HiCrypt™ 2.0

Installationsanleitung und Einführung

digitronic
computersysteme gmbh

Oberfrohnaer Straße 62
D-09117 Chemnitz
Telefon: +49 371 81539-0
Fax: +49 371 81539-900
Internet: www.digitronic.net
E-Mail: info@digitronic.net

© 2018 digitronic computersysteme gmbh

Dieses Dokument ist urheberrechtlich geschützt, und seine Verbreitung unterliegt den Lizenzen, die seine Verwendung, Vervielfältigung und Verbreitung einschränken. Kein Teil dieses Produkts oder Dokuments darf ohne vorherige schriftliche Genehmigung von digitronic in irgendeiner Art und Weise reproduziert werden.

Verfasser: Sven Grzeszczuk, Alexander Schuschies
Stand: 2. März 2018

Inhaltsverzeichnis

1 Einleitung 1

2 Installation 2

3 Lizensierung 5

4 Erste Schritte mit HiCrypt™ 2.0 9

4.1 HiCrypt™ 2.0 starten 9

4.2 Netzlaufwerk verbinden 10

4.3 Netzlaufwerk verschlüsseln 13

4.4 Sicherheitsrichtlinien 19

4.5 Benutzerverwaltung 21

4.6 Kennwort-Generator 26

5 Entschlüsselung 27

6 Wiederherstellung 30

7 Reparieren 34

8 Weitere Optionen 37

9 Verwendung von Online-Speichern 39

10 Verwendung von Dropbox und ähnlicher Dienste 44

A Technische Daten 50

B Häufig gestellte Fragen 51

C Glossar 58

KAPITEL 1

1 Einleitung

HiCrypt™ 2.0 stellt die Schlüsselalleinbesitzgarantie wieder her. Dies ist das Privileg eines Verantwortungsträgers allein zu entscheiden, wer den Inhalt wichtiger Daten einsehen kann. Früher lagen diese Daten in Papierform vor und waren eingeschlossen. Inzwischen sind sie häufig digitalisiert und meist auf einem zentralen Server gespeichert. Somit kann jeder, der Zugriff auf diese Dateien hat, diese auch einsehen.

Solche Zugriffe können entstehen, wenn bei der Vergabe von Zugriffsrechten etwas übersehen wurde. Des Weiteren besitzen Administratoren umfangreiche Zugriffsrechte um ihre Aufgaben wahrnehmen zu können. HiCrypt™ 2.0 verschlüsselt aus diesem Grund die Dateien bereits am Client. Der Verantwortungsträger vergibt die Schlüssel selbst an diejenigen Nutzer, welche die Inhalte der Dateien einsehen dürfen. In HiCrypt™ 2.0 wird der Verantwortungsträger Manager genannt. Dabei bleiben die Dateizugriffsrechte des Betriebssystems unberührt, damit die Administratoren weiterhin Ihre Aufgaben erfüllen können.

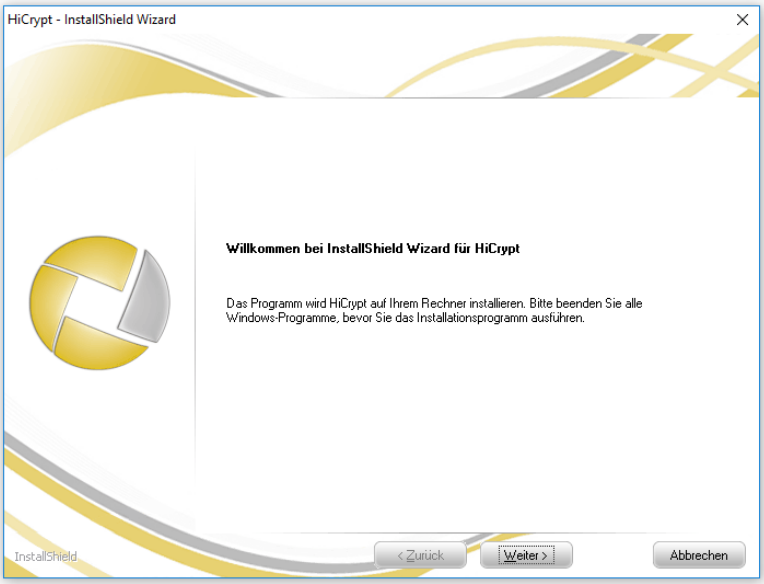
In dieser Dokumentation wird Schritt für Schritt erklärt, wie HiCrypt™ 2.0 installiert und eingerichtet wird. Des Weiteren werden einige Recovery-Szenarien erläutert und die Benutzerverwaltung erklärt.

Im Anhang befinden sich technische Details. Bei Fragen wenden Sie sich bitte an support@digitronic.net. Die aktuellste Version von HiCrypt™ 2.0 mit Standard-Lizenzierung steht für Sie immer unter http://www.hicrypt.com/download zur Verfügung.

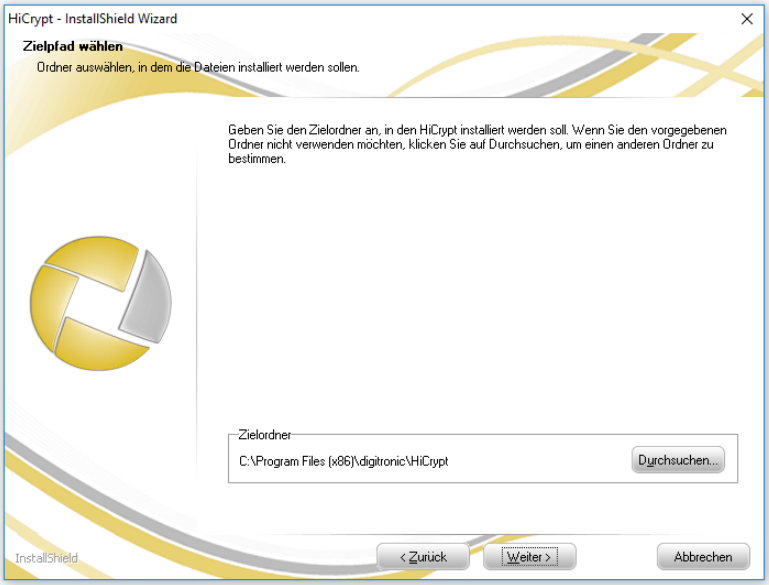
KAPITEL 2

2 Installation

Starten Sie das Installationsprogramm „HiCrypt.exe" und folgen Sie den Anweisungen.



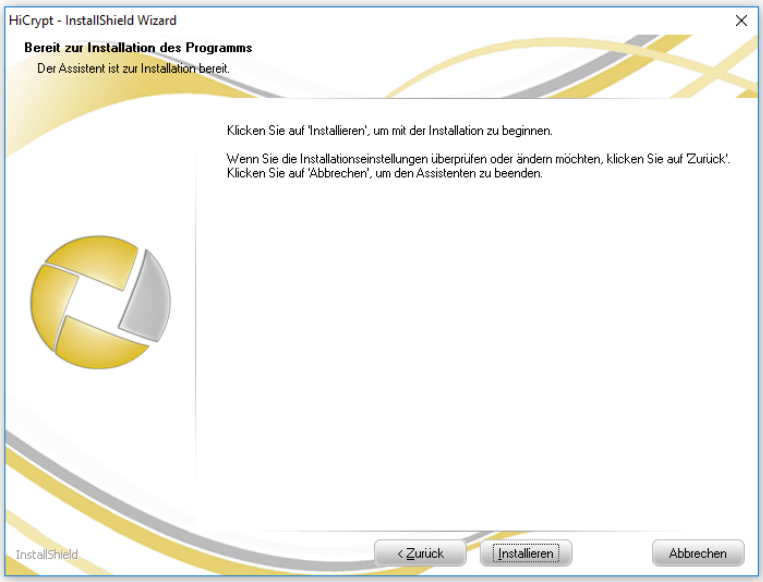
Betätigen Sie die Schaltfläche „Weiter", um den Assistenten zur Installation von HiCrypt™ 2.0 fortzusetzen.



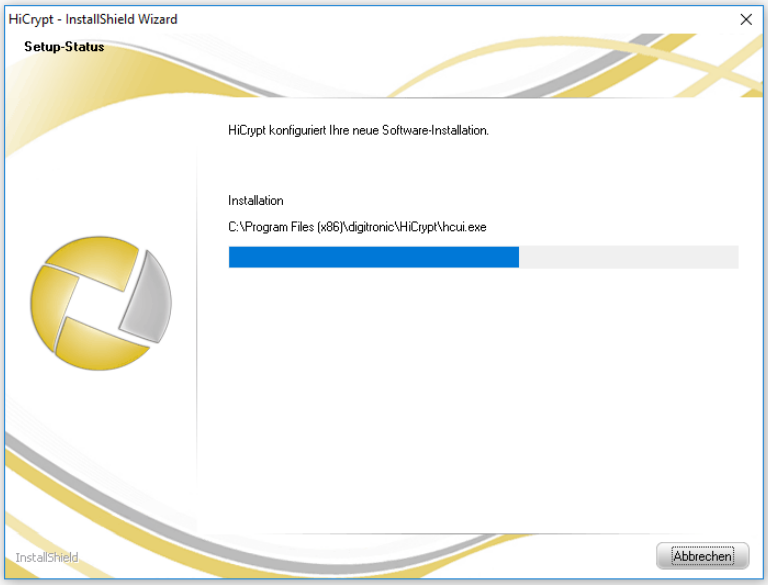
Wählen Sie den gewünschten Zielordner für die Installation von HiCrypt™ 2.0 aus und bestätigen Sie diesen mit der Schaltfläche „Weiter".

An dieser Stelle entscheiden Sie, ob das Entfernen des SecurityTokens ignoriert werden soll oder nicht.
Diese Einstellung ist sinnvoll, wenn Sie den SecurityToken mit anderer Software für die Anmeldung am Computer verwenden (beispielsweise Secure Logon™ 2.0). Wenn der SecurityToken entfernt wird, wird der Computer in der Regel gesperrt. HiCrypt™ 2.0 würde ebenfalls auf das Entfernen des SecurityTokens reagieren. Dadurch würden Sie von den Netzlaufwerken an denen Sie angemeldet sind abgemeldet. In diesem Fall wäre ein Datenverlust nicht auszuschließen, sollten Dateien auf dem Netzlaufwerk geöffnet sein.

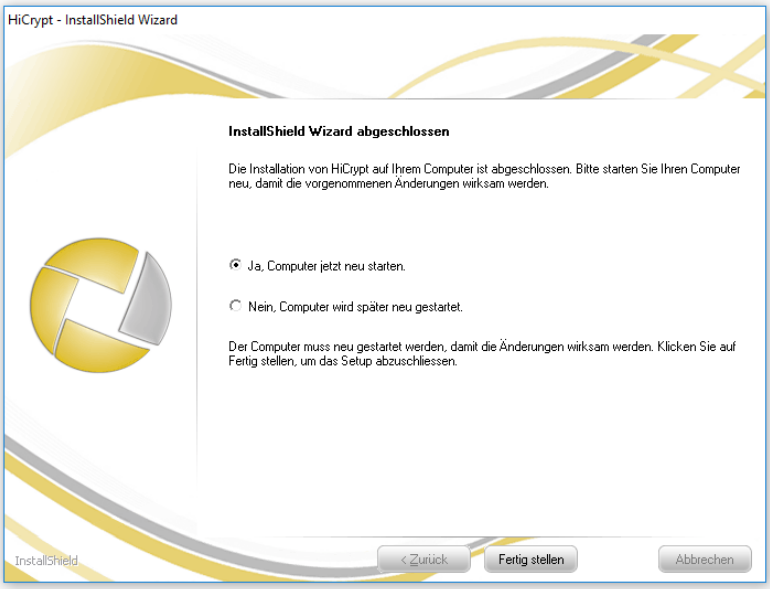
Entscheiden Sie, ob das Entfernen des SecurityTokens von HiCrypt™ 2.0 ignoriert werden soll und fahren Sie mit „Weiter" fort.



Mit „Installieren" starten Sie die Installation.



Während der Installation werden die Dateien von HiCrypt™ 2.0 kopiert und auf Ihrem Computer eingerichtet.

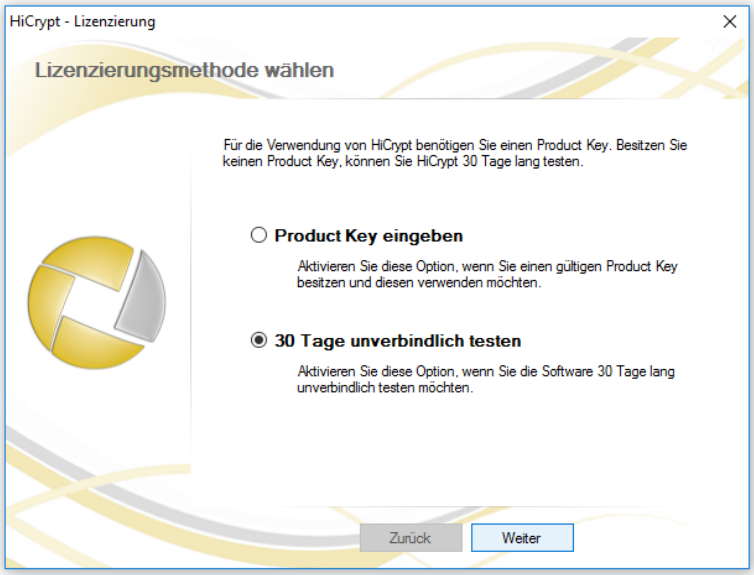


Um die Installation abzuschließen, ist ein Neustart des Computers erforderlich. HiCrypt™ 2.0 können Sie erst verwenden, nachdem Sie einen Neustart durchgeführt haben.

KAPITEL 3

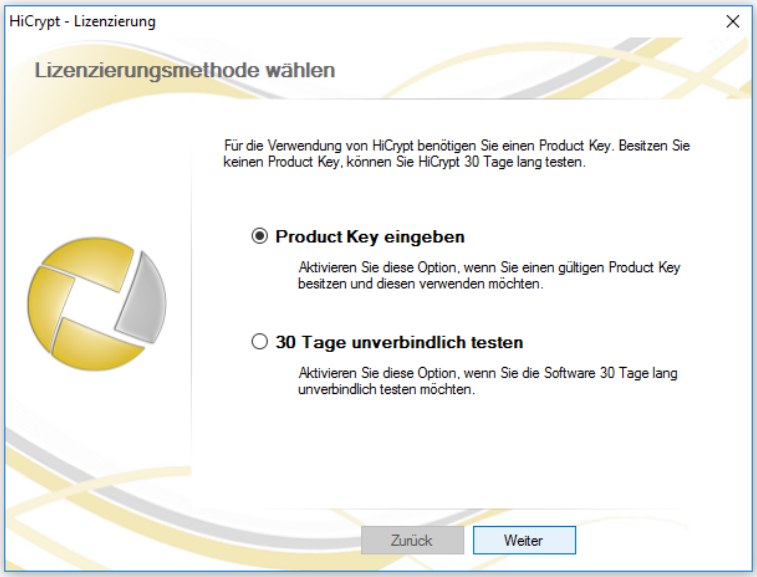
3 Lizensierung

HiCrypt™ 2.0 muss vor der ersten Verwendung aktiviert werden. Der Assistent, der Sie durch diesen Vorgang leiten wird, startet automatisch nach dem Neustart.

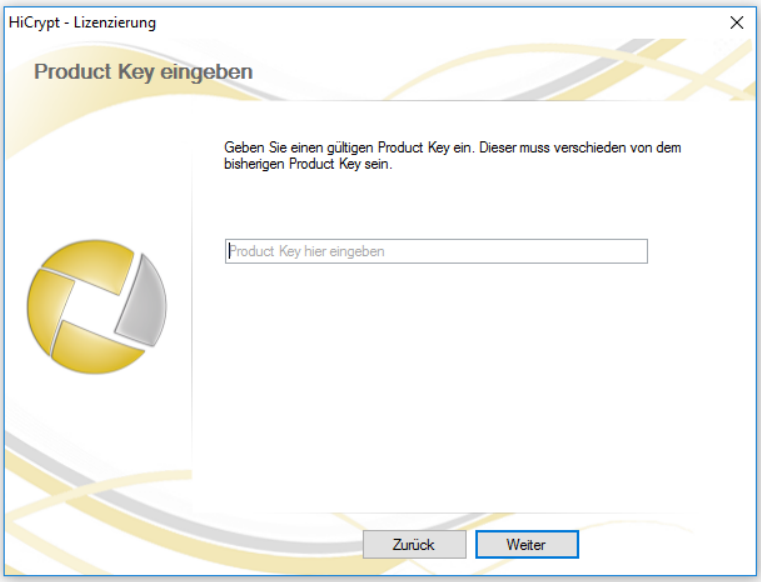


Während der Evaluierungsphase benötigen Sie keinen Product Key.

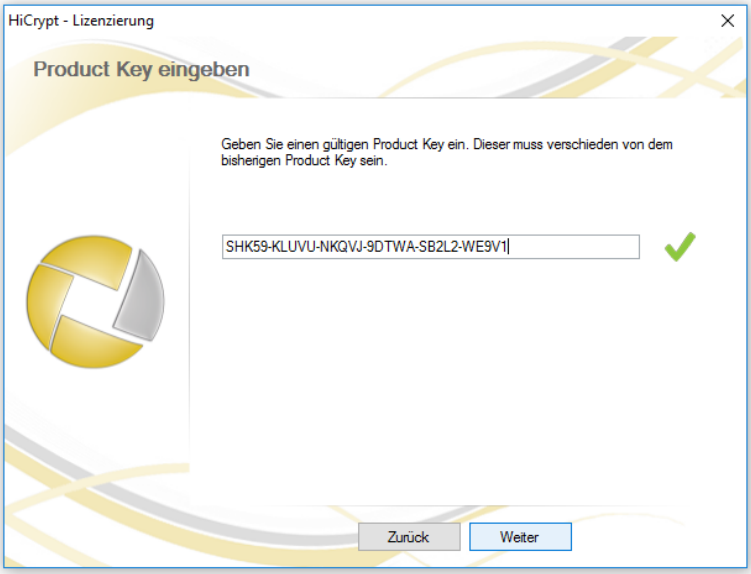
Aktivieren Sie für die Evaluierungsphase die Option „30 Tage unverbindlich testen" und bestätigen Sie Ihre Auswahl mit „Weiter".



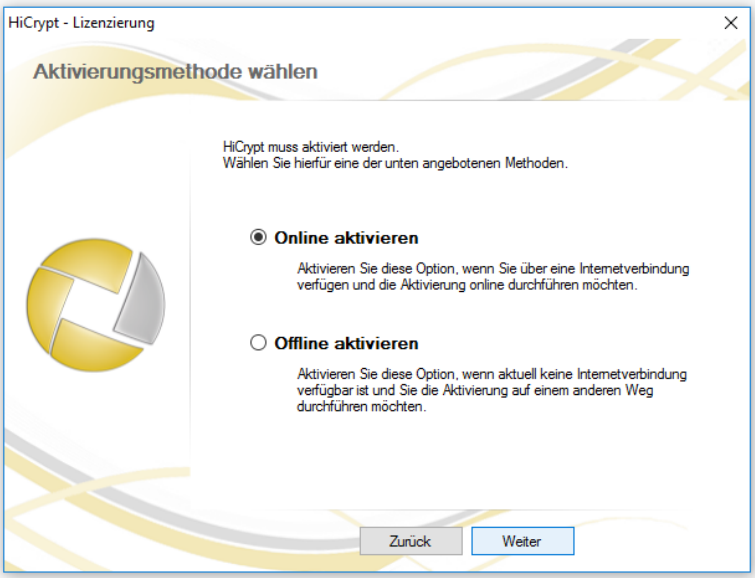
Wenn Sie bereits einen Product Key erworben haben, geben Sie diesen bitte hier ein.



Geben Sie hier Ihren Product Key ein.

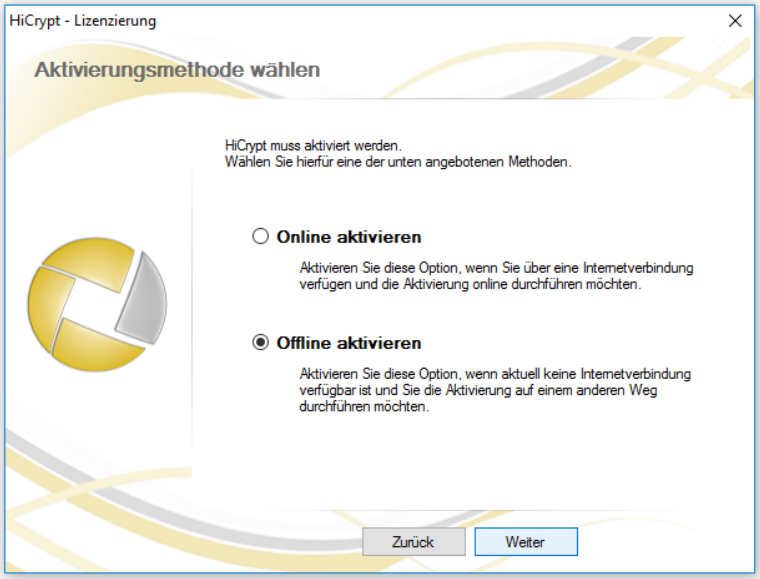


Ein grünes Häkchen signalisiert, dass das Format dem eines Product Keys entspricht.

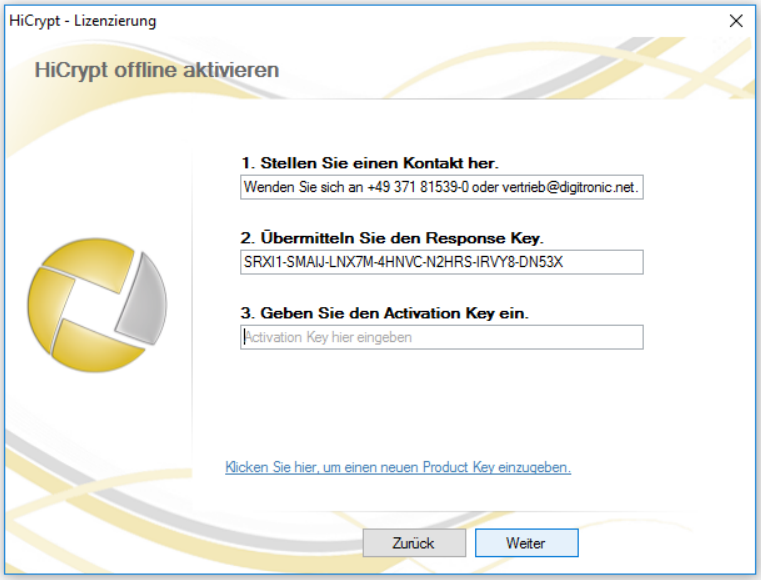


Egal, ob Sie einen Product Key eingegeben oder die Evaluierungsphase gewählt haben: Sie müssen HiCrypt™ 2.0 vor der Verwendung aktivieren. Dieser Vorgang kann sowohl online, als auch offline erfolgen.

Wählen Sie die gewünschte Option und bestätigen Sie Ihre Auswahl mit „Weiter".

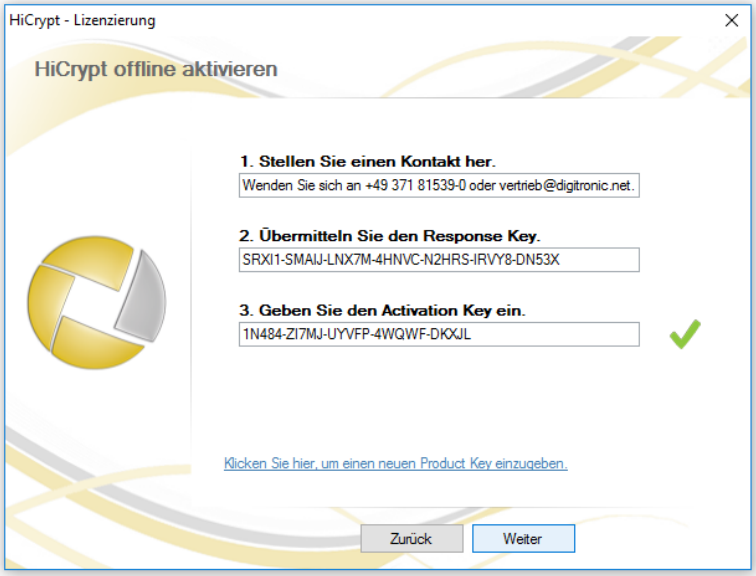


Während die Online-Aktivierung sofort durchgeführt wird, ist bei der Offline-Aktivierung ein weiterer Schritt notwendig.



Für die Offline-Aktivierung benötigen Sie einen Response Key, der automatisch erzeugt wird. Diesen geben sie entweder unter https://www.digitronic.net/service/lizenzaktivierung-deaktivierung ein oder senden diesen per E-Mail an vertrieb@digitronic.net.

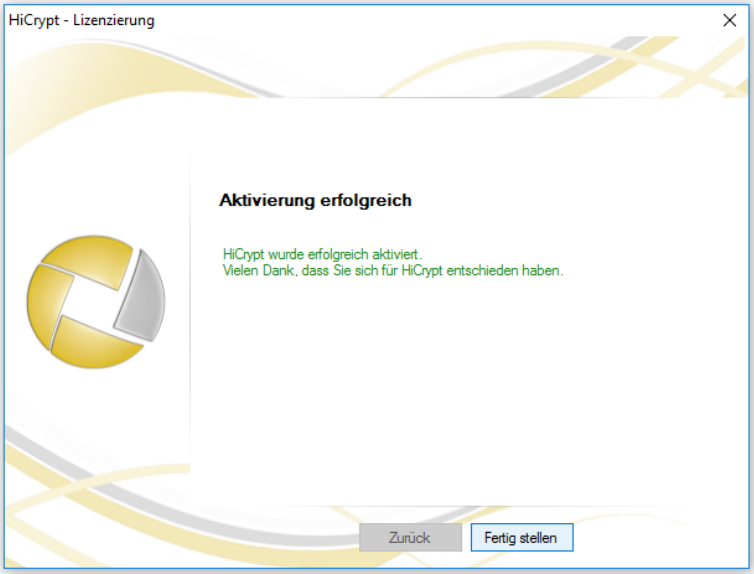
Sie erhalten dann einen entsprechenden Activation Key, den Sie in diesem Dialog eintragen müssen.



Sobald der Activation Key ein gültiges Format besitzt, wird ein grünes Häkchen angezeigt.

Sie aktivieren die Software mit „Weiter".

Warten Sie bitte ein paar Sekunden, während die Aktivierung durchgeführt wird.



Die erfolgreiche Aktivierung wird mit „Fertig stellen" abgeschlossen. HiCrypt™ 2.0 kann jetzt verwendet werden.

KAPITEL 4

4 Erste Schritte mit HiCrypt™ 2.0

Nachdem HiCrypt™ 2.0 installiert und aktiviert wurde, kann die Software verwendet werden.

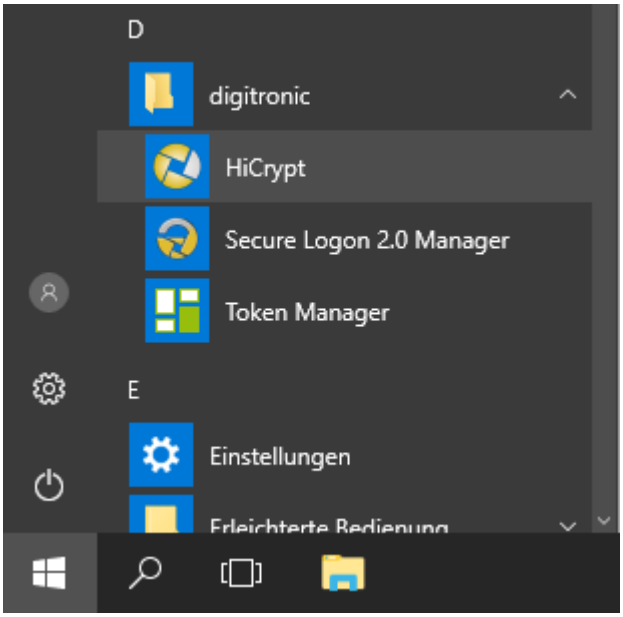
4.1 HiCrypt™ 2.0 starten

HiCrypt™ 2.0 wird automatisch mit dem Betriebssystem gestartet. Um die Benutzeroberfläche von HiCrypt™ 2.0 zu öffnen, haben Sie folgende Möglichkeiten:

Klicken Sie auf das HiCrypt™ 2.0-Symbol im Infobereich der Startleiste, um das Programm zu öffnen.

Möglicherweise wird das Symbol dort nicht sofort angezeigt, weil es ausgeblendet ist. Verwenden Sie die Schaltfläche links neben dem Infobereich der Startleiste, um ausgeblendete Symbole anzuzeigen.

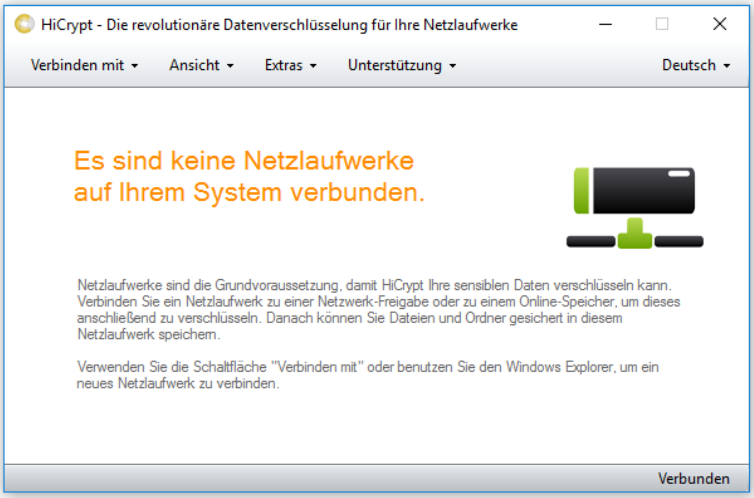
Mittels „Anpassen" können Sie das HiCrypt™ 2.0-Symbol dauerhaft einblenden, so dass Sie immer sofort darauf zugreifen können.



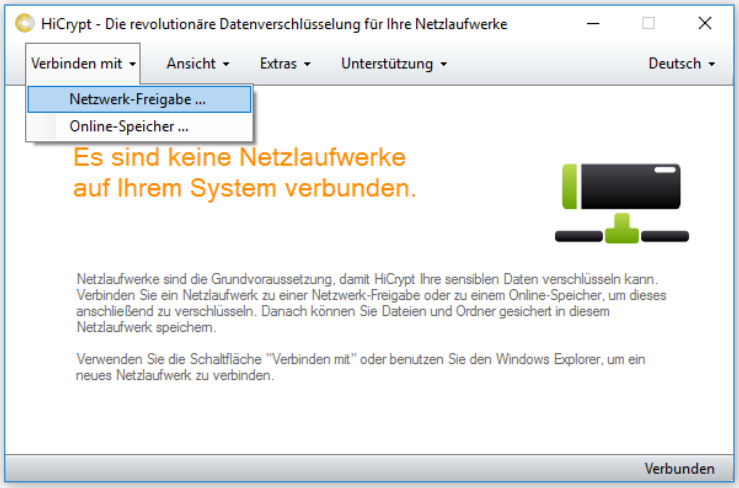
Alternativ können Sie HiCrypt™ 2.0 über die Verknüpfung im Startmenü öffnen.

4.2 Netzlaufwerk verbinden

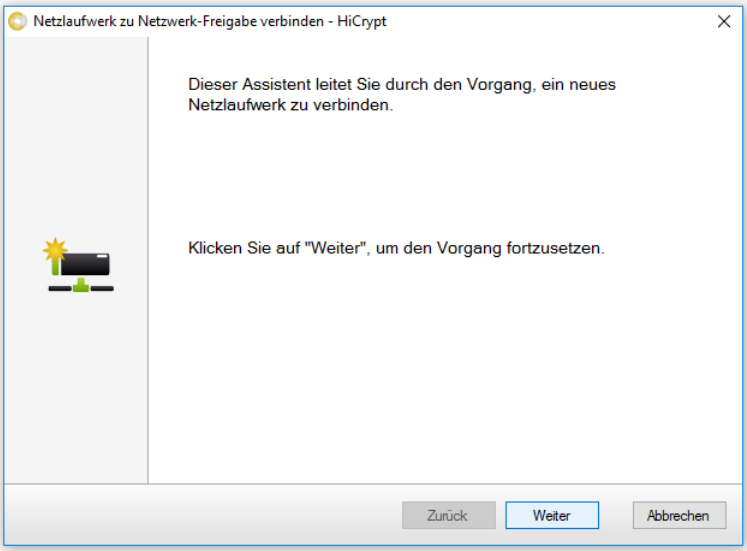
Netzlaufwerke sind die grundlegende Voraussetzung, damit HiCrypt™ 2.0 Ihre Daten verschlüsseln kann.



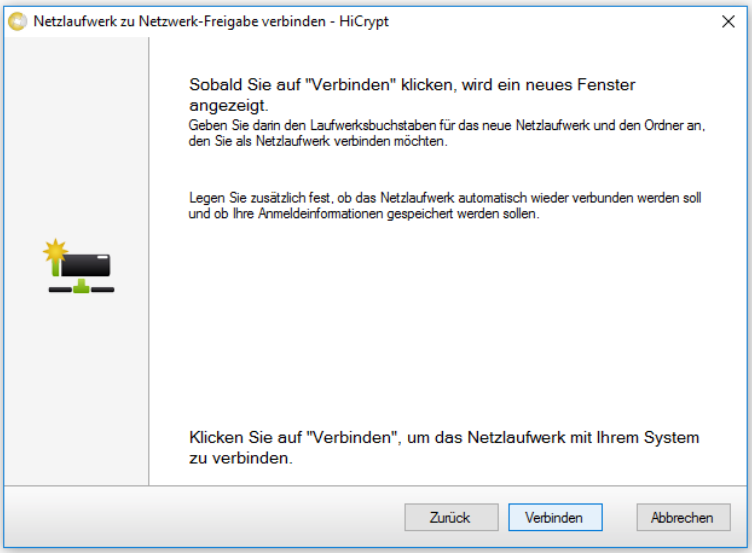
Sofern Sie kein Netzlaufwerk verbunden haben, können Sie dies mit HiCrypt™ 2.0 tun.



Wählen Sie „Verbinden mit" und anschließend „Netzwerk-Freigabe ...", um ein neues Netzlaufwerk zu einem freigegebenen Ordner zu verbinden.

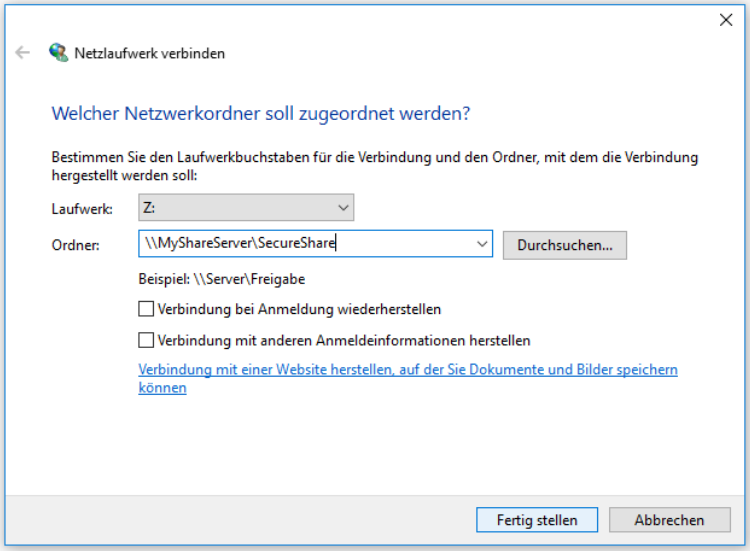


Mit „Weiter" startet der Assistent zum Einrichten eines neuen Netzlaufwerkes.

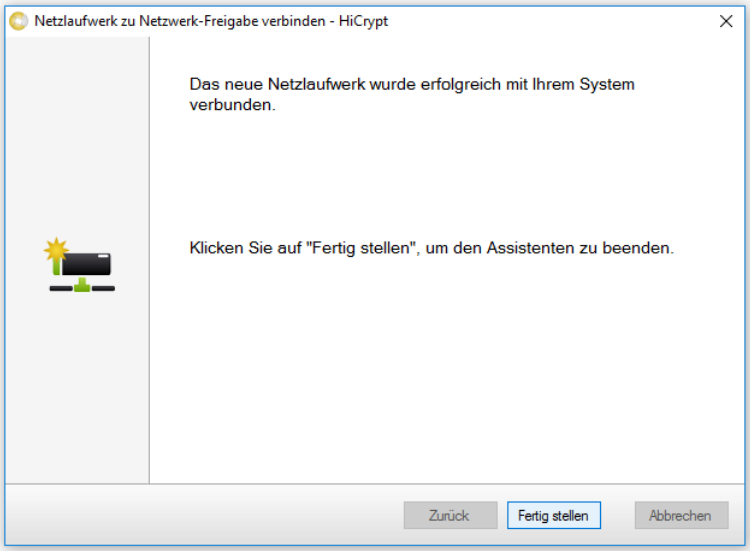


Lesen Sie sich die Informationen in diesem Dialog durch, um die Einstellungen für das neue Netzlaufwerk vornehmen zu können.

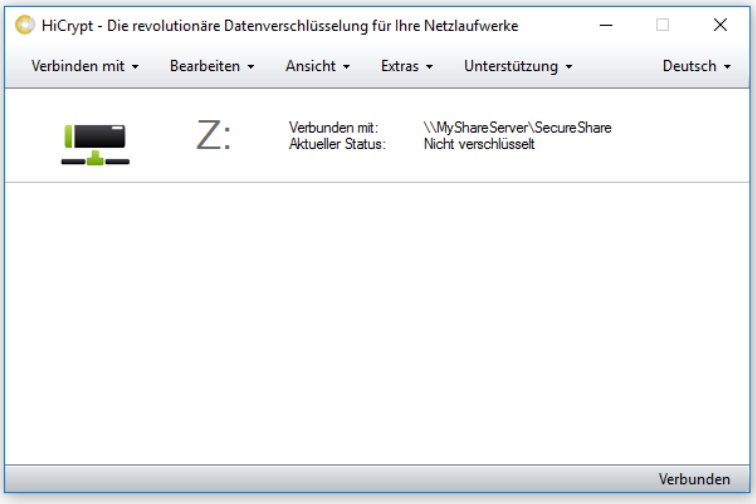
Mit „Verbinden" öffnen Sie den Dialog zum Verbinden eines Netzlaufwerks.



Wählen Sie den gewünschten Laufwerksbuchstaben aus und geben Sie den Pfad zu der Netzwerk-Freigabe ein, zu der das Netzlaufwerk verbunden werden soll. Verwenden Sie die gebotenen Optionen um die Verbindung nach Ihren Wünschen anzupassen und bestätigen Sie Ihre Eingaben mit „Fertig stellen", um das Netzlaufwerk zu verbinden.



Beenden Sie den Assistenten mit „Fertig stellen".

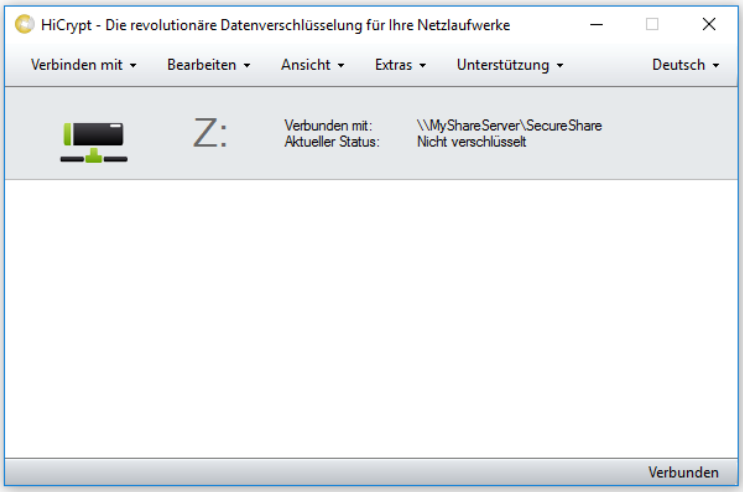


Das verbundene Netzlaufwerk wird in HiCrypt™ 2.0 angezeigt.

4.3 Netzlaufwerk verschlüsseln

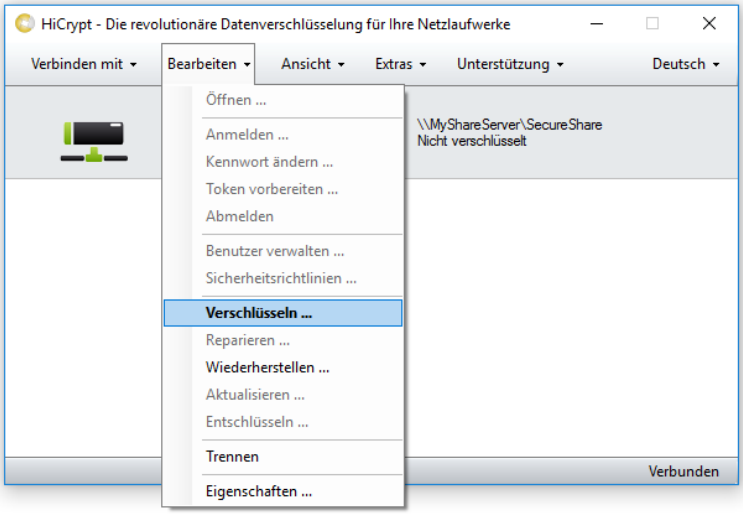
Der Status des Netzlaufwerks wird zunächst als „nicht verschlüsselt" angegeben. Die folgenden Schritte zeigen, wie das Netzlaufwerk verschlüsselt wird. Dabei wird ein Manager Nutzer angelegt, der das verschlüsselte Laufwerk verwalten darf.

Beachten Sie, dass das Netzlaufwerk für diesen Vorgang leer sein muss. Erst im Anschluss können Dateien und Ordner darin gespeichert beziehungsweise erzeugt und dabei automatisch verschlüsselt werden.

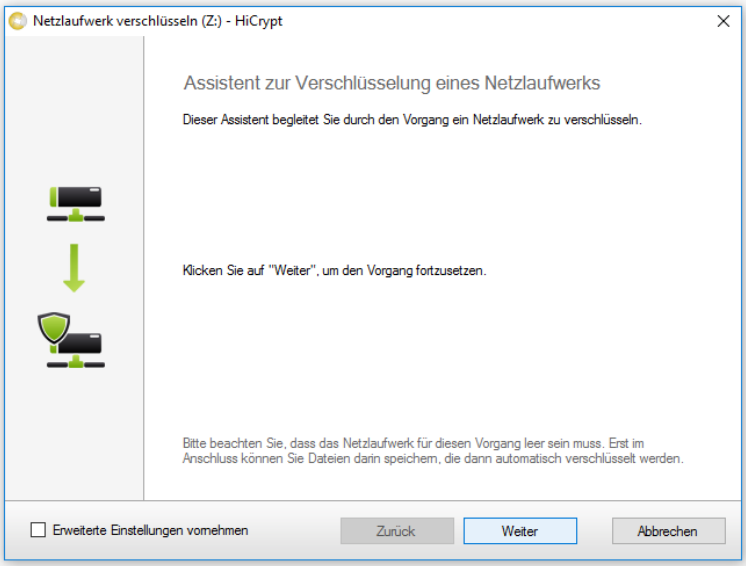


Der Status des Netzlaufwerkes ist „Nicht verschlüsselt".

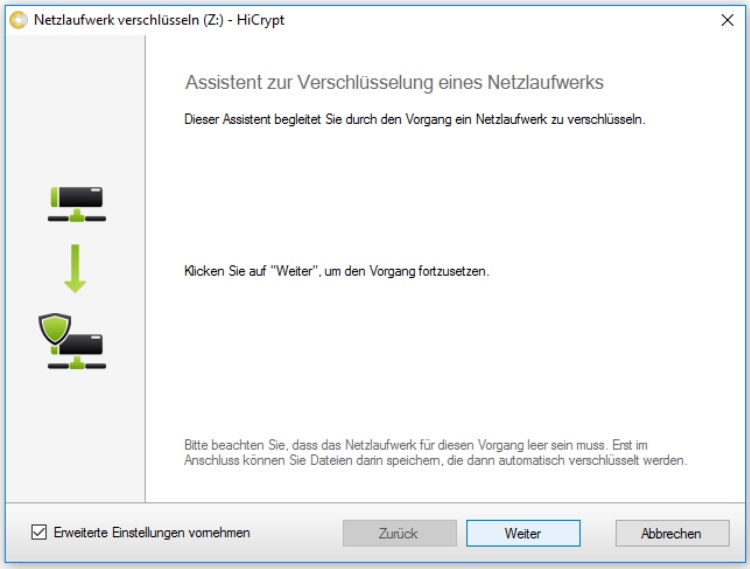
Führen Sie einen einfachen Klick aus, um das Laufwerk zu markieren.



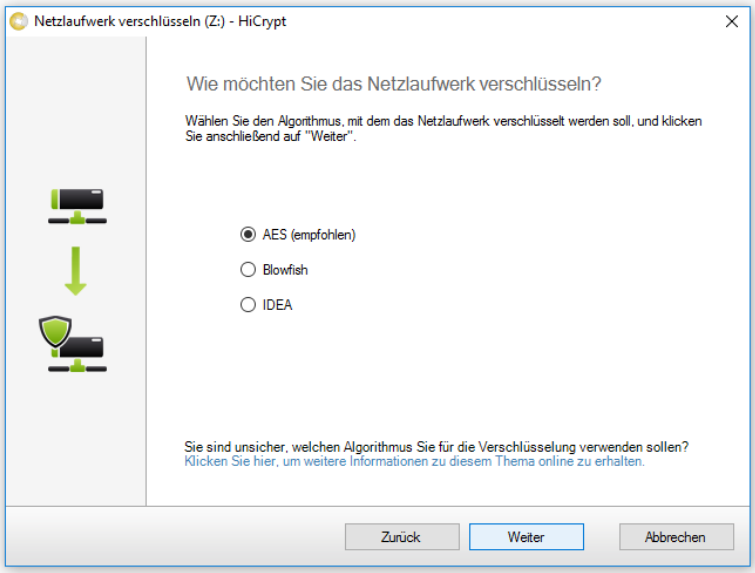
Wählen Sie nun im Menü „Bearbeiten" oder im Kontextmenü „Verschlüsseln ...", um das Netzlaufwerk zu verschlüsseln.



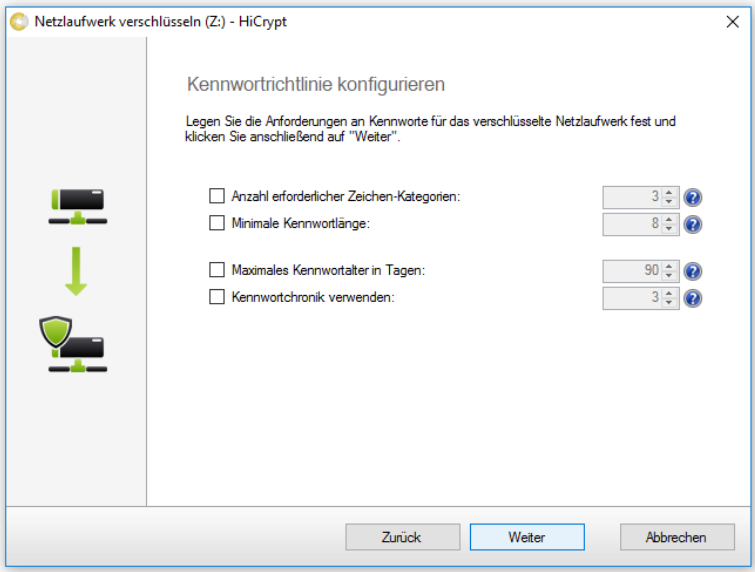
Betätigen Sie die Schaltfläche „Weiter" um den Assistenten zu starten, der Sie durch den Verschlüsselungsvorgang für das Netzlaufwerk leiten wird.



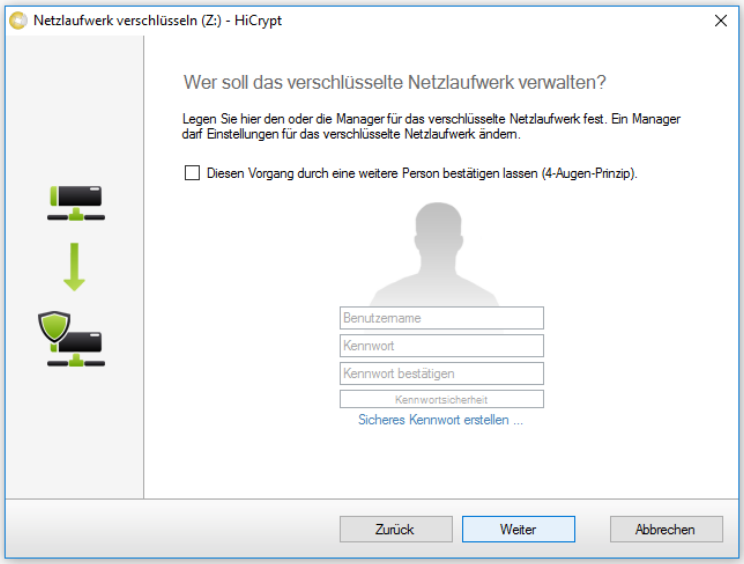
Sollten Sie erweiterte Einstellungen bei der Verschlüsselung vornehmen wollen, wie zum Beispiel das Festlegen des verwendeten Algorithmus, setzen Sie unten links den Haken bei „Erweiterte Einstellungen vornehmen" bevor Sie mit „Weiter" fortfahren.



Erweiterte Einstellung: Wählen Sie hier die Verschlüsselungsmethode aus und bestätigen Sie Ihre Auswahl mit „Weiter".

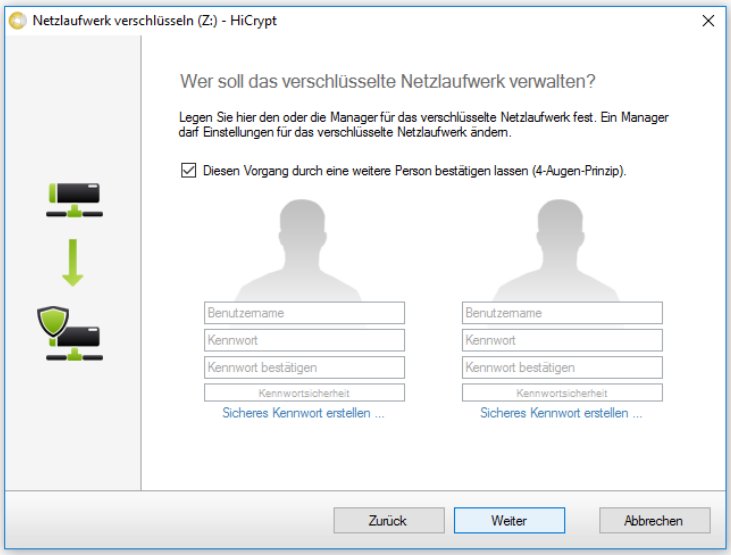


Erweiterte Einstellung: Legen Sie die Kennwortrichtlinie fest. Sollten Sie mit einer Tokenunterstützung arbeiten, bei der außer dem/den Manager(n) die Nutzer Ihre Kennworte nicht kennen, dann empfehlen wir, hier „nicht ablaufende Kennworte" zu wählen.

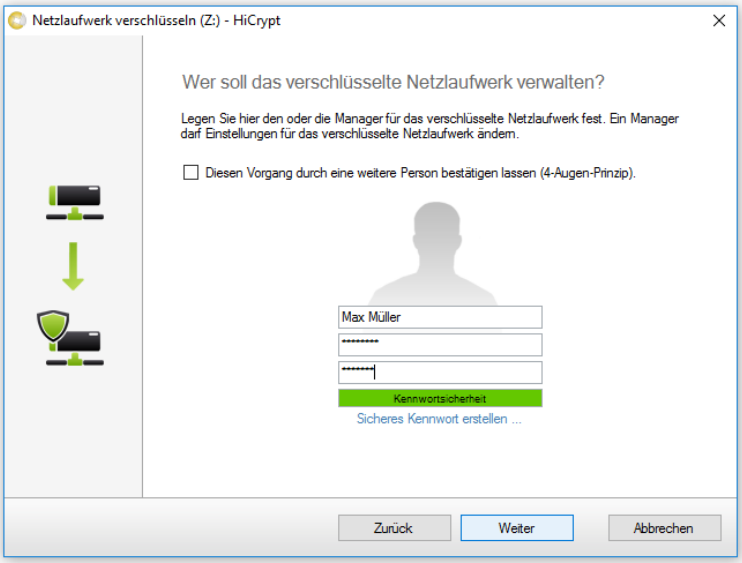


Im nächsten Schritt wird der erste Manager für das Netzlaufwerk angelegt. Hierzu müssen Sie neue Anmeldeinformationen eingeben. Diese sind von Ihrer Windows-Anmeldung unabhängig.

Den angelegten Benutzernamen und das festgelegte Kennwort benötigen Sie um auf das verschlüsselte Netzlaufwerk zugreifen zu können.

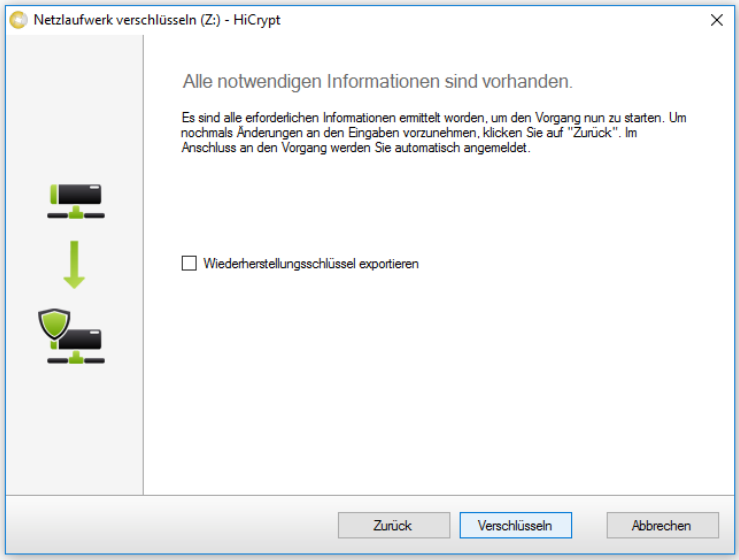


Vier-Augen-Prinzip: Es besteht die Möglichkeit, ein Vier-Augen-Prinzip einzuführen. Dann werden bei der Verschlüsselung zwei Manager angelegt. Zur Ausübung der Manaqer-Funktionen müssen dann immer 2 Manager angemeldet sein.

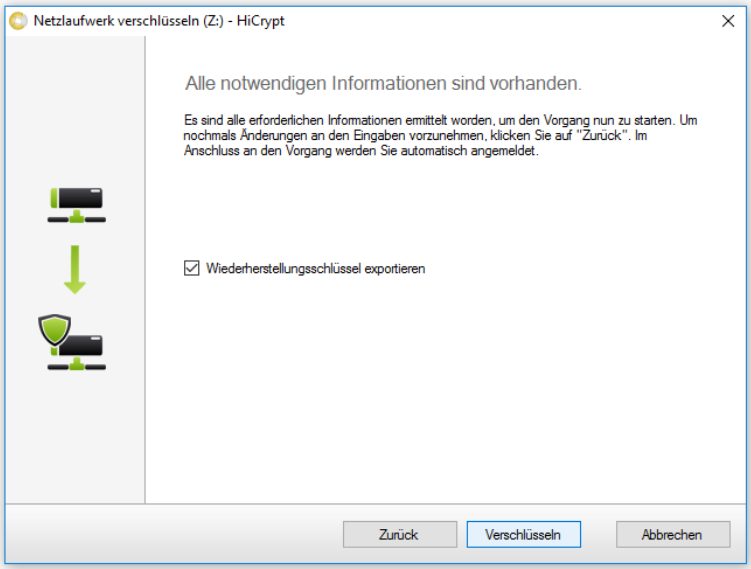


Der/die angelegte/-n Manager sind in der Lage, weiteren Benutzern den Zugriff auf das verschlüsselte Netzlaufwerk zu gewähren, die Sicherheitsrichtlinien zu bearbeiten oder das Laufwerk wieder zu entschlüsseln.

Bestätigen Sie Ihre Eingaben mit „Weiter".

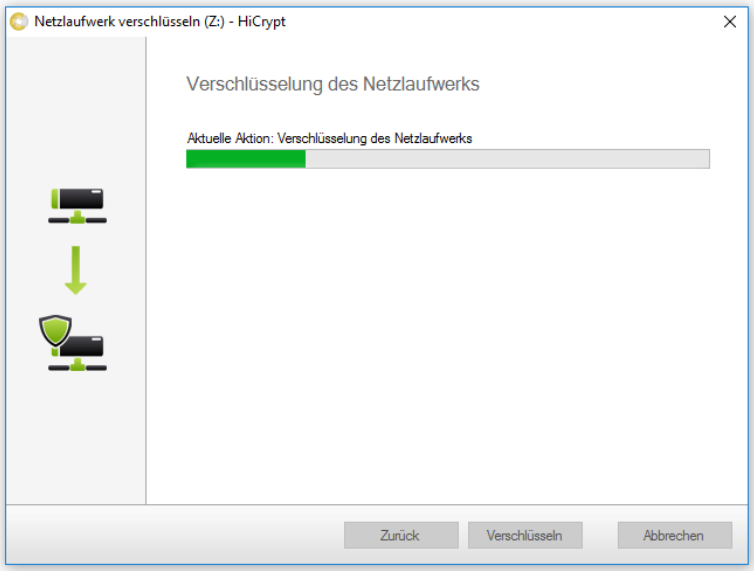


Verschlüsseln Sie das Netzlaufwerk mit „Verschlüsseln".

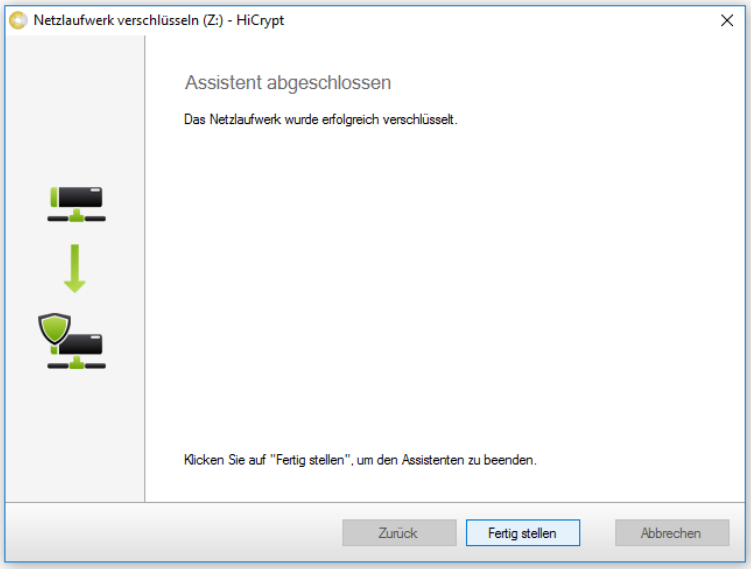


Wiederherstellungsschlüssel:
Bevor Sie „Verschlüsseln", können Sie nun, einmalig und nur an dieser Stelle, den Wiederherstellungsschlüssel exportieren.

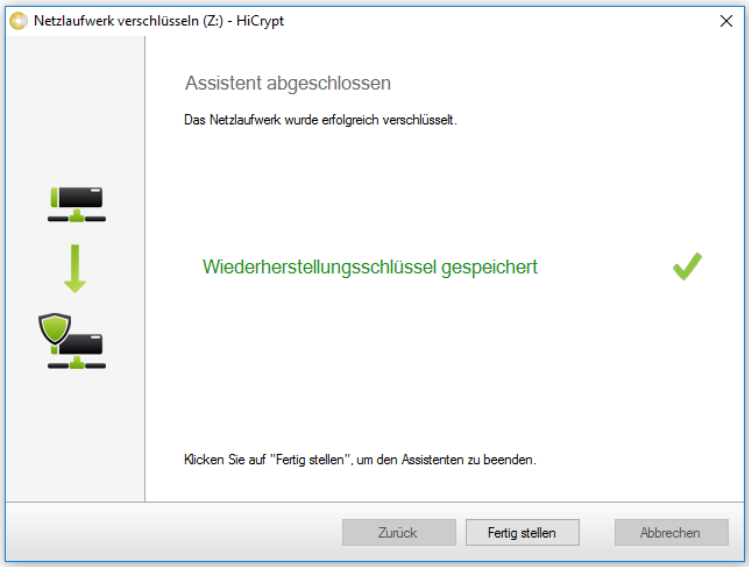
Speichern Sie den Wiederherstellungsschlüssel auf einem externen Datenträger und verschließen Sie diesen an einem sicheren Ort.

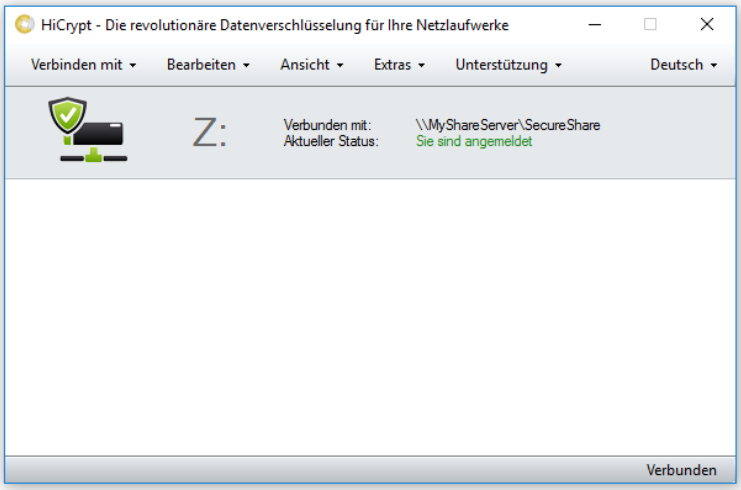


Nach erfolgreicher Verschlüsselung werden Sie automatisch an dem verschlüsselten Netzlaufwerk angemeldet.



Beenden Sie den Assistenten mit „Fertig stellen".





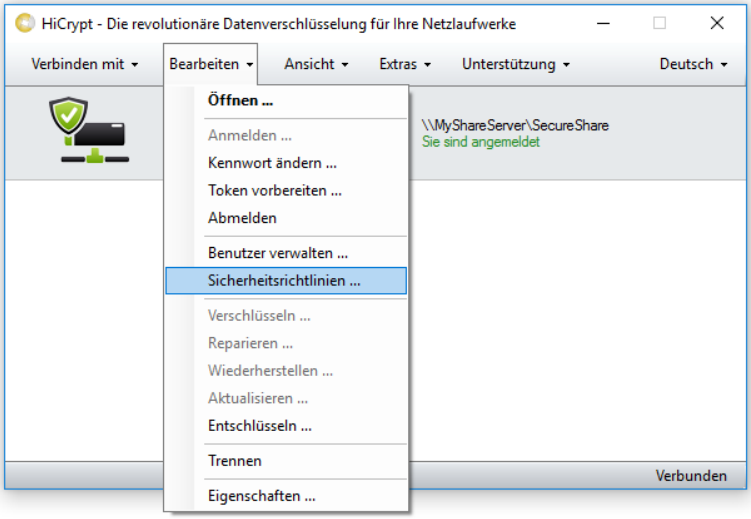
Das Netzlaufwerk ist nun verschlüsselt. Dateien, die Sie darin ablegen, werden automatisch und ohne weitere Aktionen Ihrerseits verschlüsselt.

Die beschriebene Vorgehensweise zum Verschlüsseln eines Netzlaufwerks muss für jedes Laufwerk wiederholt werden, das verschlüsselt werden soll.

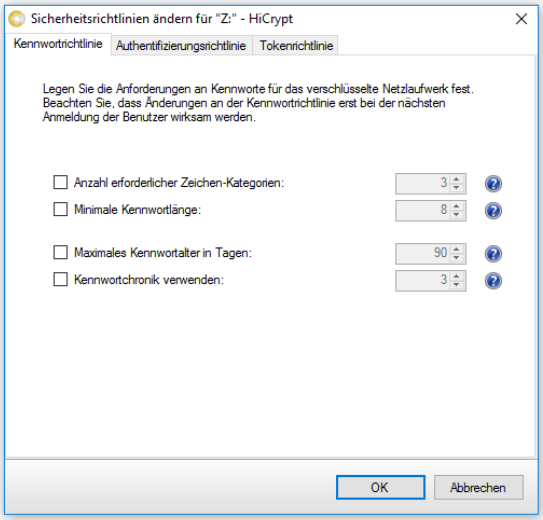
Sobald ein verschlüsseltes Netzlaufwerk verbunden wird, fragt HiCrypt™ 2.0 automatisch nach den Anmeldeinformationen. Diese können gespeichert werden, so dass eine Anmeldung an verschlüsselten Netzlaufwerken automatisch erfolgt.

4.4 Sicherheitsrichtlinien

Die Sicherheitseinstellungen müssen für jedes verschlüsselte Laufwerk separat getroffen werden.

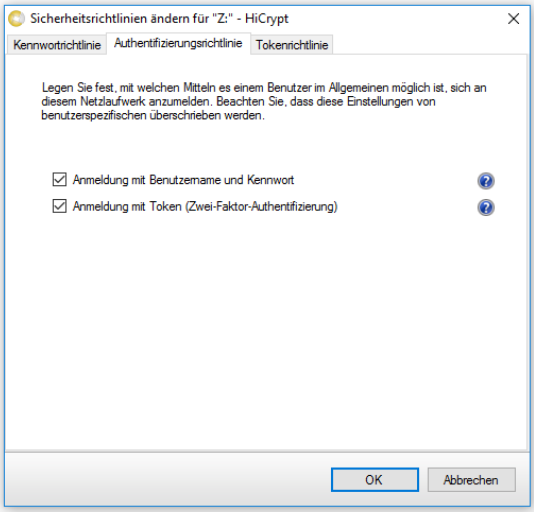


Um die Einstellungen der Sicherheitsrichtlinien zu öffnen, markieren Sie das entsprechende Laufwerk und wählen im Menü „Bearbeiten" oder im Kontextmenü „Sicherheitsrichtlinien ...".



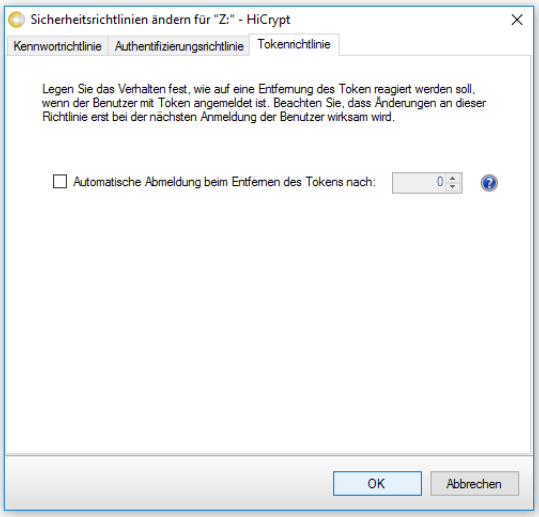
In den Sicherheitsrichtlinien können Sie die Kennwortrichtlinie ein- und ausschalten.

Wenn Sie Änderungen bei der Kennwortsicherheit vornehmen, finden diese erst bei der nächsten Kennwortänderung Anwendung.



Sie können hier die Standard-Einstellung für die erlaubten Anmeldemethoden am Netzlaufwerk einstellen.

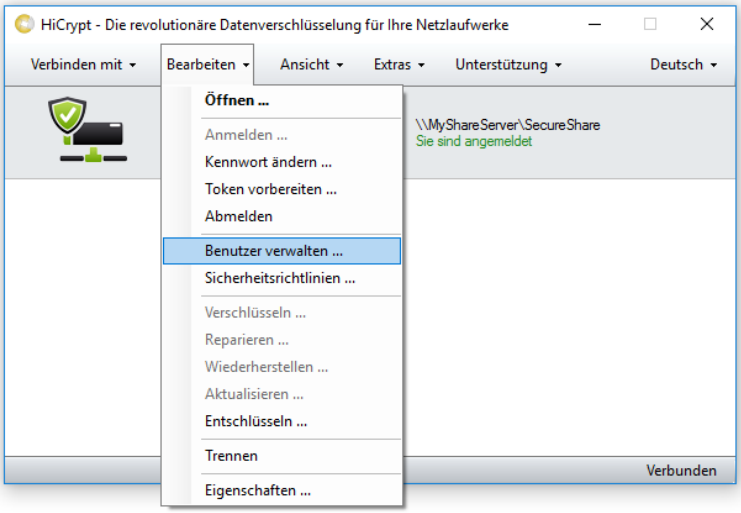
Nach der Verschlüsselung ist die Anmeldung mit Nutzername und Kennwort erlaubt, die mit SecurityToken aber verboten.



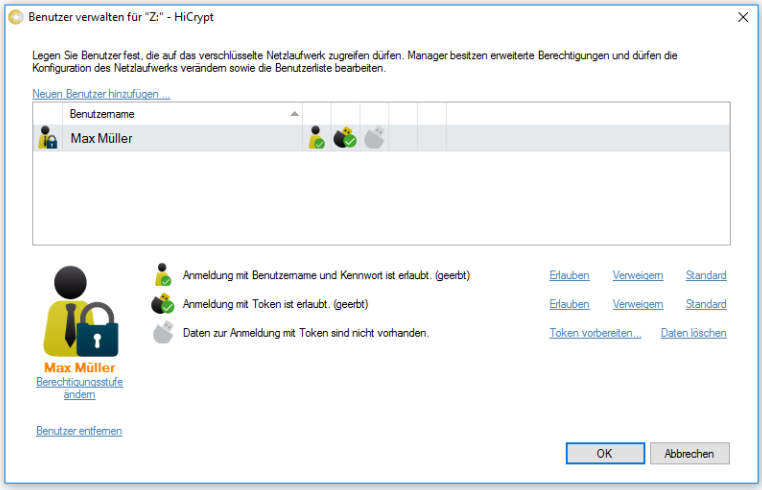
Unter dem Reiter „Tokenrichtlinie" können Sie feststellen ob eine automatische Abmeldung vom Laufwerk erfolgen soll, sobald der Token entfernt und wenn ja, wie viele Sekunden vergehen sollen, bevor die Abmeldung vom Laufwerk erfolgt.

4.5 Benutzerverwaltung

Um weiteren Benutzern den Zugriff auf das verschlüsselte Netzlaufwerk zu ermöglichen, können Sie zusätzliche Benutzer einrichten und deren Berechtigungsstufe konfigurieren.



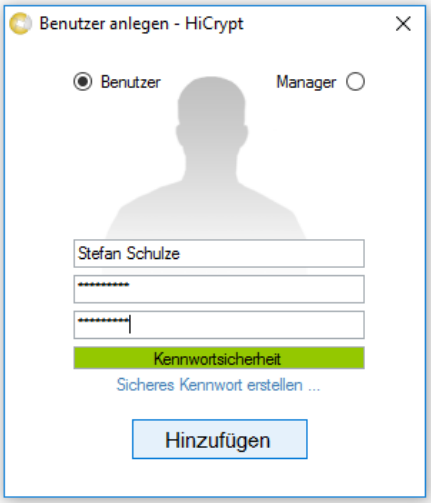
Wenn Sie die Benutzerverwaltung für das verschlüsselte Laufwerk öffnen wollen, markieren Sie das Laufwerk und wählen im Menü „Bearbeiten" oder im Kontextmenü den Punkt „Benutzer verwalten ...".



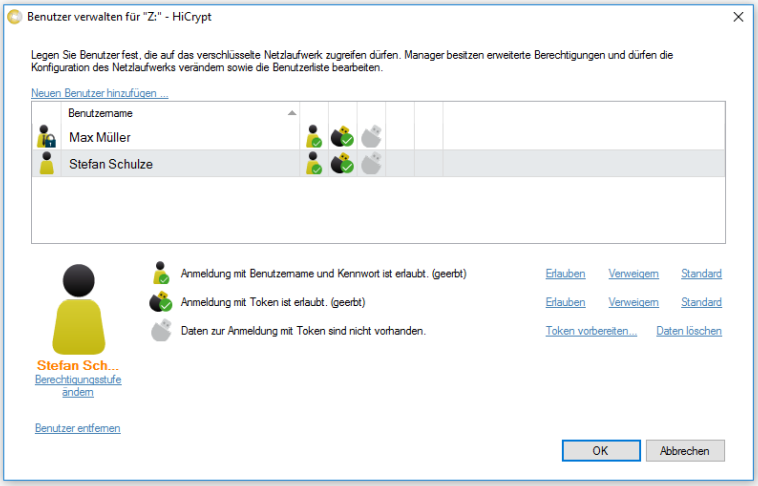
Im „Benutzer verwalten"-Dialog können neue Benutzer hinzugefügt und vorhandene gelöscht oder deren Berechtigungsstufe bearbeitet werden. Der Manager, der die Benutzerverwaltung geöffnet hat, ist bei diesem Vorgang geschützt und kann nicht bearbeitet werden.

Ein Klick auf den Link „Neuen Benutzer hinzufügen ..." öffnet den folgenden Dialog.

Ein neuer Benutzer wird immer mit Benutzername und Kennwort angelegt, egal ob er sich mit Benutzername und Kennwort anmelden darf oder nicht.



Sobald Sie den Benutzernamen und das Kennwort vergeben haben, fügen Sie den Benutzer mithilfe von „Hinzufügen" der Benutzerliste hinzu.



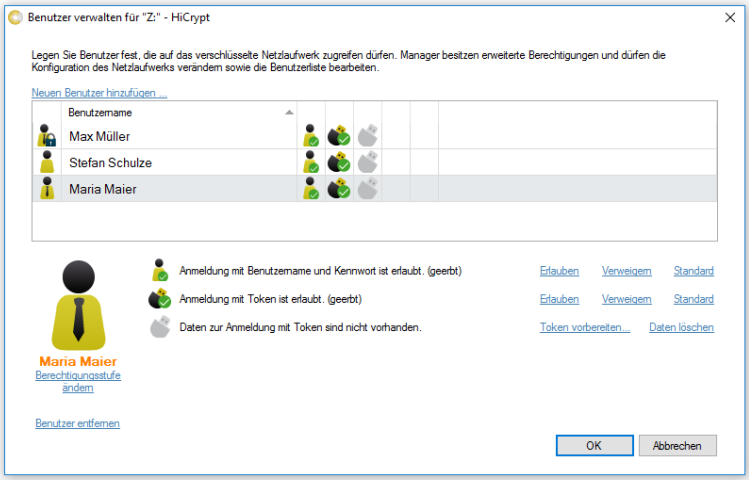
In der Benutzerliste ist nun der neue Benutzer mit der Berechtigungsstufe „Benutzer" zu sehen. Benutzer mit der Berechtigungsstufe „Benutzer" sind an der fehlenden Krawatte zu erkennen.

Um einen Benutzer mit der Berechtigungsstufe „Manager" hinzuzufügen, wird erneut ein neuer Benutzer hinzugefügt. Benutzer mit der Berechtigungsstufe „Manager" sind an der Krawatte zu erkennen.

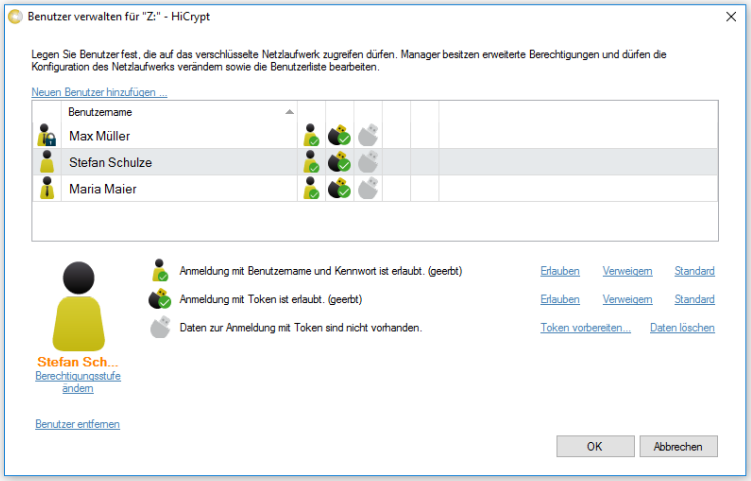
Am oberen Ende des Dialogs ist für einen neu anzulegenden Benutzer die Berechtigungsstufe „Benutzer" voreingestellt. Ein solcher Benutzer darf lediglich auf Inhalte eines verschlüsselten Netzlaufwerkes zugreifen. Die Verwaltung (Benutzer oder Sicherheitsrichtlinien verwalten oder Entschlüsseln) ist nicht möglich.

Soll der Benutzer verwaltende Berechtigungen besitzen, so ist die Berechtigungsstufe „Manager" zu wählen.

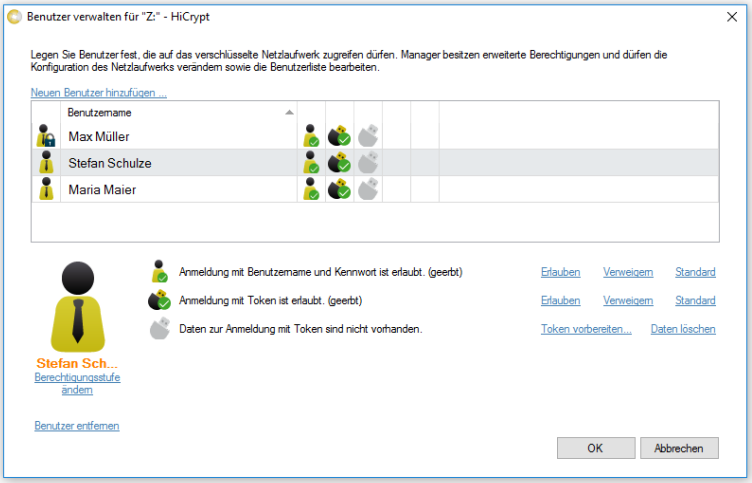
Mit „Hinzufügen" wird der neue Manager der Benutzerliste hinzugefügt.



Der neue Manager ist der Benutzerliste hinzugefügt.

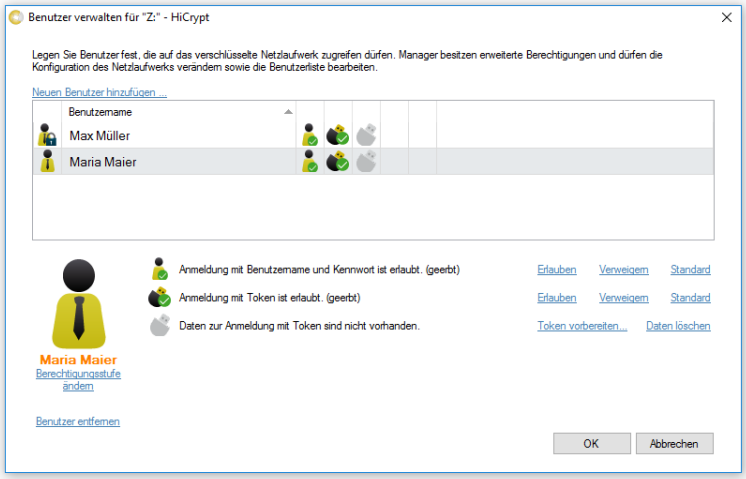


Um die Berechtigungsstufe eines Benutzers zu ändern, wird dieser markiert und der Link „Berechtigungsstufe ändern" verwendet.



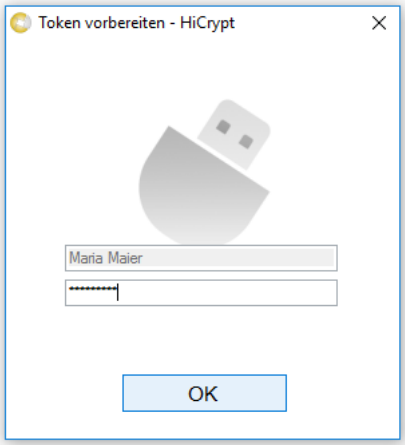
Die Änderung ist in der Benutzerliste sofort sichtbar.

Soll ein markierter Benutzer gelöscht werden, wird der Link „Benutzer entfernen" verwendet.

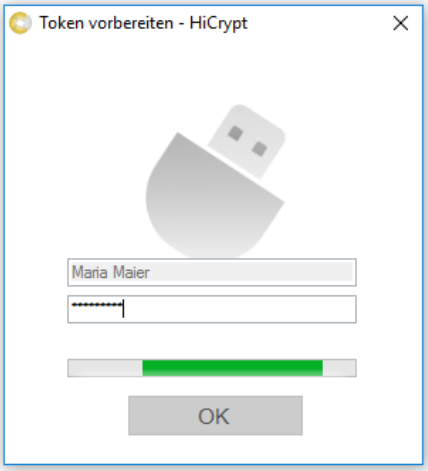


Auch in diesem Fall sind Änderungen der Benutzerliste sofort sichtbar.

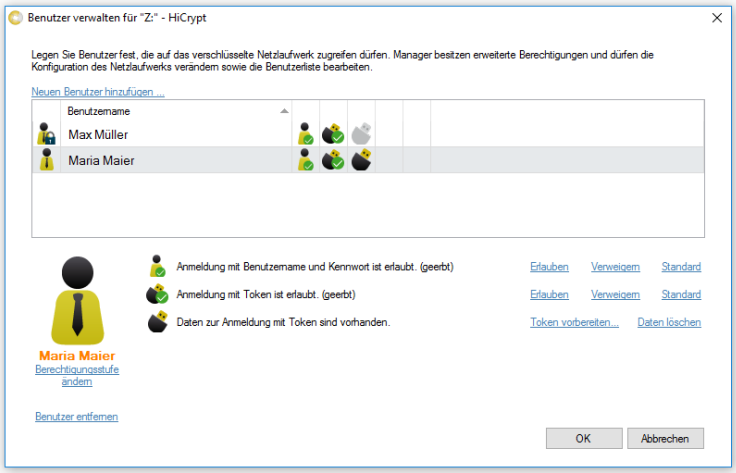
Um einen Token vorzubereiten, markieren Sie den entsprechenden Nutzer, stecken den SecurityToken an und wählen den Link „Token vorbereiten…".



Sie benötigen dann das Passwort des Nutzers und die PIN/Benutzer-PIN des SecurityTokens.

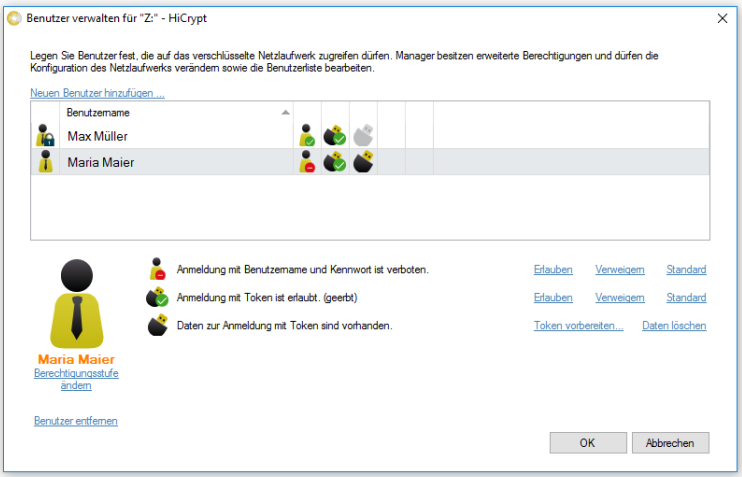


Warten Sie während auf dem SecurityToken ein Schlüsselpaar erzeugt wird und dieses mit dem HiCrypt™ 2.0-Nutzer verbunden wird.



Wenn der SecurityToken erfolgreich vorbereitet wurde, ist das Tokensymbol in der dritten Spalte nicht mehr monochrom, sondern farbig dargestellt.

„Daten löschen" löst nur die Verbindung zwischen HiCrypt™ 2.0-Nutzer und dem Schlüsselpaar. Das Schlüsselpaar selbst bleibt auf dem Security-Token erhalten.



Bei ausgewähltem Benutzer kann man für diesen festlegen, welche Anmeldemethoden erlaubt sind. Wenn hinter der Anmeldemethode in Klammern „geerbt" steht, dann handelt es sich um die „Standard"-Einstellung aus den Sicherheitsrichtlinien.

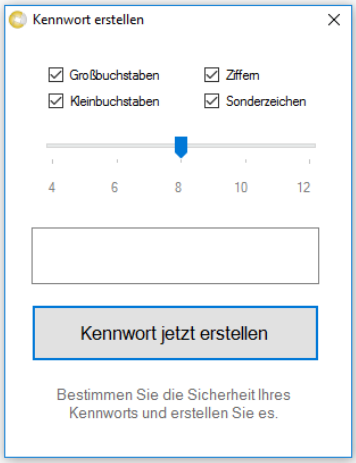
Ist das Symbol am Umriss oder Token ein „Einbahnstraßenschild", dann ist die betreffende Anmeldemethode im Moment nicht erlaubt.

Vorgenommene Änderungen werden erst dann übernommen, wenn Sie diesen Dialog mit „Ok" beenden.

Wenn Sie Änderungen an den Benutzern vorgenommen haben, dann werden diese erst übernommen, wenn dieser sich das nächste Mal anmeldet. Ein Nutzer, der gelöscht wird, aber noch angemeldet ist, hat bis zu seiner Abmeldung Zugriff auf die Daten.

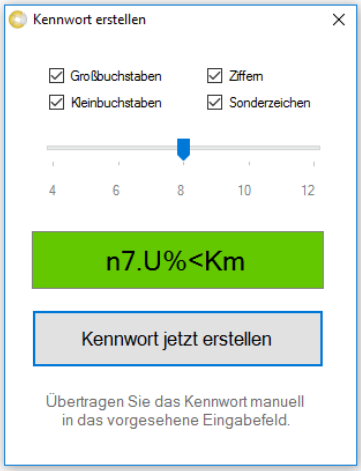
4.6 Kennwort-Generator

Um das Erstellen von Kennworten zu erleichtern, gibt es in den Dialogen, in denen Kennworte angelegt werden, die Möglichkeit einen Kennwortgenerator zu aktivieren.



Wählen Sie aus, aus wie vielen Zeichen Ihr Kennwort bestehen soll und welche Zeichenkategorien enthalten sein sollen.

Sobald Sie „Kennwort jetzt erstellen" betätigen, wird das Kennwort erstellt.

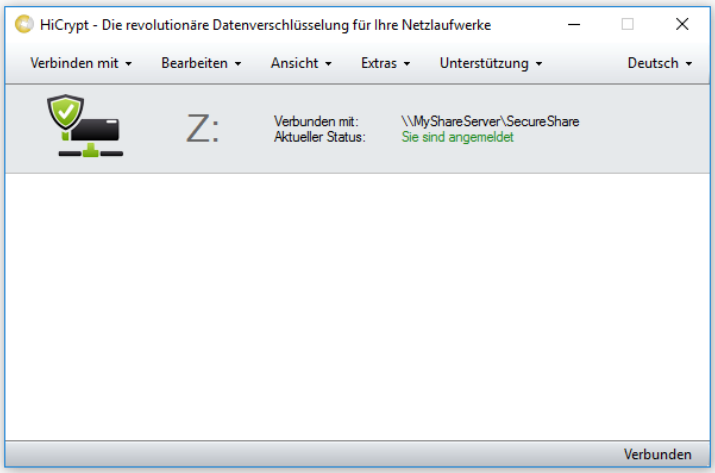


Dieses Kennwort kann nicht kopiert werden, damit dem Benutzer verdeutlicht wird, dass man es tatsächlich benötigt und nicht vergessen sollte.

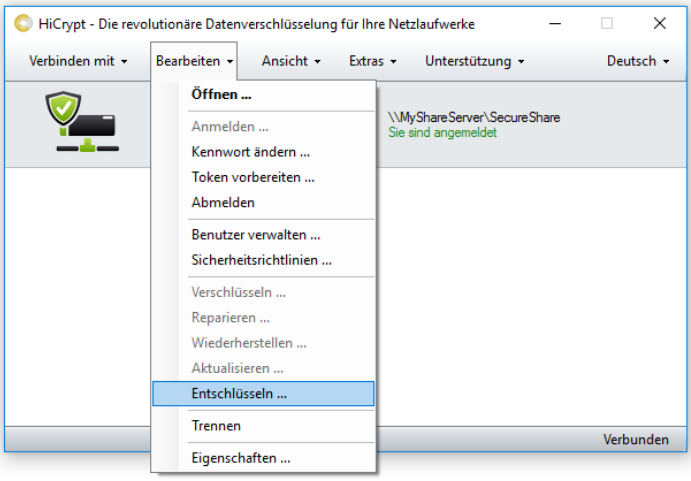
KAPITEL 5

5 Entschlüsselung

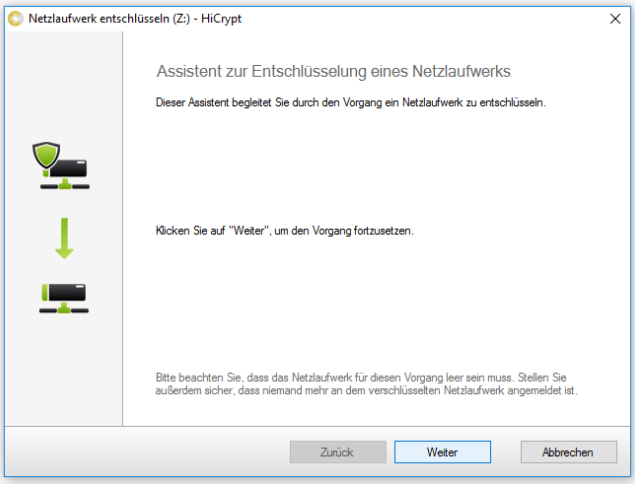
Bitte beachten Sie, dass das Netzlaufwerk zur erfolgreichen Entschlüsselung leer sein muss und nur noch der Manager angemeldet ist, der die Entschlüsselung durchführt.



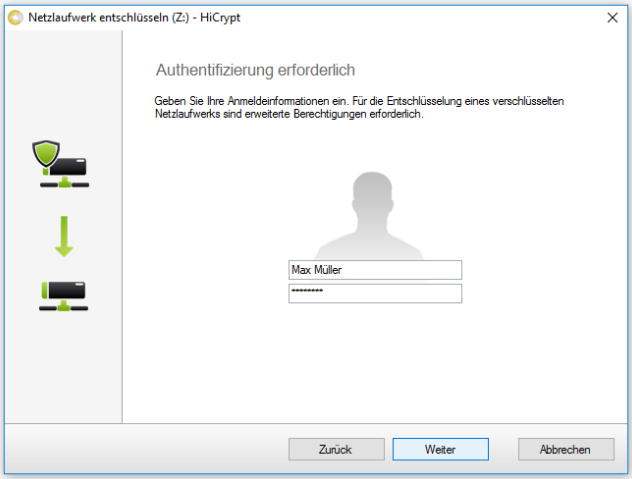
Markieren Sie das verschlüsselte Laufwerk.



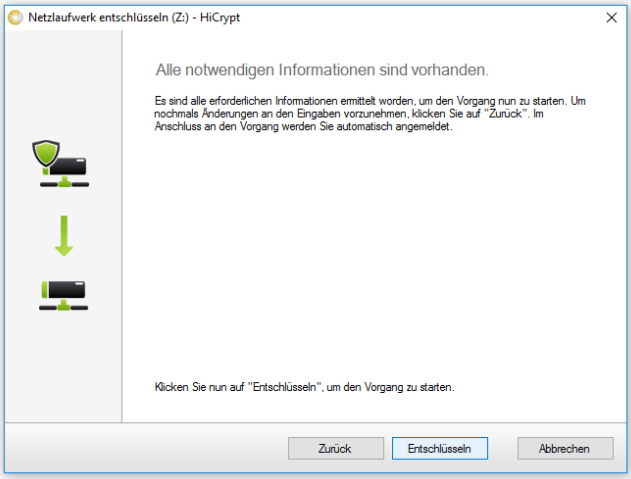
Um das Laufwerk zu entschlüsseln, wählen sie im Menü „Bearbeiten" oder im Kontextmenü den Punkt „Entschlüsseln …".



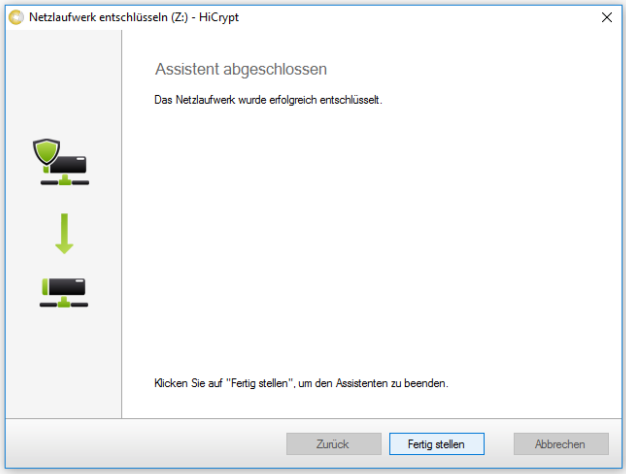
Um fortzufahren wählen Sie im erscheinenden Dialog „Weiter".



Geben Sie im nächsten Dialog die Anmeldedaten eines Managers an und bestätigen Sie diese mit „Weiter".



Um die Entschlüsselung zu starten, klicken Sie auf „Entschlüsseln".

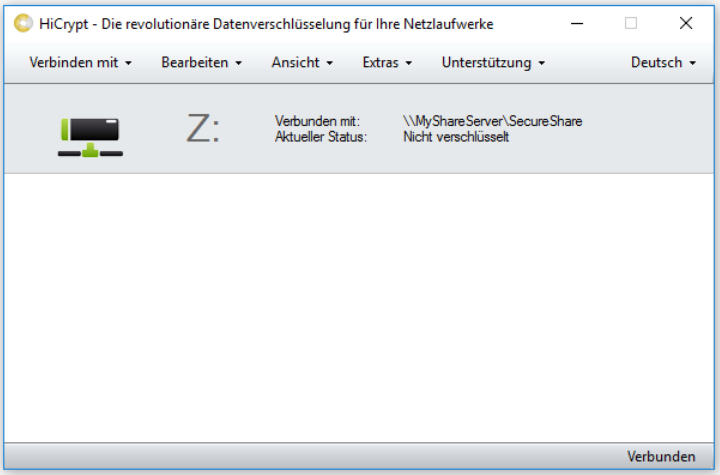


Um den Assistenten nach der Entschlüsselung zu beenden, nutzen Sie „Fertig stellen".

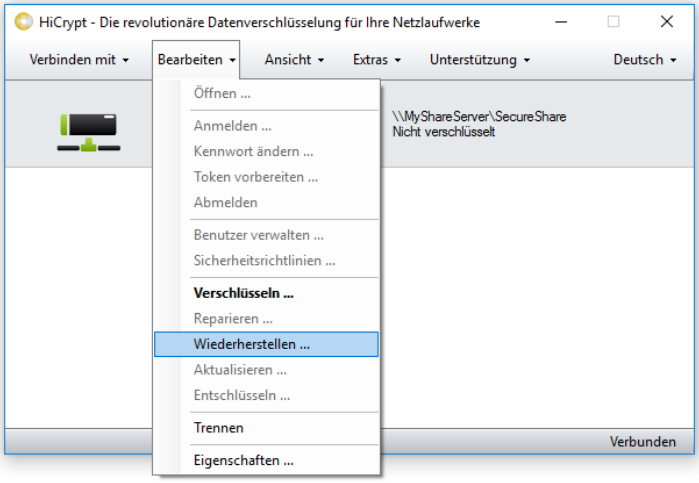
KAPITEL 6

6 Wiederherstellung

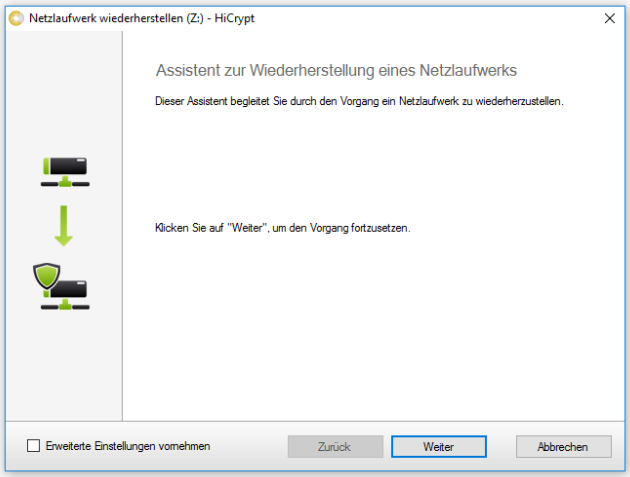
In diesem Kapitel wird die Verwendung des Wiederherstellungsschlüssels erläutert. Dazu benötigen Sie zunächst ein unverschlüsseltes, leeres Netzlaufwerk.

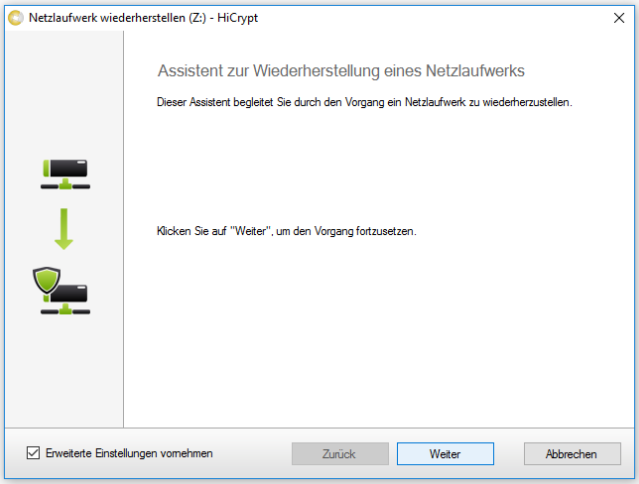


Markieren Sie zuerst das Laufwerk.

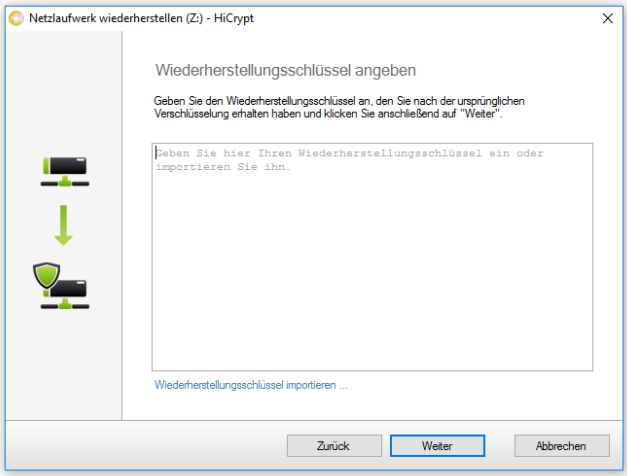


Wählen Sie im Menü „Bearbeiten" oder im Kontextmenü den Punkt „Wiederherstellen ...".

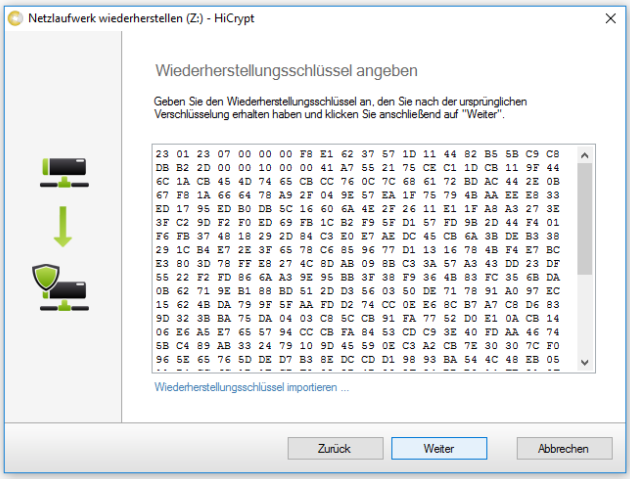




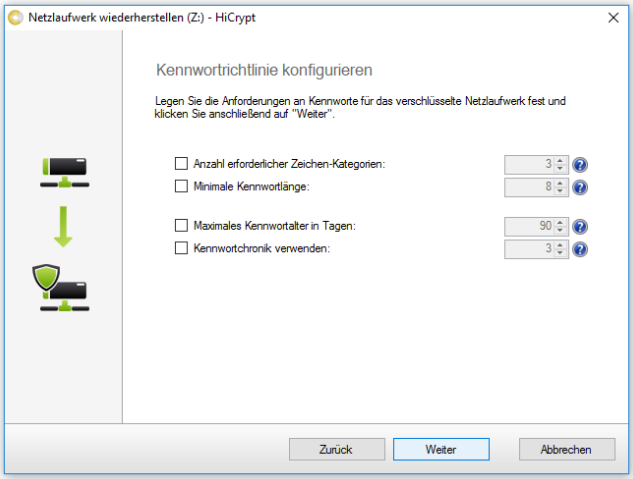
Wie bei der Verschlüsselung besteht nun die Möglichkeit, erweiterte Einstellungen vorzunehmen oder nicht. Bei der Wiederherstellung wird hierbei nur eine Kennwortrichtlinie festgelegt, da der Verschlüsselungsalgorithmus bereits durch den Wiederherstellungsschlüssel festgelegt ist.



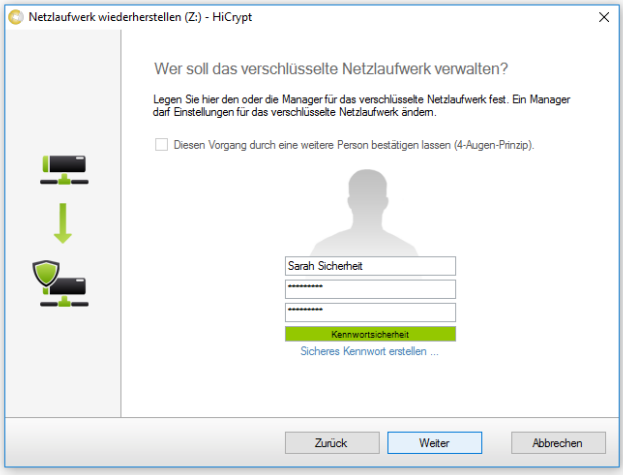
Geben Sie nun den Wiederherstellungsschlüssel ein, oder importieren Sie diesen aus der gesicherten *.hrk-Datei.



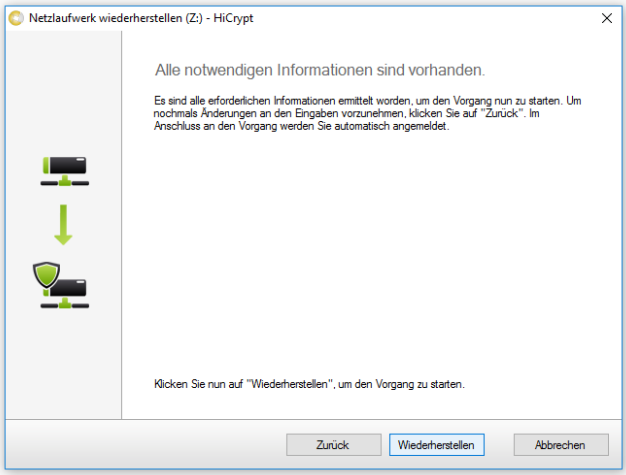
Bestätigen Sie die Eingabe mit „Weiter".



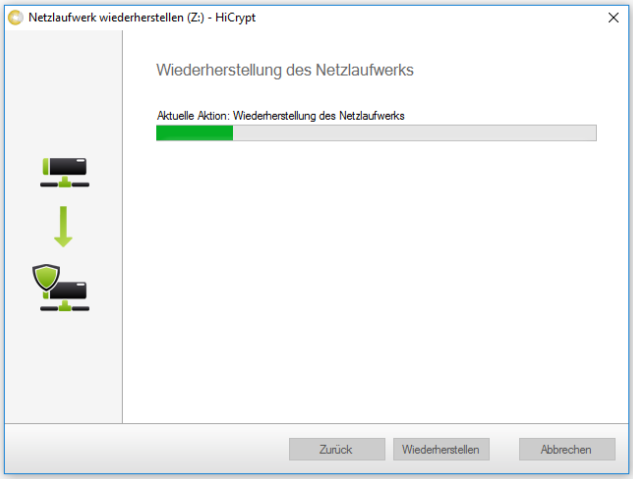
Erweiterte Einstellung: Sie können jetzt die Kennwortrichtlinie festlegen und die Wiederherstellung mit „Weiter" fortsetzen.



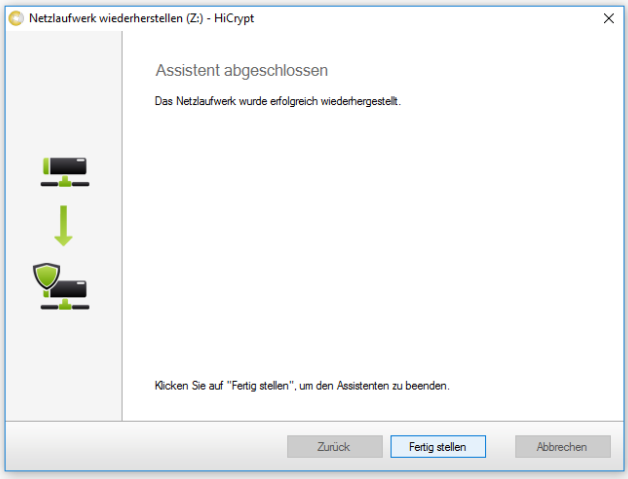
Legen Sie nun einen neuen Manager an. Sollten Sie für das alte Laufwerk das „Vier-Augen-Prinzip" verwendet haben, werden Sie dieses nun erneut verwenden müssen. Bestätigen Sie mit „Weiter".



Um fortzufahren wählen Sie „Wiederherstellen".



Warten Sie einen Augenblick, während HiCrypt™ 2.0 das Laufwerk für Sie wiederherstellt.



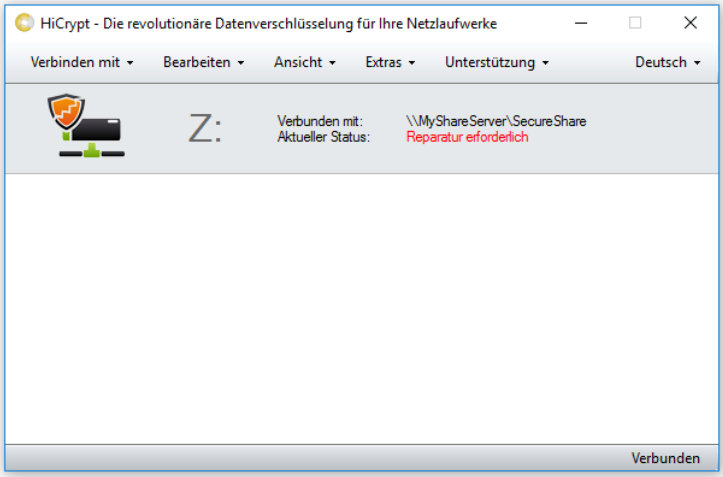
Mit „Fertig stellen" beenden Sie den Prozess und das Fenster schließt sich.

Kopieren Sie nun die verschlüsselten Dateien **am Dateiserver** aus dem alten Verzeichnis in die neu verschlüsselte Freigabe.

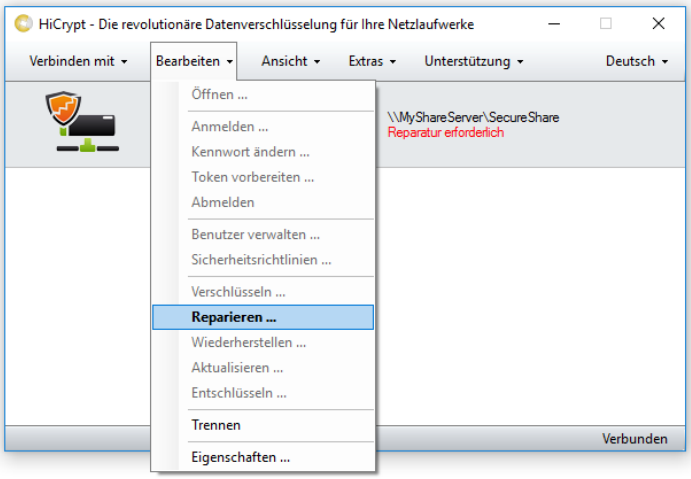
KAPITEL 7

7 Reparieren

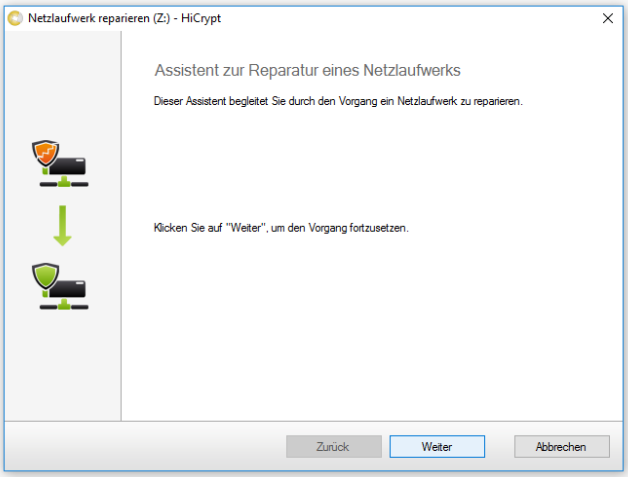
Reparieren wird dann notwendig, wenn das Keyfile beschädigt ist. Um ein Laufwerk reparieren zu können, benötigen Sie ein intaktes Backupfile.



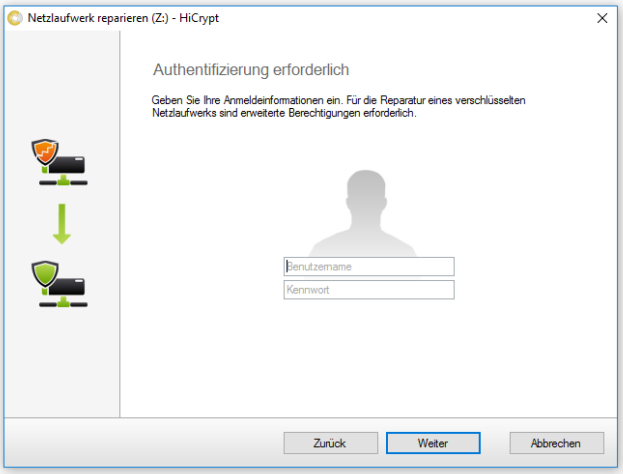
An dem zerbrochenen Schild am Laufwerk ist zu erkennen, dass eine Reparatur erforderlich ist.



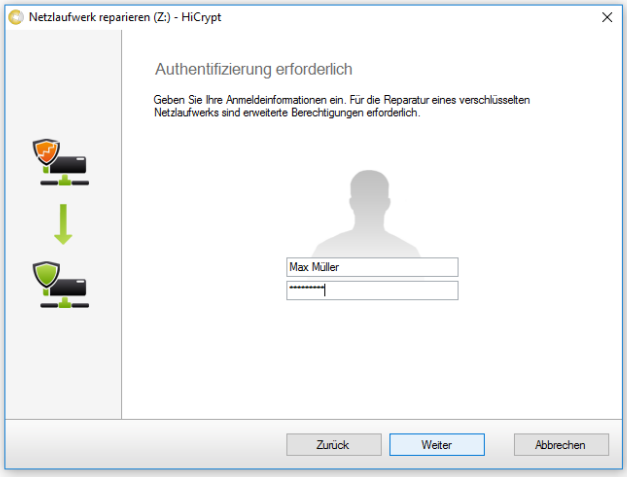
Markieren Sie das zu reparierende Laufwerk und wählen Sie im Menü „Bearbeiten" oder im Kontextmenü den Punkt „Reparieren ...".



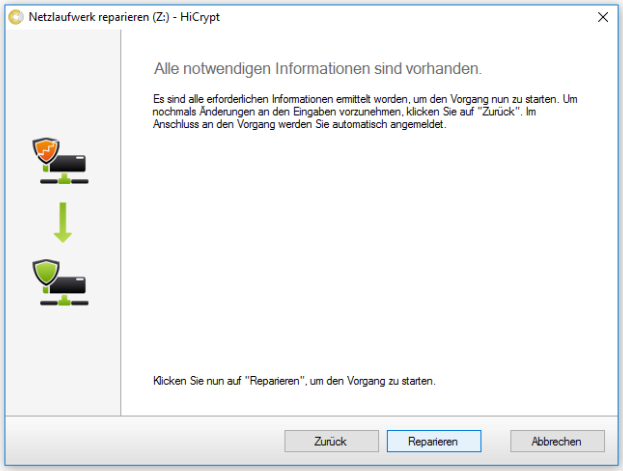
Um den Assistenten zur Reparatur des Netzlaufwerkes fortzuführen, betätigen Sie die Schaltfläche „Weiter".



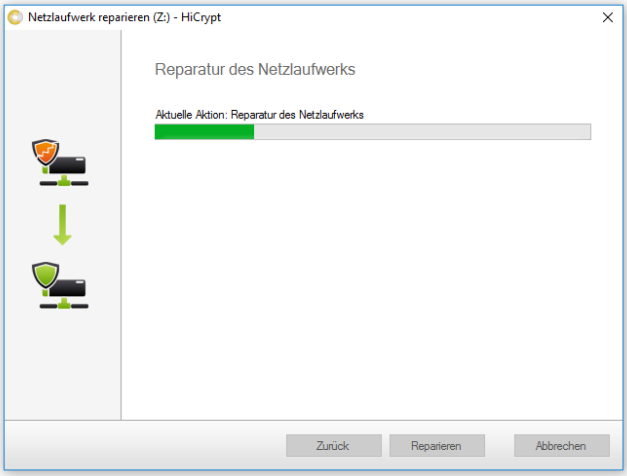
Um mit dem Reparieren fortzufahren, tragen Sie hier die Anmeldedaten eines Managers ein. Wenn das Laufwerk mit dem Vier-Augen-Prinzip verschlüsselt wurde, muss dieser Vorgang von 2 Managern bestätigt werden.



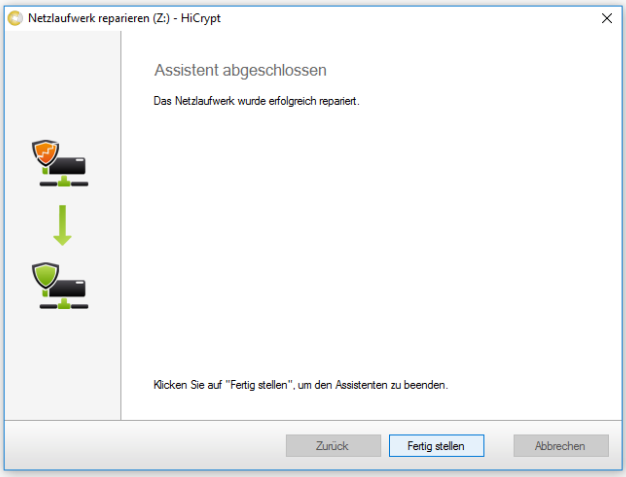
Wenn Sie die Manager Daten eingegeben haben, fahren Sie mit „Weiter" fort.



Starten Sie die Reparatur mit der Schaltfläche „Reparieren".



Warten Sie, während HiCrypt™ 2.0 aus dem Backupfile ein neues Keyfile erzeugt.



Um den Assistenten zu beenden, wählen Sie „Fertig stellen".

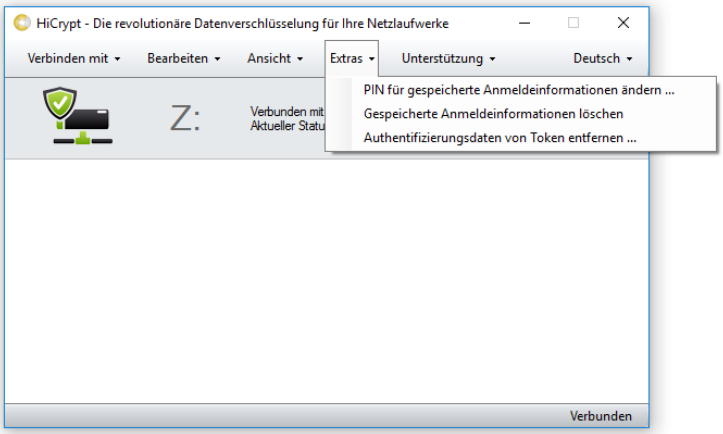
KAPITEL 8

8 Weitere Optionen

In diesem Kapitel werden die Menü-Optionen erläutert und vorgestellt, die bisher keine Erwähnung fanden.

Wenn Sie ein Laufwerk markiert haben, können Sie im Menü „Bearbeiten" oder im Kontextmenü den Punkt „Eigenschaften" auswählen.

Dort erhalten Sie einige Informationen über das Netzlaufwerk angezeigt, wie zum Beispiel den Status und den Algorithmus der Verschlüsselung.



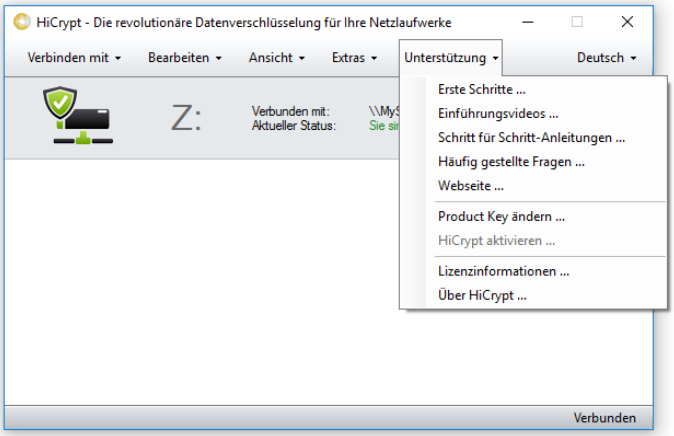
Im Menü „Extras" stehen drei Punkte zur Verfügung.

Der Punkt „PIN für gespeicherte Anmeldeinformationen ändern ..." ermöglicht es, eine PIN für gespeicherte Anmeldeinformationen festzulegen, sollte es noch keine geben, oder die vorhandene PIN zu ändern.

Mit „Gespeicherte Anmeldeinformationen löschen" werden bereits gespeicherte Anmeldeinformationen gelöscht.

„Authentifizierungsdaten von Token entfernen ..." löscht das auf dem SecurityToken erstellte Schlüsselpaar von diesem.

Das vergeben einer PIN für gespeicherte Anmeldedaten ist dann sinnvoll, wenn man mehrere verschlüsselte Laufwerke eingebunden hat und keine Token zur Anmeldung benutzt.



Im Menu Unterstützung finden sich im oberen Block Informationen zu HiCrypt™ 2.0 und seiner Einrichtung. Außer dem Punkt „Erste Schritte …" verweisen alle anderen auf online abrufbare Inhalte.

Über „Product Key ändern …" kann man einen neuen Product Key eingeben.

Sollte HiCrypt™ 2.0 noch nicht aktiviert sein, so kann man mit „HiCrypt aktivieren …" den eingegebenen Product Key aktivieren.

Im Dialog Lizenzinformationen werden die aktuellen Lizenzinformationen angezeigt, sowie die aktuell lizenzierten Features.

Außerdem kann man über „Lizenz jetzt online aktualisieren" die aktuellen Features seiner Lizenz abrufen oder über „Feature Key eintragen" den aktuellen Feature Key offline eintragen, wenn ein Online-Abruf nicht möglich ist.

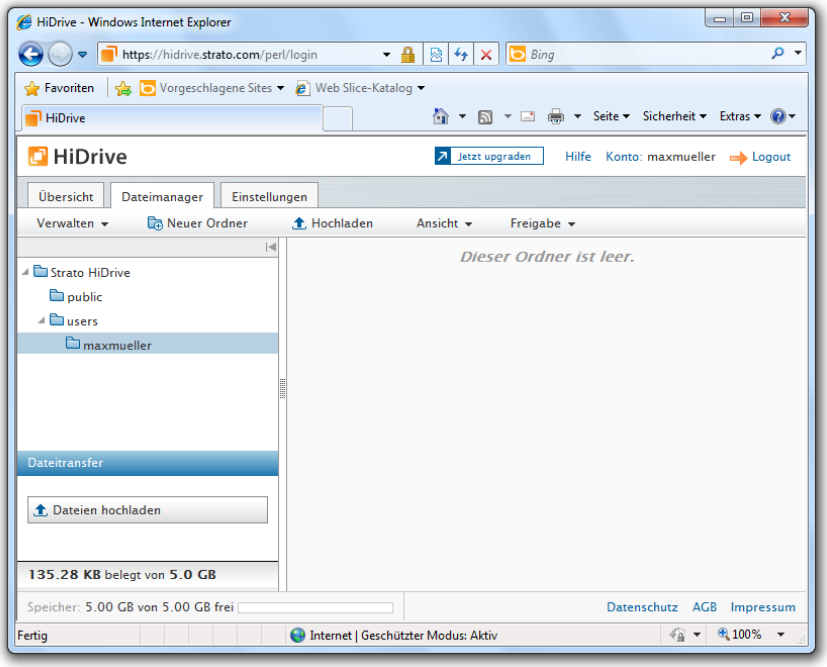
Das Fenster „Über HiCrypt …" erläutert kurz die Funktion von HiCrypt™ 2.0. Unten Links finden sich detaillierte Versionsinformationen und daneben finden Sie die Kontaktdaten des Herstellers.

KAPITEL 9

9 Verwendung von Online-Speichern

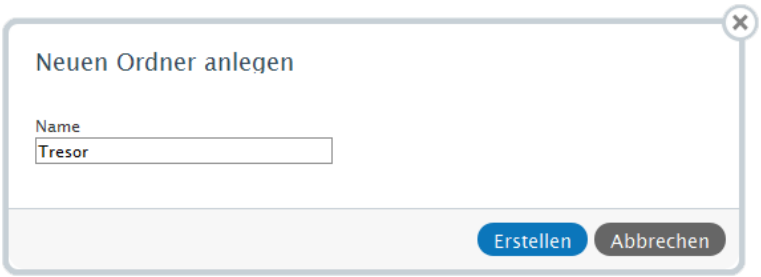
Online-Speicher können mit HiCrypt™ 2.0 ebenfalls verschlüsselt werden. Hierfür sind nur wenige zusätzliche Schritte notwendig, um den jeweiligen Online-Speicher für die Verschlüsselung mit HiCrypt™ 2.0 vorzubereiten.

Die Verwendung von HiCrypt™ 2.0 mit Online-Speichern wird hier beispielhaft an Strato's HiDrive erläutert. Die dargestellten Schritte sind bei allen Online-Speichern ähnlich. Ziel dieser Vorbereitungen ist es, ein Netzlaufwerk zu einem Online-Speicher zu verbinden, welches schließlich mit HiCrypt™ 2.0 verschlüsselt werden kann.

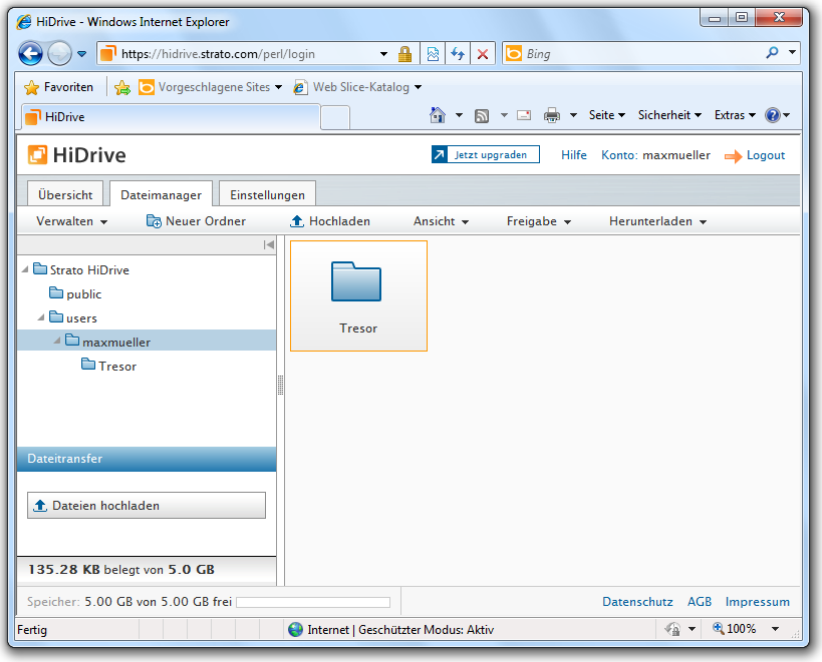


Diese Abbildung zeigt die WEB-Ansicht des Online-Speichers. Hier können Ordner und Dateien ähnlich wie auf der eigenen Festplatte gespeichert werden.

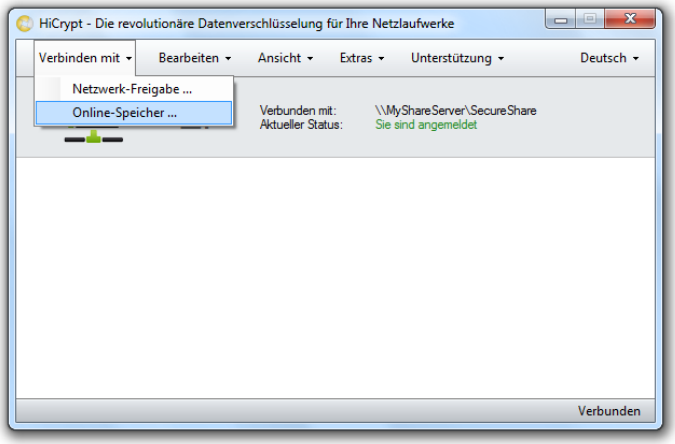
Viele Online-Speicher enthalten von Haus aus bereits Dateien. Das Netzlaufwerk muss bei der Verschlüsselung jedoch zunächst leer sein. Dadurch kann nicht der gesamte Online-Speicher verschlüsselt werden. Es gilt, einen Unterordner anzulegen, dessen Inhalt verschlüsselt werden soll.



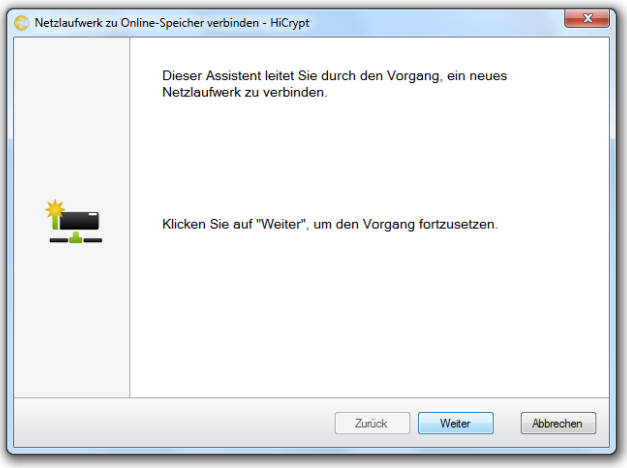
Es wird daher ein neuer Ordner angelegt und benannt. In unserem Beispiel wurde der Ordner „Tresor" genannt.



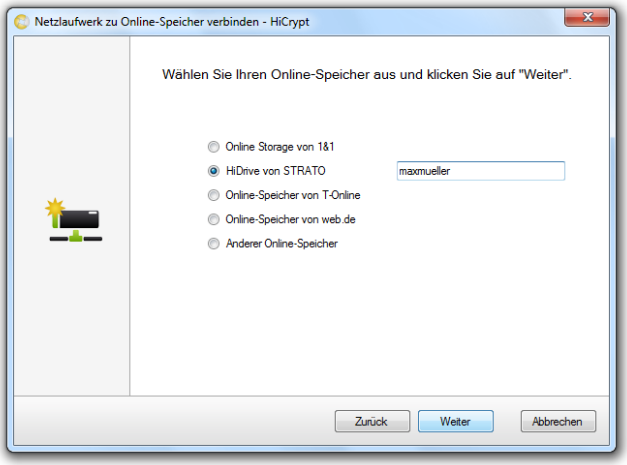
Dieser Ordner kann nun mit HiCrypt™ 2.0 zu einem Netzlaufwerk verbunden werden.



Hierfür stellt HiCrypt™ 2.0 einen weiteren Assistenten bereit, mit dem speziell Online-Speicher verbunden werden. Über „Verbinden mit" und dem Punkt „Online-Speicher ..." wird dieser Assistent gestartet.



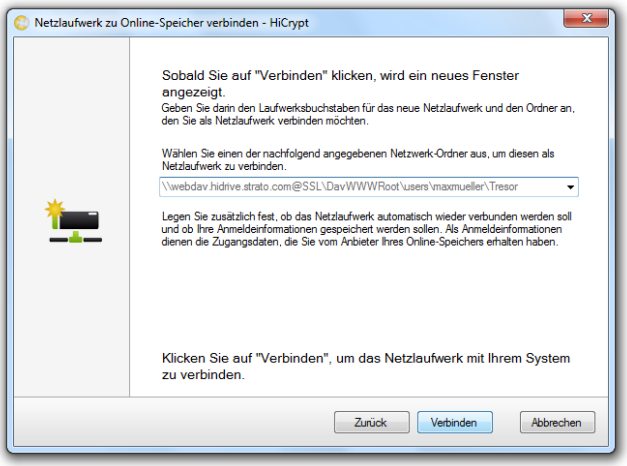
Der Willkommensdialog wird mit der Schaltfläche „Weiter" bestätigt.



Im nächsten Schritt wird bereits eine Auswahl an Online-Speichern angezeigt. Sollte der gewünschten Online-Speicher nicht aufgeführt sein, wird „Anderer Online-Speicher" ausgewählt.

Im Beispiel von Strato's HiDrive wird zusätzlich die Angabe des Benutzernamens erforderlich.

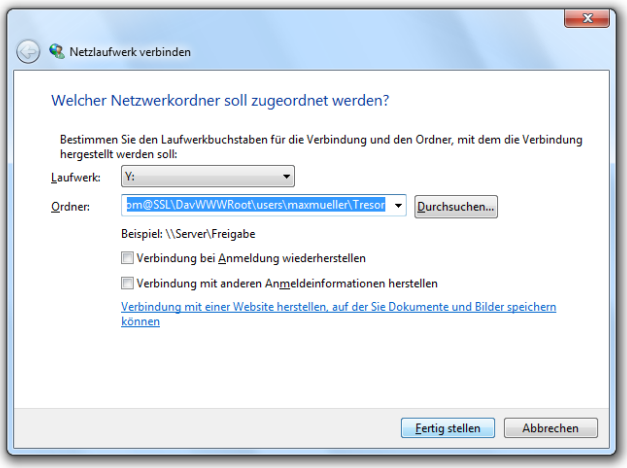
Durch Betätigen der Schaltfläche „Weiter" wird der nächste Dialog des Assistenten angezeigt.



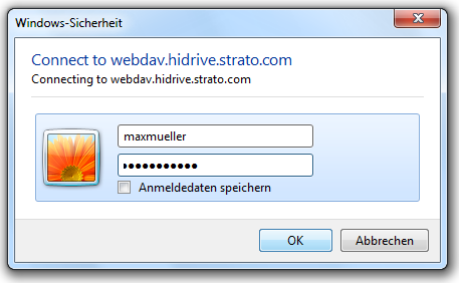
Die im vorherigen Dialog getroffene Auswahl sowie die Eingabe des Benutzernamens führt an dieser Stelle zu einem generierten Pfad, über den die Verbindung zu dem Online-Speicher hergestellt und so das Netzlaufwerk verbunden wird.

Sofern ein nicht in der Liste aufgeführter Online-Speicher verwendet werden soll, muss der hier generierte Pfad manuell im nächsten Dialog eingegeben werden.

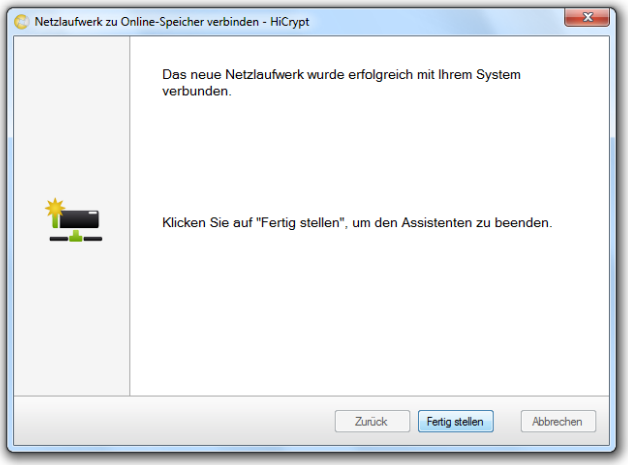
Mit dem Betätigen der Schaltfläche „Verbinden" wird der Windows-Standard-Dialog zum Verbinden eines Netzlaufwerks angezeigt.



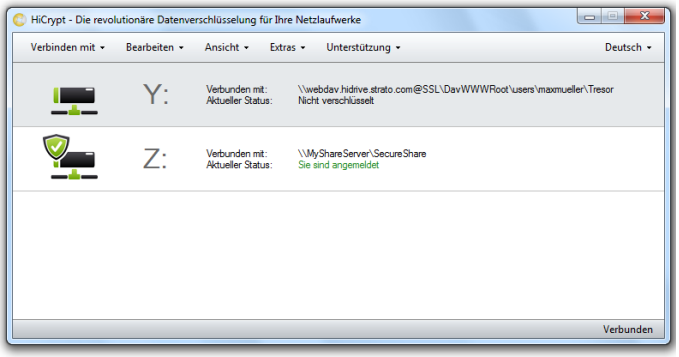
Der Pfad zu dem Online-Speicher wurde bereits vorausgefüllt, so dass das Betätigen der Schaltfläche „Fertig stellen" ausreicht, um das Netzlaufwerk zu verbinden.



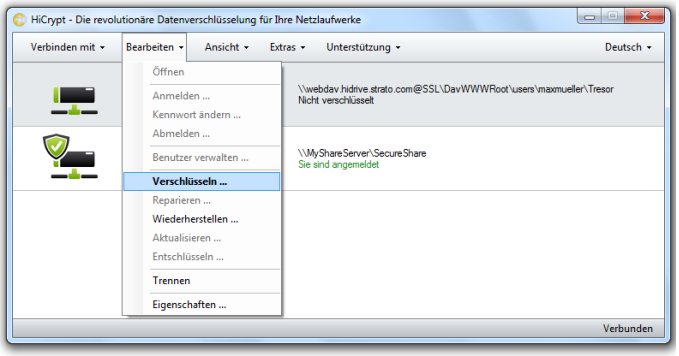
Für den Zugriff auf den Online-Speicher ist eine Anmeldung bei dem jeweiligen Anbieter erforderlich. Die erforderlichen Zugangsdaten sind identisch mit denen bei der Anmeldung mittels Browser.



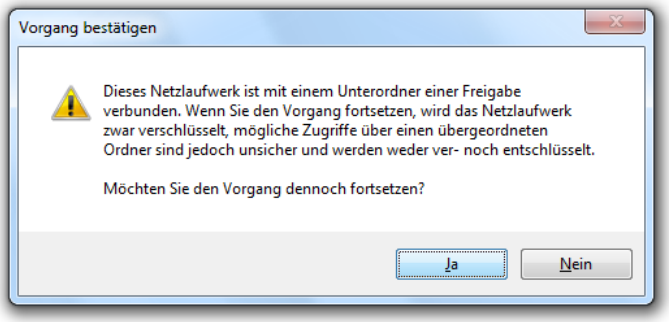
Nachdem das Netzlaufwerk erfolgreich verbunden wurde, kann der Assistent zum Verbinden eines Netzlaufwerks zu einem Online-Speicher durch Betätigen der Schaltfläche „Fertig stellen" geschlossen werden.



HiCrypt™ 2.0 zeigt das neu verbundene Netzlaufwerk zu dem Online-Speicher in der Liste der verbundenen Netzlaufwerke an.

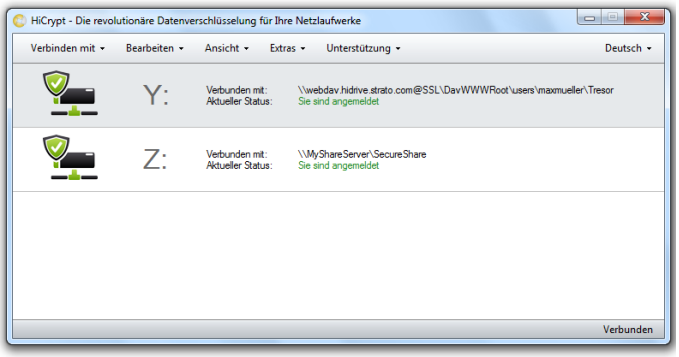


Dieses Netzlaufwerk kann nun wie gewohnt verschlüsselt werden.



Während der Verschlüsselung wird diese Warnung angezeigt. Sie deutet darauf hin, dass das Netzlaufwerk mit einem Unterordner des Online-Speichers verbunden ist. Dies war notwendig, da bei einigen Online-Speicher-Anbietern bereits Dateien im Online-Speicher vorhanden sind und eine Verschlüsselung damit nicht möglich ist.

Zum Verschlüsseln des Netzlaufwerks zum Online-Speicher wird diese Warnung mit „Ja" beantwortet.



Im Anschluss an die Verschlüsselung wird der Online-Speicher in HiCrypt™ 2.0 verschlüsselt angezeigt.

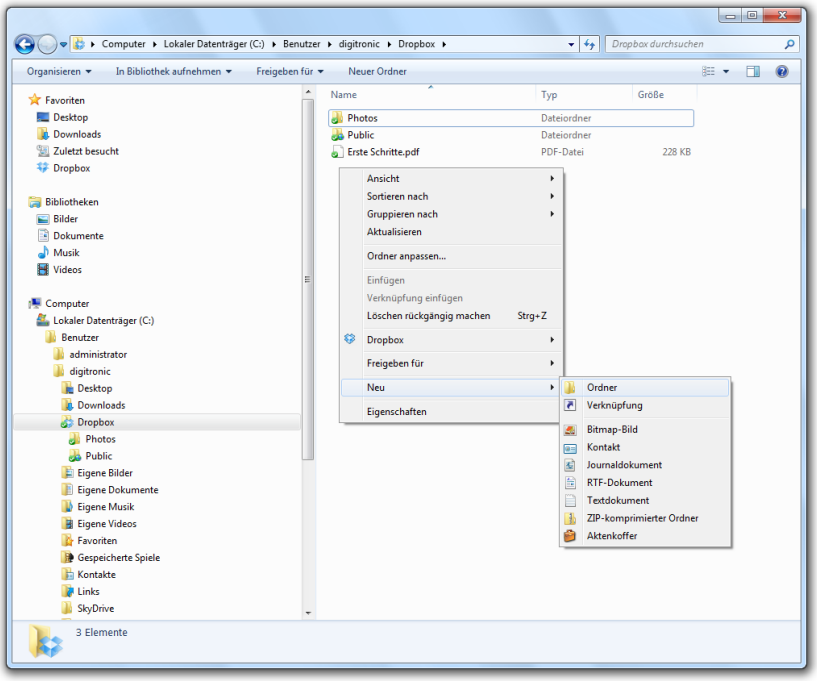
Der Zugriff auf den verschlüsselten Online-Speicher ist nun nur noch mittels HiCrypt™ 2.0 möglich. Der Zugriff über den Browser und die WEB-Ansicht des Online-Speicher-Anbieters ist nicht möglich, da dann die Daten nicht entschlüsselt werden. Eine Entschlüsselung der Daten geschieht nur dann, wenn der Online-Speicher zu einem Netzlaufwerk verbunden und der Benutzer mit HiCrypt™ 2.0 an diesem Netzlaufwerk angemeldet ist.

Viele Anwendungen nutzen in neueren Versionen eigene WebDAV-Verbindungen anstatt über das verbundene Netzlaufwerk zuzugreifen. Dies führt dazu, dass diese Anwendungen an HiCrypt™ 2.0 vorbei arbeiten. Deshalb wird eine Verwendung von WebDAV nicht mehr empfohlen.

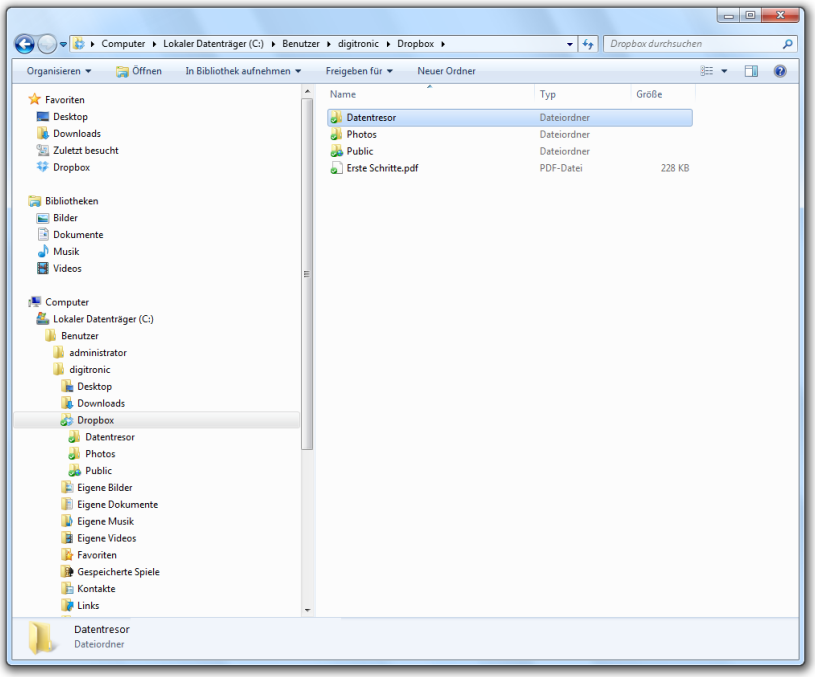
KAPITEL 10

10 Verwendung von Dropbox und ähnlicher Dienste

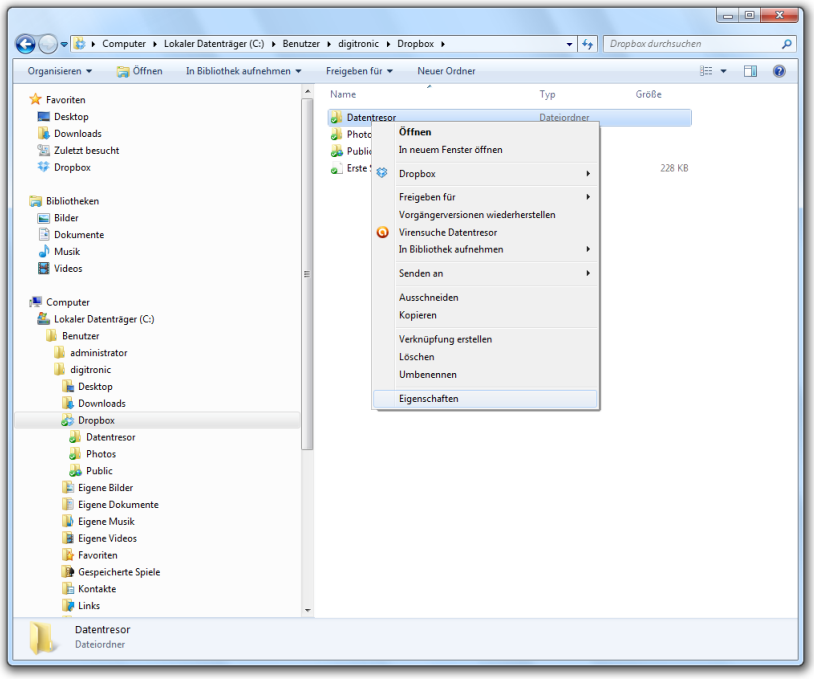
Ähnlich wie bei der Verwendung von Online-Speichern, ist es erforderlich, ein Netzlaufwerk zu verbinden, welches mit HiCrypt™ 2.0 verschlüsselt werden kann. Das Vorgehen wird hier am Beispiel von Dropbox dargestellt.



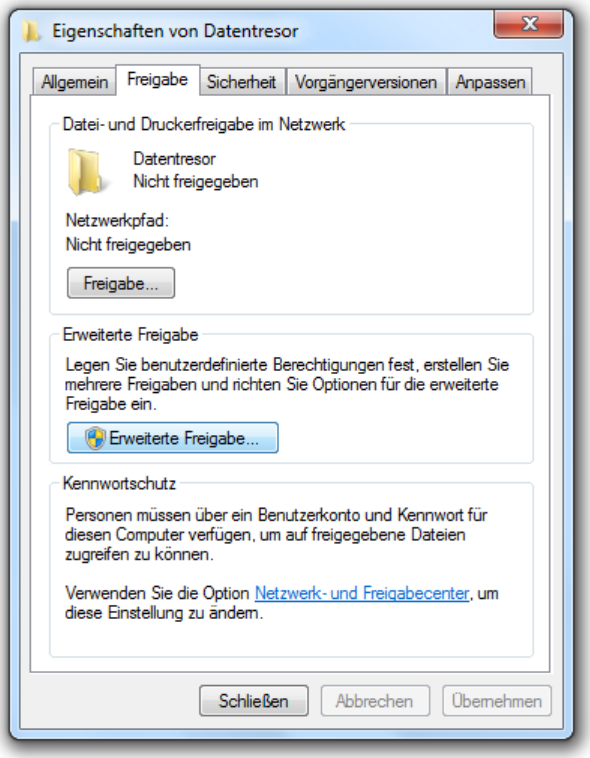
In dem Dropbox-Ordner wird ein neuer Ordner angelegt, der anschließend zu einem Netzlaufwerk verbunden wird.



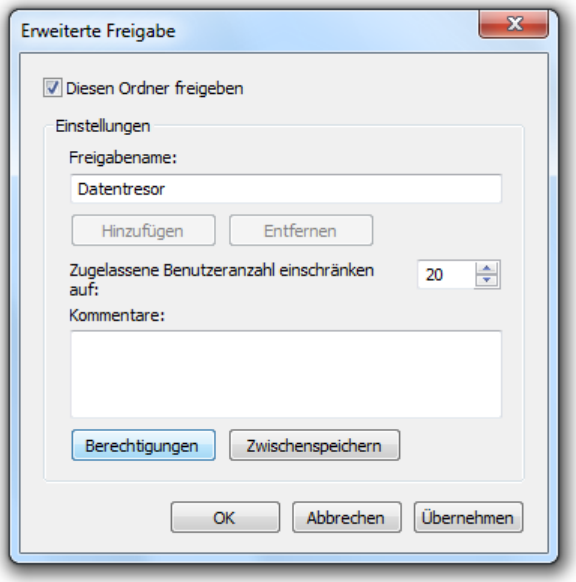
Dieser Ordner wird hier beispielhaft als „Datentresor" benannt.



Um diesen Ordner zu einem Netzlaufwerk verbinden zu können, muss er freigegeben werden. Hierzu werden die Eigenschaften des Ordners angezeigt.

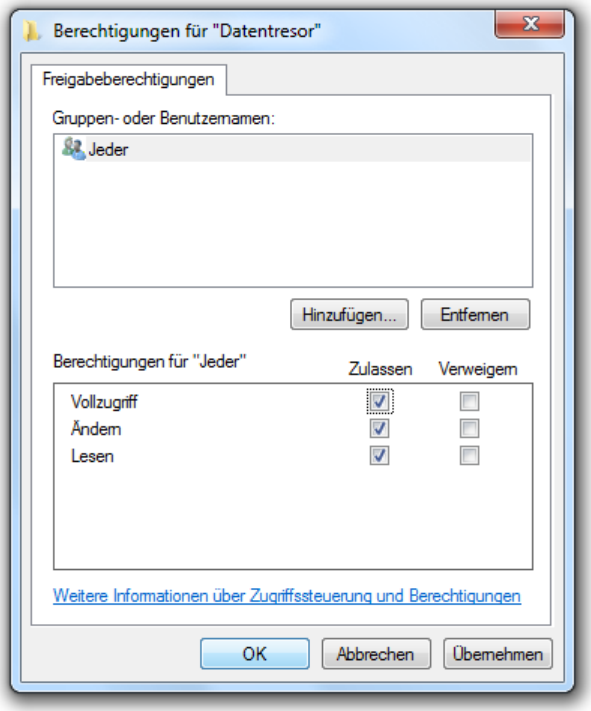


Auf der Registerkarte „Freigabe" wird die Schaltfläche „Erweiterte Freigabe…" betätigt. Das Symbol auf der Schaltfläche zeigt an, dass für diesen Vorgang administrative Berechtigungen erforderlich sind.



Im sich öffnenden Dialog wird die Option „Diesen Ordner freigeben" aktiviert. Der Freigabename ist frei wählbar. Standardmäßig wird der Name des Ordners verwendet.

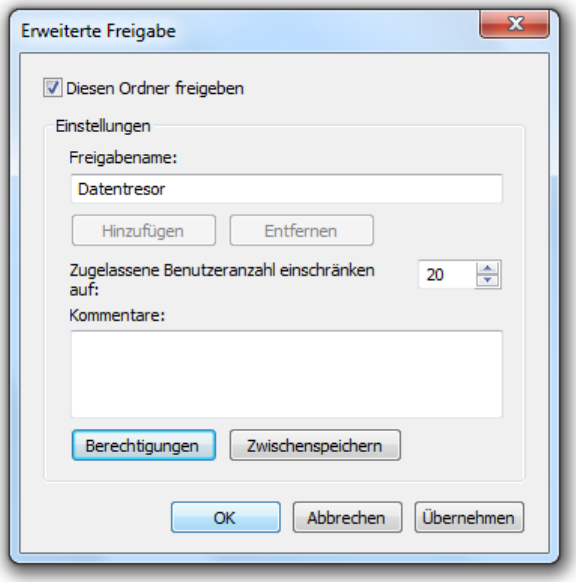
Nun müssen die Berechtigungen noch geändert werden. Hierfür wird die Schaltfläche „Berechtigungen" betätigt.



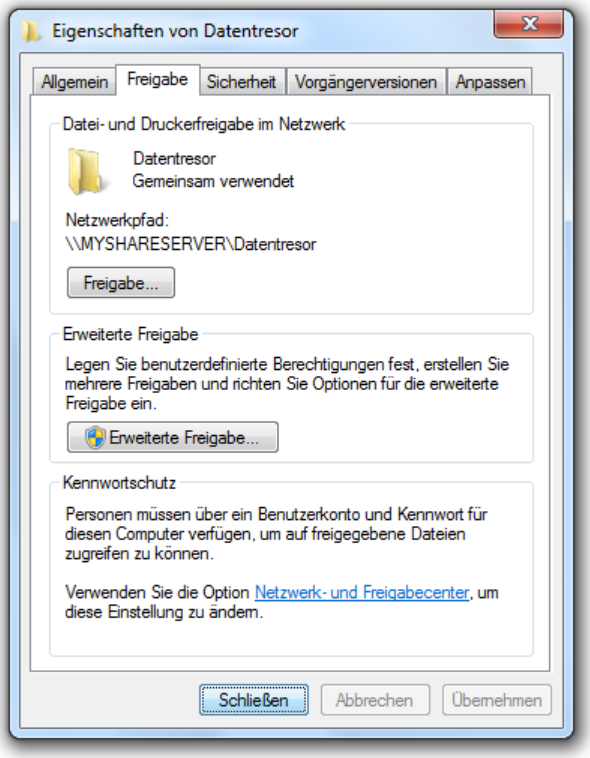
Für die Verschlüsselung mit HiCrypt™ 2.0 benötigt HiCrypt™ 2.0 Vollzugriff auf das Netzlaufwerk. Im einfachsten Fall wird hier also der Gruppe „Jeder" die Berechtigung „Vollzugriff" erteilt.

Die Berechtigungen werden mit „OK" bestätigt und der Dialog geschlossen.

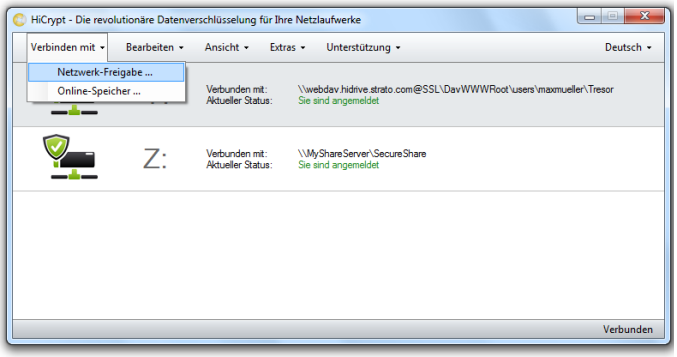
Die Freigabe-Berechtigungen sind unabhängig von den NTFS-Berechtigungen. Wird hier für Jeden Vollzugriff gewährt, bedeutet dies, dass jeder Benutzer, der über entsprechende NTFS-Berechtigungen verfügt, Vollzugriff auf die Freigabe hat. Ein Benutzer, der keine ausreichenden NTFS-Berechtigungen besitzt, hat auch keinen Vollzugriff auf die Freigabe.



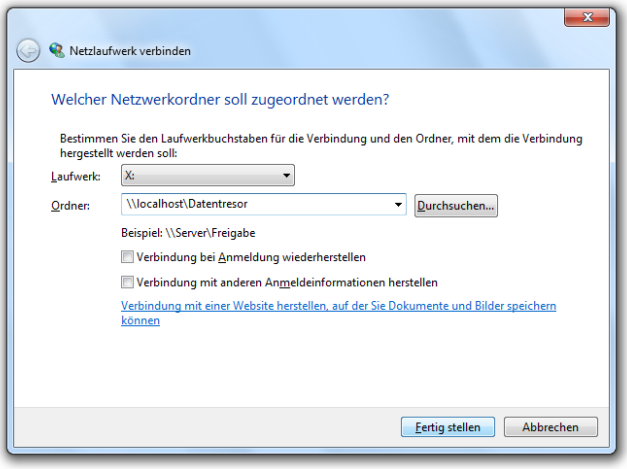
Nachdem die Freigabeberechtigungen angepasst wurden, kann der Ordner nun durch Betätigen der Schaltfläche „OK" freigegeben werden.



Die Eigenschaften des Ordners werden mit der Schaltfläche „Schließen" geschlossen.

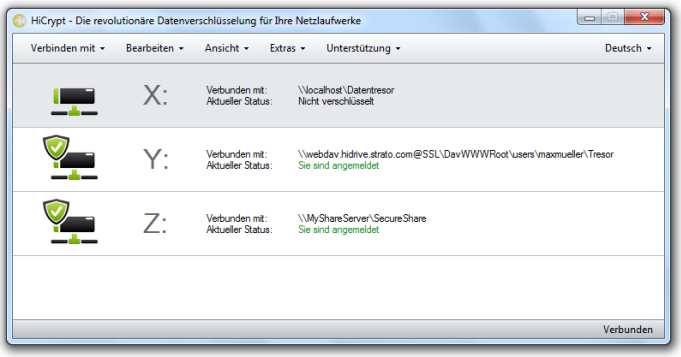


Nun wird mit HiCrypt™ 2.0 der soeben freigegebene Ordner zu einem Netzlaufwerk verbunden.

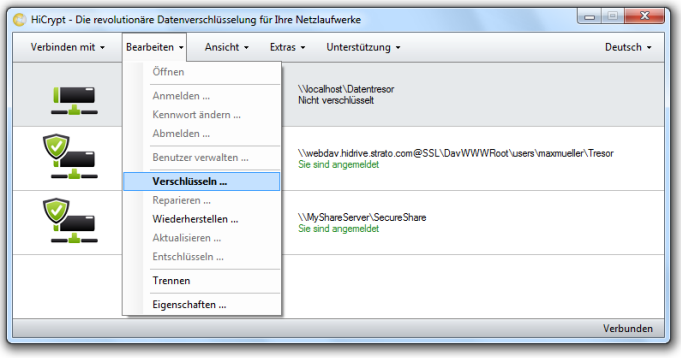


Bei den Verbindungseinstellungen wird als Ordner der eigene Computer, gefolgt von dem Namen der Ordner-Freigabe angegeben.

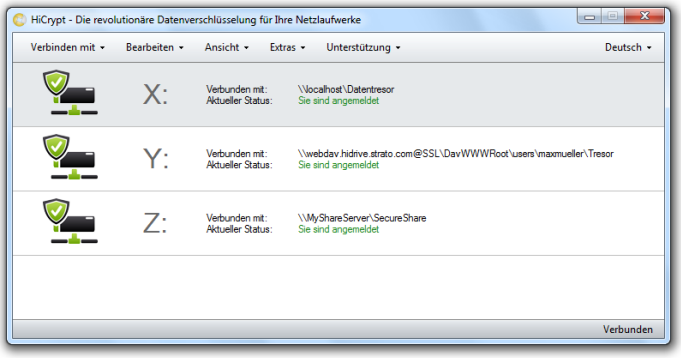
Mit „Fertig stellen" wird das Netzlaufwerk verbunden und der Dialog geschlossen.



In HiCrypt™ 2.0 wird das neue Netzlaufwerk nun angezeigt…



… und kann verschlüsselt werden.



Im Anschluss ist der Dropbox-Ordner, der zu einem Netzlaufwerk verbunden ist, verschlüsselt. Zugriffe auf diesen Bereich dürfen nun nur noch über das Netzlaufwerk erfolgen. Zugriffe über den Dropbox-Ordner werden nicht ver- oder entschlüsselt.

Das Verwenden von Netzlaufwerken, die mit lokalen Freigaben verbunden sind, wird nicht vollständig unterstützt. Dies liegt daran, dass Windows lokale Freigaben erkennt und deshalb nicht über das Netzwerk auf die Dateien zugreift, sondern direkt. Durch diesen Umstand wird HiCrypt™ 2.0 umgangen und es kommt zum Fehler.

ANHANG

A Technische Daten

Unterstützte Betriebssysteme	Windows 7, 8, 8.1, 10 Windows Server 2008 r2, 2012/r2, 2016
Implementierte Verschlüsselungsalgorithmen	AES 256, IDEA, Blowfish
Benötigter Speicherplatz	4 MB
Benötigter Speicherplatz auf dem Dateiserver	20 KB HiCrypt™ 2.0 Systemdateien Pro abgelegter Datei 4 KB zusätzlicher Speicher
Voraussetzung Software	Microsoft .net Framework 4.7
Unterstützte Token	MiFare DESFire EV1, MiFare DESFire EV2, Java Card OS 2.1.1, 2.2+, 3.0.1, 3.04, STARCOS, Multos, TCOS, CardOS, Yubikey, Legic Advant
Unterstützte Netzwerkprotokolle	SMB, CIFS, WebDAV

ANHANG B

B Häufig gestellte Fragen

Wie kann ich meinen nicht leeren Online-Speicher mit HiCrypt™ 2.0 verschlüsseln?

HiCrypt™ 2.0 benötigt für die Verschlüsselung ein leeres Netzlaufwerk. Bei den meisten Anbietern von Online-Speichern enthalten diese bereits Daten, die unter Umständen auch nicht gelöscht werden dürfen. Um den Online-Speichern dennoch mit HiCrypt™ 2.0 verschlüsseln zu können, legen Sie einen neuen Ordner (bspw. "Datentresor") darin an und verbinden das Netzlaufwerk zu diesem Ordner. Dabei geben Sie als Verbindungsziel für das zu verschlüsselnde Netzlaufwerk den gleichen Pfad wie bisher gefolgt von einem Backslash und dem Namen des neu angelegten Ordners an.

Hier ein kleines Vorher-Nachher-Beispiel:

Vorher: **\\webdav.mediencenter.t-online.de@SSL\DavWWWRoot**
Nachher: **\\webdav.mediencenter.t-online.de@SSL\DavWWWRoot\Datentresor**

Dieses neue Netzlaufwerk ist leer und kann nun mit HiCrypt™ 2.0 problemlos verschlüsselt werden.

Welchen Algorithmus soll ich für die Verschlüsselung meiner Daten auswählen?

HiCrypt™ 2.0 bietet die folgenden Verschlüsselungsalgorithmen an. Die Algorithmen werden nach spezifischen Kriterien unterschieden, Sie sind jedoch für die Verschlüsselung von Daten gleichermaßen geeignet.

- AES 256
- Blowfish
- IDEA

Standardmäßig verwendet HiCrypt™ 2.0 ***AES 256*** für die Verschlüsselung von Daten auf Netzlaufwerken. Wenn Sie keine speziellen Anforderungen an einen Verschlüsselungsalgorithmus haben, verwenden Sie die Voreinstellung. Sollten Sie jedoch besondere Anforderungen an das verwendete Verschlüsselungsverfahren haben, so können Sie anhand der jeweiligen Spezifikationen der Algorithmen eine entsprechende Auswahl vornehmen.

Wie kann ich HiCrypt™ 2.0 auf vielen Computern einfach installieren?

Zunächst muss das Setup von HiCrypt™ 2.0 ***aufgezeichnet*** werden. Die folgende Kommandozeile startet das Setup im sogenannten RECORD-Modus.

HiCrypt.exe -r -f1"C:\Temp\HiCrypt_install.iss"

Mit dieser Kommandozeile wird die Protokoll-Datei ***C:\Temp\HiCrypt_install.iss*** erzeugt, die für eine automatische Installation erforderlich ist. Zu beachten ist, dass zwischen dem Parameter **-f1** und der Angabe des Pfades **KEIN** Leerzeichen stehen darf.

Eine automatische Installation im sogenannten SILENT-Modus erfolgt schließlich mit den folgenden Parametern.

HiCrypt.exe -s -f1"C:\Temp\HiCrypt_install.iss"

Der Pfad und der Name der Protokoll-Datei sind natürlich individuell anpassbar.

Diese Variante der Installation kann ebenfalls für die Deinstallation verwendet werden. Bei Bedarf kann die Kommandozeile für den SILENT-Aufruf um einen weiteren, optionalen Parameter ergänzt werden, mit dem das entstehende Protokoll in einen benutzerdefinierten Pfad gespeichert werden kann. Der Aufruf lautet dann wie folgt.

HiCrypt.exe -s -f1"C:\Temp\HiCrypt_uninstall.iss" -f2"C:\Temp\HiCrypt_uninstall.log"

Beachten Sie, dass auch hier **KEIN** Leerzeichen zwischen dem Parameter **-f2** und dem Pfad stehen darf.

Für die Installation von HiCrypt™ 2.0 sind administrative Berechtigungen erforderlich. Dies gilt ebenfalls für die Aufzeichnung im RECORD-Modus als auch für die automatische Installation im SILENT-Modus.
Während der Installation im SILENT-Modus werden dem Anwender keinerlei Dialoge angezeigt. Die erforderlichen Benutzereingaben werden anhand der Protokoll-Datei vorgenommen. Darin sind alle während der im RECORD-Modus durchgeführten Installation vorgenommenen Aktionen gespeichert. Sollten Sie während der Aufzeichnung den abschließenden Neustart durchgeführt haben, wird dieser ohne Nachfrage durchgeführt. Nicht gespeicherte Daten, die der Anwender gerade bearbeitet, gehen dabei möglicherweise verloren.

Kann ich mit HiCrypt™ 2.0 Dateinamen verschlüsseln?

Nein, HiCrypt™ 2.0 verschlüsselt Dateinamen nicht.

Der Vorteil besteht darin, dass einzelne Dateien aus Datensicherungen schnell wiederhergestellt werden können. Im Gegensatz zu Containerverschlüsselungen muss also nicht der gesamte Inhalt wiederhergestellt und anschließend durchsucht werden.

Da die Dateinamen nicht verändert werden, kann jede Datensicherungssoftware die gewünschten Dateien ermitteln und einfach wiederherstellen. Dies ist insbesondere bei der Arbeit mit Online-Speichern von Vorteil.

Aus den genannten Gründen ist das Nichtverschlüsseln von Dateinamen als Leistungsmerkmal für Systemadministratoren zu sehen.

Welche Bedeutung haben die Dateien, die sich nach der Verschlüsselung eines Netzlaufwerks darin befinden?

HiCrypt™ 2.0 legt bei der Verschlüsselung eines Netzlaufwerks drei Dateien in der Freigabe(dem Netzlaufwerk) an. Diese sind als versteckte Systemdateien gekennzeichnet und standardmäßig nicht sichtbar. Sobald diese Dateien in den Ansichtseinstellungen des Betriebssystems eingeblendet werden, sind sie sichtbar.

- .hicrypt.kf
- hicrypt.bf
- hicrypt.af

Die wichtigste dieser Dateien ist "**.hicrypt.kf** ". Darin sind alle Verschlüsselungsinformationen einschließlich aller berechtigten Benutzer gespeichert. Diese Datei ist durch Sicherheitsmaßnahmen vor

unbeabsichtigtem Löschen geschützt. Sie kann daher weder kopiert noch gelöscht werden.

Um Datensicherungen zu gewährleisten wird bei jeder Veränderung dieser Datei eine weitere Datei angelegt: "hicrypt.bf". Diese ist eine Kopie von "**.hicrypt.kf** ", kann aber im Gegensatz dazu wie jede gewöhnliche Datei kopiert und damit in Datensicherungsstrategien aufgenommen werden. Bei einer Wiederherstellung der Daten eines mit HiCrypt™ 2.0 verschlüsselten Netzlaufwerks wird die Datei "**hicrypt.bf**" ebenso wiederhergestellt. HiCrypt™ 2.0 bemerkt, dass die Konfigurationsdatei fehlt aber die Sicherung dieser vorhanden ist und bietet eine Reparatur des verschlüsselten Netzlaufwerks an. Dabei wird aus der Datei "**hicrypt.bf**" die Datei "**.hicrypt.kf** " erzeugt.

Achtung:
Ohne mindestens eine der beiden Dateien ist eine Entschlüsselung der in dem Netzlaufwerk gespeicherten, verschlüsselten Daten nicht mehr möglich!*

Die Datei "**hicrypt.af**" ist eine Verlaufsdatei, in der HiCrypt™ 2.0 Informationen darüber speichert, welcher Benutzer an einem verschlüsselten Netzlaufwerk gerade angemeldet ist. Diese Informationen sind in HiCrypt™ 2.0 nicht einsehbar. Sie werden aber beim Entschlüsseln eines Netzlaufwerks beachtet, um Datenverluste zu vermeiden.

Alle Informationen, die in diesen drei Dateien enthalten sind, sind verschlüsselt und vor Manipulation geschützt. Die drei Dateien werden beim Entschlüsseln eines Netzlaufwerks von HiCrypt™ 2.0 wieder entfernt.

*Es sei denn, es wurde bei der Verschlüsselung des Netzlaufwerkes ein Wiederherstellungsschlüssel exportiert. Dann kann mithilfe dieses Wiederherstellungsschlüssels ein leeres Laufwerk Wiederhergestellt werden (siehe Kapitel 6).

Wie kann ich diejenigen Anwender Festlegen, die HiCrypt™ 2.0 verwenden dürfen?

Grundsätzlich startet HiCrypt™ 2.0 automatisch für jeden Anwender nach der Benutzeranmeldung. Dies gilt für alle Anwender eines Computers gleichermaßen.
Arbeiten mehrere Anwender mit dem gleichen Computer oder kommt gar ein Terminal-Server zum Einsatz, so kann die Benutzergruppe, die HiCrypt™ 2.0 verwenden darf, eingeschränkt werden. Hierfür wird ein Wert in der Windows-Registrierung verwendet, in dem die Benutzergruppen angegeben werden, denen die Verwendung von HiCrypt™ 2.0 gestattet ist.
Führen Sie die nachfolgenden Schritte aus, um den Beispielgruppen "HiCrypt-Anwender" und "HiCrypt-Manager" die Verwendung von HiCrypt™ 2.0 zu gestatten (für diesen Vorgang benötigen Sie administrative Berechtigungen für den Computer).

- Starten Sie die Windows-Registrierung.
- Legen Sie in dem Schlüssel ***HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HiCryptSvc\Parameters*** einen "Wert der mehrteiligen Zeichenfolge" mit dem Namen ***AllowedUserGroups*** an.
- Tragen Sie darin die beiden Gruppen "HiCrypt-Anwender" und "HiCrypt-Manager" in jeweils eine eigene Zeile ein. Verwenden Sie hierzu das Format für Down Level-Logon-Namen (DOMAIN\GroupName) oder das UPN-Format (GroupName@DNSDomainName.com).
- Starten Sie anschließend den Computer neu, um die vorgenommenen Änderungen zu übernehmen.

Wie kann ich verhindern, dass HiCrypt™ 2.0 bei Anwendern gestartet wird, denen die Verwendung nicht gestattet ist?

Wenn Sie die Anwender, die HiCrypt™ 2.0 verwenden dürfen, wie in der Frage zuvor erläutert eingeschränkt haben, können Sie mit Hilfe eines weiteren Wertes in der Windows-Registrierung verhindern, dass HiCrypt™ 2.0 für alle übrigen Anwender gestartet wird.
Führen Sie die nachfolgenden Schritte aus, um dies zu erreichen (für diesen Vorgang benötigen Sie administrative Berechtigungen für den Computer).

- Starten Sie die Windows-Registrierung.

- Legen Sie in dem Schlüssel ***HKEY_LOCAL_MACHINE\Software\digitronic\HiCrypt*** (32bit) oder in dem Schlüssel ***HKEY_LOCAL_MACHINE\Software\Wow6432Node\digitronic\HiCrypt*** (64bit) einen "DWORD-Wert (32-Bit)" mit dem Namen ***SilentQuitIfUserIsNotInAllowedGroups*** an.
- Setzen Sie dessen Wert auf ***1***, um den Start von HiCrypt™ 2.0 bei Anwendern zu verhindern, denen die Verwendung von HiCrypt™ 2.0 nicht gestattet ist.
- Starten Sie anschließend den Computer neu, um die vorgenommenen Änderungen zu übernehmen.

Diese Einstellung ist seit der HiCrypt™ 2.0 Version 1.0.7 verfügbar.

Wie kann ich verhindern, dass Anwender Ihre Anmeldeinfomationen für ein verschlüsseltes Netzlaufwerk speichern?

Wenn Sie verhindern möchten, dass Anwender ihre HiCrypt™ 2.0-Anmeldeinformationen für verschlüsselte Netzlaufwerke speichern, können Sie diese Option deaktivieren.
Führen Sie die nachfolgenden Schritte aus, um dies zu erreichen (für diesen Vorgang benötigen Sie administrative Berechtigungen für den Computer).

- Starten Sie die Windows-Registrierung.
- Legen Sie in dem Schlüssel ***HKEY_LOCAL_MACHINE\Software\digitronic\HiCrypt*** (32bit) oder in dem Schlüssel ***HKEY_LOCAL_MACHINE\Software\Wow6432Node\digitronic\HiCrypt*** (64bit) einen "DWORD-Wert (32-Bit)" mit dem Namen ***DisableSaveCredentialOption*** an.
- Setzen Sie dessen Wert auf ***1***, um die Option zum Speichern von HiCrypt™ 2.0-Anmeldeinformationen auszublenden.
- Starten Sie anschließend den Computer neu, um die vorgenommenen Änderungen zu übernehmen.

Diese Einstellung ist seit der HiCrypt™ 2.0 Version 1.0.8 verfügbar.

Wie kann ich verhindern, dass Anwender ein verschlüsseltes Netzlaufwerk mit HiCrypt™ 2.0 trennen können?

Wenn Sie verhindern möchten, dass Anwender mit HiCrypt™ 2.0 verschlüsselte Netzlaufwerke trennen, können Sie die entsprechenden Menü-Punkte deaktivieren.
Führen Sie die nachfolgenden Schritte aus, um dies zu erreichen (für diesen Vorgang benötigen Sie administrative Berechtigungen für den Computer).

- Starten Sie die Windows-Registrierung.
- Legen Sie in dem Schlüssel ***HKEY_LOCAL_MACHINE\Software\digitronic\HiCrypt*** (32bit) oder in dem Schlüssel ***HKEY_LOCAL_MACHINE\Software\Wow6432Node\digitronic\HiCrypt*** (64bit) einen "DWORD-Wert (32-Bit)" mit dem Namen ***DisableMenuItemDisconnect*** an.
- Setzen Sie dessen Wert auf ***1***, um den Menü-Punkt "Trennen" in den HiCrypt™ 2.0-Menüs zu deaktivieren.
- Starten Sie anschließend den Computer neu, um die vorgenommenen Änderungen zu übernehmen.

Diese Einstellung ist seit der HiCrypt™ 2.0 Version 1.0.8 verfügbar.

Es besteht keine HiCrypt™ 2.0-Verbindung. Was kann ich tun?

Die HiCrypt™ 2.0-Verbindung ist eine Verbindung zwischen den einzelnen Programm-Komponenten von HiCrypt™ 2.0. Sollte diese Verbindung nicht hergestellt werden können, prüfen Sie bitte die folgenden Punkte.

Ist die Installation einwandfrei verlaufen?

Prüfen Sie, ob HiCrypt™ 2.0 korrekt installiert wurde. Im einfachsten Fall wird das Installationsprogramm von HiCrypt™ 2.0 erneut durchgeführt und die Option "Reparieren" verwendet.

AntiVirus-Programme

Sollte die Installation einwandfrei sein, so können AntiVirus-Programme die Einzelkomponenten von HiCrypt™ 2.0 an der Ausführung hindern. Damit ist eine Kommunikation zwischen den HiCrypt™ 2.0-Komponenten ausgeschlossen. Es ist daher zu prüfen, ob das verwendete AntiVirus-Programm HiCrypt™ 2.0-Komponenten blockiert. Deaktivieren Sie hierzu einfach vorübergehend Ihr Antivirus-Programm. Sollte die HiCrypt™ 2.0-Verbindung nicht sofort hergestellt werden können, starten Sie bitte die HiCrypt™ 2.0-Komponenten erneut. Beenden Sie hierfür zunächst den HiCrypt™ 2.0-Dienst und beenden Sie den Prozess "hcui.exe" im Task-Manager. Starten Sie anschließend den HiCrypt™ 2.0-Dienst erneut. Dieser startet die Anwendung (hcui.exe) automatisch.

Sollte nun bei deaktiviertem AntiVirus-Programm der Verbindungsfehler in HiCrypt™ 2.0 nicht mehr auftreten, müssen Sie in Ihrem AntiVirus-Programm die HiCrypt™ 2.0-Prozesse als vertrauenswürdige Prozesse angeben und festlegen, dass diese nie blockiert werden sollen. Kontrollieren Sie außerdem, ob Ihr AntiVirus-Programm das sogenannte Auto-Sandboxing unterstützt. Dabei werden Anwendung in virtuellen Umgebungen gestartet. Auch dies behindert HiCrypt™ 2.0 in seiner Funktion. Deaktivieren Sie daher mögliche Einstellungen, die HiCrypt™ 2.0 in einer Sandbox laufen lassen.

Firewall

Sollten trotz deaktiviertem AntiVirus-Programm die HiCrypt™ 2.0-Verbindung noch immer nicht hergestellt werden können, prüfen Sie bitte, ob Ihre Firewall die HiCrypt™ 2.0-Prozesse blockiert und geben Sie diese ggf. frei.

Berechtigungen

Hat der HiCrypt™ 2.0-Benutzer die benötigten NTFS und Freigabe Berechtigungen? Er muss wenigstens Lesen, Schreiben und Ändern können, zumindest bei den drei von HiCrypt™ 2.0 angelegten Dateien.

Wie kann ich manuell einen http-Proxy für die Online-Aktivierung von HiCrypt™ 2.0 festlegen?

Bei einer Online-Aktivierung versucht HiCrypt™ 2.0 zunächst direkt Kontakt mit dem Aktivierungsserver aufzunehmen. Ist dies nicht erfolgreich, so wird die Einstellung des HTTP-Proxys des Internet Explorer verwendet, um mit dessen Hilfe eine Verbindung zum Aktivierungsserver herzustellen. Es besteht die Möglichkeit den von HiCrypt™ 2.0 für die Online-Aktivierung zu verwendenden Proxy explizit anzugeben. In diesem Fall werden die Einstellungen des Internet Explorer ignoriert.

Führen Sie die nachfolgenden Schritte aus, um dies zu erreichen (für diesen Vorgang benötigen Sie administrative Berechtigungen für den Computer).

- Starten Sie die Windows-Registrierung.
- Legen Sie in dem Schlüssel ***HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HiCryptSvc\Parameters*** eine "Zeichenfolge" mit dem Namen ***UserDefinedProxy*** an.
- Tragen Sie darin den Proxy-Server mit Port ein (z.B. "10.9.8.7:3128").
- Führen Sie anschließend die Online-Aktivierung durch.

Diese Einstellung ist seit der HiCrypt™ 2.0-Version 1.2.0 verfügbar.

Office-Dokumente sind gesperrt, obwohl sie niemand anderer benutzt, was ist zu tun?

HiCrypt™ 2.0 verursacht diesen Effekt im Zusammenspiel mit dem Detailbereich des Windows Explorers. Es gibt noch andere Fälle in denen das Problem auch ohne HiCrypt™ 2.0 auftreten kann.

Schalten Sie den Detailbereich im Windows Explorer aus, um das Problem zu beheben. Führen Sie dazu die nachfolgenden Schritte aus.

- Klicken Sie im Windows Explorer auf ***Organisieren***.
- Wählen Sie den Punkt ***Layout*** aus.
- Klicken Sie auf ***Detailbereich***, so dass der Haken und der Detailbereich nicht mehr zu sehen sind.

Wie kann HiCrypt™ 2.0 deaktiviert werden?

Seit der Version 2.1.0 ist unsere Software HiCrypt™ 2.0 mit der Funktion "Automatische Deaktivierung von aktiven Installationen" ausgestattet. Mit der Deinstallation von HiCrypt™ 2.0 auf Arbeitsplätzen, die keinen Zugriff mehr auf die verschlüsselten Daten erhalten sollen, wird automatisch auch die Anzahl der vergebenen Aktivierungen auf unserem Lizenzserver zurückgesetzt. Bitte denken Sie rechtzeitig daran, z. B. vor der Außerbetriebnahme von Arbeitsplatzrechnern oder Notebooks, auf denen sich noch aktive HiCrypt™ 2.0-Installationen befinden, diese zu deaktivieren, um sie für Neuinstallationen nutzen zu können. Nur zeitlich unbefristete Lizenzen können automatisch deaktiviert werden.
Sie können und sollten diese automatische Deaktivierung auch für ältere Versionen von HiCrypt™ 2.0 nutzen, indem Sie die ältere Version vor der Deinstallation aktualisieren. Für die Aktualisierung laden Sie bitte die aktuelle Version von http://www.hicrypt.com/download/index.php herunter. Im Setup wählen Sie dann den Punkt "Ändern", wenn Sie eine Version älter als Version 2.2 einsetzen.

Um eine aktivierte Installation von HiCrypt™ 2.0 zu deaktivieren, muss HiCrypt™ 2.0 deinstalliert werden. Am Ende der Deinstallation, vor dem Abschluss Dialog, erscheint eine Meldung, welche Auskunft über die automatische Deaktivierung gibt.

Bei einer Deinstallation erscheint diese Meldung in jedem Fall – egal, ob die automatische Deaktivierung erfolgreich war oder nicht. Zusätzlich wird der Inhalt der Meldung auch im Windows-Ereignisprotokoll unter „Anwendung" protokolliert . und im Logfile des Setups.

Sollte eine Deaktivierung nicht automatisch durchgeführt werden können, so enthält die Meldung einen Deactivation Key.

Bitte geben Sie diesen unter https://www.digitronic.net/service/lizenzaktivierung-deaktivierung ein, oder senden Sie diesen via E-Mail an support@digitronic.net oder vertrieb@digitronic.net, damit die Deaktivierung durch einen digitronic® Mitarbeiter abgeschlossen werden kann.

Wie kann ich auf das verschlüsselte Netzlaufwerk zugreifen, wenn ich mein Kennwort vergessen habe?

Wenn ein einzelner Benutzer sein Kennwort vergessen hat, dann öffnet ein Manager die Benutzerverwaltung des verschlüsselten Netzlaufwerks, löscht diesen Benutzer und legt ihn neu an.

Sollte ein Manager sein Kennwort vergessen, jedoch noch mindestens ein Benutzer Zugriff auf das verschlüsselte Netzlaufwerk haben, so kann dieser Benutzer die Daten aus dem Laufwerk heraus auf eine lokale Festplatte kopieren. Parallel dazu stellt die Administration ein neues, leeres Netzlaufwerk zur Verfügung. Ein dort einzurichtender Manager verschlüsselt das neue Netzlaufwerk wieder und kopiert die Daten dorthin zurück.

Sollte keiner der Benutzer mehr Zugriff auf das verschlüsselte Netzlaufwerk haben, dann wird der bei seiner Einrichtung erzeugte Wiederherstellungsschlüssel benötigt. Auch dann stellt die Administration zunächst ein neues, leeres Netzlaufwerk zur Verfügung. Nach Ausführung der Installation von

HiCrypt™ 2.0 ist in der Bedienoberfläche die Funktion "Wiederherstellen ..." auszuwählen und während des dann erscheinenden Wizards der Wiederherstellungsschlüssel einzutragen. Anschließend wird auch hier ein neuer Manager angelegt. Wenn dieser Prozess abgeschlossen ist, muss ein Administrator die verschlüsselten Dateien auf dem Server von der alten in die neue Freigabe kopieren. Dabei dürfen die drei von HiCrypt™ 2.0 erzeugten Dateien nicht kopiert werden.

Nur dann, wenn der bei der Einrichtung des verschlüsselten Netzlaufwerks erzeugte Wiederherstellungsschlüssel nicht exportiert und sicher verwahrt wurde und gleichzeitig keiner der Benutzer mehr Zugriff auf die verschlüsselten Daten hat, gibt es auch keine Chance mehr, an die Daten in unverschlüsselter Form heranzukommen, im Falle von vergessenen Kennworten. Bitte beachten Sie hierzu die Kapitel sechs und sieben.

Woran kann es liegen, dass die Online Aktivierung nicht funktioniert?

Eine Ursache dafür, dass die Online Aktivierung nicht funktioniert kann die Firewall sein. Dort muss Port 2301 in beide Richtungen freigegeben sein.

ANHANG C

C Glossar

2-Faktor-Authentifizierung: Bei der 2-Faktor-Authentifizierung handelt es sich um eine Authentifizierungsmethode, bei welcher 2 Faktoren zum Einsatz kommen. Dabei kann es sich zum Beispiel um das Wissen um eine PIN, Anmeldedaten oder ein Kennwort und den Besitz eines bestimmten eineindeutig identifizierbaren Tokens handeln.

Activation Key: Ein Activation Key wird bei der Offline-Aktivierung benötigt. Er ist die Antwort auf den Response Key.
Mithilfe des Activation Keys wird HiCrypt™ 2.0 dann aktiviert. Er besteht aus einer Kombination von Zahlen und Buchstaben und ist 25 Zeichen lang.

AES: AES steht für **A**dvanced **E**ncryption **S**tandard, es handelt sich dabei um ein symmetrisches Verschlüsselungsverfahren. Bei HiCrypt™ 2.0 wird eine Schlüssellänge von 256 bit verwendet.

Backupfile: Die versteckte Systemdatei „hicrypt.bf" wird von uns als Backupfile bezeichnet. Sie wird immer dann geändert, wenn Änderungen an der Benutzerverwaltung oder den Sicherheitsrichtlinien vorgenommen werden. Mit Hilfe des Backupfiles kann ein beschädigtes oder verloren gegangenes Keyfile wiederhergestellt werden.

Blowfish: Bei Blowfish handelt es sich um ein symmetrisches Blockverschlüsselungsverfahren, welches 1993 von Bruce Schneier entworfen wurde. Es ist als public domain veröffentlicht und kann somit frei verwendet werden.

CIFS: Beim **C**ommon **I**nternet **F**ile **S**ystem handelt es sich um eine erweiterte Version des SMB Protokolls. Diese kann zur Freigabe von Ordnern und Dateien über das Internet verwendet werden.

Deactivation Key: Ein Deactivation Key wird benötigt, wenn eine automatische Deaktivierung gescheitert ist. Er dient dazu, die Installation zu identifizieren und die Aktivierungsanzahl der entsprechenden Lizenz zu verringern.

Freigabe/Netzlaufwerk/Share: Ein am Dateiserver freigegebener Ordner, welcher am Client als Laufwerk eingebunden wird, wird als Netzlaufwerk bezeichnet. Korrekterweise wäre der Ordner am Server die Freigabe, in dieser Dokumentation werden diese Begriffe allerdings nahezu Synonym verwendet. Die Freigabe muss vom Administrator bereitgestellt werden.

Eine Freigabe kann auch vom Nutzer eingebunden werden, für gewöhnlich geschieht dies jedoch über das Anmeldeskript der Domäne.

IDEA: Der **I**nternational **D**ata **E**ncryption **A**lgorithm ist ein symmetrisches Blockverschlüsselungsverfahren. Es war bis Mai 2011 patentgeschützt.

Keyfile: Die Datei ".hicrypt.kf " ist die wichtigste Datei eines mit HiCrypt™ 2.0 verschlüsselten Laufwerkes. Sie wird auch Keyfile genannt. Darin sind alle Verschlüsselungsinformationen einschließlich aller berechtigten Benutzer gespeichert. Diese Datei ist durch Sicherheitsmaßnahmen vor unbeabsichtigtem Löschen geschützt. Sie kann daher weder kopiert noch gelöscht werden.

NTFS-Berechtigungen: Das proprietäre Dateisystem NTFS (**N**ew **T**echnology **F**ile **S**ystem) ist von der Firma Microsoft entwickelt worden. Es ermöglicht für Benutzer und Benutzergruppen explizite Berechtigungen für Dateizugriffe zu setzen. Diese sind als NTFS-Berechtigungen bezeichnet. Es handelte sich dabei um reine Zugriffsrechte des Microsoft Betriebssystems, diese sind von HiCrypt™ 2.0 völlig unabhängig.

Product Key: Der Product Key stellt die eigentliche Lizenz dar. Es handelt sich dabei um eine Kombination aus 30 Zahlen und Buchstaben. Sie erhalten den Product Key beim Kauf unseres Produktes oder bei der Übergabe der Vor-Ort-Installation.

Response Key: Beim Response Key handelt es sich um einen 35-stelligen Schlüssel bestehend aus Zahlen um Buchstaben. Er dient bei der Offline Aktivierung dazu eine Installation zu identifizieren und einen Activation Key zu erzeugen.

SecurityToken: Der SecurityToken ist eine Hardwarekomponente. Es ist einer der beiden Faktoren, bei der 2-Faktor-Authentifizierung. Es kann sich hierbei um einen „USB-Stick", eine Chipkarte oder eine kontaktlose Technologie handeln.

Auf dem SecurityToken wird ein Schlüssselpaar erstellt und dieses mit dem HiCrypt™ 2.0 Benutzer verbunden.

SMB: Das **S**erver **M**essage **B**lock Protokoll ist ein von Microsoft verwendetes Standardprotokoll zur Datei und Druckerfreigabe.

WebDAV: Um Dateien wie eine Online-Festplatte benutzen zu können wurde der **Web**-based **D**istributed **A**uthoring and **V**ersioning Standard entwickelt. Dieser Standard ist offen und dient der Bereitstellung von Dateien im Internet.

HiCrypt™ 2.0 unterstützt diesen Standard. Inzwischen gibt es jedoch viele Anwendungen, die nicht über ein per WebDAV eingebundenes Laufwerk zugreifen, sondern aus Performancegründen eigene Verbindungen zum Online-Speicher aufbauen, was an HiCrypt™ 2.0 vorbei greift. Dies führt dazu, dass wir die Benutzung von WebDAV nicht mehr empfehlen.