Challenger - Kurzanleitung

Allgemeine Informationen

Das Challenger-Konzept besitzt Merkmale, die im Vergleich mit anderen Verschlüsselungstools deutlich werden. Die meisten Verschlüsselungsprogramme benötigen Administratorenrechte für die Installation. Oft werden Windows-Explorer-Erweiterungen installiert oder neue virtuelle Partitionen eingerichtet. Es werden tiefe Eingriffe ins System vorgenommen. Nicht selten bestehen Abhängigkeiten zu umfangreichen Runtime-Bibliotheken. Challenger stellt einen Kompromiss aus einfacher Bedienung, sicherem Umgang, sowie hoher Flexibilität dar. Das Programm ist auf allen Windows-Systemen (32 und 64 Bit) einsetzbar. Es werden keine Runtime-Bibliotheken oder Systemupdates benötigt. Zur Installation von Challenger genügen einfache Benutzerrechte. Sie können beliebige Dateien, Ordner oder Laufwerke verschlüsseln. Bei der Verschlüsselung von Ordnern und Laufwerken werden alle darin enthaltenen Dateien chiffriert. Die Software kann entweder auf Ihrem Computer oder auf einen mobilen Datenträger (USB-Stick, Flash Karte, CD) installiert werden. Mit einem mobilen Datenträger können Sie die Software sofort auf jedem Rechner benutzen. Die verwendete synchrone Stromchiffrierung liefert eine schnelle Verschlüsselung.

Die Grundlage der Stromchiffrierung bildet ein umfangreicher und komplexer Schlüssel, der neben der verwendeten Passphrase (Passwort) den zweiten Verfahrensschlüssel darstellt. Nach der Installation ist der zweite Verfahrensschlüssel immer gleich und damit öffentlich bekannt. In diesem Fall entspricht der Schutz dem, was bei anderen Verschlüsselungsprogrammen üblich ist (Passphrase oder Passwort). Wenn Sie den zweiten Verfahrensschlüssel durch eine individuelle Zufallszahlenliste ersetzen, wird die Sicherheit stark erhöht. Im übertragenen Sinn könnte man davon sprechen, dass Sie ein eigenes Verschlüsselungsverfahren besitzen, sobald Sie den zweiten Schlüssel aktivieren. Die Kurzanleitung zur Generierung des zweiten Verfahrensschlüssels (PAD) finden Sie auf der Homepage.

Wichtige Sicherheitshinweise:
Wird eine Passphrase (Passwort) vergessen, sind die damit verschlüsselten Daten unwiederbringlich verloren. Eventuell notieren Sie die verwendeten Passphrasen und bewahren diese zugriffsgeschützt auf. Ebenso wichtig sind Sicherheitskopien der PAD-Datei, wenn Sie den zweiten Verfahrensschlüssel aktivieren. Die Sicherheitskopien sind wichtig, da die Computer, die verwendeten USB-Sticks oder sonstige externe Datenträger kaputt gehen könnten. Wenn Sie dadurch den zweiten Verfahrensschlüssel (PAD-Datei) verlieren, können Sie die verschlüsselten Daten ebenfalls nicht mehr entschlüsseln. Denken Sie bei Sicherheitskopien auch an die Haltbarkeit, Kratz- und Stoßfestigkeit der verwendeten Sicherungsmedien!

Installation

Grundsätzlich werden zwei Installationsarten unterschieden.

1. Installation auf die Festplatte **in den Windows-Programmordner** „C:\Programme“. Diese Installationsart entspricht dem Windows-Standard. Challenger arbeitet bei dieser Installation im Mehrbenutzerbetrieb. Jeder Benutzer, der sich mit seinem Benutzerprofil am Computer anmeldet, kann seine Programm- und Verschlüsselungseinstellungen vornehmen.

2. Installation auf die Festplatte in einem beliebigen Ordner **außerhalb vom Windows-Programmordner** oder die Installation auf einen beliebigen externen Datenträger. Bei dieser Installationsart werden immer alle Programmdateien innerhalb des gewählten Installationsordners abgelegt. Diese Installationsart wählen Sie beispielsweise, wenn mehrere Benutzer mit den gleichen Programm- und Verschlüsselungseinstellungen an einem gemeinsamen Computer arbeiten oder wenn Sie eine USB-Stick-Installation benutzen möchten.

Das Installationspaket der Challenger-Freeware-Version finden Sie auf der Homepage unter Download. Die Lite- und die Vollversion wird als Downloadlink per Email zur Verfügung gestellt oder auf CD-ROM versendet. Eine integrierte Kontrollfunktion erkennt korrupte Installationspakete. Dennoch sollten Sie an Hand der im Internet oder auf dem Lieferschein publizierten Prüfsummen das Paket vor der Installation mit geeigneter Software auf Unversehrtheit prüfen.

Die neuen Windows Versionen verfügen über die SmartScreen Technik. Wenn SmartScreen aktiviert ist, kann folgende Meldung erscheinen:

SmartScreen (Abb.1)

Die SmartScreen Technik soll Windows Anwender darüber informieren, ob eine aus dem Internet geladene Software sicher ist oder ob sie eventuell Schadfunktionen beinhalten könnte. Wenn Sie das Challenger-Installationspaket aus einer sicheren Quelle bezogen oder Sie die oben angesprochenen Prüfsummen verifiziert haben, können Sie durch einen Klick auf „Weitere Informationen“ die Installation trotzdem ausführen.

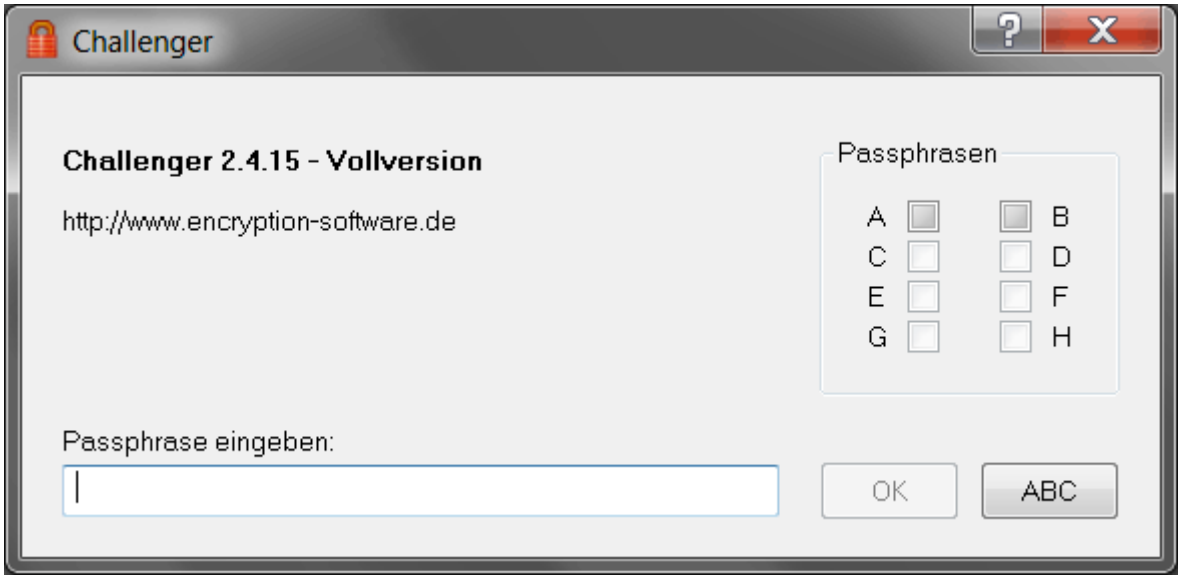
Installation (...Fortsetzung)

Wenn Sie die Installation gestartet haben, können Sie zuerst die Sprache wählen und müssen den Lizenzvertrag akzeptieren. Danach wählen Sie aus, ob Sie Challenger auf die Festplatte oder auf ein USB-Stick bzw. auf einen beliebigen Datenträger installieren möchten. Wenn Sie die Festplatte wählen, können Sie den Zielordner anpassen oder die Vorgabe „C:\Programme\Challenger“ belassen.
Für den Fall, dass Sie Challenger in den Windows-Programmordner „C:\Programme“ installieren (Installationsart ❶), erscheint zur Bestätigung die Windows-Benutzerkontosteuerung. Die übrigen Installationsschritte werden hier nicht erwähnt. Bitte folgen Sie den Anweisungen des Installationsprogramms.

Challenger starten

Wenn die Software in den Windows-Programmordner „C:\Programme“ installiert wurde, finden Sie einen entsprechenden Eintrag im Startmenü zum Starten von Challenger. Falls der Startmenüeintrag während der Installation abgewählt wurde oder bei jeder Installation außerhalb vom Windows-Programmordner, wechseln Sie zum Starten von Challenger mit dem Windows-Explorer in den Installationsordner und doppelklicken Sie „cha.exe“. Falls das Installationsziel ein USB-Stick war, rufen Sie mit dem Windows-Explorer den USB-Stick auf. Im Wurzelverzeichnis finden Sie zum Starten die Datei „Challenger.exe“.

Wenn Sie Challenger starten, erscheint zuerst das Fenster zur Eingabe der Passphrase (Passwort). Wenn Sie bereits eigene Passphrasen programmiert haben, geben Sie eine dieser Passphrasen ein. Im rechten Fensterbereich (Abb.2) sehen Sie wie viele der acht möglichen Passphrasen bereits programmiert wurden. In diesem Fall sind die Kanäle A und B belegt.

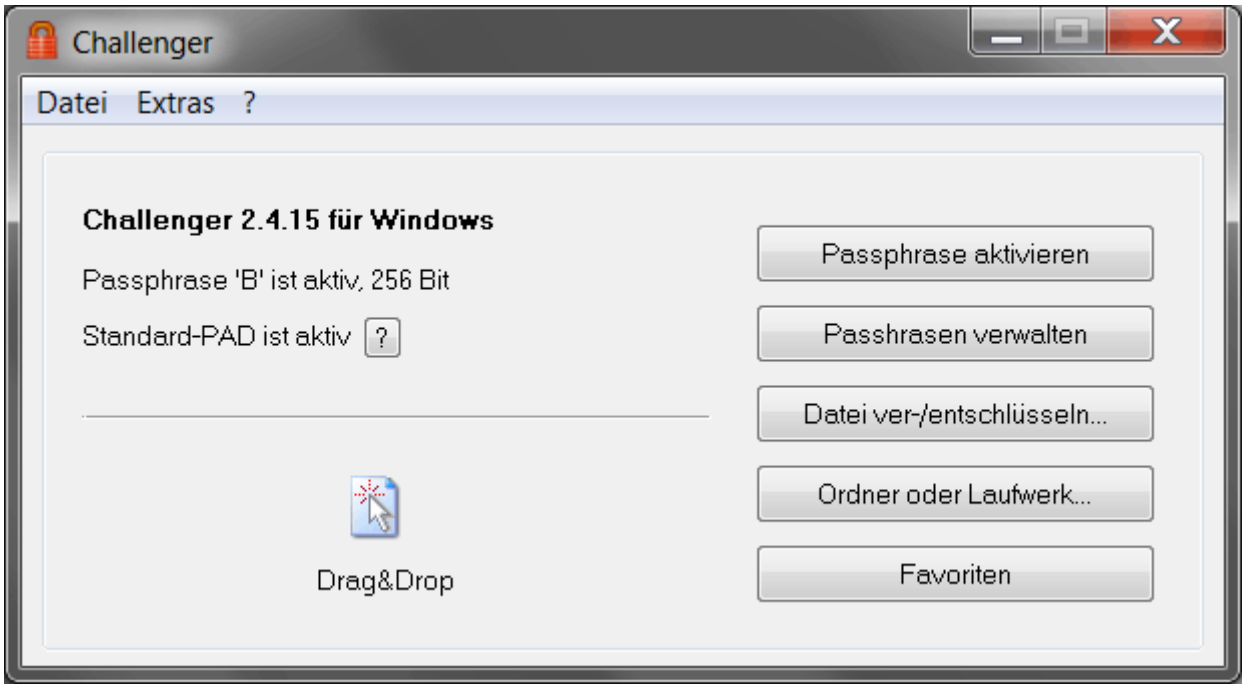


Phrasenfenster (Abb.2)

Nach der Erstinstallation können Sie das Programm nur durch die Eingabe eines Startpasswortes öffnen. Das Startpasswort der Freeware lautet stets „**Berlin**“.
Das Startpasswort der Vollversion wird im Lieferschein ausgewiesen.

Hauptfenster

Wenn Sie Challenger gestartet und eine gültige Passphrase eingegeben haben öffnet sich das Hauptfenster.



Hauptfenster (Abb.3)

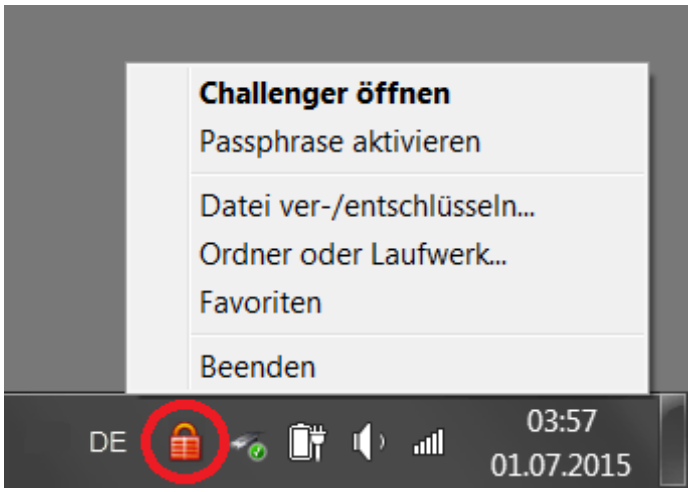
Sie können über das Hauptfenster auf alle Funktionen der Software zugreifen. Eine Möglichkeit zur Verschlüsselung und Entschlüsselung ist es, Dateien, Ordner oder Laufwerke im Windows-Explorer auszuwählen, und die markierten Objekte auf das Hauptfenster zu ziehen.

Unter stark modifizierten Windows-Systemen und unter Linux-Wine wird die Drag&Drop-Arbeitsweise mit dem Hauptfenster eventuell nicht unterstützt. In diesem Fall verwenden Sie die entsprechenden Buttons oder Menüpunkte. Wenn Sie die Buttons oder Menüpunkte anklicken, öffnen sich die Windows-Standard-Dialogboxen zur Auswahl einer Datei oder eines Ordners.

Unter „Favoriten“ können Sie eine Liste mit Dateien und Ordner zusammenstellen, die in der Folge durch wenige Klicks verschlüsselt oder entschlüsselt werden können.

Windows-Systemtray

Anwender, die gerne mit dem Windows-Systemtray arbeiten, können in Challenger unter „Einstellungen“ ➙ „Start“ die Option "Dialogfenster statt Traysymbol" deaktivieren. Nach einem Programmneustart wird so nicht das Hauptfenster geöffnet, sondern das Challenger-Programmsymbol im Windows-Systemtray angezeigt.

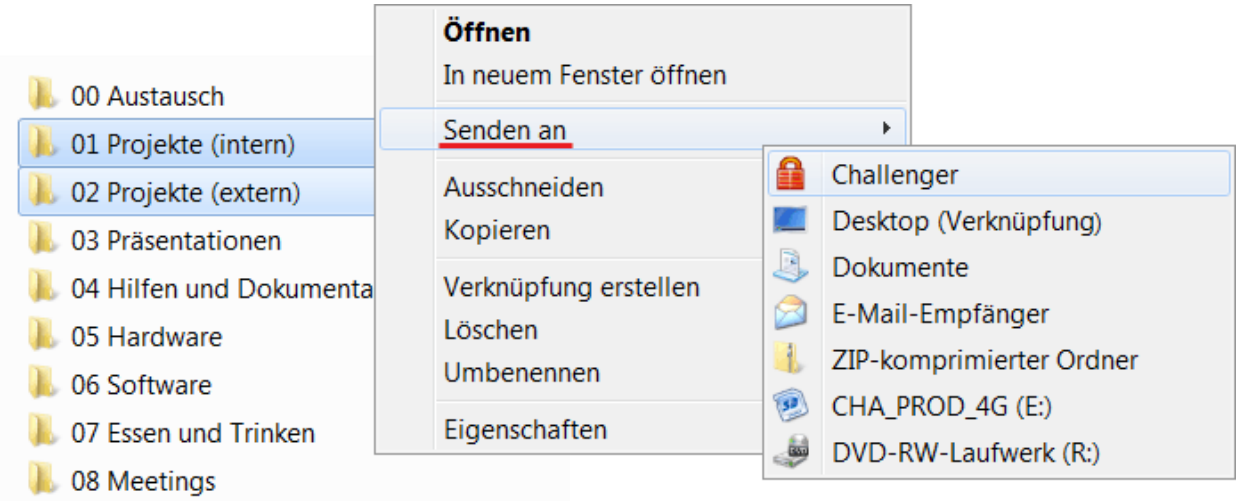


Windows-Systemtray (Abb.4)

Wenn Sie im Windows-Systemtray auf das Challenger-Programmsymbol mit der rechten Maustaste klicken, öffnet sich das Challenger-Menü.

Windows-Explorer-Menü „Senden an“

Eine gute Möglichkeit ist das Arbeiten mit dem Windows-Explorer-Menü „Senden an“. Diese Option finden Sie in Challenger unter „Einstellungen“ ➙ „Start“.

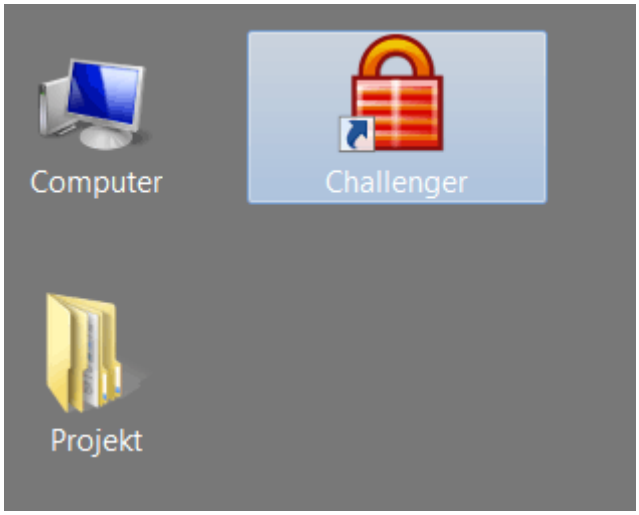


Windows-Explorer-Menü „Senden an“ (Abb.5)

Wählen Sie im Windows-Explorer Dateien und Ordner aus, öffnen Sie mit der rechten Maustaste das Kontextmenü und wählen dort „Senden an“ ➙ „Challenger“.

Programmverknüpfungen

In Challenger können Sie unter „Einstellungen“ ➙ „Start“ eine Programmverknüpfung auf Ihren Windows-Desktop anlegen.



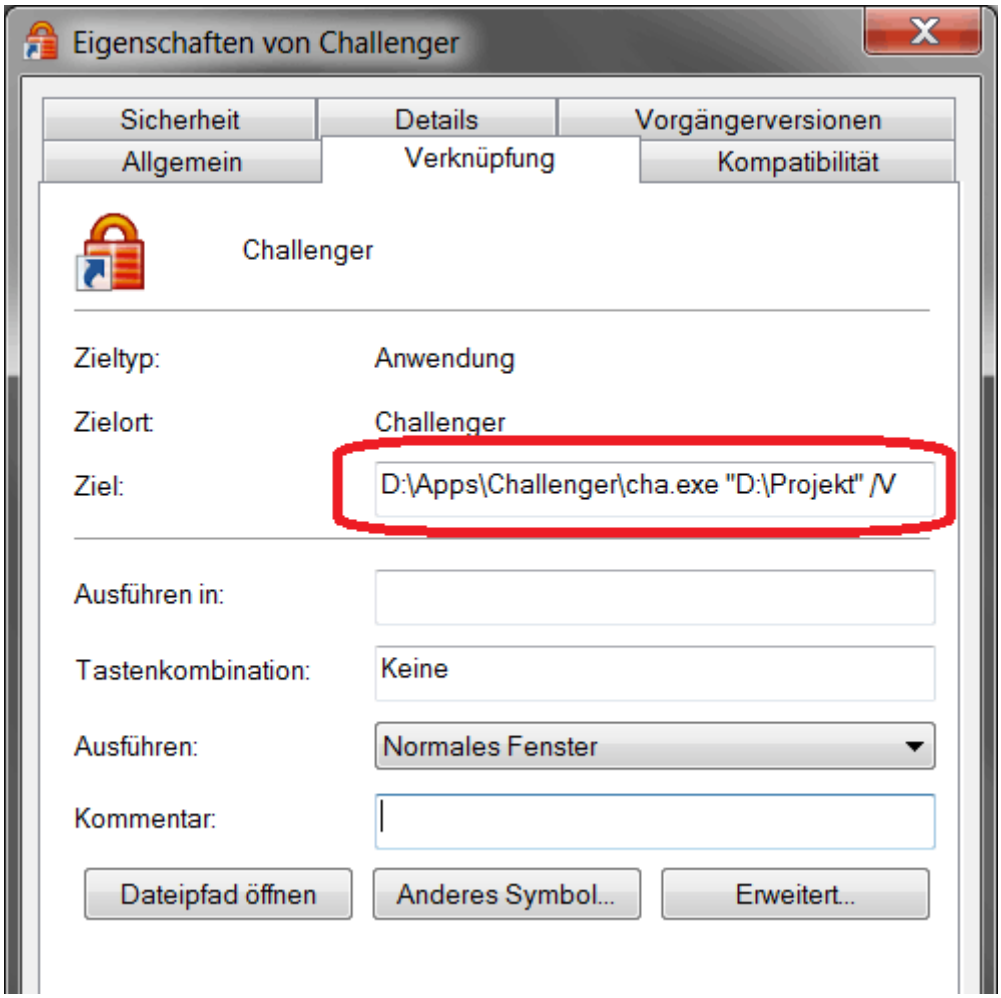
Desktop-Verknüpfung (Abb.6)

Wenn mehrere Installationen parallel installiert sind, sollte der Name ggf. geändert werden, um Verwechslungen zu vermeiden.

Sie können die Desktopverknüpfung nutzen, in dem Sie diese doppelt anklicken. Alternativ können Sie im Windows-Explorer Dateien und Ordner auswählen und die Auswahl auf die Desktopverknüpfung ziehen.

Programmverknüpfungen (...Fortsetzung)

Sie können aber auch mit dem Windows-Explorer eine Verknüpfung selbst erstellen und verschiedene Parameter hinzufügen.



Verknüpfungseigenschaften (Abb.7)

Folgendes Beispiel verschlüsselt den Ordner „D:\Projekt“:
"...\cha.exe" "D:\Projekt" /V

Folgendes Beispiel entschlüsselt den Ordner wieder:
"...\cha.exe" "D:\Projekt" /E

Die Parameterschalter **/V** und **/E** können auch sinnvoll beim Start oder Herunterfahren des Computers eingesetzt werden. Der Schalter **/FAV** bewirkt, dass die Favoriten verschlüsselt bzw. entschlüsselt werden.

Das Passphrasenkonzept

Bei der Challenger-Verschlüsselung spielen Passphrasen (Pass-Sätze) eine zentrale Rolle. Der Ausdruck **Phrase** soll unterstreichen, dass Sie keine simplen Passwörter verwenden sollten. Jede Passphrase dient als Zugang zum Programm und bildet zusätzlich jeweils den ersten geheimen Verfahrensschlüssel.

Nach der Erstinstallation können Sie das Programm nur durch die Eingabe eines Startpasswortes öffnen. Das Startpasswort der Freeware lautet stets „**Berlin**“.
Das Startpasswort der Vollversion wird im Lieferschein ausgewiesen.

Wenn Sie eine bestehende Challenger-Installation aktualisieren, bleiben die bisherigen Passphrasen erhalten. Das Startpasswort ist also nur nach der Erstinstallation wirksam und bleibt solange erhalten, bis dieses durch Ihre eigene Passphrase ersetzt wird.

Mit Challenger können Sie bis zu acht Passphrasen programmieren, die später zur Chiffrierung aktiviert werden können. Beispielsweise könnte eine Passphrase zur Verschlüsselung von Daten auf der Festplatte, und eine weitere Passphrase zum Datenaustausch mit einem Partner verwendet werden. Eine Passphrase kann bis zu 64 Zeichen lang sein.

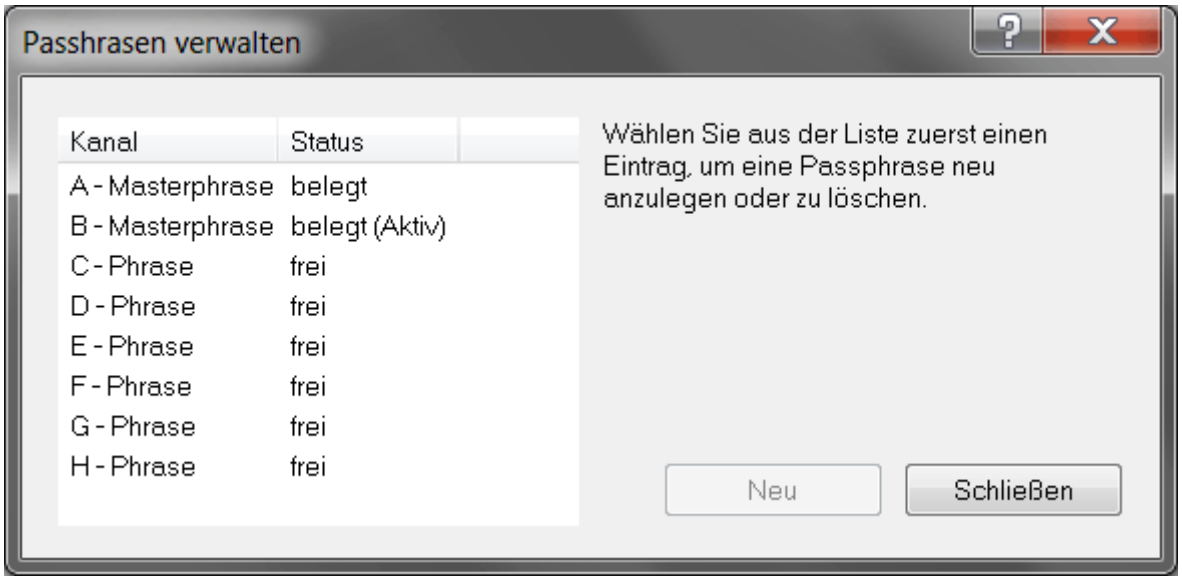
Beispiel-Passphrase:
Im Bierglas sitzen 2 Bienen & schwitzen 90 Minuten.

Bei der Phrasenprogrammierung wird eine kryptografische Prüfsumme von der eingegebenen Passphrase erzeugt. Die Prüfsumme wird gespeichert und dient fortan zur Authentifizierung. So können Sie bei jeder akzeptierten Phraseneingabe sicher sein, dass diese korrekt ist. Andererseits würde ein Hinweis "Passphrase nicht programmiert" erscheinen.

Wichtiger Sicherheitshinweis:
Wird eine Passphrase vergessen, sind die damit verschlüsselten Daten unwiederbringlich verloren. Eventuell notieren Sie die verwendeten Passphrasen und bewahren diese zugriffsgeschützt auf.

Das Passphrasenkonzept (...Fortsetzung)

Zum Programmieren oder Löschen von Passphrasen rufen Sie das Fenster „Passphrasen verwalten“ auf. Dies können Sie nur tun, wenn eine Masterphrase (A-B) aktiv ist.



Passphrasen verwalten (Abb.8)

Jede Passphrase (A-H) ist ein separater Verschlüsselungskanal. Eine Besonderheit stellen die so genannten **Masterphrasen** auf den Kanälen **A und B** dar. Mit einer Masterphrase können Sie neben einer Verschlüsselung zusätzlich folgende Programmfunktionen aufrufen:

- Erzeugung des zweiten Verfahrensschlüssel
- Menüpunkt "Dateien sicher löschen"
- Einstellungen
- Phrasen programmieren und löschen

Für Privatanwender wird die Unterscheidung zwischen Masterphrasen (A-B) und den normalen Passphrasen (C-H) wahrscheinlich keine große Bedeutung zukommen. Für Teamleiter könnte die Unterscheidung jedoch sinnvoll werden. Wenn Sie die Passphrasen für die Mitarbeiter nur auf den Kanälen C-H programmieren, können die Anwender nur mit diesen vorgegebenen Passphrasen verschlüsseln. Die o.g. zusätzlichen Programmfunktionen sind gesperrt.

Deinstallation

Je nachdem wie Sie Challenger installiert haben, gibt es zwei Möglichkeiten zur Deinstallation.

❶ Wenn Sie Challenger mittels Setup auf die Festplatte **in den Windows-Programmordner** installiert hatten, finden Sie zur Deinstallation einen Eintrag in der Windows-Systemsteuerung. Beachten Sie, dass einige Arbeitsdateien in den Benutzerprofilen nicht deinstalliert werden. Wenn Sie die Arbeitsdateien löschen möchten, dann wechseln Sie mit dem Windows-Explorer in den entsprechenden Windows-Benutzerprofile-Ordner und löschen Sie dort den Challenger-Arbeitsordner. Sie finden diesen Ordner unter „C:\Users\%USERNAME%\AppData\Roaming\Challenger“.

❷ Bei jeder anderen Installation **außerhalb vom Windows-Programmordner**, wechseln Sie mit dem Windows-Explorer zum entsprechenden Challenger-Programmordner und löschen Sie diesen Ordner. Bei einer USB-Stick-Installation finden Sie im Wurzelverzeichnis zusätzlich die Datei „Challenger.exe“.

Wichtiger Sicherheitshinweis:
Falls Sie den zweiten Verfahrensschlüssel aktiviert und noch verschlüsselte Daten haben, sollten Sie bereits über Sicherheitskopien verfügen. Wenn nicht, sollten Sie unbedingt Sicherheitskopien anfertigen, bevor Sie die Arbeitsdateien löschen. Wenn Sie den zweiten Verfahrensschlüssel (PAD-Datei) verlieren, können Sie die verschlüsselten Daten nicht mehr entschlüsseln. Denken Sie bei Sicherheitskopien auch an die Haltbarkeit, Kratz- und Stoßfestigkeit der verwendeten Sicherungsmedien!