilfe der Schlüssel-Sicherung durchführen. Sie können so ein Reserve- oder Notpasswort festlegen. Diese Sicherung kann bei Bedarf zurückgeschrieben werden. Ein Zugriff auf korrupte Trägerdateien ist mit diesen Maßnahmen gegebenenfalls möglich.

Siehe auch Schlüssel-Backup und -Recovery

13.2 Schlüssel-Backup und -Recovery

siehe auch: Wichtige Begriffe - Begriffserläuterungen
Schlüssel-Sicherung

Sicherung der Laufwerksschlüssel

Jedes ArchiCrypt Laufwerk verfügt mindestens über einen Zugangsschlüssel (Laufwerk-Administrator-Schlüssel), den Sie beim Erstellen des Laufwerks angegeben haben.
Daneben kann ein Laufwerk bis zu 3 Gastzugänge und einen Zugang zu einem Geheim-Container aufweisen. Mit ArchiCrypt Live Schlüssel-Sicherung ist es möglich, den Bereich des Laufwerkes zu sichern, in dem Prüfwerte aktueller Schlüssel und andere Informationen verschlüsselt abgelegt sind. Dieser Bereich wird auch als Laufwerksheader bezeichnet.

Der Laufwerksheader ist "*lebenswichtig*" für Ihr ArchiCrypt Live Laufwerk und sollte unmittelbar nach dem Erstellvorgang gesichert werden.

Das entsprechende Werkzeug finden Sie unter Werkzeuge - Schlüssel - Sicherung

14 Technischer Teil

14.1 Warum Verschlüsselung?

Ist Verschlüsselung sinnvoll?

"Ich habe nichts zu verbergen, ich habe keine Geheimnisse!"

Während man Menschen, die beruflich mit dem Computer arbeiten inzwischen Gott sei Dank nicht mehr erläutern muss, warum der Schutz bestimmter Daten Pflicht ist, sind viele Privatanwender immer noch der Meinung, Verschlüsselung sei nicht notwendig. Schließlich mache man nichts Illegales am Rechner, weswegen man auch nichts verbergen müsse. In dieser Aussage steckt implizit die Annahme, die Angreifer auf die Daten im Rechner seien Justiz- und Polizeibehörden. Doch genau hier irrt man. Die "Dunklen Seiten des Internet" lassen erahnen, wer es auf die Daten in Ihrem Rechner abgesehen hat. Es

geht um Identitätsdiebstahl, Diebstahl von Passwörtern, Ausspähen, Erpressen, Fernsteuern und Missbrauch von Rechnern. Also um all die Dinge, die man noch vor wenigen Jahren nur aus Science Fiction Filmen kannte. Heute ist dies traurige Realität.

Der Verlust vertraulicher Daten kann zum Ruin führen.

Im privaten Bereich kann es um die eigene Existenz gehen, im beruflichen Alltag um ein Unternehmen. In meinem Berufsleben habe ich viele Mitarbeiter und Kollegen gesehen, die, falls überhaupt, die eingebaute Möglichkeit von Kompressions- oder Office-Produkten nutzten um selbst eingestufte Informationen abzulegen und zu versenden. Eine trügerische Sicherheit! Selbst die Hersteller solcher Produkte verweisen in Ihren Hilfetexten auf die Unsicherheit der integrierten Verfahren. Jedoch dringt dies meist nicht bis zum Nutzer durch, da dieser bei dem Menüpunkt Verschlüsselung oder bei dem Reizwort Passwort direkt davon ausgeht, behandelte Daten seien gut geschützt.

Informationen haben sich zu einem der wichtigsten Wirtschaftsgüter entwickelt. Der Schutz dieser Daten ist die Herausforderung des 21 ten Jahrhunderts. In den letzten Jahren ist folgender Umstand hinzugekommen. Zahlreiche Rechner mit sensiblen Informationen (Kundendaten/Verträge/Urkunden/etc.) sind Bestandteil eines Netzwerks. Oft kennen Nutzer die Gefahr nicht, die droht, wenn Sie sich in das Internet einwählen oder im Falle eines DSL Zugangs ständig mit dem Internet verbunden sind. Die Software Firewall Systeme, die eine trügerische Sicherheit vermitteln, verleiten viele Nutzer zu einem sehr arglosen Umgang mit Daten auf Rechnern mit Verbindung zum Internet.

Da oft kein gesonderter Rechner zur Verfügung steht, über den ausschließlich auf das Internet zugegriffen wird, hilft nur Verschlüsselung.

Man sollte sich allerdings darüber im Klaren sein, dass es eine absolute Sicherheit nicht gibt. Auch die besten und ausgefeiltesten Tools können an diesem Umstand nichts ändern. Ziel jedoch muss es sein, das Risiko, sensible Daten zu verlieren, zu minimieren. Hierbei spielt die eingesetzte Software eine entscheidende Rolle.

"Verschlüsselung ist mir zu kompliziert"

Viele Menschen denken bei dem Thema Verschlüsselung an hochkomplizierte Vorgänge und Anwendungen, von denen man Alpträume bekommt. Viele Hersteller tragen diesem Vorurteil Rechnung und liefern entsprechende Anwendungen aus. Wer aber sagt, dass man die zugrundeliegende Komplexität von

Verschlüsselung an den Anwender weiter geben muss? ArchiCrypt Live ist eine unüberbietbar einfach zu bedienende Verschlüsselungssoftware, die den Anwender mit kryptographischen Fachbegriffen und komplizierten Vorgängen verschont. Mit dieser Einfachheit wird die Aussage "Verschlüsselung ist mir zu kompliziert" ungültig.

14.2 Verschlüsselung was ist das?

Was versteht man unter Verschlüsselung?

Verschlüsselungsverfahren sind immer dann gefordert, wenn es darum geht, vertrauliche Informationen über unsichere Informationskanäle zu übertragen oder allgemein, Daten vor dem Zugriff unbefugter zu schützen.

Man unterscheidet dabei grundsätzlich zwei Verfahren. Das symmetrische Verfahren, bei welchem zur Verschlüsselung und Entschlüsselung der gleiche Schlüssel zum Einsatz kommt und das asymmetrische Verfahren, bei dem man für das Ver- und Entschlüsseln unterschiedliche Schlüssel nutzt.

Bei asymmetrischen Kryptographie-Techniken wird mit einem öffentlich zugänglichen, nicht geheimen Code, dem so genannten Öffentlichen Schlüssel („public key") und einem Privaten Schlüssel („private key", Secret Key) gearbeitet. Eine Kombination aus beiden Verfahren wird als Hybrid-Codierung bezeichnet. Reine asymmetrische Verfahren kommen sehr selten vor und wenn, dann nur, wenn es um geringe Datenmengen geht. In Echtzeitumgebungen werden hingegen Hybride Verfahren genutzt, wobei die tatsächliche Datenverschlüsselung mit einem symmetrischen Verfahren durchgeführt wird.

ArchiCrypt Live nutzt sowohl reine symmetrische Verfahren als auch hybride Verfahren (Signatur, Versand).

Mein Verschlüsselungsprogramm hat aber eine 4096 BIT Verschlüsselung!

Im Zusammenhang mit der Sicherheit eines Verfahrens wird sehr gerne die s.g. Schlüssellänge in BIT herangezogen. Dabei können asymmetrische Verfahren mit sehr großen Schlüssellängen auf sich aufmerksam machen. Während AES (*Advanced Encryption Standard*) mit vergleichsweise kleinen 256 BIT aufwartet, bietet das berühmte RSA Verfahren (*benannt nach seinen Erfindern Ron Rivest, Adi Shamir, and Leonard Adleman.*) bis zu 4096 BIT lange

Schlüssel. Auf den ersten Blick ein überwältigender Vorteil des RSA Verfahrens. In Wahrheit handelt es sich hier jedoch um Äpfel und Birnen, die man bekanntermaßen nicht miteinander vergleichen kann. Dies ist durch die unterschiedliche mathematische Basis begründet, die den jeweiligen Verfahren zu Grunde liegt. Bei symmetrischen Verfahren werden 128 BIT als sicher angesehen, bei asymmetrischen 1024 BIT; immer unter bestimmten Rahmenbedingungen!
In diesem Zusammenhang tritt eine weitere Unart auf. Bestimmte Verfahren expandieren (*erweitern*) Schlüssel während des eigentlichen Verschlüsselungsvorgangs. Bestimmte Hersteller nutzen diesen Wert in Ihrer Werbung. Gelegentlich erfinden Sie auch neue Verfahren und warten mit gigantischen Schlüssellängen auf. Hüten Sie sich vor solchen Produkten, es könnte sich um Snake Oil (Snake Oil bei Wikipedia) handeln!

Was ist Kryptologie

Kryptologie ist wörtlich die „Wissenschaft der Verschlüsselung" und basiert auf mathematischen Algorithmen, die man heutzutage in Software umsetzt.
Im alten Rom wurde ein extrem simples Verfahren verwendet, welches darin bestand, jeden Buchstaben „X" der Nachricht durch einen anderen Buchstaben zu ersetzen, der sich aus einem bestimmten Abstand „X+n" zu dem Original ergibt. So wurde z. B. aus einem „A" ein „C", aus „B" ein „D", aus „C" ein „E", usw. Diese Methoden sind noch schwächer als die s.g. XOR-Verschlüsselung.

Die Sicherheit solcher Verfahren beruht auf der Schwierigkeit, aus den umgewandelten Daten ohne Kenntnis des Schlüssels, die Originaldaten wieder herzustellen.

Die Wahl des Verfahrens ist daher mit entscheidend für die Sicherheit eines Produktes! (siehe Eingesetzte Verfahren)

14.3 Eingesetzte Verfahren

Welche Verfahren nutzt ArchiCrypt Live

ArchiCrypt Live setzt per Voreinstellung den neuen AES (Advanced Encryption Standard) ein.
Dieser Algorithmus ging aus einem Wettbewerb als Sieger hervor, der 3 Jahre andauerte und in dem die vorgestellten Methoden strengsten Untersuchungen unterzogen wurden. Das Verfahren hat die Eigenschaft, dass die einzige Möglichkeit, unbefugt an Daten zu gelangen der s.g. Brute-Force Angriff ist. ArchiCrypt Live setzt die besonders sichere Variante mit einer Schlüssellänge von 256 BIT ein.

Das von Ihnen eingegebene Passwort wird dabei nicht direkt eingesetzt, sondern dient als Eingangsgröße für eine s.g. kryptografische Einweg-Hash-Funktion. Die notwendige Funktion muss 256 BIT liefern, die gegen s.g. Kollisionsattacken resistent sind. Die Umsetzung in ArchiCrypt Live orientiert sich dabei am SHS (Secure Hash Standard) des NIST (*National Institut of Standards and Technology*) und setzt das Verfahren SHA ein.
(*siehe auch Secure Hash Standard im Internet*)

ArchiCrypt Live setzt gleichzeitig eine s.g. KDF (*Key-Derivation-Function*) ein. Dabei wird die SHA Funktion 1000 mal durchlaufen. Grundlage für dieses Verfahren war der PKCS #5 Password-Based Cryptography Standard, welcher klare Vorgaben macht.

In der Endausscheidung waren von den anfänglich 15 Verfahren noch 5 Kandidaten im Rennen.
Obwohl die Verfahren von zum Teil äußerst renommierten Firmen eingebracht wurden, waren bei einigen Methoden schnell Schwachstellen und Lücken entdeckt. Dies sollte uns einmal mehr davor warnen, ein Verfahren unter Ausschluss der Öffentlichkeit zu entwickeln. Glauben Sie auch keinem Unternehmen, welches Ihnen einen neuen selbst entwickelten Algorithmus verkaufen will. Die Versuchung dies doch zu tun, ist aber offensichtlich sehr hoch.

Die Methoden der Endrunde lieferten sich hinsichtlich der Leistungen ein Kopf an Kopf Rennen. Letztlich fiel folgende Entscheidung:

Rijndael:	86 Stimmen
Serpent:	59 Stimmen
Twofish:	31 Stimmen
RC6:	23 Stimmen
MARS:	13 Stimmen

Die Entscheidung zu Gunsten von Rijndael kam letztlich dadurch zu Stande, dass er die Anforderungen (siehe AES), die unterschiedlich gewichtet wurden, am besten erfüllte. Gleichzeitig bedeutet dies jedoch, dass die anderen Verfahren durchaus in bestimmten Einsatzgebieten bessere Eigenschaften aufweisen, als der Gewinner. Sicher, nach heutigem Verständnis, sind alle der oben aufgeführten Methoden.

Sicher bedeutet in diesem Zusammenhang, dass die beste Methode ohne Passwort an die Klartextdaten zu gelangen die s.g. Brute-Force Methode ist. Man geht den Daten sozusagen mit roher Gewalt an den Kragen und testet alle möglichen Passwörter durch, bis man das korrekte Passwort erwischt hat.

Verschlüsselungsverfahren werden in einem bestimmten Modus aufgeführt (z.B. ECB - Electronic Code Book oder CBC Cipher Block Chaining).

ArchiCrypt Live greift seit Version 6 auf den Standard SISWG (*Security in Storage Workgroup*) (P1619.0 December 19, 2007 - Standard Architecture for Encrypted Shared Storage Media) – www.siswg.org zurück. In diesem Standard wird das Verfahren XTS-AES oder kurz XEX-Verfahren beschrieben.

XEX-AES

XEX ist ein Modus in dem AES ausgeführt wird. Es gibt 2 Schlüssel, die jeweils 256 BIT (256 BIT AES Verschlüsselung ECB und 256 BIT AES Verschl. Tweak) lang sind.

Warum XEX?

Von 2004 - 2006 war im Entwurf des P1619 AES im LRW Modus vorgesehen, eine Testabstimmung im August 2006 zeigte, dass die meisten SISWG Mitglieder dem Entwurf so nicht zustimmen würden. Man wechselte daher von LRW-AES zu XEX-AES (auch XTS-AES ab. Entwurf 11).

Gründe für die fehlende Unterstützung durch die SISWG Mitglieder:

- Ein Angreifer kann unter bestimmten Voraussetzungen den LRW Tweak Schlüssel ableiten, wenn der Klartext den Tweak Schlüssel selbst und einen Nullblock enthält.

- Wenn der Tweak Schlüssel bekannt ist (*dies war zunächst sogar so vorgesehen [Tweak Key nicht geheim; in ArchiCrypt Live jedoch nicht umgesetzt, sondern ebenfalls geheim)* ist die LRW Variante nicht mehr von der ECB Variante zu unterscheiden. Der Verlust des Tweak Schlüssels wirkt sich jedoch nicht auf die Sicherheit des Algorithmus im ECB Modus aus.

Ein weiterer wichtiger Grund ist die höhere Geschwindigkeit von XEX gegenüber LRW AES.

```
/* SINGLE 128 BIT block
The XEX-AES encryption procedure for a single 128-bit block is modeled
with this equation:
C = XEX-AES-blockEnc(Key, P, i, j)
where:
Key is the 256, 320, or 384 bit XEX-AES key
P is a block of 128 bits (i.e., the plaintext)
i is a 128-bit tweak value, representing the number of the data unit
(see clause  6.1)
j is the sequential number of the 128-bit block inside the data unit
```

```
C is the block of 128 bits of ciphertext resulting from the operation
The key is parsed as a concatenation of two fields, Key = Key1 | Key2,
with Key2
consisting of the last 128 bits of Key and Key1 consisting of the first
128, 192, or 256 bits.
The ciphertext shall then be computed by the following or an equivalent
sequence of
steps:
j
1.  T = AES-enc(Key2,i) GFMUL (GF(2) mod x^128+x^7+x^2+x+1
2.  PP = P XOR  T
3.  CC = AES-enc(Key1 ,PP)
4.  C = CC XOR  T

AES-enc(K,P) is the procedure of encrypting plaintext P using AES
algorithm with key
K, according to FIPS-197. The multiplication and computation of power in
line 1 is
128 executed in GF(2 ) field.
*/
/* 128 oder mehr BIT
The XEX-AES encryption procedure for a data unit of plaintext of 128 or
more bits is modeled with this
equation:
C = XEX-AES-Enc(Key, P, i),
where
Key is the 256, 320, or 384 bit XEX-AES key
P is the plaintext
i is a 128-bit tweak, representing number of the data unit  (see clause
 6.1)
C is the ciphertext resulting from the operation, of the same bit-size
as P

The plaintext data unit is first partitioned into m+1 blocks,
P = P0 … Pm 1Pm
where m is the largest integer such that 128m is no more than the bit-
size of P, the first m
blocks P0,…, Pm 1 are all exactly 128-bit long, and the last block Pm is
between 0 and
127-bit long. The ciphertext C is then computed by the following or an
equivalent
sequence of steps:
1.  for q=0 to m-2
2.      Cj = XEX-AES-blockEnc(Key, Pj, i, q)    //
3.  endfor
4.  b = bit-size of Pm
5.  if b=0
6.      Cm-1 = XEX-AES-blockEnc(Key, Pm-1, i, m-1) //
7.      Cm = empty
8.  else
// Pm is a partial block
9.      CC = XEX-AES-blockEnc(Key, Pm-1, i, m-1)  //
10.      Cm = first b bits of CC
11.      CP = last (128-b) bits of CC
```

```
12.      PP = Pm | CP
// PP is a 128-bit block
13.      Cm-1 = XEX-AES-blockEnc(Key, PP, i, m)  //
14.  endif
15.  C = C1 … Cm-1 Cm

*/
```

Informationen über die Verfahren erhalten Sie unter den angegebenen Internetadressen:

- MARS - IBM
- RC6 - RSA Laboratories
- RIJNDAEL - Joan Daemen, Vincent Rijmen
- Serpent - Ross Anderson, Eli Biham, Lars Knudsen
- Twofish - Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson
- Blowfish - Bruce Schneier

Um den sicheren Versand zu realisieren und die Funktionen zur Signatur bereitzustellen, nutzt ArchiCrypt Live das berühmte RSA Verfahren. Es wurde im Jahre 1977 von Ron Rivest, Adi Shamir und Leonard Adleman entwickelt. Das Verfahren basiert auf der Tatsache, dass es zwar ohne Weiteres möglich ist, das Produkt n zweier großer Primzahlen p und q zu berechnen, der umgekehrt Weg, die beiden Primzahlen aus dem Produkt zu berechnen (faktorisieren), derzeit technisch eine unüberwindbare Hürde darstellt.
Der RSA-Algorithmus nutzt diese Eigenschaft, indem er als öffentlichen Schlüssel eine Zahl O und als privaten Schlüssel eine weitere Zahl R verwendet, die aus diesen beiden Primzahlen p und q über ein Verfahren gebildet werden. Die Primzahlen p und q werden hingegen nicht veröffentlicht!

Die Schlüssel, die ArchiCrypt Live generiert und zur Verschlüsselung und zur Signatur einsetzt, haben eine Bitlänge von 1024. Zum Signieren wird MD5 (Message Digest 5) verwendet. MD5 definiert ein Verfahren zur Erzeugung digitaler Unterschriften; es ist in RFC 1321 (RFC = Request for comment) definiert.

Alle der aufgeführten Verfahren sind als Referenzimplementierung in der Programmiersprache C, teilweise auch in Java frei verfügbar. Zudem gibt es für jedes Verfahren s.g. Testvektoren, mit denen man sicherstellen kann, dass die Implementation der Verfahren korrekt ist.

14.4 ArchiCrypt Card (Info)

Die ArchiCrypt Card zeichnet sich durch folgende Eigenschaften aus

Hardware-Zufallszahlengenerator
ArchiCrypt Card kann echte Zufallszahlen generieren

➡HINWEIS***: Zum Erstellen von sicheren Passwörtern/Schlüsseln werden ECHTE Zufallszahlen benötigt. Ein normaler Computer kann keine echten Zufallszahlen generieren. Daher müssen Sie zum Beispiel beim Erstellen von Schlüsseldateien die Maus bewegen.***

Speicher für Nutzerinformationen
Die ArchiCrypt Card bietet die Möglichkeit Informationen über den Nutzer/Besitzer zu speichern.

Verschlüsselter Datentransfer
Die Daten zwischen SmartCard Reader und Anwendung werden automatisch mit dem Advanced Encryption Standard AES 128 BIT verschlüsselt.

SHA1 Hashing
ArchiCrypt Card kann Hashwerte nach dem SHA1 Standard bilden

3DES
ArchiCrypt Card kann Daten mit Hilfe des 3DES Verfahrens ver- und entschlüsseln. Die Ver-/Entschlüsselung erfolgt dabei mit 256 BIT Schlüsseln, die auf der Karte generiert oder abgelegt sind.

AES Advanced Encryption Standard
ArchiCrypt Card kann Daten mit Hilfe des Advanced Encryption Standard (AES) Verfahrens ver- und entschlüsseln. Die Ver-/Entschlüsselung erfolgt dabei mit 256 BIT Schlüsseln, die auf der Karte generiert oder abgelegt sind.

Unterstützt PC/SC (Personal Computer/SmartCard) Standard
Nahezu alle aktuellen SmartCard Reader unterstützen den PC/SC Standard und können mit der ArchiCrypt Card zusammenarbeiten.

Erweiterte PIN
Die ArchiCrypt Card kann mit PIN geschützt werden, wobei es sich nicht um eine normale PIN, sondern um eine Passwort/Schlüssel handelt, der aus bis zu 100 beliebigen Zeichen bestehen kann.

Erweiterte Master-PIN
Die Master PIN, ebenfalls ein Passwort/Schlüssel von bis zu 100 Zeichen kann eingesetzt werden, um Nutzerinformationen gegen

Änderung zu schützen. Gleichzeitig verhindert die Master-PIN, dass Schlüssel von der Karte gelöscht werden können.

Schutz der Schlüssel

Die Schlüssel können ausschließlich mit den durch die ArchiCrypt Card bereitgestellten Funktionen ausgelesen werden. Sind die Schlüssel mit PIN geschützt, ist ein Auslesen ohne Angabe der PIN nicht möglich.

➡HINWEIS***: Nicht jede Anwendung, die auf die ArchiCrypt Card zurückgreift, nutzt alle Funktionen.***

14.5 Was sind Zertifikate

Der Begriff Zertifikat

In der freien Enzyklopädie Wikipedia (www.Wikipedia.de) findet sich folgende Definition:

Durch ein Zertifikat kann man den Nachweis erbringen, dass ein öffentlicher Schlüssel eines asymmetrischen Verschlüsselungsverfahrens zu der vorgeblichen Person oder Institution gehört.
Dies ist vor allem im Zusammenhang mit digitalen Signaturen von Bedeutung. Dabei verschlüsselt der Sender der Signatur eine Nachricht mit seinem privaten Schlüssel. Der Empfänger kennt den öffentlichen Schlüssel der Person und kann die Nachricht daher entschlüsseln. Es ist jedoch durch dieses Verfahren noch nicht sichergestellt, dass der öffentliche Schlüssel auch tatsächlich zu der Person gehört, die der Sender zu sein vorgibt. Diese Sicherheit kann erst durch ein Zertifikat erreicht werden. Sie wird dabei durch eine Zertifizierungsstelle (engl. Certification Authority [CA] oder Trust Center [TC]) ermöglicht.

Ein Zertifikat ist ein Datensatz, der Informationen über den Namen des Inhabers, dessen öffentlichen Schlüssel, eine Seriennummer, eine Gültigkeitsdauer und den Namen der Zertifizierungsstelle enthält. Diese Daten sind in der Regel mit dem privaten Schlüssel der Zertifizierungsstelle signiert und können somit mit dem öffentlichen Schlüssel der Zertifizierungsstelle überprüft werden. Zertifikate für Schlüssel, die nicht länger sicher sind, können über eine so genannte Certificate Revocation List gesperrt werden.

Aus dieser Struktur ergibt sich die Notwendigkeit einer obersten Zertifizierungsinstanz, denn auch der öffentliche Schlüssel einer Zertifizierungsstelle muss schließlich mittels eines Zertifikats überprüfbar sein. In Deutschland übernimmt die

Regulierungsbehörde für Telekommunikation und Post (RegTP) diese Aufgabe. In der neuesten Terminologie wurde im übrigen der Begriff Zertifizierungsstelle durch Zertifizierungsdiensteanbieter ersetzt. Die RegTP führt eine Liste aller akkreditierten Zertifizierungsdiensteanbieter.

Privater Schlüssel

Ihr Privater Schlüssel (oft auch als geheimer Schlüssel, private-key oder secret key bezeichnet), wird verwendet um Daten zu entschlüsseln, die jemand mit Ihrem öffentlichen Schlüssel verschlüsselt hat. Neben dieser Aufgabe können Sie mit dem Privaten Schlüssel Daten signieren und damit Authentizität und Integrität sicherstellen.
Ihren privaten Schlüssel gilt es um jeden Preis geheim zu halten. Er darf keinesfalls weitergegeben werden.

Öffentlicher Schlüssel

Der Öffentliche Schlüssel (public-key) kann frei verteilt und jedem zugänglich gemacht werden. Sie können den Schlüssel also zum Beispiel per Email versenden oder auf Ihrer Internetseite veröffentlichen. Er dient Ihren Kommunikationspartnern dazu, Signaturen zu überprüfen und Daten zu verschlüsseln, zu denen ausschließlich Sie Zugriff haben sollen. Möchten Sie einer Person ein Laufwerk übersenden, benötigen Sie entsprechend seinen öffentlichen Schlüssel.

Eigenschaften von Öffentlichem und Privatem Schlüssel

Die nachfolgenden Funktionen beruhen auf einer verblüffenden Eigenschaft der Verschlüsselung mit Privatem und Öffentlichem Schlüssel. Daten, die mit einem öffentlichen Schlüssel verschlüsselt wurden, können nur von dem wieder entschlüsselt werden, der im Besitz des Privaten Schlüssels ist.
Zur Verdeutlichung kann man sich z.B. einen Briefkasten vorstellen. Das Einwerfen eines Briefes könnte man mit dem Verschlüsseln (der öffentliche Schlüssel kann jedem zugänglich gemacht werden) bezeichnen. Jeder kann hier Schriftstücke einwerfen.
Um jedoch an die Nachrichten heranzukommen, benötigt man hingegen den Schlüssel für den Briefkasten (geheimer Schlüssel). Das Öffnen ist auf den Besitzer dieses Schlüssels begrenzt, der entsprechend sorgfältig darauf achten muss, dass niemand seinen Schlüssel stielt.

14.6 Passwörter

Regeln zur Passwortgestaltung

Passwörter werden meist als Schlüssel oder als Ausgangspunkt für eine Schlüsselberechnung genutzt (siehe Eingesetzte Verfahren). Sie sind quasi der Schlüssel zum Schloss, welches unsere Daten vor unbefugtem Zugriff schützt. Es ist sicher einleuchtend, dass es auf zwei Dinge ankommt. Die Methode (*der Algorithmus*) die zur Ver- und Entschlüsselung genutzt wird und das Passwort müssen sicher sein. Was nutzt die beste Methode wenn Sie als Passwort den Buchstaben A wählen. Was nutzt das beste Passwort, wenn Sie als Methode eine XOR-Verknüpfung wählen.

Keine Begriffe aus Ihrem soziallen Umfeld

Sie sollten keinesfalls Geburtsdaten, Namen, Hobbys, Lieblingsverein, usw. nutzen. Die Passworte entstammen Ihrem sozialen Umfeld. Einem Angreifer der sich über Ihre Lebensumstände, Ihre Vorlieben etc. informiert, fällt es leicht, auf die Lösung zu kommen.
Vor diesem Fehler kann die Passwortbewertung von ArchiCrypt Live Sie nicht bewahren!

Keine lexikalischen Begriffe

Vermeiden sollten Sie auch lexikalische Begriffe. Ein Wörterbuch enthält um die 120.000 Einträge. Für einen Angreifer ist es leicht die 120.000 Wörter mit Hilfe eines Computers in wenigen Sekunden zu testen. Um aus diesem Fundus dennoch zu schöpfen, müssten Sie ein Passwort bilden, welches aus ca. acht Einzelworten mittlerer Länge besteht (siehe auch Bewertung von Passwörtern).
Vor diesem Fehler kann die Passwortbewertung von ArchiCrypt Live Sie nicht bewahren!

Keine Passwörter nur aus Ziffern

Zahlen sind verlockend, aber höchst gefährlich, wenn man das Passwort ausschließlich aus Ziffern aufbaut. Geben Sie in ArchiCrypt ein Passwort ein und achten Sie auf die Bewertung (siehe Passworteingabe). Um ein einigermaßen sicheres Passwort zu erhalten müssen Sie sich sehr viele Ziffern merken. Leider sind es 77 Ziffern, die Sie sich merken müssen, um ein Maximum an Sicherheit aus ArchiCrypt Live und AES herauszuholen.

Um dennoch die Sicherheit der Methoden zu nutzen, wurden die s.g. Schlüsseldateien, ArchiCrypt Cards und Security Tokens

integriert, die als Schlüssel eine zufällige und ausreichend große Datenmenge liefern.

Nicht nur Groß- /oder Kleinbuchstaben

Wir haben 26 Groß- und 26 Kleinbuchstaben, 10 Ziffern und 42 Sonderzeichen zur Verfügung. Sie müssen sich "nur noch" ca. 38 Zeichen merken um ein sicheres Passwort aufzubauen. Es ist allerdings schwierig, sich solche Zeichenkombinationen zu merken. Man kann eigene Methoden zur Passwortgenerierung entwickeln. Man schreibt sich einen genügend langen Satz auf, den man sich gut merken kann. Darunter eine Ziffernfolge die man sich merken kann. Vom Satz behalten Sie nur noch die Anfangsbuchstaben der Einzelworte bei. Alle 2 oder drei Buchstaben schreiben Sie jetzt eine Ziffer im Wechsel mit einem beliebigen Sonderzeichen auf. Merken müssen Sie sich das Ergebnis oder den Konstruktionsweg allerdings immer noch. Abhilfe schafft gegebenenfalls die Schlüsseldatei, eine SmartCard oder ein Token.

Sichere Passwörter

Ein für ArchiCrypt Live sicheres Passwort (*genauer gesagt ein Schlüssel*) besteht aus 32 zufälligen Zeichen aus dem ASCII-Bereich (siehe ASCII-Tabelle). Zur Speicherung eines Zeichens wird ein Byte verwendet. Bekanntlich besteht ein Byte aus 8 Bit. Mit diesen 8 Bit kann man 2^8 verschiedene Zeichen erzeugen. Das sind 256. Genau aus diesen 256 Zeichen besteht die ASCII-Tabelle.

So könnte Ihr Passwort aussehen

12-16 Zeichen sollte es jedoch umfassen. Es sollte neben Ziffern auch Groß- und Kleinbuchstaben, sowie Sonderzeichen enthalten.

Bsp.:
JaMatasaKa12+2

14.7 Bewertung von Passwörtern

siehe auch Angriff auf Verschlüsseltes

Wie wird das Passwort bewertet

➡ACHTUNG: ArchiCrypt Live kann nicht beurteilen, ob ihr Passwort trotz ausreichender Länge für einen Angreifer leicht zu erraten ist. Beachten Sie unbedingt die Hinweise im Kapitel Passwörter. Die Bewertung arbeitet stupide und rein mathematisch, eine Wortsinnanalyse ist nicht integriert.

Die Passwortbewertung in ArchiCrypt Live ist äußerst ausgeklügelt. Sie bewertet das Passwort statistisch mathematisch und schützt in Echtzeit vor s.g. Wörterbuchattacken. Während der Eingabe prüft ArchiCrypt Live, ob das von Ihnen angegebene Passwort so oder ähnlich in einem Wörterbuch enthalten ist. Wörterbücher werden von Angreifern genutzt, um Zugang zu sensiblen Daten zu erhalten.

14.8 Sinnvoller Einsatz von Schlüsseldateien

Was ist eine Schlüsseldatei?

Eine Schlüsseldatei ist eine Datei, die einen optimal auf die Erfordernisse der Verschlüsselung abgestimmten Schlüssel enthält.

Beim Erstellen der Schlüsseldatei werden Zufallsdaten gesammelt. Um wirklich zufällige Daten zu erhalten, ist Ihre Mithilfe erforderlich. Die Bewegungen des Mauszeigers liefern Werte, aus denen mit Hilfe bestimmter mathematischer Verfahren (*u.a. basierend auf SHA-1 und SHA-512*) geeignete Zufallsdaten gesammelt werden. Der Computer selbst ist nicht in der Lage, wirklich zufällige Daten zu erzeugen. Sie würden sich auch beschweren, wenn es anders wäre. Ein vorhersagbares (*deterministisches*) Verhalten ist Grundvoraussetzung für einen produktiven Einsatz des Rechners.

Für wen eignet sich eine Schlüsseldatei?

Schlüsseldateien sind besonders für all jene geeignet, die es leid sind, sich Passwörter zu merken oder diese umständlich einzutippen.
Besonders gut geeignet ist diese Methode auch für kleinere Teams, die miteinander kommunizieren und Daten austauschen. Dazu sollte bei einem der ersten Meetings der Besprechungspunkt Datenaustausch mit auf die Tagesordnung gesetzt werden. Für jeden Teilnehmer sollte jetzt ein Medium mit identischer Schlüsseldatei bereit liegen. Ein paar einleitende Worte über die Wichtigkeit des sicheren Datenaustausches und den richtigen Umgang mit der Schlüsseldatei schließen diesen Punkt ab.

Wie sollte man mit der Schlüsseldatei umgehen?

Die Schlüsseldatei (*in der unverschlüsselten Form; siehe* Schlüsseldatei erstellen), erlaubt den Zugriff auf ein ArchiCrypt Live Laufwerk. Entsprechend sorgfältig sollten Sie die Datei/den Datenträger auf dem diese Datei abgelegt ist, aufbewahren.

Bedenken Sie, dass Wechselmedien (*Disketten/CD-R/RW,etc.*) derart beschädigt werden können, dass die darauf befindliche Schlüsseldatei nicht mehr gelesen werden kann. Arbeiten Sie also immer nur mit einer Kopie der Schlüsseldatei!

 ***TIPP: Als Alternative bietet sich die ArchiCrypt Card oder ein Security Token an. Beachten Sie jedoch die*** Systemvoraussetzungen!

14.9 AES

siehe auch Eingesetzte Verfahren

Der Advanced Encryption Standard

Das NIST (National Institute of Standards and Technology) rief 1997 weltweit dazu auf, ein neues symmetrisches Verschlüsselungsverfahren zu entwickeln.

Am 02.10.2000 erklärte der amerikanische Staatssekretär Norman Mineta den Algorithmus der beiden belgischen Kryptographen Joan Daemen von der Firma Proton-Welt International und Vincent Rijmen Mitglied von der Katholischen Universität Leuven zum neuen Standard der Nation.

Der Rijndael Algorithmus ist damit der Gewinner eines dreijährigen Wettbewerbes, an denen sich einige der führenden Kryptographen der Welt beteiligten.

Der Wettbewerb selbst wurde mit großer Begeisterung aufgenommen. Auf der 2. AES-Konferenz am 22./23. März 1999 in Rom wurden die zur Diskussion stehenden Algorithmen sowie die dazu durchgeführten Analysen vorgestellt und diskutiert. Die Konferenz hatte ca. 180 Teilnehmer aus 23 Ländern und es wurden 21 White-Papers vorgestellt. In der ersten Runde gab es hierzu 15 Vorschläge, aus welchen in mehreren Schritten der endgültige AES Algorithmus ausgewählt werden sollte. Informationen hierzu finden Sie unter http://www.nist.gov/aes.
In der zweiten Runde gab es noch die Kandidaten: MARS, RC6, Rijndael, Serpent und Twofish.

Der Gewinner sollte folgenden Anforderungen genüge leisten:

Aufruf des NIST vom 12.09.1997

Symmetrische Blockchiffre

- Unterstützt mindestens die Schlüssellängen 128, 192 und 256 bits und eine Blocklänge von 128 bits
- Besser als derzeitige Verfahren: Sicherer und effizienter (hinsichtlich Laufzeit, Platzbedarf auf Chip) als Triple-DES
- Einsetzbar in verschiedenen Anwendungsumgebungen
- Verwendbar für Stream Cipher, Message Authentication Code (MAC) Generator, Pseudozufallszahlen-Generator, Hashfunktion etc.
- Implementierbar in Hard- und Software
- Weltweit lizenzfrei verfügbar
- Sicherheit soll für 20-30 Jahre gewährleistet sein
- Der Algorithmus soll öffentlich definiert und evaluiert sein.

War es bisher ein Privileg von Regierungen und Militärs, sensible Daten mit kryptographischen Mitteln zu schützen, verwendet heute fast jeder solche Mittel, ohne es zu merken. Beim Surfen im Internet, bei der Nutzung von Pay-TV, beim Gebrauch der EC-Karte, beim Telefonieren usw.

Das neue AES-Verfahren hat sich inzwischen auf unseren gesamten Lebensbereich ausgedehnt. Viele Unternehmen und Dienstleister setzen das Verfahren ein.

14.10 Angriff auf Verschlüsseltes

Verschlüsselung knacken

Zuverlässige Kryptographie-Verfahren sollten fast unmöglich zu knacken sein. Der Aufwand für einen hochwertigen Algorithmus muss im Übrigen nicht unbedingt höher sein als für eine weniger effektive Lösung. Verfolgt man keine besondere Strategie, um einen Code zu knacken, muss man notfalls jede erdenkliche Kombinationen durchprobieren, bis man zufällig (*siehe auch* Entropie)- irgendwann die Lösung findet. Mit steigender Codelänge wächst zwar die benötigte Rechenzeit exponentiell, doch alle 18 Monate verdoppelt sich gemäß Mooreschen Gesetz die Performance der jeweils aktuellen Rechner. Für einen 56-Bit-Schlüssel benötigt man bereits ein Computernetzwerk. 64- bis 80-Bit-Schlüssel sind vorerst nur von wenigen Staaten und Institutionen zu knacken, so dass man einen 128-Bit-Schlüssel zurzeit als noch sicher einstuft.
ArchiCrypt Live setzt 256 BIT ein und ist nach heutigen Gesichtspunkten auf der absolut sicheren Seite.

Aus der Länge des Schlüssels kann man nur ableiten, wie viele Versuche ein potentieller Angreifer im ungünstigsten Fall unternehmen muss um den Code zu brechen. In der Regel werden sehr viele solche Kombinationen durchgerechnet, bevor der Code

gebrochen ist. Eine Methode, die sich mittels Brute-Force innerhalb einer Woche knacken lässt, kann auch schon zufällig nach drei oder vier Tagen, in Ausnahmefällen auch innerhalb eines Tages - aber nur mit sehr niedriger Wahrscheinlichkeit - geknackt sein. Wie man sieht, ist die bloße Länge des Schlüssels nicht der einzige Garant für hohe Sicherheit. Wurde der Schlüssel aus einer Zufallssequenz abgeleitet und wurde diese Sequenz nur „pseudo"-zufällig erzeugt, so kann auch ein vergleichsweise langer Schlüssel brechbar sein. Dann nämlich, wenn sich die Regel, nach der er errechnet wurde, ermitteln lässt. ArchiCrypt Live nutzt daher Ihre Mausbewegungen und viele andere Systemereignisse zur Erzeugung eines Zufallszahlenpools.

Ein kryptografisches Verfahren gilt als sicher, wenn die beste Methode ohne Schlüssel an die Daten zu gelangen die s.g. Brute-Force-Methode ist. D.h. man testet jeden möglichen Schlüssel.

Im Falle von ArchiCrypt Live wird die besonders sichere AES Implementierung mit einer 256 BIT Schlüssellänge. Im schlechtesten Fall muss ein Angreifer 2^256 verschiedene Schlüssel testen, bis er den richtigen Schlüssel findet.

Dies ergibt ca. 1,157920892373161954235709850086 9e+77 verschiedene Schlüssel. Geht man davon aus dass ein Rechner 1000000 (1 Million) Schlüssel pro Sekunde durchtesten kann, bleiben

1,157920892373161954235709850086 9e+71 Sekunden

1,929868153955269923726183083478 1e+69 Minuten

3,216446923258783206210305139130 2e+67 Stunden

1,340186218024493002587627141304 3e+66 Tage

3,671743063080802746815416825491 1e+63 Jahre

Sie sehen also, dass es recht lange dauern kann, bis man auf diese Art an die geheimen Informationen kommt.
Es gibt auch interessante Berechnungen darüber, ob die Masse der Erde ausreicht (E=m*C^2), um die bei den Berechnungen nötigen Energiemengen aufzubringen.

Das Ziel eines Angriffs muss nicht unbedingt sein, alle Daten als Klartext zu erhalten. Ziel kann zum Beispiel schon sein, eine Aussage darüber zu treffen, ob in einer bestimmten verschlüsselten Datei ganz bestimmte Daten vorliegen (*die der Angreifer als Klartext besitzt*). Um solche Angriffe (*Wasserzeichen-Angriff*) zu vereiteln, die durchaus kritischer Natur sein können, setzt ArchiCrypt Live ab Version 5 den

kommenden Standard P1619 ein, der speziell diese Art der Angriffe auf sektorbasierte Verschlüsselungsverfahren vereitelt.

14.11 Hashfunktionen

Eindeutige Prüfsummen

Eine Hashfunktion ist eine Funktion, die eine Eingabe beliebiger Länge erhält und einen Funktionswert, den so genannten Hashwert liefert. Dieser Hashwert hat eine vorgegebene Länge. Die Funktionen die bei ArchiCrypt Live zum Einsatz kommen sind SHA 1 (Secure Hash Algorithm 1), der einen Hashwert der Länge 160 Bit liefert und SHA-512 der einen 256 BIT langen kryptografisch sicheren Wert liefert.

Im kryptografischen Umfeld kommen nur Hashfunktionen zum Einsatz mit denen es möglich ist, einen Hashwert zu einer Eingabe zu ermitteln. Eine Berechnung der Eingabe aus dem Hashwert hingegen ist unmöglich. (Diese Eigenschaft wird auch als Einweg-Eigenschaft bezeichnet, Funktionen mit dieser Eigenschaft als Einweg-Hashfunktionen.)

Die Anforderungen reichen weiter: Die Funktion muss öffentlich sein, d.h. jeder muss Zugriff auf die Funktion haben. Weiterhin soll es unmöglich sein, 2 unterschiedliche Eingabewerte zu finden, die den gleichen Hashwert liefern (Kollisionsfreiheit; wegen Kollisionsattacken). Da die Hashwerte genutzt werden, um Identitäten zu überprüfen, wäre es sonst nicht mehr möglich, eindeutig zu identifizieren.

ArchiCrypt Live setzt diese Funktion für verschiedene Zwecke ein. Der erste Einsatzfall ist die Aufbereitung der Zufallsdaten die bei der Generierung von Passwörtern und Schlüsseldaten gesammelt werden. Der zweite Einsatz kommt bei der Identifikation von Passwörtern und der Ableitung von Schlüsseln aus Passwörtern zum Einsatz.

14.12 Entropie

Informationsgehalt

Die Entropie einer Datei ist ein Maß für den Informationsgehalt.
Die Entropie wird in bit/char (sprich Bit pro Zeichen) angegeben.

Informationsgehalt:

Für die Berechnung des Informationsgehaltes betrachtet man die Wahrscheinlichkeitsverteilung der Zeichen in einer Datei. Man geht davon aus, dass die einzelnen Bytes der Datei stochastisch unabhängig voneinander sind und mit gleicher Wahrscheinlichkeit in der Datei auftreten.

Der Informationsgehalt einer Nachricht N[I] ist definiert:

Informationsgehalt(N[I]) := log2(1/P[I]) = -log2(P[I]).

P[I] ist dabei die Wahrscheinlichkeit, mit der die Nachricht N[I] in der Datei auftritt. log2 bezeichnet den Logarithmus zur Basis 2.
Der Informationsgehalt hängt damit ausschließlich von der Wahrscheinlichkeitsverteilung ab. Der semantische Inhalt geht dabei nicht in die Berechnung ein.
Da der Informationsgehalt einer seltenen Nachricht höher als der einer häufigen Nachricht ist, wird in der Definition der Kehrwert der Wahrscheinlichkeit verwendet.

Der Informationsgehalt zweier unabhängig voneinander ausgewählter Nachrichten ist gleich der Summe der Informationsgehalte der einzelnen Nachrichten.

Entropie

Mit der Definition des Informationsgehaltes kann nun die mittlere Information berechnet werden.

Für die Mittelwertbildung werden die einzelnen Nachrichten mit der Wahrscheinlichkeit ihres Auftretens gewichtet.

Entropie(P[1], P[2], ..., P[r]):= -(P[1] * log(P[1]) + P[2] * log(P[2]) + ... + P[r] * log(P[r]))

Man kann das etwas verständlicher wie folgt beschreiben:
Die Entropie gibt die Unsicherheit als Anzahl der notwendigen Ja / Nein-Fragen zur Klärung einer Nachricht oder eines Zeichens an. Hat ein Zeichen eine sehr hohe Auftrittswahrscheinlichkeit, so hat es einen geringen Informationsgehalt. Dies entspricht etwa einem Gesprächspartner, der regelmäßig mit "ja" antwortet. Antworten, die sehr selten auftreten, haben einen hohen Informationsgehalt.

In diesem Zusammenhang sind die Extremwerte interessant:
Ein Dokument, welches nur Ziffern enthält, kann im schlechtesten Fall 0 bit/char Entropie besitzen, ein Dokument, in welchem alle Ziffern mit gleicher Wahrscheinlichkeit auftreten kann die Entropie (im Höchstfall) log2(10) = 3,3219 besitzen.

Für uns ist noch von Interesse, welche maximale Entropie in Dateien auftreten kann. Unsere Dateien sind aus Bytes aufgebaut. Also 8 Bit. Mit diesen 8 Bit kann man 256 verschiedene Zeichen darstellen (siehe auch ASCII_Tabelle).
Die Entropie für solche Dokumente beträgt mindestens 0 bit/char und höchstens 8 bit/char, falls in der Datei alle Zeichen gleich häufig vorkommen.

Entropie einer Datei
Die Entropie einer vorliegenden Datei kann also relativ leicht ermittelt werden. Man ermittelt für eine gegebene Datei, wie oft jedes Zeichen vorkommt.

das war schon immer so, man glaubt es kaum, aber es stimmt.

a := 6
b := 2
c := 1
d := 1
e := 4
h := 1
i := 2
k :=1
l := 1
m := 6
n := 2
o := 2
r := 3
s := 6
t := 3
u := 2
w := 1

Anschließend setzt man die Werte in obige Gleichung ein und erhält einen Entropiewert von 3,2682.
Wobei P[a] = 6 / 58, P[b] = 2 / 58 usw.
Verschlüsselte Dokumente kann man eventuell am Entropiewert erkennen. Je näher dieser Wert am Maximum liegt, desto größer ist die Wahrscheinlichkeit, dass es sich um eine verschlüsselte Datei handelt. Man kann diese Methode dazu nutzen, abzuschätzen, ob ein Angriff auf eine Datei erfolgreich war. Man testet verschiedene Passworte und nimmt das Ergebnis als Klartext, bei welchem der Entropiewert am geringsten ist.
Auf der anderen Seite sollte ein Verschlüsselungsverfahren immer Daten liefern, die einen fast maximalen Entropiewert besitzen. In unserem Fall also bei 7,9 und höher.

14.13 XOR

Das exklusive Oder

Dieses Verfahren können Sie selbst auf einem Blatt Papier nachvollziehen.
Der Schlüssel für dieses Verschlüsselungsverfahren besteht aus einer Folge von Bits (siehe auch Passwörter).

Der Schlüssel wird bitweise mit den Bits des Klartextes mittels exklusivem Oder (XOR) verknüpft.
Der Schlüssel selbst wird dabei zyklisch verwendet. D.h. Sind die Bits des Schlüssels aufgebraucht, beginnt man erneut beim ersten Schlüsselbit.
Die Entschlüsselung geschieht durch erneute Anwendung der Verknüpfung mit XOR. Dies ist eine Eigenschaft der XOR-Verknüpfung, die in der Fachsprache mit Involution bezeichnet wird.

Es gilt ((A XOR B) XOR B) = A für alle Wahrheitswerte A und B.

Das exklusive Oder ermittelt aus zwei Wahrheitswerten (FALSCH=0 und WAHR=1) einen neuen Wahrheitswert.

In der nachfolgenden Wahrheitstabelle ist dies aufgeführt:

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

Falls beide Werte gleich sind, wird also 0 = FALSCH geliefert. Falls genau ein Wert WAHR ist, liefert die Verknüpfung 1 = WAHR.

Beispiel:

Klartext:	1	0	1	1	0	0	1	0
Schlüssel:	1	0	0	0	1	1	1	1
Ergebnis:	0	0	1	1	1	1	0	1

Um aus dem Verschlüsselungsergebnis erneut den Klartext zu erhalten,
wenden wir erneut die XOR-Operation unter Verwendung des Schlüssels an.

Ergebnis:	0	0	1	1	1	1	0	1
Schlüssel:	1	0	0	0	1	1	1	1
Klartext:	1	0	1	1	0	0	1	0

Kennt man das am häufigsten vorkommende Zeichen im Klartext, so ist die Ermittlung des Schlüssels und somit auch des Klartextes möglich.

14.14 ASCII Tabelle

ASCII Tabelle

Diese ASCII Tabelle enthält alle 256 ASCII Zeichen. In der ersten Spalte steht der dezimale Wert (Dez), in der zweiten der hexadezimale Wert (Hex) und in der dritten das Zeichen, sofern darstellbar. Die Hex Angabe ist wichtig um in ArchiCrypt spezielle Zeichen in Passwörtern nutzen zu können. Damit können Sie Zeichen nutzen, die sich nicht auf Ihrer Tastatur befinden. Wenn Sie ein solches Zeichen eingeben wollen, leiten Sie das Zeichen bei der Eingabe durch das Zeichen $ ein. Schreiben Sie dahinter den 2-teiligen Hex Code. Z.B.bedeutet: $28 das Zeichen (.Wenn Sie das $ Zeichen eingeben möchten, geben Sie $$ ein).

14.15 Token Bibliotheken

Nachfolgend finden Sie die Namen einiger PKCS#11 Bibliotheken.

Falls Sie Ihren Hersteller nicht finden oder die Datei nicht auf Ihrem Rechner zu finden ist, wenden Sie sich bitte an den Hersteller Ihrer Token-Hardware.

Aladdin eToken, und einige Siemens Card OS Karten
eTpkcs11.dll

G&D StarCos / Rainbow iKey 3000

aetpkss1.dll

DataKey and Rainbow iKey 2000 series
dkck201.dll

Rainbow CryptoSwift HSM
iveacryptoki.dll

Utimaco CryptoServer
cs2_pkcs11.dll

Utimaco Cryptoki for SafeGuard
pkcs201n.dll

IBM MFC
CccSigIT.dll

GemSAFE
pk2priv.dll
gclib.dll

Dallas iButton
dspkcs.dll

Schlumberger Cryptoflex / Cyberflex Access
slbck.dll

SeTec
SetTokI.dll

ActivCard
acpkcs.dll

A-Sign Premium
psepkcs11.dll

ID2 PKCS#11
id2cbox.dll

SmartTrust PKCS#11
smartp11.dll

Eracom CSA
cryptoki.dll

Oberthur AuthentIC
AuCryptoki2-0.dll

nCipher nFast oder nShield
cknfast.dll

Chrysalis LUNA
cryst201.dll

IBM 4758
cryptoki.dll

Mozilla oder Netscape crypto module
softokn3.dll

Eutron CryptoIdentity oder Algorithmic Research MiniKey
sadaptor.dll

TeleSec
pkcs11.dll

Siemens HiPath SIcurity Card API
siecap11.dll

Athena Smartcard System ASE Card
asepkcs.dll

15 FAQ

15.1 Frequently asked questions

Häufig gestellte Fragen

Wie kann ich mein ArchiCrypt Live Laufwerk löschen?

Achten Sie zunächst darauf, dass das entsprechende Laufwerk nicht in ArchiCrypt Live geladen ist. Falls Sie ein dateibasiertes Live Laufwerk (Trägerdatei) löschen möchten, löschen Sie im Windows Explorer einfach die zugehörige Datei (Trägerdatei). Handelt es sich um eine Live Partition, formatieren Sie die Partition mit Betriebssystemmitteln.

Ab ArchiCrypt Live 7:

Haben Sie ein Live Laufwerk als Favorit angelegt, können Sie mit dem Löschen des Favoriten optional auch die zugehörige Datei löschen lassen.

Ich habe eine Umleitung eingerichtet und erhalte beim Schreiben in das Quellverzeichnis eigenartige Fehlermeldungen

Vermutlich ist auf dem Live Laufwerk, auf dem das Ziel der Umleitung liegt, nicht ausreichend Speicherplatz vorhanden. Anwendungen erfragen oft, wie viel Speicherplatz auf dem Datenträger vorhanden ist, auf dem das Quellverzeichnis liegt. Also zum Beispiel für E:\ anstatt für E:\Quelle. Ist auf E: genug Speicherplatz für eine Operation vorhanden, beginnt das Anwendungsprogramm ohne Rücksicht auf die tatsächlichen Gegebenheiten, Daten nach E:\Quelle und damit, durch die Umleitung verursacht, auf T:\Ziel (*das Live Laufwerk, auf welches umgeleitet wird*) zu schreiben. Ist das Live Laufwerk zu klein, kommt es zu entsprechend unaussagekräftigen Fehlermeldungen.

Legen Sie die Umleitung in diesem Fall auf ein größeres Live Laufwerk.

Ich finde die Daten einer Umleitung nicht mehr

Um die Daten einer Umleitung wieder in dem Verzeichnis anzuzeigen, dessen Inhalt Sie umgeleitet haben, müssen Sie die Umleitung wieder aktivieren. Dazu das Live Laufwerk laden, auf welches die Daten umgeleitet wurden und dann in den Werkzeugen für das Laufwerk die Umleitung einrichten, indem Sie das Verzeichnis als Quellverzeichnis angeben.

Die Daten sind auch auf dem entsprechenden Live Laufwerk vorhanden. Um also auf die Daten zugreifen zu können, genügt es, das Live Laufwerk zu laden und dort in das gleichnamige Verzeichnis zu wechseln.

Sollten Sie das Verzeichnis nachträglich umbenannt haben, wird das Aktivieren der Umleitung fehlschlagen. Sie müssten in diesem Fall die Umbenennung des Quellverzeichnisses zurücknehmen oder das Verzeichnis auf dem Live Laufwerk vor dem Aktivieren der Umleitung manuell ebenfalls umbenennen. Gleiche Namen der beiden Verzeichnisse sind ein Muss.

Ich kann eine Umleitung nicht mehr aktivieren

Vermutlich haben Sie Daten in das Quellverzeichnis kopiert, ohne dass die Umleitung aktiv war. Sichern Sie die Daten aus dem Quellverzeichnis in einem anderen Verzeichnis. Löschen Sie dann das

Quellverzeichnis komplett. Jetzt können Sie die Umleitung wieder aktivieren und die eben gesicherten Daten erneut in das Quellverzeichnis verschieben. Durch die aktive Umleitung laden die Daten jetzt auf dem Live Laufwerk.

Ich möchte eine Umleitung deaktivieren, ohne dabei die Daten zu verlieren

---

Zunächst einmal sind die Daten einer Umleitung nicht verloren, sondern auf dem Live Laufwerk, auf welches umgeleitet wurde. Wenn Sie die Trägerdatei des Live Laufwerks löschen oder das Zielverzeichnis der Umleitung direkt auf dem Live Laufwerk, sind die Daten tatsächlich verschwunden.
Deaktivieren Sie eine bestehende Umleitung und wechseln dann im Windows Explorer in das Zielverzeichnis der ehemaligen Umleitung. Kopieren Sie die Daten jetzt einfach in das Quellverzeichnis der ehemaligen Umleitung.

Kann ich mehrere Umleitungen auf ein ArchiCrypt Live Laufwerk einrichten?

Nein, je ArchiCrypt Live Laufwerk ist nur eine Umleitung möglich.

Auf meinem Rechner ist ein SmartCard-Leser einer Firma installiert, die nicht von ArchiCrypt Live unterstützt wird. Beim Start von ArchiCrypt Live erscheint immer die Meldung Device Error. Wie kann ich diese Meldung umgehen?

Falls Sie ein nicht-kompatibles SmartCard-Lesegerät installiert haben, kann dies dazu führen, dass beim Start von ArchiCrypt Live eine Fehlermeldung angezeigt wird. Um dies zu verhindern, erstellen Sie bitte im Anwendungsverzeichnis von ArchiCrypt Live eine Datei mit dem Namen NoSmartCard.txt
Die Datei kann leer bleiben, lediglich deren Existenz ist wichtig. ArchiCrypt Live blendet automatisch alle SmartCard-Funktionen aus und prüft beim Start nicht, ob ein Lesegerät installiert ist, falls es die Datei NoSmartCard.txt findet. Sie können alternativ die ArchiCrypt Card nutzen, die mit allen Card Readern zusammenarbeitet, die den PC/SC Standard unterstützen (nahezu jeder Kartenleser unter Windows erfüllt diesen Standard). Die ArchiCrypt Card erhalten Sie als gesondertes Produkt z.B. über unseren Online-Shop.

Welche SmartCard-Typen werden unterstützt?

Sie benötigen die ArchiCrypt Card und einen PC/SC kompatiblen SmartCard Reader(nahezu jeder SmartCard Leser unter Windows

erfüllt diesen Standard). Die ArchiCrypt Card erhalten Sie als gesondertes Produkt z.B. über unseren Online-Shop.

➔ACHTUNG: *Verwechseln Sie den SmartCard Reader nicht mit dem oft in Rechner eingebauten Reader für Speicherkarten (z.B. aus MP3 Playern oder Kameras!). Die SmartCard hat das gleiche Format wie eine EC-Karte!*

Warum kann ich mein auf CD gebranntes Laufwerk nicht laden

Voraussetzung für das Laden von CD:
ISO Level 1
Mode 1
Joliet
CD abgeschlossen (keine offene Multisession)
ArchiCrypt Live Laufwerk nicht NTFS formatiert

Bei DVDs müssen Sie das s.g. UDF Format auswählen. Dies gilt jedoch nur für Laufwerke > 2 GByte und für die Betriebssysteme Windows 2003, XP

AUSNAHME ist Windows **Vista, Windows 7/8**, hier können Laufwerke nicht!!! von DVDs geladen werden, die im UDF Format angelegt wurden. Hier müssen Sie beim Erstellen das normale ISO Format (maximale Größe der Trägerdatei 2 GByte) wählen oder die Datei auf einem anderen Medium sichern.

Warum kann ich ein Laufwerk nicht im reinen Lesemodus öffnen

Vermutlich handelt es sich um ein ArchiCrypt Live Laufwerk, welches im NTFS Format formatiert wurde. NTFS Datenträger können nie im reinen Lesemodus geöffnet werden, da das Betriebssystem immer schreibend auf den Datenträger zugreifen will. Ist dies nicht möglich, wird dies mit einem entsprechenden Fehler quittiert.

Dies hat zur Folge, dass NTFS formatierte ArchiCrypt Live Laufwerke nicht für den Mehrfachzugriff von ArchiCrypt Live NET geeignet sind. Es kann auf solche Laufwerke immer nur exklusiv mit Schreib-/Leserechten geladen werden. Eine gemeinsame gleichzeitige Nutzung ist demzufolge nicht möglich!

Wie sicher ist eine Schlüsseldatei

Die Schlüsseldatei als Passwortersatz ist hervorragend, da der darin gespeicherte Schlüssel bestimmte Eigenschaften aufweist, die normale Passwörter im Allgemeinen nicht aufweisen (Länge, Zufälligkeit, Zeichenvorrat). Wird die Schlüsseldatei auf einer Diskette gespeichert, achten Sie unbedingt darauf, dass Sie immer

eine funktionstüchtige Diskette an einem sicheren Ort verwahren. Generell gilt zu beachten, dass Wechseldatenträger sehr anfällig gegenüber äußeren Einflüssen sein können. Starke Temperaturschwankungen, magnetische und chemische Einflüsse etc. können ein Wechselmedium und damit den Schlüssel schnell unbrauchbar machen.

Wie sicher ist eine SmartCard

Die SmartCard ist vergleichbar mit der Schlüsseldatei. Was die Eigenschaften des Schlüssels angeht, gelten die gleichen Aussagen. Die Widerstandsfähigkeit der SmartCard gegenüber äußeren Einflüssen ist dabei deutlich größer als z.B. bei einer Schlüsseldatei, die auf einer Diskette abgelegt ist. Dennoch gilt, nachdem Sie eine SmartCard personalisiert haben, klonen Sie die SmartCard und verwahren Sie die Kopie an einem sicheren Ort.

Sofern Sie eine ArchiCrypt Card nutzen, erreichen Sie ein Maximum an Sicherheit und Komfort. Die speziell entwickelte SmartCard bietet höchsten Schutz der gespeicherten Schlüssel und erlaubt bequemes Öffnen/Schließen der Laufwerke. Während normale SmartCards/Schlüsseldateien lediglich als Speichermedium für einen Schlüssel dienen, kann die ArchiCrypt Card mit Hilfe spezieller Programme, die auf der ArchiCrypt Card selbst laufen, Schlüssel hoch-sicher Verwalten, mit Hilfe eines Zufallszahlengenerators der als Hardware vorliegt echte zufällige Schlüssel erzeugen und sogar den Datenaustausch vom Kartenleser zu ArchiCrypt Live selbst verschlüsseln.

Passwort vergessen, Schlüsseldatei defekt, SmartCard verloren, wie komme ich an die Daten

In diesem Fall gibt es keine Chance mehr an die Daten zu gelangen. Auch die Programmierer mit Quellcodekenntnis haben keine Möglichkeit Ihre Daten zu entschlüsseln. Daher beachten Sie unbedingt unsere Hinweise zur Sicherung der Laufwerke und nutzen Sie die Möglichkeiten der Software bevor es zu spät ist!

Wer garantiert, dass ArchiCrypt Live keine s.g. Backdoor besitzt

In Deutschland gibt es, Gott sei Dank, keine gesetzliche Bestimmung, die Hersteller von Verschlüsselungssoftware zwingt eine solche Hintertür in ihre Software zu integrieren. Hersteller können also die volle Leistungsfähigkeit eines Verschlüsselungsverfahrens einsetzen.

Man wäre somit äußerst schlecht beraten, eine Art Hintertür einzubauen. Diese würde früher oder später entdeckt werden, wodurch

der Hersteller in seinem Ansehen sicher derart beschädigt werden würde, dass er aus dem Markt verdrängt wird.

Neben diesen sehr schwerwiegenden äußeren Zwängen wurde die ArchiCrypt Live Engine (der Anteil, der die Verschlüsselung übernimmt) im Rahmen eines Datenschutzaudits des Produktes Opti.List durch das unabhängige Landeszentrums für Datenschutz Schleswig-Holstein, am 25.08.2003 untersucht. Das Produkt erhielt das Datenschutz-Gütesiegel (gem. §4 Abs. 2 LDSG SH i.V.m. der Datenschutzauditverordnung (DSAVO)in der Fassung vom 03.April 2001).

Trotz des richtigen Passwortes/Schlüsseldatei/SmartCard lässt sich das Laufwerk nicht öffnen

---

Die Ursache liegt in einem zerstörten Laufwerksheader (siehe Schlüssel-Sicherung) oder das Passwort stimmt doch nicht überein. Dieses Verhalten tritt auf, wenn der hochsensible Bereich eines ArchiCrypt Live Laufwerkes zerstört wird. Dies kann durch Viren, System- oder Hardwarefehler verursacht werden. Führen Sie daher nach einem Erstellvorgang eine s.g. Schlüssel-Sicherung durch und verwahren den Laufwerksheader mit zugehörigem Schlüssel an einem sicheren Ort. Im Falle einer Störung kann dann dieser Laufwerksheader zurück gespielt werden, wodurch sich das Laufwerk eventuell wieder öffnen lässt. Dennoch können je nach schwere der Laufwerkszerstörung starke Schäden am Laufwerk auftreten. Beachten Sie daher die Grundsätze des verantwortlichen Umgangs mit wichtigen Daten. Dazu gehört ein regelmäßiges Backup am besten täglich und vor jedem Eingriff in das System!

Wenn Sie eine Trägerdatei auf einem komprimierten NTFS Laufwerk ablegen, können Sie das Laufwerk nicht mehr laden. Kopieren Sie das Laufwerk auf einen nicht komprimierten Datenträger. In diesem Zusammenhang ist es gut zu wissen, dass korrekt verschlüsselte Daten nahezu NICHT komprimiert werden können!

Müssen ArchiCrypt Live Laufwerke immer die Endung ACL oder ACYL tragen?

Sie können die Laufwerke benennen, wie Sie möchten. Bei großen Trägerdateien wählen Sie möglichst Dateiendungen die bei großen Dateien gängig sind. Dazu zählen mpeg, mp3, avi, aber auch Bilddatenformate wie bmp.

Warum lädt ArchiCrypt Live ein Laufwerk aus dem Netz nicht

Binden Sie die Netzwerkressource als Laufwerk ein und laden Sie dann die Datei über den vergebenen Laufwerksbuchstaben. UNC

Pfadangaben werden jedoch unterstützt. Beim Anlegen neuer Laufwerke muss für die Netzwerkfreigabe jedoch zwingend ein Laufwerksbuchstabe angelegt werden.

Fehlermeldung: Für diesen Befehl ist nicht genug Serverspeicher verfügbar

---

Dieser Fehler kann auftreten, wenn Sie auf ein im Netzwerk freigegebenes ArchiCrypt Live Laufwerk zugreifen, oder mit ArchiCrypt Live NET eine Trägerdatei laden, die auf einem Server abgelegt ist.

Gehen Sie wie im folgenden Microsoft Artikel beschrieben vor:
http://support.microsoft.com/kb/177078/de

Einsatz von MOD Laufwerken

MOD Laufwerke bis zu einer Größe von 540 MByte können problemlos eingesetzt werden. Bei MOD Datenträgern jenseits dieser Größe ändert sich die Struktur der Datenträger, die dann nicht mehr so genutzt werden können, dass man Live Laufwerke direkt vom Medium einbinden kann.

Index

- " -

- 1 -

- 3 -

- 4 -

- A -

- B -

- C -

- D -

- E -

- F -

- G -

- H -

- I -

- K -

- L -

- M -

- N -

- O -

- P -

- R -

- S -

- T -

- U -

- V -

- W -

- X -

- Z -