

Handbuch ArchiCryptX Change

Dok.-Nr.: ACXNB-HB-0023

Ausgabedatum: 15.04.2008

Ausgabe-Nr.: 2.1



1998 - 2008 Softwareentwicklung Dipl.-Ing. Patric Remus, alle Rechte vorbehalten.

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

ArchiCryptX Change

Nutzerhandbuch

by Dipl.-Ing. Patric Remus

Der sichere Austausch von Daten über das Internet ist nahezu unmöglich. Auf dem Weg zum Empfänger landen Ihre vertraulichen Informationen auf beliebigen Rechnern und können dort ohne Probleme protokolliert und mitgelesen werden. Was sich zunächst harmlos anhört, kann bei sensiblen Daten zur Katastrophe führen. ArchiCryptX Change erstellt aus beliebigen Dateien ein Paket, welches in der Lage ist, sich nach Eingabe eines Passwortes, selbst zu entschlüsseln. Neben der Verschlüsselung mit der starken AES (Advanced Encryption Standard) Methode in der besonders sicheren 256 Bit Variante, werden die Daten komprimiert und sind im Idealfall um bis zu 95% kleiner als die Ursprungsdaten. Das spart Zeit und Geld beim Email-Versand. Der Empfänger benötigt keine spezielle Software, denn ArchiCryptX Change-Pakete entschlüsseln sich nach Passwordeingabe selbst. Die Pakete schützen die Daten nicht nur auf dem Weg durchs Internet, sondern auch auf dem PC des Empfängers. Gleichzeitig haben Sie ab jetzt das Recht auf Ihrer Seite, denn nach dem § 202a des Strafgesetzbuchs werden Datendiebe nur dann bestraft, wenn die gestohlenen Daten "gegen unberechtigten Zugang besonders gesichert" sind

Mit einem speziellen Themen-Editor können Sie die Pakete mühelos an eigene Vorstellungen anpassen und das Thema Sicherheit perfekt mit einem neuartigen Marketinginstrument verknüpfen.

Die neue Version ist in 3 Varianten erhältlich. Einer Standard-Version, die sich an den Privatanwender richtet, einer Professional-Version für ambitionierte Privatanwender und den Einsatz im gewerblichen Umfeld und schließlich in einer Enterprise Version, mit der Sie den Zugriff auf ArchiCryptX Change Pakete zentral verwalten und selbst dann noch die Kontrolle über die Pakete behalten, wenn der Empfänger das Paket inkl. seiner Nutzerdaten besitzt.

Inhalt

Teil I Hilfe zur Hilfe	2
Teil II Bestellung	4
Teil III Neu in dieser Version	7
Teil IV Einleitung	18
1 Willkommen	18
Teil V Allgemeine Informationen	20
1 Installationshinweise	20
2 Systemvoraussetzungen	20
Teil VI Wichtige Begriffe - Begriffserläuterungen	22
Teil VII Gegenüberstellung Standard-Professional-Enterprise	26
Teil VIII Bedienung ArchiCryptX Change	30
1 Überblick	30
2 Paket Erstellen	31
Schritt 1 Dateien festlegen	31
Schritt 2 Thema - Information - Sprachnotiz - Abfrage	33
Schritt 3 Namen Mail Kompression	37
Schritt 4 Vertrauliche Nachricht	40
Schritt 5 Passwort	42
Schritt 6 Erstellen des Pakets	45
3 Kommandozeilenparameter	47
ArchiCryptX Change	47

ArchiCryptX Change Paket	47
SmallXChange	49
WEB Access Kommandozeilentool	58
Teil IX Einstellungen ArchiCryptX Change	64
1 Allgemeines	64
2 Kompression	65
3 Passworteigenschaften und Passwortgenerator	65
4 Administrator	67
Teil X Bedienung Themen-Editor	70
1 Übersicht	70
2 Erstellen eines Themas-Logo	72
3 Erstellen eines Themas-Layout	73
4 Erstellen eines Themas-Meldungen	78
Teil XI ArchiCrypt WEB Access Manager (WAM)	81
1 Überblick	81
2 Schritt 1 Dateinamen und Passwort	82
3 Schritt 2 Lizenzen erstellen und bearbeiten	86
4 Schritt 3 Erzeugen und Upload der Lizenzkontrolldatei	89
5 Schritt 4 Anpassen und Upload Kontrollskript	90
6 Schritt 5 Lizenzdatenbank lokal speichern	91
7 Lizenzdaten verteilen und exportieren	92
8 Ein Lizenznehmer - mehrere ArchiCryptX Change Pakete	95
9 Schlüssel / Passwort ändern	99
10 Kontextmenü Lizenztafel	100
11 Suchen und Filtern von Lizenzen	102
12 Einstellungen	103
13 PHP-Editor	107
14 Sicherheit	108
Teil XII Technischer Teil	110
1 Warum Verschlüsselung?	110
2 Verschlüsselung was ist das?	111
3 Eingesetzte Verfahren	112

4	Passwörter	113
5	Bewertung von Passwörtern	114
6	AES	115
7	Angriff auf Verschlüsseltes	116
8	Hashfunktionen	118
9	Entropie	118
10	XOR	120
	Index	122

Teil



1 Hilfe zur Hilfe

Nutzen Sie die Hilfe

Sie sollten sich etwas Zeit nehmen, und die wichtigsten Kapitel zumindest überfliegen.

Als **Anwender** sollten Sie die folgenden Kapitel lesen.

- [Installationshinweise](#)
- [Systemvoraussetzungen](#)
- [Bedienung](#)

Grundsätzlich gilt.

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

Symbole

Innerhalb der Hilfe sind besondere Textstellen durch bestimmte Symbole hervorgehoben.

UNBEDINGT LESEN

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



WICHTIGE HINWEISE

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



TIPPS und Tricks

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

Teil



2 Bestellung

Allgemeines:

Grundsätzlich können Sie zwischen den Varianten CDR-Version und Passwortversand wählen. Bei der CDR- Version erhalten Sie meist innerhalb von 2-3 Werktagen die Software auf CD-ROM. Bei der Passwortvariante erhalten Sie an Werktagen zwischen 09.00 und 19.00 Uhr umgehend [meist innerhalb von 1-2 Stunden] ein zur Freischaltung der Software notwendiges Kennwort. Die Software kann in diesem Fall sofort produktiv eingesetzt werden.

Bezahlung:

Keine lästige Vorkasse, keine Nachnahmegebühr. Kauf auf Rechnung. Sie erhalten die Ware zeitgleich mit einer Rechnung, die innerhalb von 14 Tagen zu begleichen ist. Wir behalten uns vor, im Einzelfall von dieser Methode abzuweichen.

Online-Shop	zum Online-Shop	Sobald Sie den Bestellvorgang starten, wird eine verschlüsselte SSL-Verbindung aufgebaut. Alle Daten, die zwischen Ihrem Rechner und unserem Bestellsystem übertragen werden, sind dadurch gegen fremden Zugriff geschützt. Internet-Shopping auf sichere Art!
Telefon	(089) 66000-893 Montag - Freitag 09.00 - 19.00 Uhr	Teilen Sie uns die Rechnungsanschrift mit und halten Sie einen Stift und ein Stück Papier bereit. Der Bearbeiter teilt Ihnen das Passwort zur Freischaltung sofort am Telefon mit, das Produkt kann sofort produktiv eingesetzt werden. Gerne beantworten wir auf diesem Wege auch offene Fragen.
FAX	(089) 66000-875	Bestellformular PDF Bestellformular Word Laden Sie sich zu diesem Zweck das von uns vorbereitete Formular von unserer Internetseite. Füllen Sie die entsprechenden Felder bitte leserlich aus und FAXen uns die Bestellung. Falls Sie die Versandart "Nur Passwort" gewählt haben, senden wir Ihnen das Passwort an die angegebene Emailadresse, oder teilen Ihnen das Passwort telefonisch unter der angegebenen Rufnummer mit. Während unserer Geschäftszeiten (Montag - Freitag 09.00 - 19.00 Uhr), erhalten Sie nach dem Bestelleingang umgehend das zur Freischaltung notwendige Passwort.

Brief	<p><u>Anschrift:</u> Softwareentwicklung Dipl.-Ing. Patric Remus Am Brunneck 6 85521 Ottobrunn</p>	<p>Bestellformular PDF Bestellformular Word Laden Sie sich zu diesem Zweck das von uns vorbereitete Formular von unserer Internetseite. Füllen Sie die entsprechenden Felder bitte leserlich aus und senden uns die Bestellung. Falls Sie die Versandart "Nur Passwort" gewählt haben, senden wir Ihnen das Passwort an die angegebene Emailadresse, oder teilen Ihnen das Passwort telefonisch unter der angegebenen Rufnummer mit.</p>
Anonym	<p><u>Anschrift:</u> Softwareentwicklung Dipl.-Ing. Patric Remus Am Brunneck 6 85521 Ottobrunn</p>	<p>Voraussetzung für den anonymen Bezug der Software ist ein Email-Zugang bei einem Anbieter, der ihre persönlichen Angaben nicht überprüft. Senden Sie uns einen Brief mit Bargeld in EURO in Höhe des Produktpreises. Fügen Sie dem Brief die Email-Adresse bei. Sie erhalten Ihren Key dann an diese Mailadresse.</p>

Teil



3 Neu in dieser Version



Neu in Version 2

ArchiCryptX Change wurde komplett überarbeitet und bietet zahlreiche neue Funktionen.

Versionen

Neben der Standard- und Professionalversion bieten wir eine s.g. Enterprise Version, die es erlaubt, den Zugriff auf ArchiCryptX Change Pakete zentral über einen WEB Server zu steuern.

Die Unterschiede zwischen den einzelnen Versionen finden Sie als Tabelle zusammengefasst unter [Gegenüberstellung Standard-Professional-Enterprise](#)

Neu in der Standardversion

Überarbeitete Bedienoberfläche

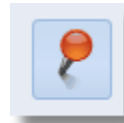
Die Bedienoberfläche zeigt sich in neuem Gewand. Nutzer der Vorversion werden sich sofort zurechtfinden. Neueinsteiger können die Software dank der intuitiven Bedienoberfläche sofort produktiv einsetzen.

Ein neues Hilfesystem steht immer mit einer Kurzhilfe zur Seite.



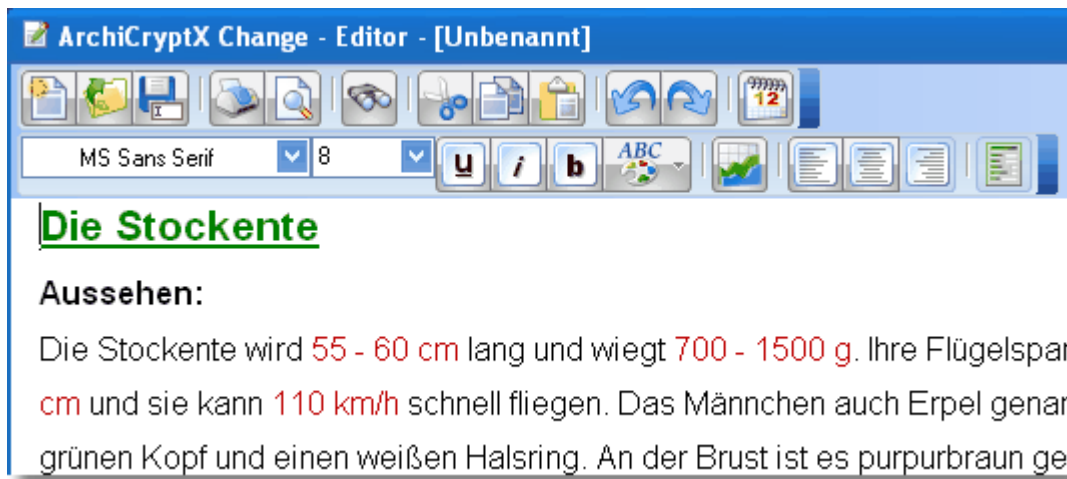
Stay-on-top Funktion

Insbesondere dann, wenn Sie per Drag&Drop Dateien für ein Paket zusammenstellen wollen, ist es sinnvoll, ArchiCryptX Change im Vordergrund zu haben.



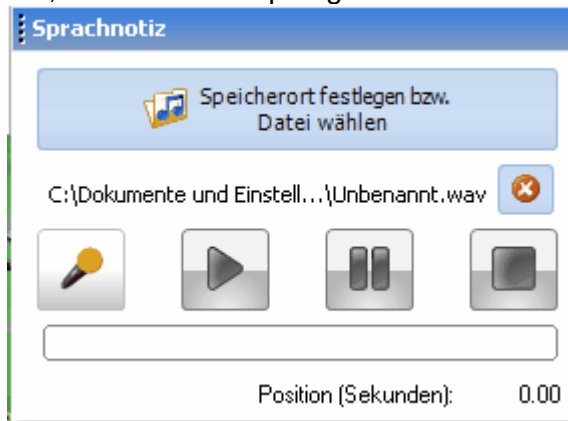
Texteditor

ArchiCryptX Change bringt einen kompletten Texteditor für die Eingabe von Informationstext und vertraulicher Nachricht mit.



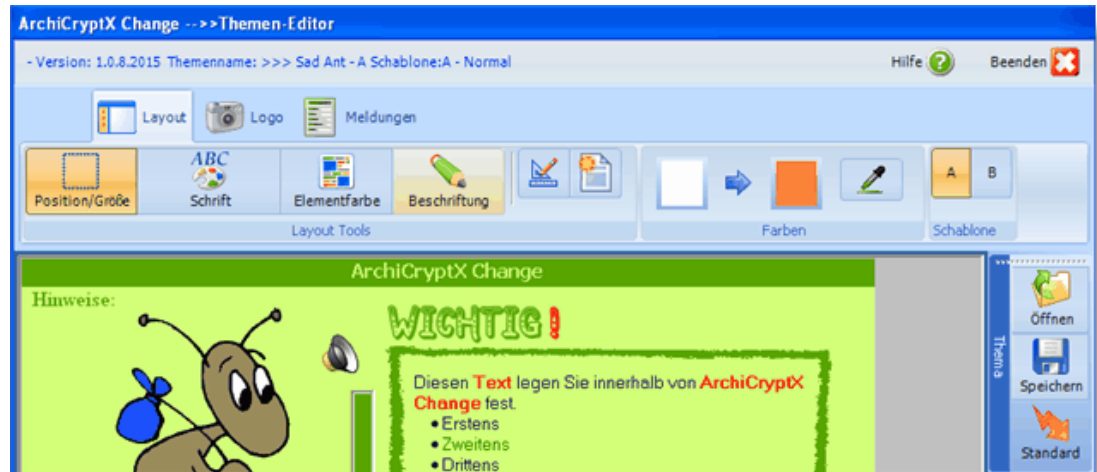
Sprachnotiz

Erstellen und Anfügen einer Sprachnotiz. Nehmen Sie eine kurze Sprachnachricht auf, die sich der Empfänger der Nachricht anhören kann.



Themen-Editor

Mit so genannten Themen legen Sie das Aussehen der ArchiCryptX Change Pakete fest. Der Themen Editor bringt alle Werkzeuge mit, um neue Themen zu erstellen oder vorhandene Themen zu bearbeiten. Das Aussehen eines ArchiCryptX Change Pakets kann in jeder Einzelheit (Position, Größe und Farbe der einzelnen Elemente, Schriftart, -farbe und -typ, Links) bestimmt werden.

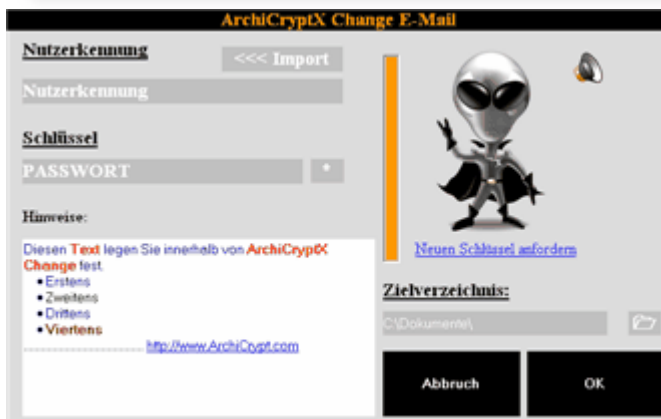


Beschriftungen und Meldungstexte können beliebig angepasst und so zum Beispiel mühelos in andere Sprachen übersetzt werden.

	Erläuterung	Original	Übersetzung (Ihr Text)
1	Wird als Titel des Dialogs angezeigt	ArchiCryptX Change	ArchiCryptX Change
2	Hilfetext Maus über Passworteingabe	Geben Sie hier Ihr Passwort ein	Geben Sie hier Ihr Passwort ein
3	Hilfetext Maus über Schaltfläche für das Umschalten der	Schaltet zwischen Klartext und verdeckter Ansicht um	Schaltet zwischen Klartext und verdeckt um

Vorgefertigte Themen

Zahlreiche vorgefertigte Themen können sofort genutzt oder als Vorlage für eigene Themen verwendet werden. Die Verfügbarkeit bestimmter Themen hängt von der verwendeten Version (Standard, Professional, Enterprise) ab.

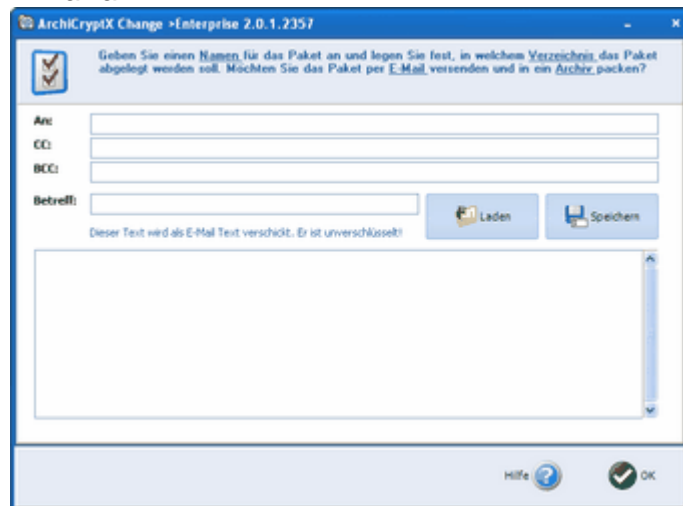




u.v.a.m.

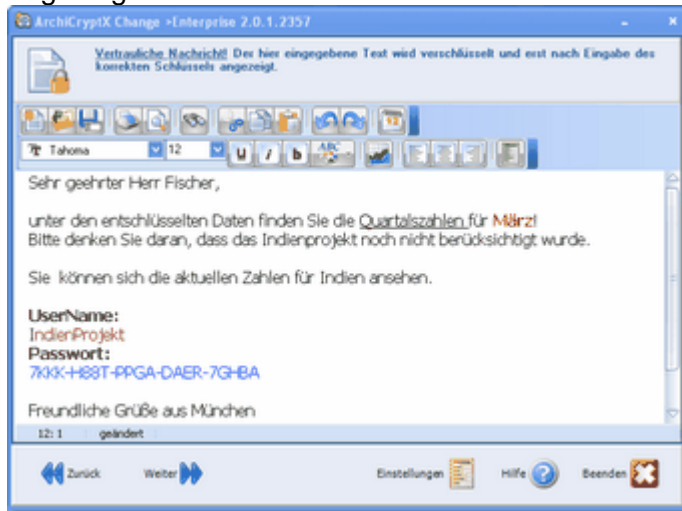
E-Mail Funktion

ArchiCryptX Change Pakete können nach dem Erstellen sofort als E-Mail versendet werden. Geben Sie in XChange Empfänger, den Betreff und den Klartexttext für Ihre E-Mail an.



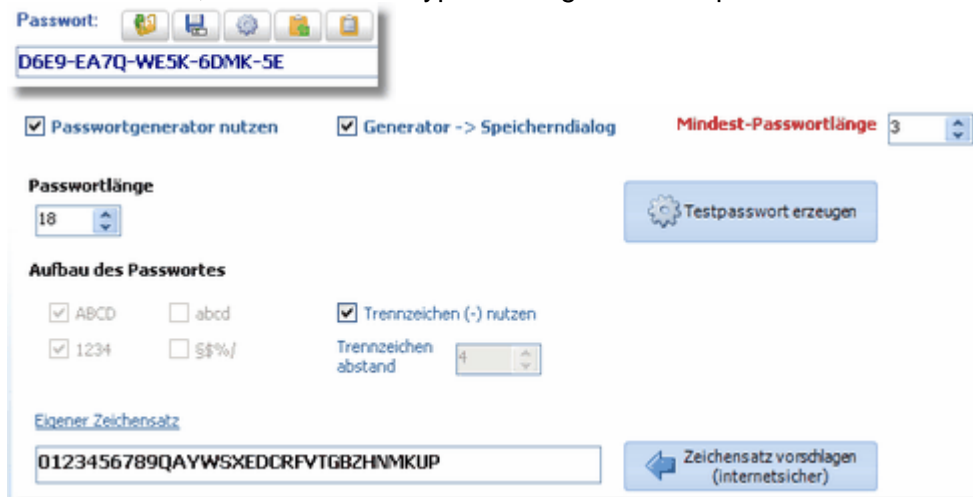
Vertrauliche Nachricht

In einem eigenen Texteditor können Sie dem Empfänger des Pakets eine vertrauliche Nachricht zukommen lassen. Diese Nachricht wird verschlüsselt und beim Empfänger erst nach Eingabe des korrekten Passwortes entschlüsselt und angezeigt.



Passwortgenerator

Automatisches Generieren sicherer Passwörter mit eigenem Zeichenvorrat. Export in Schlüsseldatei, die vom ArchiCryptX Change Paket importiert werden kann.



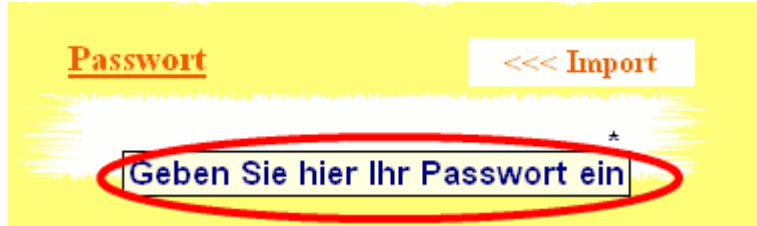
Sie können eine Mindestlänge für Passwörter festlegen.

Jobdateien

Jobdateien speichern die Angaben, die Sie zum Erstellen eines ArchiCryptX Change Pakets machen müssen. Jobdateien können jetzt mit Passwort gespeichert werden. Pakete die man häufig erstellt, können somit sofort erstellt werden.

ArchiCryptX Change Paket

Das ArchiCryptX Change Paket kann mit Hilfe der Themen nahezu beliebig gestaltet werden. Sie können Text frei definieren, der dem Text als Hilfe angezeigt wird, sobald dieser die Maus über eines der Bedienelemente bewegt.



Ersparen Sie dem Empfänger des ArchiCryptX Change Pakets das mühsame Eintippen von Passwort und Nutzerdaten. Das Paket kann diese Daten bequem aus einer Datei oder von der Zwischenablage importieren.



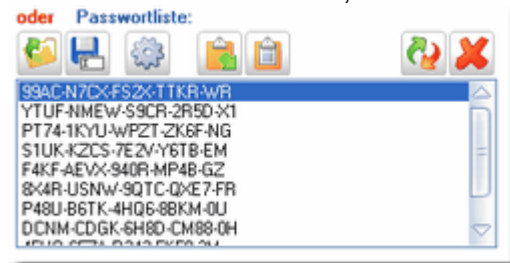
Das Paket kann bei Bedarf über die Kommandozeile oder eine Kontrolldatei ohne Anzeige des Dialogs entschlüsselt werden.

Neu in der Professional Version

Die Professional Version enthält neben allen Funktionen der Standardversion folgende zusätzliche Neuerungen.

Multi-Passwort Pakete

ArchiCryptX Change Pakete können so erstellt werden, dass Sie mit bis zu 100 völlig verschiedenen Passwörtern geöffnet werden können. Falls Sie ein ArchiCryptX Change an mehrere Benutzer verteilen müssen und dabei nicht identische Passwörter nutzen wollen, ist diese Variante ideal geeignet.



Administrator Schutz

Beim Einrichten der Software können Sie Einstellungen festlegen, die der Nutzer nicht mehr ändern kann. Diese Einstellungen können Sie exportieren und für die Einrichtung anderer Clients nutzen.

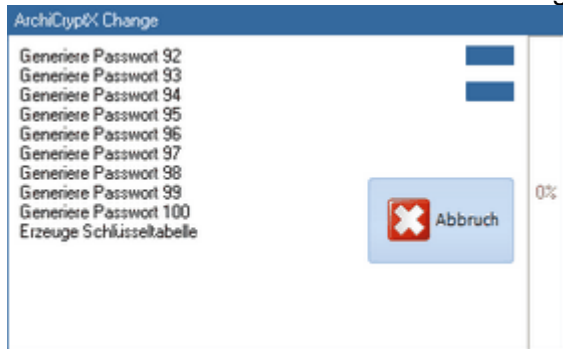


Kommandozeilenversion SmallXChange

Die Kommandozeilenversion wurde so angepasst, dass neue Funktionen wie

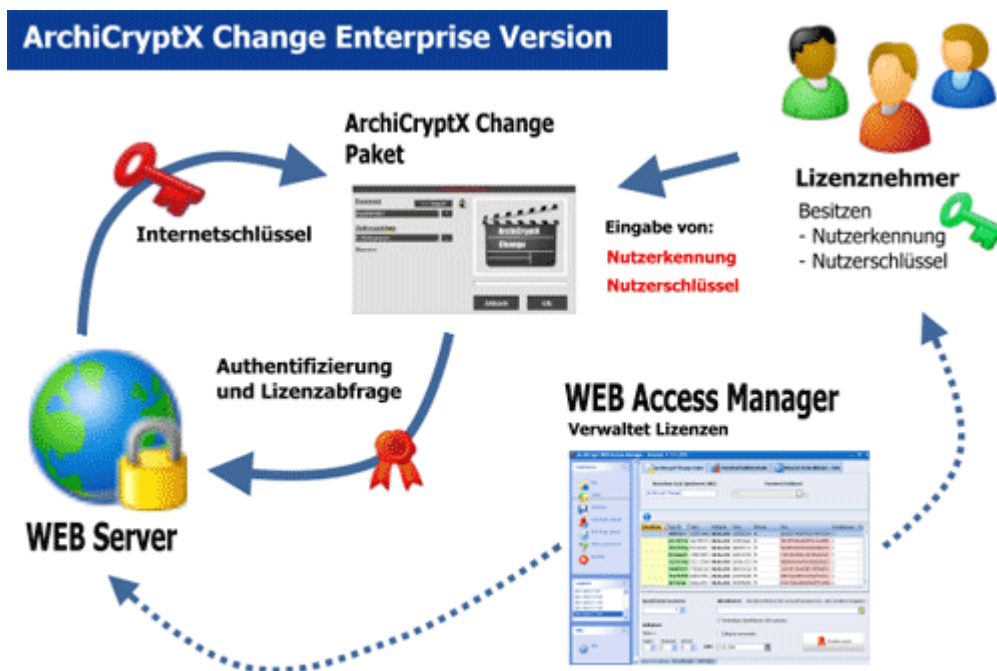
- Sprachnotiz
- Vertrauliche Nachricht
- Neue Passwortgeneratorfunktionen nutzbar sind.

Die Kommandozeilenversion kann über s.g. Kommandodateien gesteuert werden.



Enterprise Version

Die Enterprise Version erlaubt die zentrale Kontrolle des Zugriffs auf ArchiCryptX Change Pakete. Sie enthält neben allen Funktionen der Standard- und Professionalversion folgende Funktionen.



Copyright 2006 - Dipl.-Ing. Patric Remus - www.ArchiCrypt.com

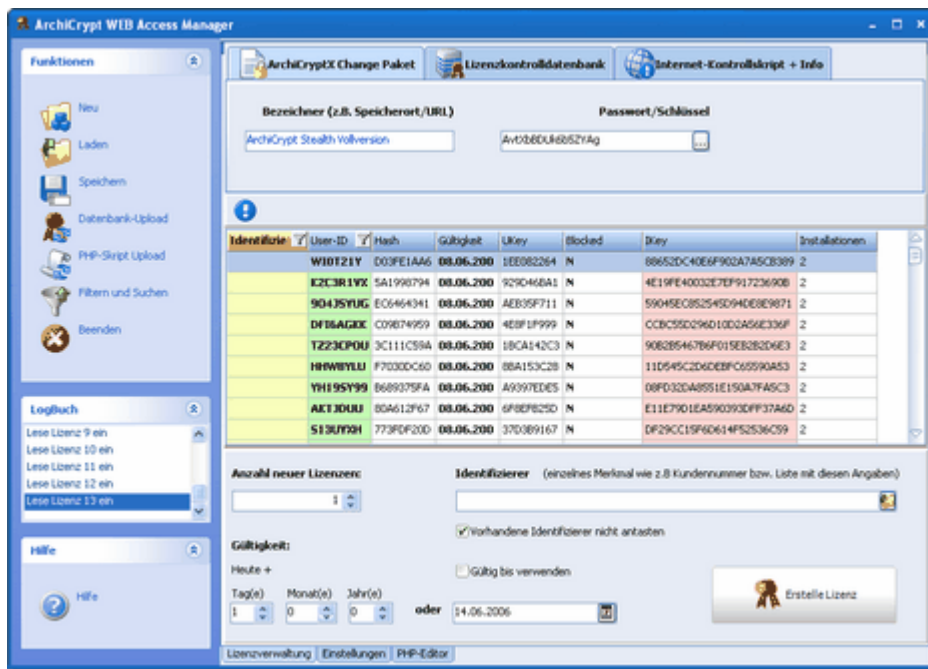
Themen-Schablone

Eine zusätzliche Themen-Schablone, mit der Themen speziell für die Nutzung bei Zugriffskontrolle via Internet erstellt und angepasst werden können.



WEB Access Manager

Der WEB Access Manager ist ein Werkzeug, mit dessen Hilfe Sie Ihren WEB Server rasch um die Funktion einer zentralen Zugriffskontrolle auf ArchiCryptX Change Pakete erweitern. Der Manager unterstützt Sie beim Erzeugen und bei der Verwaltung von Lizenzen und bei der Vorbereitung Ihres WEB Servers für die Zugriffskontrolle.



Sie können eine nahezu beliebige Anzahl an Lizenzen erzeugen und Verwalten. Der Manager erzeugt aus dieser **Lizenzdatenbank** eine s.g. **Lizenzkontrolldatei**, die zusammen mit einem Kontrollskript die Kommunikation mit dem ArchiCryptX Change Paket übernimmt.

Sie können so folgende Daten zentral festlegen:

- kann ein Lizenznehmer das Paket generell entschlüsseln (besitzt er eine Lizenz)
- sperren einer Lizenz (z.B. wegen Missbrauch) und Anzeige einer Informationsseite im Internet
- wie lange eine Lizenz gültig ist. Nach Ablauf der Lizenz kann eine Informationsseite angezeigt werden
- wie viele Installationen/Entschlüsselungen darf der Lizenznehmer vornehmen

Teil



4 Einleitung

4.1 Willkommen



Vielen Dank, dass Sie sich für ArchiCryptX Change© entschieden haben.

Die Menge vertraulicher Daten und deren Schutzbedürfnis steigt mit dem Wachstum der öffentlichen und firmeninternen Netzwerke. In dieser neuen "Digitalen Welt" besteht die größte Herausforderung darin, eigene Informationen vor Unbefugten zu schützen.

ArchiCryptX Change © leistet seinen Beitrag zum Schutz dieser Daten und setzt dazu die neusten Standards und Verfahren ein. Die Verfahren sind von unabhängigen Kryptologen entwickelt und von den besten Kryptanalytikern der Welt ausgiebig getestet. ArchiCryptX Change © setzt das Verfahren AES (Advanced Encryption Standard) mit einer Schlüssellänge von 256 BIT ein.

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

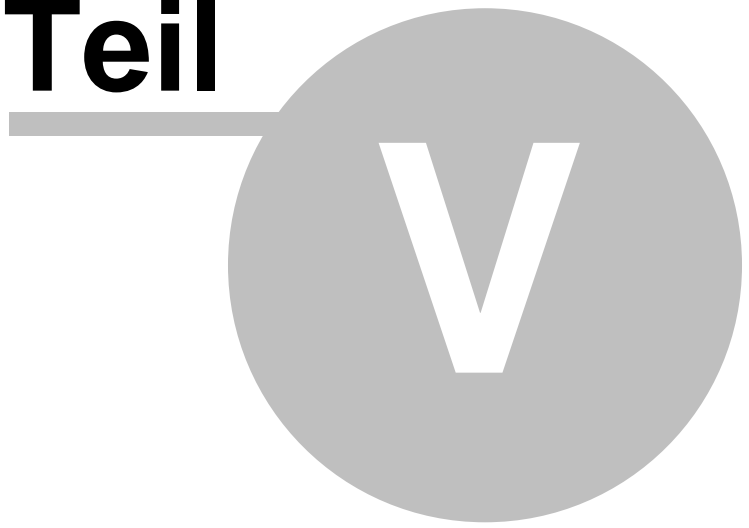
ArchiCryptX Change © ist ideal für

- Firmen die mit sensiblen Daten umgehen
 - Banken und Versicherungen
 - Rechtsanwälte und Notare
 - Steuerberater und Finanzdienstleister
 - Unternehmens- und Personalberatungen
 - Ärzte
- und
- alle, die sensible Daten mit Ihren Geschäftspartnern austauschen.

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

Dipl.-Ing. Patric Remus

Teil



5 Allgemeine Informationen

5.1 Installationshinweise

Das Programm wird mit einer eigens entwickelten Installationsroutine geliefert, die Ihnen die Arbeit abnimmt. Die Installation erfolgt automatisch so, dass Sie für jeden Nutzer eingerichtet wird.

Achten Sie darauf, dass Sie unter den Betriebssystemen Windows 2000, Windows XP und Windows 2003 zur Installation der Software lokale Administratorrechte besitzen müssen.

Bei der Installation werden keine Systemdateien ersetzt oder geändert.

➡ **ACHTUNG:** Themen, die mit der Vorversion erstellt wurden, müssen neu erstellt werden. JOB Dateien können geladen werden, müssen insbesondere was das verwendete Thema angeht, angepasst werden.

5.2 Systemvoraussetzungen

Um ArchiCryptX Change verwenden zu können, muss Ihr System folgende Voraussetzungen erfüllen:

- mindestens Pentium-Prozessor oder vergleichbare CPU
- mindestens 256 MB empfohlen
- Festplatten-Platz: ca. 70 MB
- Windows 98SE, ME, 2000, Windows XP, Windows 2003, Windows Vista
- Bildschirmauflösung mindestens 1024x768 bei einer Farbtiefe von mindestens 32 BIT Farbtiefe
- Maus oder anderes Windows-kompatibles Zeigegerät
- Mikrofon zur Aufnahme von Sprachnotizen
- MAPI kompatibler E-Mail Client für E-Mail Funktion
- PHP fähiger WEB Server mit FTP Zugang (nur Enterprise Version)

ArchiCryptX Change Pakete können auf Windows 98,ME,2000,XP und 2003 Rechnern genutzt werden.

➡ **Hinweis für 64 BIT Systeme:**

ArchiCryptX Change bietet hier kein Kontextmenü im Explorer an. Um dennoch auf das Kontextmenü zurückgreifen zu können, gehen Sie bitte vor, wie von [Microsoft beschrieben](#).

Teil



6 Wichtige Begriffe - Begriffserläuterungen

Wichtige Begriffe:

ArchiCryptX Change Paket = Die Datei, die von ArchiCryptX Change erstellt wird. Die Datei ist eine Anwendung, die in der Lage ist, sich selbst zu entschlüsseln.

Thema = Ein Thema legt das Aussehen eines ArchiCryptX Change Paketes fest. Ein Thema ist eine Datei, in der folgende Informationen zusammengefasst sind:

- Logo/Bild des Dialogs
- Farb-, Schrift- und Positionsinformationen
- Beschriftungen und Meldungstexte

Job = Ein Job ist eine Datei, in der Informationen für das Erstellen eines ArchiCryptX Change Paketes enthalten sind.

Sie enthält:

- Dateien, die in das Paket aufgenommen werden sollen
- Thema
- Informationstext (Nur Verweis auf Datei)
- Sprachnotiz (Nur Verweis auf Datei)
- Abfrage
- Speicherort
- Pfadinformationen
- Kompression
- Passwort/Passwortliste (sofern Option "Inklusive Passwort" beim Speichern gewählt wurde)

Wichtig für WEB Access Manager (Enterprise Version)

WEB Access Manager = WAM = Programm zur Verwaltung von Lizenzen für ArchiCryptX Change Pakete

MasterKey = Schlüssel/Passwort, mit dem ein ArchiCryptX Change Paket erstellt/ verschlüsselt.

siehe dazu [Schritt 5 Passwort](#)

Teilschlüssel = UserKey und InternetKey sind Teilschlüssel. Mit keinem der beiden Schlüssel alleine ist es möglich, die Daten eines ArchiCryptX Change Pakets zu entschlüsseln. Aus verschiedenen Teilschlüsseln kann man den MasterKey berechnen, mit dessen Hilfe man die Daten entschlüsseln kann.

UserKey = Nutzerschlüssel = UKey = Das (Teil-)Passwort, welches der Empfänger des ArchiCryptX Change Pakets zusammen mit der User-ID erhält.

User-ID = Nutzerkennung = UID = Eindeutige, einmalige, zufällige Zeichenfolge, die als SALT Wert für die Berechnung eines Prüfwertes herangezogen wird. Die User-ID als SALT ist im Allgemeinen nicht schützenswert.

Lizenzdatensatz = Kombination aus User-ID und UserKey. Beide Werte sind nötig um mit der Enterprise Version die WEB Kontrolle durchzuführen.

Kenndaten= Alle Daten einer Lizenz mit Ausnahme des InternetKey. Es sind insbesondere die User-ID, der UserKey und die Lizenzinformationen enthalten. Diese Kenndaten können im WEB Access Manager exportiert und importiert werden. Beim Import der Kenndaten wird ein zum verknüpften ArchiCryptX Change Paket passender Internetschlüssel erzeugt.

SALT = Zufällige Bitfolge, die zusammen mit dem Passwort als Eingangsgröße für eine Funktion zur Berechnung eines Prüfwertes dient. Mit Hilfe des Salt Wertes werden s.g. **Wörterbuchattacken ("Dictionary Attack")** wirkungsvoll unterbunden. Bei einer Wörterbuchattacke wird eine Tabelle genutzt, bei dem jedem Eintrag (Klartextpasswort) des Wörterbuchs der Prüfwert (Hashwert) gegenübergestellt ist. Besitzt ein Angreifer diesen Prüfwert (häufig der Fall, da Prüfwerte zumeist offen abgelegt werden), kann man in der Tabelle suchen und zum passenden Prüfwert das Klartextpasswort ablesen. Solche Tabellen sind vorberechnet und benötigen je nach angenommener Länge des Passwortes verschieden viel Speicherplatz. Das Berechnen einer solchen Tabelle benötigt viel Zeit. Durch den SALT Wert werden erstens die vorberechneten Tabellen wertlos und der Platzbedarf zur Speicherung der Tabellen steigt sprunghaft an.

Warnung: Der Einsatz von SALT schützt wirkungsvoll gegen Wörterbuchattacken, aber nicht gegen schwache Einzelpasswörter!

InternetKey = Internetschlüssel = IKey = Das (Teil-)Passwort, welches in der Lizenzkontrolldatenbank abgelegt ist und im Falle einer gültigen Anfrage an den Sender der Anfrage überstellt wird.

Notschlüssel = Schlüssel, der keine Kommunikation mit dem WEB Server/Kontrollskript benötigt um ein entsprechendes ArchiCryptX Change Paket zu entschlüsseln. Weitergabe führt dazu, dass zentrale Kontrolle nicht mehr möglich ist und meist eine Neuverschlüsselung des Pakets und ein Anpassen der Lizenzkontrolldatei nötig ist.

Prüfwert = Hash = Wert der sich aus dem UserKey und der UserID ergibt. Der Prüfwert lässt keine Rückschlüsse auf UserKey oder UserID zu. Der Prüfwert wird vom Internet-Kontrollskript herangezogen um zu prüfen, ob es gültige Einträge für diesen Nutzer in der Lizenzkontrolldatenbank gibt.

Lizenzdatenbank = Textdatei/Datenbank, mit allen Informationen über das ArchiCryptX Change Paket inkl. aller Lizenzen. Die Datenbank darf nicht in unautorisierte Hände gelangen. Sie wird verschlüsselt gespeichert. Die Lizenzdatenbank dient als Grundlage für die Lizenzkontrolldatenbank, die aus ihr generiert wird. Die Lizenzdatenbank darf (sollte nicht, weil ohne Sinn) nicht auf Ihre Internetpräsenz geladen werden.

Nicht verwechseln mit Lizenzkontrolldatenbank!

Lizenzkontrolldatenbank = Textdatei/Datenbank, mit folgenden Informationen.

- Prüfwert der zur eindeutigen Zuordnung von Anfragen genutzt wird
- Internetschlüssel
- Informationen über Gültigkeitsdauer der Lizenz
- Anzahl erlaubter Installationen
- Status Zugang gesperrt Ja/Nein

Mit Hilfe der Informationen in der Lizenzkontrolldatenbank alleine, ist es nicht möglich, den MasterKey zu berechnen.

Die Lizenzkontrolldatenbank wird in Ihrer Internetpräsenz gespeichert und steuert

zusammen mit dem PHP-Kontrollskript (greift auf die Lizenzkontrolldatenbank zu), den Zugriff auf ArchiCryptX Change Pakete.

Nicht verwechseln mit Lizenzdatenbank!

Internet-Kontrollskript = Kontrollskript = PHP Skript, welches unter Zugriff auf die Lizenzkontrolldatenbank mit dem ArchiCryptX Change Paket kommuniziert und entsprechend den Werten in der Lizenzkontrolldatenbank den Internetschlüssel oder andere Informationen überträgt.

Teil



7 Gegenüberstellung Standard-Professional-Enterprise

Feature Matrix

ArchiCryptX Change ist in 3 Versionen verfügbar. Während sich die Standard-Version an den privaten Anwender richtet, ist ArchiCryptX Change in der professional Variante für ambitionierte Privatanwender und Firmen gedacht.

Die Enterprise-Version bietet darüber hinaus die Möglichkeit, Zugriffe auf ArchiCryptX Change Pakete zentral mit Hilfe eines WEB Servers zu steuern. Sie ist daher vorwiegend für den Einsatz in Firmen gedacht, die sensible Inhalte zentral kontrollieren und größeren Nutzergruppen verfügbar machen möchten.

	Standard	Professional	Enterprise ⁽¹⁾
Erstellen selbstentschlüsselter Pakete	X	X	X
Themen-Editor zum Erstellen und Anpassen der Themen	X	X	X
Vorgefertigte Themen	ca. 10	ca. 30	ca. 40
Passwortgenerator	X	X	X
Verschlüsseln einer Textnachricht (Vertrauliche Nachricht)	X	X	X
Aufnahme und Versand von Sprachnotizen	X	X	X
E-Mail (Festlegen von Empfänger/Betreff und Text)	X	X	X
Steuern der ArchiCryptX Change Pakete über Kommandozeile	X	X	X
Steuern der ArchiCryptX Change Pakete über Kommandodatei	X	X	X
Passwortlistengenerator		X	X
Multi Passwort Pakete. Paket kann mit bis zu 100 verschiedenen Passwörtern geöffnet werden.		X	X
Kommandozeilenversion SmallXChange *, die über Batch oder s.g. Kommandodateien automatisiert Pakete erstellen kann.		X	X
Administrator kann Einstellungen schützen und z.B. Thema vorgeben (nur Windows 2000,XP und 2003)		X	X
Import und Export von Einstellungen		X	X
Installationsmodus (1		X	X

Datei kann nach dem Entschlüsseln automatisch gestartet werden)			
WebAccessManager **			X
Notpasswort für Zugriff auf Inhalte von XChange Paketen (kontrolliert durch Kontrollskript) ohne Internetzugang			X

*

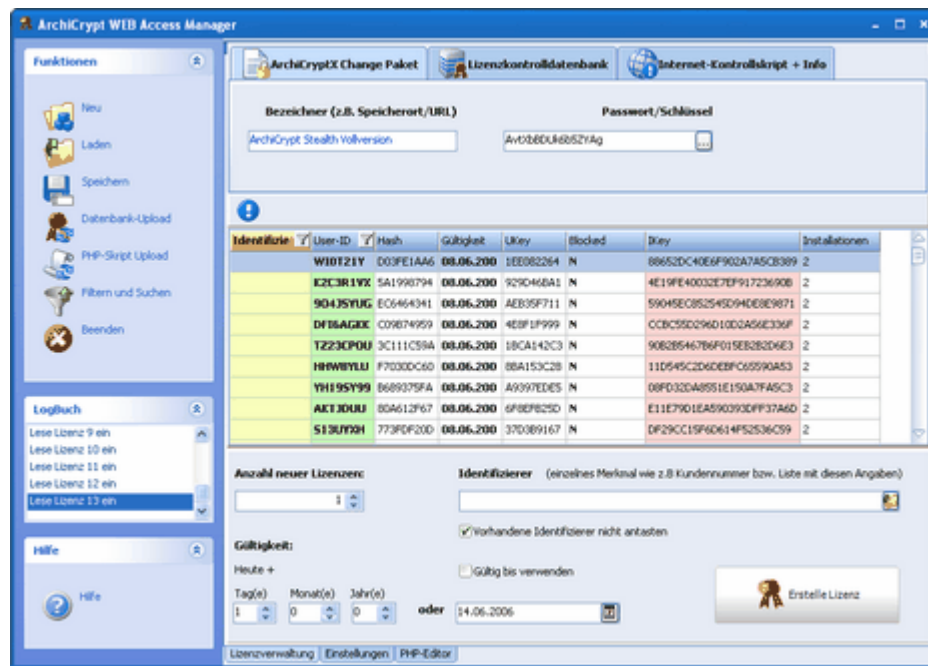
SmallXChange

Die Kommandozeilenversion von ArchiCryptX Change erlaubt das automatische Erstellen s.g. ArchiCryptX Change Pakete. Sie ist daher ideal dazu geeignet, die Funktionalität in eigene Programme einzubinden oder Arbeitsabläufe zu automatisieren.

**

WEB Access Manager (WAM)

Der WEB Access Manager ist ein Werkzeug, mit dessen Hilfe Sie Ihren WEB Server rasch um die Funktion einer zentralen Zugriffskontrolle auf ArchiCryptX Change Pakete erweitern. Der Manager unterstützt Sie beim Erzeugen und bei der Verwaltung von Lizenzen und bei der Vorbereitung Ihres WEB Servers für die Zugriffskontrolle.

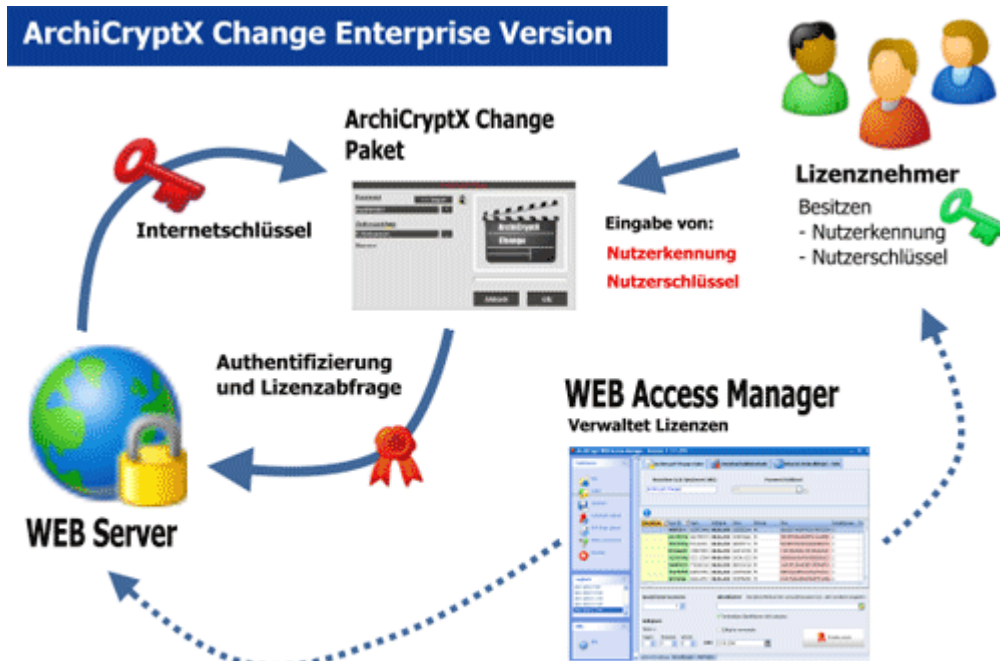


Sie können eine nahezu beliebige Anzahl an Lizenzen erzeugen und verwalten. Der Manager erzeugt aus dieser Lizenzdatenbank eine s.g. Lizenzkontrolldatei, die zusammen mit einem Kontrollskript die Kommunikation mit dem ArchiCryptX Change Paket übernimmt.

Sie können so folgende Daten zentral festlegen:

- kann ein Lizenznehmer das Paket generell entschlüsseln (besitzt er eine Lizenz)
- sperren einer Lizenz (z.B. wegen Missbrauch) und Anzeige einer Informationsseite im Internet
- wie lange eine Lizenz gültig ist. Nach Ablauf der Lizenz kann eine Informationsseite angezeigt werden
- wie viele Installationen/Entschlüsselungen darf der Lizenznehmer vornehmen

(1) Enterprise Version



Copyright 2006 - Dipl.-Ing. Patric Remus - www.ArchiCrypt.com

Teil



8 Bedienung ArchiCryptX Change

8.1 Überblick



[Demo Video ArchiCryptX Change](#)

Das 6 teilige, 20 minütige Video zeigt, wie man Schritt für Schritt zum fertigen ArchiCryptX Change Paket gelangt, erklärt zahlreiche Funktionen und gibt wertvolle Tipps für den Umgang mit ArchiCryptX Change.



Hohe Sicherheit beim Transport sensibler Daten

ArchiCryptX Change erlaubt das Erstellen s.g. selbstentschlüsselnder Datenpakete (**ArchiCryptX Change Paket**). Die Datenpakete sind Anwendungen, die die sensiblen Daten im Huckepack mit sich führen und diese erst nach Angabe des korrekten Passwortes entschlüsseln und freigeben. Der Empfänger benötigt daher auch kein bestimmtes Programm, um die Daten zu entschlüsseln.

Corporate-Identity verknüpft mit Datensicherheit

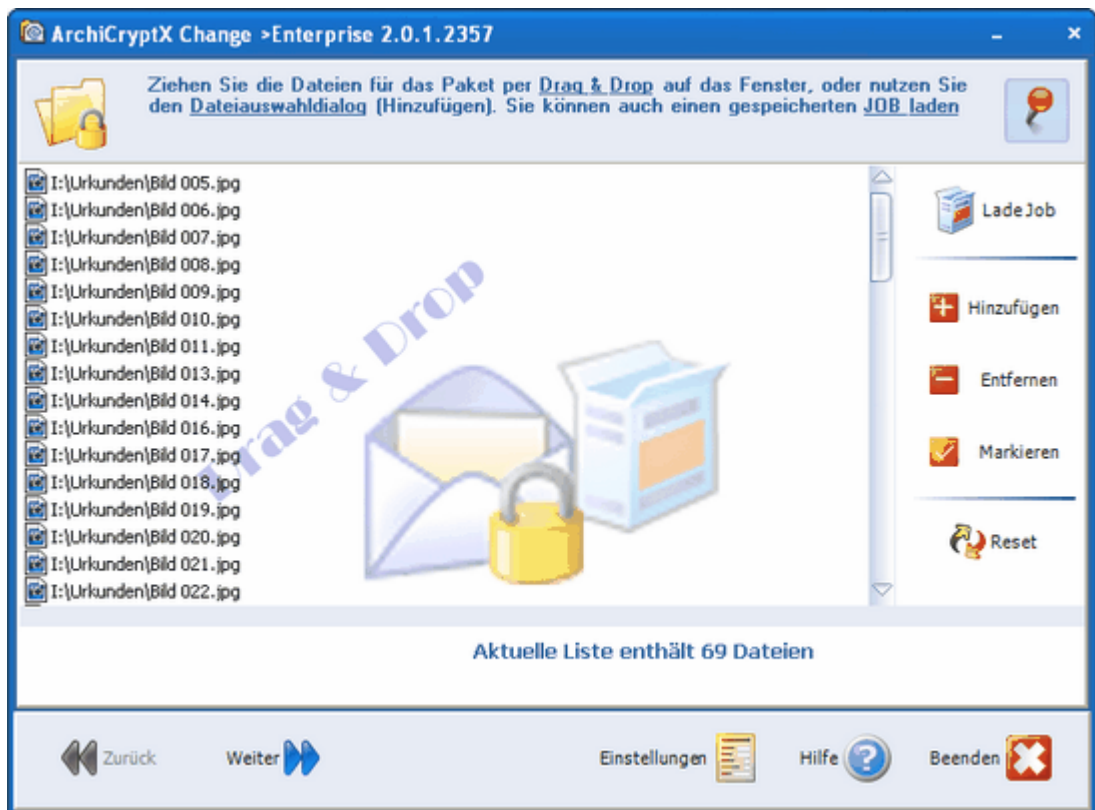
Neben Dateien können Sie dem Empfänger vertrauliche Nachrichten übermitteln und ihm sogar eine Sprachnotiz zukommen lassen. Die sensiblen Daten werden dabei mit der besonders sicheren 256 BIT Variante des Advanced Encryption Standards (AES) verschlüsselt.

Besonders interessant ist der Umstand, dass Sie das Erscheinungsbild des Datenpakets mit Hilfe des s.g. Themen-Editors in jeder Hinsicht an eigene Vorstellungen anpassen können.

Die ArchiCryptX Change Pakete können Sie via E-Mail versenden, auf CD/DVD oder auf einer Internetseite zum Download anbieten.

Volle Kontrolle

Wer die volle Kontrolle über die ArchiCryptX Change Pakete haben möchte, findet in der Enterprise Version mit dem **WebAccess-Manager** die richtige Lösung. Sie können Lizenzen erstellen und zentral steuern, wer wie lange auf welche ArchiCryptX Change Pakete zugreifen kann.



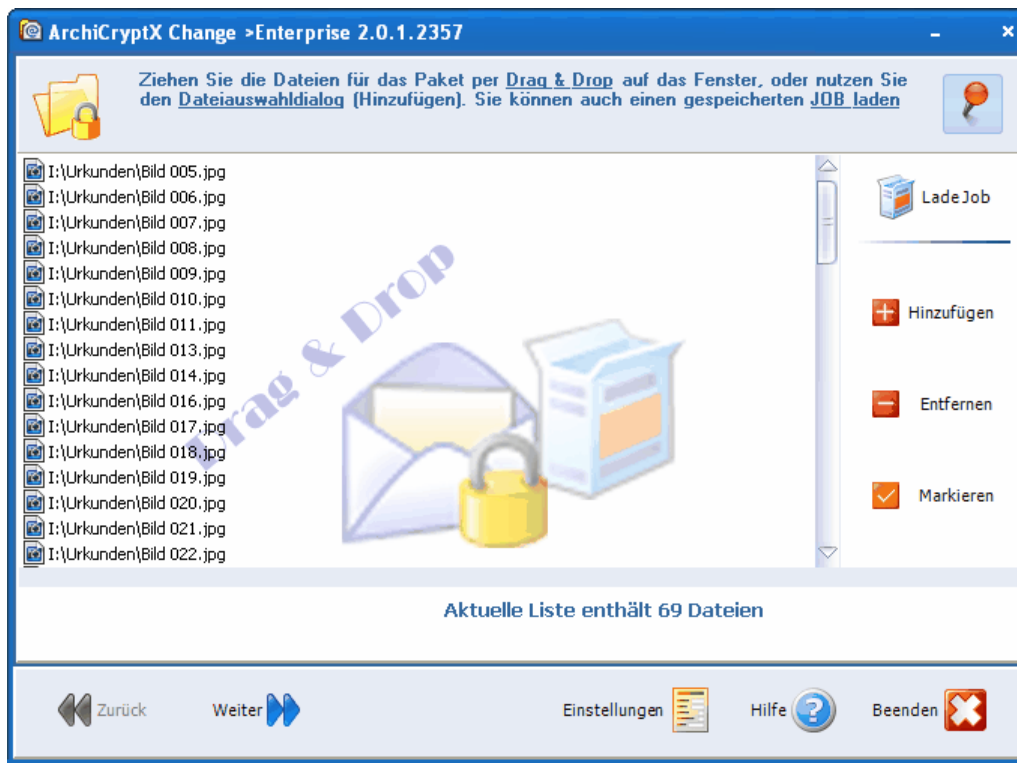
8.2 Paket Erstellen

8.2.1 Schritt 1 Dateien festlegen

Dateien für das ArchiCryptX Change Paket festlegen



[Demo Video ArchiCryptX Change](#)



Im ersten Schritt legen Sie die Dateien fest, die in das selbstentschlüsselnde Paket gepackt werden sollen.

Sie haben mehrere Möglichkeiten, um Dateien hinzuzufügen

1. Über die Schaltfläche **Hinzufügen** können Sie in einem Dialog einzelne Dateien auswählen und zum Paket hinzufügen. (Um ganze Verzeichnisse in das Paket zu übernehmen, nutzen Sie Möglichkeit 2 oder 3!)
2. Sie können aus dem betriebssystemeigenen Explorer heraus Dateien und Verzeichnisse auf die Liste ziehen (**Drag&Drop**). Verzeichnisinhalte werden dabei rekursiv eingefügt. D.h. auch Inhalte von Unterverzeichnissen werden ins Paket übernommen.



TIPP: Sobald Sie die Schaltfläche aktivieren, die in der Grafik mit einem Pfeil markiert ist, bleibt ArchiCryptX Change im Vordergrund. Drag&Drop Operationen können so bequemer durchgeführt werden.

3. Falls Sie vorwiegend mit dem Windows Explorer arbeiten, können Sie über das **Kontextmenü** (rechte Maustaste) den Menüpunkt **ArchiCryptX Change Paket ...** aufrufen. ArchiCryptX Change wird dann gestartet und die markierten Dateien aus dem Windows-Explorer sind bereits in die Liste eingefügt.
4. Wenn Sie alle Angaben gemacht haben, die zur Erstellung eines Paketes notwendig sind, können Sie diese Einstellungen als s.g. **Job** speichern. Diesen Job können Sie über die Schaltfläche **Lade Job** aufrufen.

Installer erstellen

(nur Professional und Enterprise Version)

Gelegentlich ist es sehr nützlich, wenn nach dem Entschlüsseln sofort eine bestimmte Datei ausgeführt wird. Dies kann zum Beispiel ein Installationsprogramm sein.

Markieren Sie die auszuführende Anwendung in der Liste und betätigen Sie die rechte Maustaste. Im Menü können Sie den Eintrag **Datei ausführen** wählen.

Auszuführende Datei: [Installer erstellen](#) [Aktuelle Liste enthält 70 Dateien](#)
I:\456.exe

Die Datei wird jetzt unterhalb der Liste angezeigt. Handelt es sich um eine ausführbare Datei (Endung exe, com oder bat), können Sie den Schalter **Installer erstellen** wählen. In diesem Fall werden alle im Paket enthaltenen Dateien nach der Eingabe eines Passwortes in ein temporäres Verzeichnis geschrieben. Eine Auswahl für ein Zielverzeichnis ist dann nicht möglich, es wird stattdessen der Schriftzug Installationsmodus (Kann übersetzt werden, siehe [Themen Editor](#)) angezeigt. Die Datei wird nach dem Entschlüsseln gestartet.

Falls es sich bei der gewählten Datei nicht um eine ausführbare Datei handelt oder die Option **Installer erstellen** nicht ausgewählt wurde, kann der Nutzer den Zielpfad frei wählen. Nach dem Entschlüsseln werden ausführbare Dateien normal gestartet, Datendateien werden nach Möglichkeit mit einer Anwendung geöffnet, die auf dem Zielrechner für diesen Datentyp verantwortlich ist.

8.2.2 Schritt 2 Thema - Information - Sprachnotiz - Abfrage

Thema festlegen



[Demo Video ArchiCryptX Change](#)

Legen Sie das **Aussehen** des Paketes mit einer Themendatei fest, machen Sie eine **Sprachnotiz**, definieren Sie eine **Abfrage** und legen Sie Text fest, der dem Nutzer weitergehende **Informationen** gibt.

Aktives Thema:

Hier können Sie →

Erläuternden Text eingeben
Legen Sie Text fest, der dem Nutzer weitergehende **Informationen** gibt. Der Text ist unverschlüsselt und wird beim Start des ArchiCryptX Change Paketes sofort angezeigt.

Eine Sprachnotiz anfügen
Falls Sie ein Mikrofon angeschlossen haben, können Sie dem ArchiCryptX Change Paket eine Sprachnotiz beifügen. Selbstverständlich können Sie auch bestehende Dateien im WAV Format anfügen.

Eine Frage formulieren
Die Frage wird dem Nutzer vor der Anzeige des eigentlichen Dialogs gestellt. Er kann die Frage mit Ja oder Nein beantworten. Wählt er Nein, beendet sich das ArchiCryptX Change Paket.

Information
Sprachnotiz
Abfrage

BITTE EIN THEMA LADEN

Themen-Editor starten Thema laden

Um ein Thema auszuwählen, klicken Sie auf die Grafik "**Bitte ein Thema laden**" oder auf die Schaltfläche "**Thema laden**". Wenn Sie ein eigenes Thema erstellen oder ein vorhandenes anpassen möchten, klicken Sie auf "**Themen-Editor starten**".

➔ **Anmerkung: Falls Sie keine Berechtigung zum Erstellen oder Anpassen von Themen haben, ist die Schaltfläche "Themen-Editor starten" nicht sichtbar.** (nur zutreffend für Professional und Enterprise Version)



Hinweis: Angaben wie Informationen, Sprachnotiz und Abfrage sind optional, können also auch entfallen!

Information

Aktives Thema:

BITTE EIN THEMA LA

Themen-Editor starten

Information

Text bearbeiten

UNVERSCHLÜSSELT: Wird beim Start des Dialogs abgezeigt. Sinnvoll um dem Nutzer Informationen zu übermitteln.
Optional - Kann entfallen!

Information
Sprachnotiz
Abfrage

Um einen Text einzugeben, der dem Nutzer des ArchiCryptX Change Paketes weitergehende **Informationen** gibt, bewegen Sie die Maus über die Registerseite

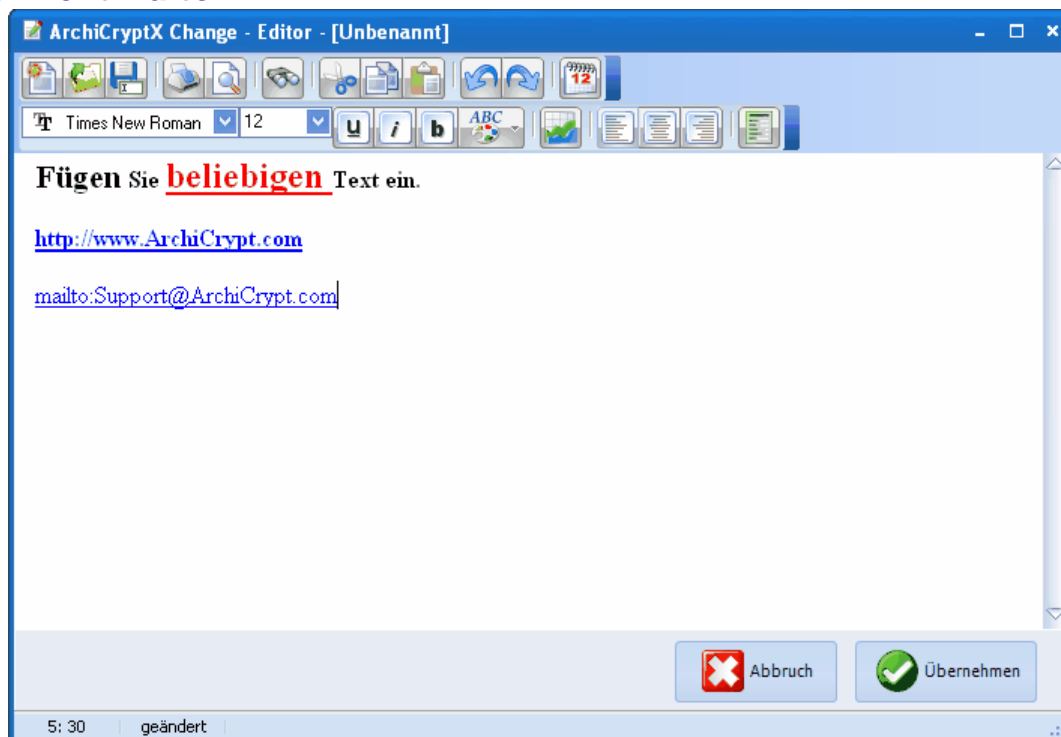
Information am linken Bildrand. Um Text einzugeben, klicken Sie bitte auf die Schaltfläche "**Text bearbeiten**". Es öffnet sich ein Texteditor.



TIPP: Der Text den Sie hier eingeben, ist unverschlüsselt und wird dem Nutzer bereits vor der Eingabe des Passwortes angezeigt. Nutzen Sie die Möglichkeiten, den Nutzer ggf. bei der Bedienung zu unterstützen.

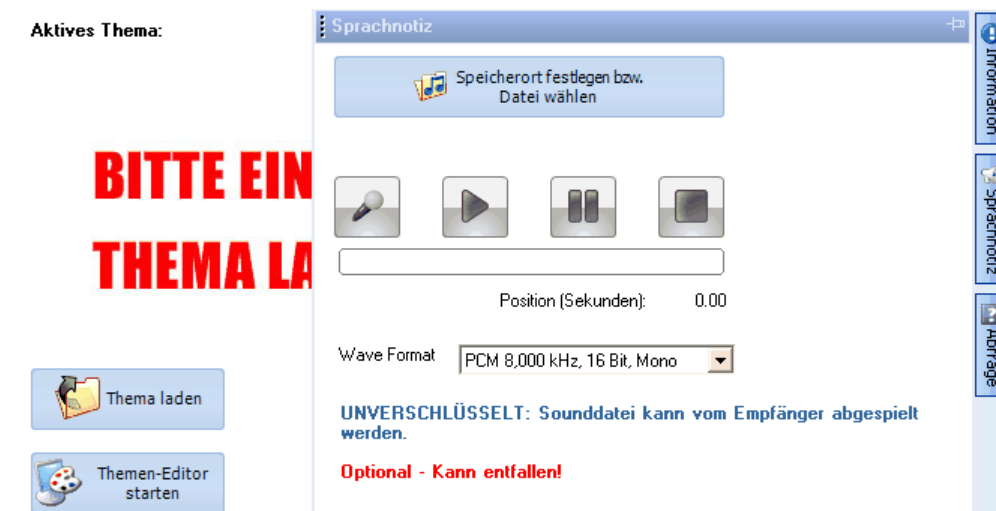
Sie können die Registerseiten "festpinnen", indem Sie auf das entsprechende Symbol klicken (markiert mit Pfeil oben).

Der Text Editor



Geben Sie den gewünschten Text ein oder laden Sie einen bereits vorhandenen Text. Bestätigen Sie Ihre Eingaben durch Betätigen der Schaltfläche **Übernehmen**.

Sprachnotiz

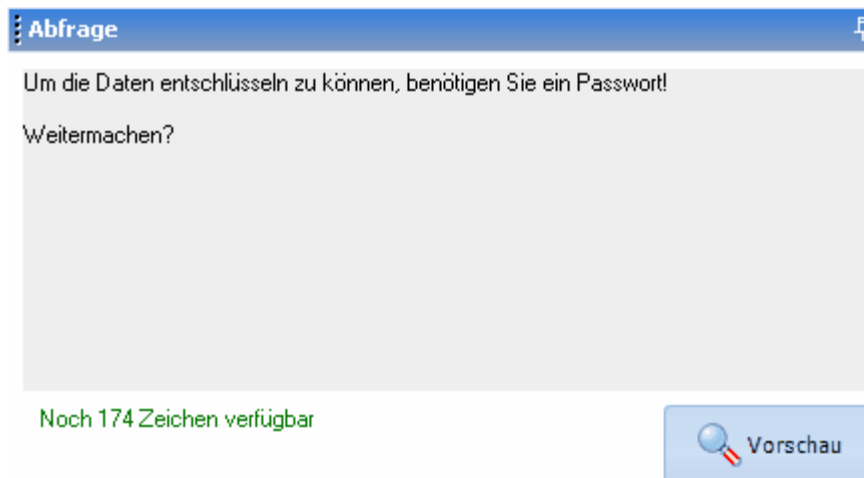


Sie können sowohl eine vorhandene Datei im WAV Format einbinden, als auch eine eigene Sprachnotiz aufzeichnen. Zum Aufzeichnen benötigen Sie ein Mikrofon!



Hinweis: Eine 1 minütige Sprachaufnahme mit 8KHz 16 Bit Mono (gute Sprachqualität) benötigt ca. 1 Megabyte Speicherplatz. ArchiCryptX Change verringert die Größe der Sprachnachricht um ca. 25% durch Kompression. Der Platzbedarf für unsere 1 minütige Beispieldatei liegt also bei ca. 750 KByte. Fassen Sie sich daher kurz!

Abfrage



UNVERSCHLÜSSELT: Erscheint als Frage, bevor der Dialog zur Entschlüsselung angezeigt wird. Falls die Frage mit Nein beantwortet wird, wird der eigentliche Dialog nicht angezeigt.

Optional - Kann leer bleiben!

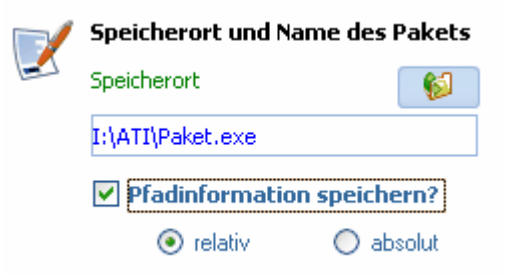
Geben Sie hier den Text für eine einfache **Ja/Nein Abfrage** ein. Die Frage wird dem Benutzer vor dem eigentlichen Dialog angezeigt. Beantwortet er die Frage mit Nein, wird der eigentliche Dialog nicht mehr angezeigt.

8.2.3 Schritt 3 Namen Mail Kompression

Name für das ArchiCryptX Change Paket festlegen



Demo Video ArchiCryptX Change



Speicherort

Klicken Sie auf die Schaltfläche



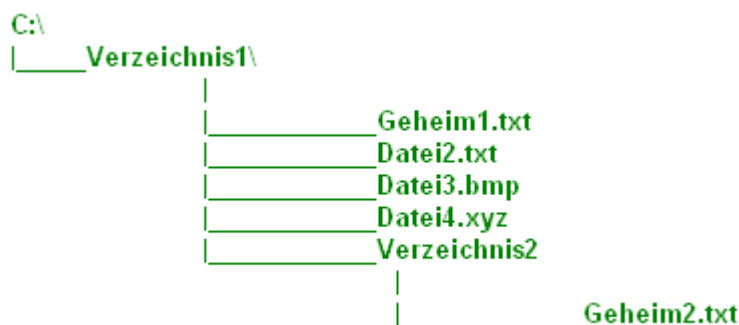
um den Windows Dialog zur [Auswahl eines Speicherortes](#) aufzurufen. Alternativ können Sie auf das Eingabefeld selbst klicken. Der Name der Datei wird immer so geändert/abgewandelt, dass er die Endung exe trägt (*Dateiendung für ausführbare Dateien*).

Pfadinformation speichern

Wenn Sie möchten, dass beim Entschlüsseln eine bestimmte Verzeichnisstruktur erzeugt wird, wählen Sie den Punkt [Pfadinformation speichern](#).

Erklärung zu relativ und absolut:

Angenommen Sie haben auf Ihrem System folgende Struktur:



Struktur auf Ihrem System

Sie packen jetzt die Dateien Geheim1.txt und Geheim2.txt in ein ArchiCryptX Change Paket. Werden keine Pfadangaben gespeichert, werden auf dem Zielrechner die

Dateien in 1 Verzeichnis entschlüsselt:

Normal:



Ohne Pfadinformationen

➔ **Info:** Wenn Sie Dateien gleichen Namens, die sich auf Ihrem System in unterschiedlichen Verzeichnissen befinden, ohne Pfadangaben in ein ArchiCryptX Change Paket packen, werden nicht alle Dateien entschlüsselt! Daher besser mit relativen Pfadangaben speichern.

Relativ:



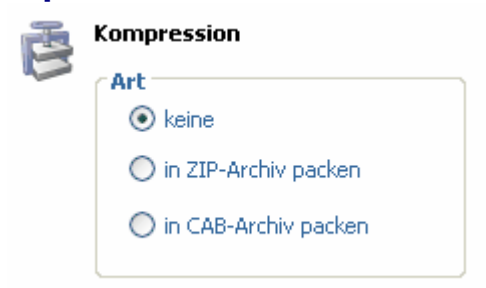
Mit relativen Pfadangaben

Absolut:



Absolute Pfadangaben

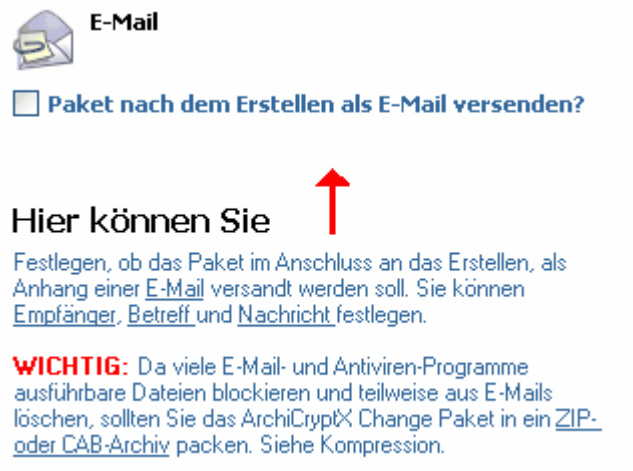
Kompression



Sofern Sie eine der Kompressionsarten aktiviert haben, wird Ihr ArchiCryptX Change Paket im Anschluss an den Erstellvorgang in ein entsprechendes Archiv gepackt. Sie erreichen durch die Kompression kaum eine Platzersparnis gegenüber dem reinen ArchiCryptX Change Paket, da XChange die Daten selbst bereits sehr gut komprimiert. Die Kompression ist jedoch für den Fall interessant, dass Sie das X Change Paket per E-Mail (ggf. auch per Download) weitergeben. Viele E-Mail Programme sperren automatisch Dateien mit bestimmten Dateiendungen. Dazu

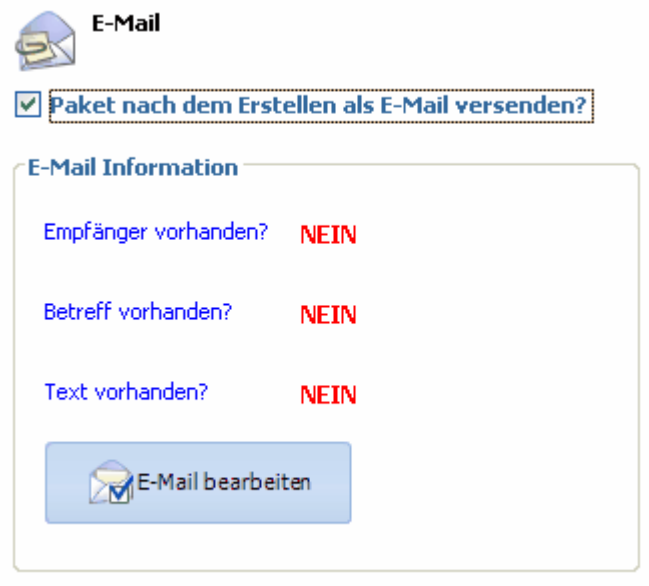
gehören insbesondere ausführbare Dateien (Endung exe). ZIP- und CAB-Archive werden zumeist unangetastet geladen.

E-Mail



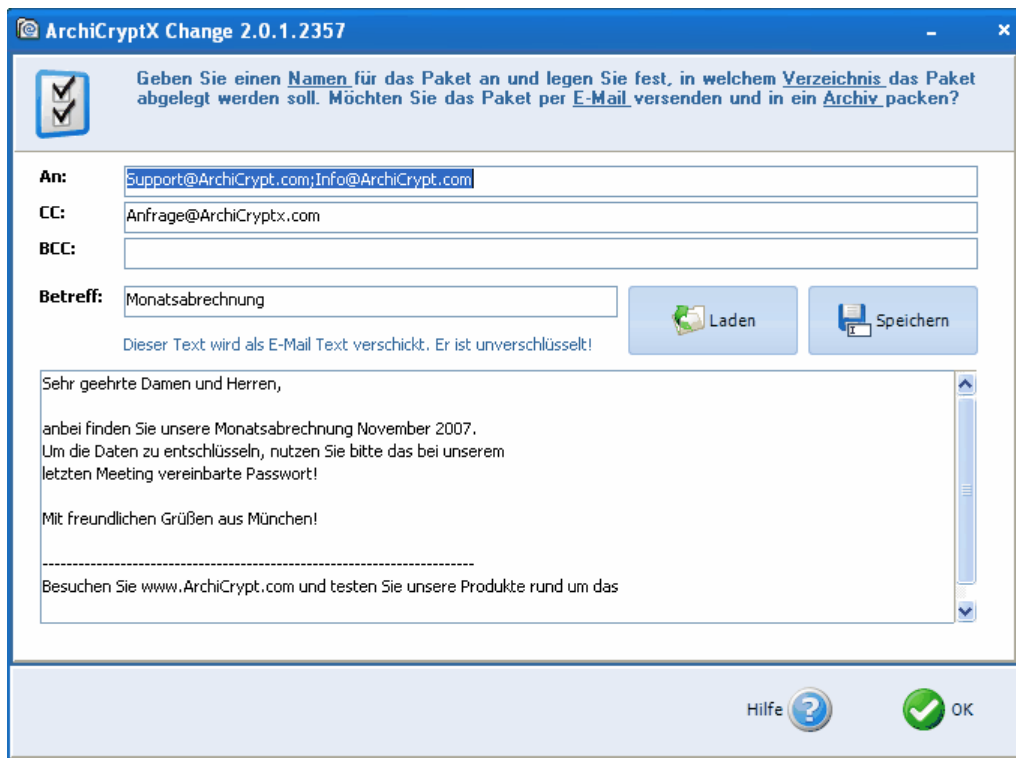
Sofern Sie das ArchiCryptX Change Paket nach dem Erstellen unmittelbar als E-Mail versenden möchten, können Sie die komplette E-Mail inkl. Text hier verfassen. Der Text, den Sie hier eingeben, wird unverschlüsselt als normaler E-Mailtext verschickt. Wenn Sie dem Empfänger vertrauliche Informationen zukommen lassen wollen, nutzen Sie den entsprechenden Editor im nächsten Schritt ([Vertrauliche Nachricht](#))!

Wählen Sie die Option "**Paket nach dem Erstellen als E-Mail versenden**" aus. Die Ansicht wechselt und Sie sehen die folgenden Daten:



Betätigen Sie jetzt die Schaltfläche **E-Mail bearbeiten**. Es wird ein Dialog zur Eingabe der E-Mail angezeigt.

Dialog zur Eingabe der E-Mail



The screenshot shows the 'ArchiCryptX Change 2.0.1.2357' application window. At the top, there is a header with a checkmark icon and the text: 'Geben Sie einen Namen für das Paket an und legen Sie fest, in welchem Verzeichnis das Paket abgelegt werden soll. Möchten Sie das Paket per E-Mail versenden und in ein Archiv packen?'. Below this, there are input fields for 'An:', 'CC:', 'BCC:', and 'Betreff:'. The 'An:' field contains 'Support@ArchiCrypt.com;Info@ArchiCrypt.com', 'CC:' contains 'Anfrage@ArchiCrypt.com', and 'Betreff:' contains 'Monatsabrechnung'. To the right of the 'Betreff:' field are two buttons: 'Laden' and 'Speichern'. Below the input fields, there is a note: 'Dieser Text wird als E-Mail Text verschickt. Er ist unverschlüsselt!'. The main text area contains the following content: 'Sehr geehrte Damen und Herren, anbei finden Sie unsere Monatsabrechnung November 2007. Um die Daten zu entschlüsseln, nutzen Sie bitte das bei unserem letzten Meeting vereinbarte Passwort! Mit freundlichen Grüßen aus München! ----- Besuchen Sie www.ArchiCrypt.com und testen Sie unsere Produkte rund um das'. At the bottom right of the window are buttons for 'Hilfe' (with a question mark icon) and 'OK' (with a checkmark icon).

Geben Sie die Empfänger ein, einen Betreff und den Text. Vor dem eigentlichen Senden wird Ihnen die Mail nochmals angezeigt!

Das Nutzen der E-Mail Funktion setzt voraus, dass Sie einen s.g. MAPI-fähigen E-Mail Client installiert haben (z.B. Outlook, Outlook Express, Thunderbird).



TIPP: Die Angaben bei E-Mail werden im Job gespeichert. Sie sollten hier möglichst statischen Text (Text, der sich nicht ändert) eingeben. Zum Beispiel einen Hinweis auf den Anhang.

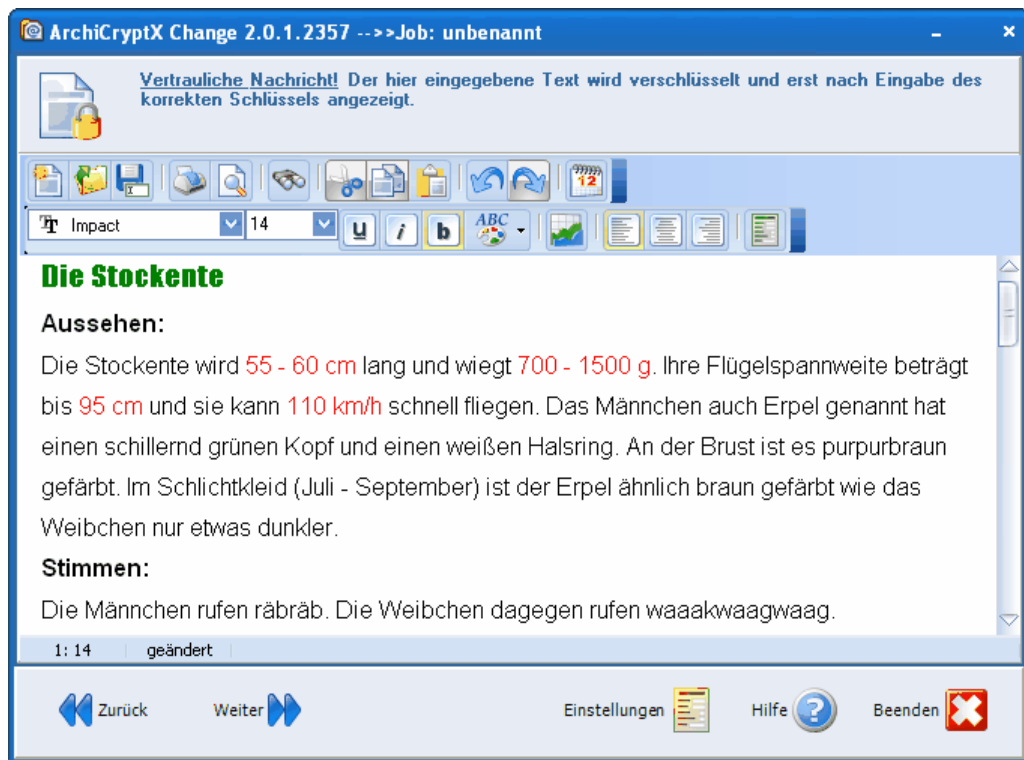
8.2.4 Schritt 4 Vertrauliche Nachricht

Vertrauliche Nachricht verfassen (Optional)



[Demo Video ArchiCryptX Change](#)

Der hier eingegebene Text wird verschlüsselt. Erst wenn der Empfänger/Nutzer das korrekte Passwort eingibt, wird der Text entschlüsselt und angezeigt. Um maximalen Platz für die Anzeige Ihrer Vertraulichen Nachricht verfügbar zu haben, organisiert das ArchiCryptX Change Paket nach Abschluss der Entschlüsselung aller Daten, die Bedienelemente um.



Beispiel:



Dialog gemäß gewähltem Thema vor der Entschlüsselung



Optimierter Dialog für Anzeige des verschlüsselten Textes nach Eingabe des korrekten Passwortes



TIPP nur vertrauliche Nachricht: Falls Sie Ihrem Gegenüber keine Daten, sondern nur eine vertrauliche Nachricht übermitteln wollen, erstellen Sie sich eine leere Datei (0 Byte groß) und speichern Sie die Einstellungen nach dem ersten Erstellen als JOB-Datei ab.

8.2.5 Schritt 5 Passwort

Passwort festlegen



[Demo Video ArchiCryptX Change](#)

Passwort Eingabe (Enterprise Version)

Geben Sie das gewünschte Passwort ein oder nutzen Sie den [Passwortgenerator](#)



um sich ein geeignetes Passwort generieren zu lassen. Das Passwort muss im

Falle der manuellen Eingabe 2 Mal eingegeben werden um Tippfehler auszuschließen.

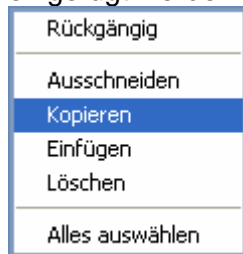
Sind Sie nicht alleine und befürchten, dass jemand Sie bei der Eingabe des Passwortes beobachtet, schalten Sie die Passworteingabefelder in den verdeckten Modus.



Weitergabe erzeugter Passwörter (Export von Passwörtern)

Das Passwort (insbesondere solche, die mit dem Passwortgenerator erstellt wurden), müssen Sie sich merken. Um das Passwort aus ArchiCryptX Change zu exportieren, gibt es 3 Möglichkeiten:

1. Passwort markieren, rechte Maustaste betätigen, kopieren wählen. Das Passwort befindet sich jetzt in der Zwischenablage und kann in andere Anwendungen eingefügt werden.



2. Passwort über das Betätigen der Schaltfläche in die Zwischenablage kopieren.



3. Passwort durch betätigen der Schaltfläche als Textdatei abspeichern.



Wenn Sie ein Passwort weitergeben möchten können Sie das Passwort in einer separaten E-Mail (niemals zusammen mit dem XChange Paket) an den Nutzer des Pakets senden. Exportieren Sie das Passwort in die Zwischenablage und von dort in Ihr E-Mail Programm.

Eine E-Mail könnte zum Beispiel so aussehen:

Sehr geehrter Herr,

wir werden künftig häufiger Daten austauschen, die nicht für Unbefugte gedacht sind. Ich werde Ihnen daher sensible Dokumente immer als XChange Paket übersenden. Es handelt sich dabei um Windows Anwendungen, die sensible Daten Huckepack verschlüsselt mit sich führen.

Die Bedienung ist sehr einfach. Starten Sie die Anwendung die im Archiv der jeweiligen E-Mail enthalten ist. Kopieren Sie den komplette Text

dieser E-Mail in die Zwischenablage
(Alles markieren, rechte Maustaste und Eintrag "Kopieren" auswählen).

Klicken Sie dann im XChange Paket auf "Import" und anschließend auf "OK".
Die Daten werden dann entschlüsselt.

[luk]123456789[/luk]

Mit freundlichen Grüßen

➔ **WICHTIG:** Das *eigentliche* Passwort steht zwischen den Begrenzern *[luk]* und */[luk]*
Dies ist zwingend notwendig, damit das XChange Paket das Passwort extrahieren kann!
Wenn Sie das Passwort manuell in die E-Mail einfügen, sollten Sie die Begrenzer ebenfalls einfügen, da der Empfänger ansonsten das Passwort nicht importieren kann, sondern manuell eingeben muss.

Import von Passwörtern

Um bereits vorhandene Passwörter zu importieren, stehen Ihnen wiederum 2 Möglichkeiten zur Verfügung

1. Import aus der Zwischenablage



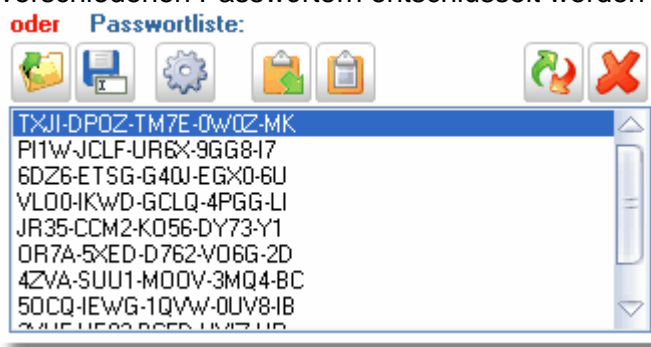
2. Import aus einer Datei



Passwortliste (Multi-Passwort Pakete)

(nur Professional und Enterprise Version)

Sowohl Professional als auch die Enterprise Version verfügen über die Fähigkeit, ein ArchiCryptX Change Paket so zu erstellen, dass die sensiblen Daten mit bis zu 100 verschiedenen Passwörtern entschlüsselt werden können.



➔ **Anmerkung:** Gibt es Einträge in der Passwortliste, werden Werte im **Passworteingabefeld** ignoriert!

Wozu diese Funktion?

1. Falls ein Passwort bewusst oder unbewusst weitergegeben wird, können Sie es aus der Liste entfernen und das ArchiCryptX Change Paket erneut verschlüsseln.
2. Wenn Sie in regelmäßigen Abständen sensible Daten an einen sich ständig ändernden Personenkreis verteilen, können Sie die Daten für bestimmte Nutzer im Bedarfsfall löschen.

Internet-Kontrollskript

(nur Enterprise Version)

In der Enterprise Version stehen Ihnen 2 Grundsätzliche Schablonen für Themen zur Verfügung. Schablonen vom Typ A erfordern auf der Empfängerseite lediglich die Eingabe eines Passwortes.

Die Schablone vom Typ B (Internet-Schablone) sieht die Eingabe einer Nutzerkennung und eines Passwortes vor. ArchiCryptX Change nimmt dann Verbindung zum Internet Kontrollskript (WEB Access Skript) auf. Damit das ArchiCryptX Change Paket weiß, wo dieses Skript zu finden ist, müssen Sie beim Erstellen die Internetadresse eingeben.

Steuerung über Internet (ArchiCrypt WEB Access Manager)

Url:

ArchiCryptX Change prüft bei der Eingabe lediglich, ob es sich der Form nach um eine gültige Internetadresse handelt. Stellen Sie also bitte sicher, dass das Skript tatsächlich unter der Adresse zu finden ist.

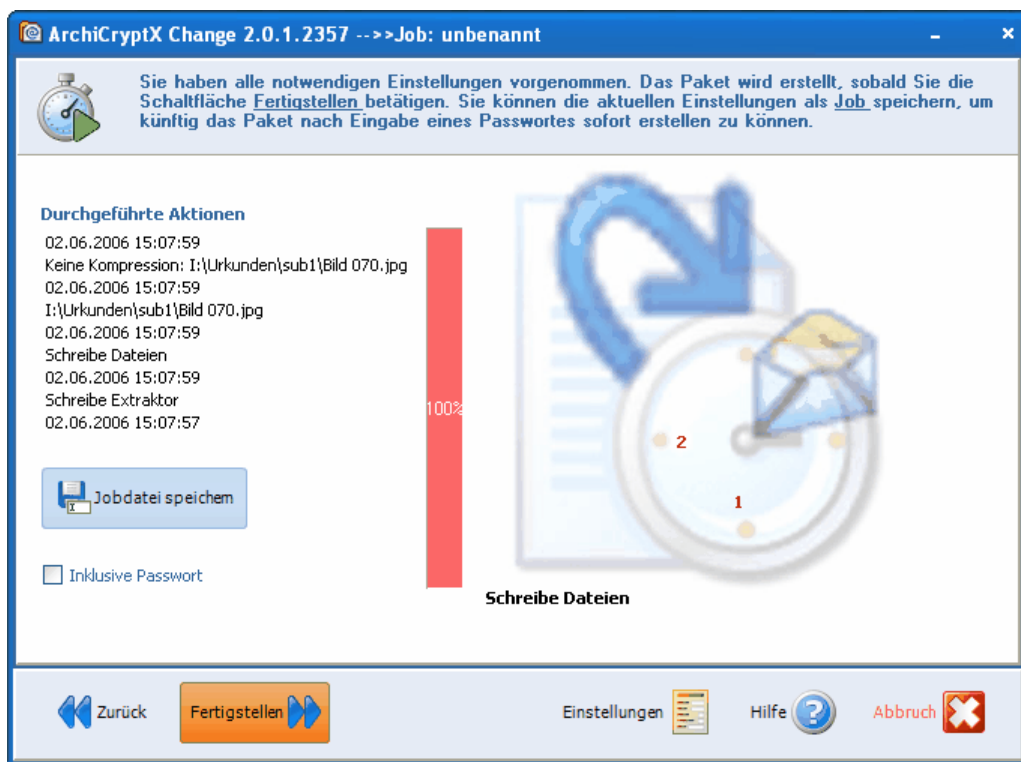
Die hier einzugebende Adresse legen Sie im WEB Access Manager fest. (siehe [Adresse des Internet-Kontrollskripts](#))

8.2.6 Schritt 6 Erstellen des Pakets

Erstellen des ArchiCryptX Change Pakets



[Demo Video ArchiCryptX Change](#)



Fertigstellen (Erstellen des Pakets)

Betätigen Sie die Schaltfläche "**Fertigstellen**" um den Erstellvorgang zu starten.

Testen (Testen des Pakets)

Nachdem der Erstellvorgang beendet wurde, können das XChange Paket testen (Schaltfläche **Testen**).

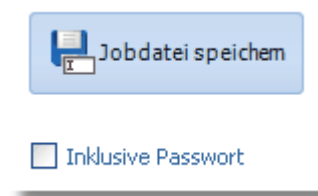
Mit der Schaltfläche **Neu starten** können Sie zum Punkt "[Dateien festlegen](#)" springen.



Die Schaltfläche Testen erscheint nicht, wenn Sie das Paket als E-Mail versenden.

Jobdatei speichern

Wenn Sie häufiger die gleichen Dateien mit gleichen Einstellungen in ein ArchiCryptX Change Paket packen möchten, sollten Sie eine s.g. Job-Datei speichern. Bei Bedarf können Sie die Job-Datei inkl. Passwort bzw. Passwortliste abspeichern und so beim nächsten Laden des Jobs sofort das ArchiCryptX Change Paket erstellen.





TIPP: Auch wenn Sie nicht immer genau diese Daten in ein Paket packen, kann es unter Umständen sinnvoll sein, die Einstellungen als Job zu sichern. Nach dem Laden eines Jobs können Sie zu jedem Punkt zurückkehren und Änderungen vornehmen.

8.3 Kommandozeilenparameter

8.3.1 ArchiCryptX Change

Wenn Sie in Ihrem Dateisystem auf eine **Job-Datei** doppelklicken, startet ArchiCryptX Change automatisch und lädt die Job Datei.

Mögliche Parameter beim Start von ArchiCryptX Change

Vorbemerkung

Startet ein Nutzer zum ersten Mal ArchiCryptX Change, werden alle Themendateien aus dem Unterverzeichnis Themes des Installationsverzeichnis in ein Nutzerspezifisches Verzeichnis (%userprofile%\Anwendungsdaten\ArchiCryptSDF2) kopiert.

Möchten Sie diesen Vorgang zu einem späteren Zeitpunkt wiederholen, können Sie ArchiCryptX Change mit dem Schalter **/CT** starten. Vorhandene, gleichnamige Themendateien werden dabei überschrieben.

8.3.2 ArchiCryptX Change Paket

Auch **ArchiCryptX Change Pakete** können mit verschiedenen **Kommandoschaltern** gestartet werden:

Schalter werden durch das Zeichen / oder das Minuszeichen - eingeleitet. Unter manchen Systemen führt das Zeichen / dazu, dass die Kommandozeile nicht erkannt wird. Nutzen Sie daher das Minuszeichen!

Schalter Passwort /p oder -p

Übergeben Sie hinter dem Schalter das Passwort in Hochkomma eingeschlossen

Bsp.:

/p "MeinPasswort"

Schalter Nutzerkennung /u oder -u

Übergeben Sie hinter dem Schalter die Nutzerkennung in Hochkomma eingeschlossen (nur erforderlich, falls Sie die Internet Schablone nutzen, Enterprise-Version).

Bsp.:

/u "Meine Nutzerkennung"

Schalter Zielverzeichnis /t oder -t

Übergeben Sie hinter dem Schalter das Zielverzeichnis in Hochkomma eingeschlossen

Bsp.:

/t "I:\Meine wichtigen Dateien"

Schalter Execute /e oder -e

Falls das Paket eine Datei enthält, die nach dem entschlüsseln ausgeführt werden soll, bewirkt der Schalter, dass die Datei ausgeführt wird. Das Weglassen unterdrückt entsprechend die Ausführung.

Schalter Open /o oder -o

Der Schalter bewirkt, dass nach dem entschlüsseln ein Explorerfenster geöffnet wird, der die entschlüsselten Daten anzeigt. Das Weglassen unterdrückt das Verhalten.

Schalter Kontrolldatei /f oder -f

Übergeben Sie hinter dem Schalter den Pfad und Dateinamen zu einer Kontrolldatei an.

Bsp.:

/f "I:\XChangeControll.ini"

Eine Kontrolldatei ist eine Textdatei, die wie folgt aufgebaut ist:

```
[Params]
Password=Hier das Passwort angeben
UID=Hier ggf. die Nutzerkennung angeben
Target=Hier das Zielverzeichnis angeben
Execute=Hier eine 1 eintragen falls Sie möchten das eine ggf. enthaltene
Installerdatei nach dem Entschlüsseln ausgeführt wird.
Open=Hier eine 1 eintragen falls Sie möchten das ein Explorer Fenster den Inhalt
des Orders anzeigt, in dem die entschlüsselten Daten abgelegt wurden.
```

Eine gültige Kontrolldatei könnte wie folgt aussehen:

```
[Params]
Password=Thaugakjhs7897
Target=C:\Meine geheimen Daten\Excel\
```

Weitere Möglichkeit, Werte an ein ArchiCryptX Change Paket zu übergeben

Sofern Sie die Enterprise Version einsetzen und den Zugriff über eine Internet Kontrolldatei steuern, muss der Zugriff auf das Internet möglich sein. In manchen Firmen wird der Datenverkehr über einen **Proxy** realisiert. Um dem ArchiCryptX Change Paket die Parameter des Proxies zu übermitteln, erstellen Sie eine Datei mit Namen **sdfproxy.ini** und legen diese im gleichen Verzeichnis ab, in dem sich auch das ArchiCryptX Change Paket befindet.

Die Textdatei muss dabei wie folgt aufgebaut sein:

```
[Proxy]
Password=Passwort um auf Proxy zugreifen zu können
Username=Nutzername für Proxy
Port=Portnummer des Proxies
Address=Adresse des Proxies
```

Eine gültige sdfproxy.ini Datei könnte wie folgt aussehen:

```
[Proxy]
Password=MyProxyPass
```

```
UserName=MyProxyUserName  
Port=8081  
Address=192.168.0.3
```

8.3.3 SmallXChange

Kommandozeilenversion von SmallXChange

Die Kommandozeilenversion von ArchiCryptX Change erlaubt das automatische Erstellen s.g. ArchiCryptX Change Pakete. Sie ist daher ideal dazu geeignet, die Funktionalität in eigene Programme einzubinden oder Arbeitsabläufe zu automatisieren. Die Kommandozeilenversion ist Bestandteil der Professional und Enterprise Version.

Vorbemerkungen:

- **Schalter** werden durch das **Zeichen / oder das Minuszeichen -** eingeleitet. Unter manchen Systemen führt das Zeichen / dazu, dass die Kommandozeile nicht erkannt wird. **Nutzen Sie daher das Minuszeichen!**
- Hinter jedem Schalter **muss** ein s.g. **Parameter** stehen. Kein Schalter darf ohne Parameter aufgeführt werden!
- Parameter in der folgenden Beschreibung stehen innerhalb geschweifter Klammern. Diese Klammern dürfen Sie nicht mit angeben.
- **Pfadangaben** sollten immer innerhalb von Hochkommata angegeben werden ("C:\Meine Dateien"). Geben Sie am besten jeden Parameter innerhalb von Hochkommata an. Insbesondere dann, wenn innerhalb des Parameters Leerzeichen vorkommen.
- Zwischen Schalter und Parameter muss ein Leerzeichen sein.
- **Bestimmte Schalterkombinationen sind unlogisch** und werden mit einer Fehlermeldung quittiert. Es macht zum Beispiel keinen Sinn, dem Programm ein Passwort und gleichzeitig eine Passwortliste als Eingabegröße zu liefern.
- Die Kommandozeilenversion benötigt immer eine Themen-Datei (siehe Anmerkung zu **Schalter Thema**)
- **Dateien werden ohne Nachfrage überschrieben, achten Sie also darauf, dass Paket- und Passwortdateien zuvor gesichert werden müssen, wenn Sie diese noch benötigen!**

Schalter Job (Job):

/J {Jobdatei} oder **-J** {Jobdatei}

Wirkung:

Alle Einstellungen aus der Jobdatei werden von SmallXChange übernommen. Jobdateien können Sie mit ArchiCryptX Change erstellen. Wurde die Jobdatei mit Passwortdaten gespeichert, können Sie das Paket nur durch Angabe des Namens der Jobdatei erstellen lassen. Übergeben Sie zusätzlich Schalter, die sich auf Passwörter beziehen, (P,PL,PLS,PLL,GEN,GENS) werden im Job enthaltene Passwortdaten ignoriert!

Beispiele:

```
SXC2.exe -P "Gz77-KL90-gZz" -J "c:\Jobs\Kataloge.jsd"
```

```
SXC2.exe -J "c:\Jobs\Kataloge.jsd"
```

(Jobdatei muss Passwortdaten enthalten)

Schalter Thema (Theme):

/TH {Themendatei} oder **-TH** {Themendatei}

Wirkung:

Sie können den kompletten Dateinamen des Themas mit Pfad angeben, oder einfach die Bezeichnung. Falls Sie nur die Bezeichnung angeben, muss sich die Themendatei im Standardverzeichnis befinden!

Beispiel:

SXC2.exe -P "Gz77-KL90-gZz" -T "c:\Pakete\Katalog.exe" -SLR "c:\Archive\Kataloge\Katalogliste.txt" /TH "Black Art.tsd"

→ ACHTUNG:

SmallXChange benötigt immer eine Themendatei. Die Angabe kann dabei durch die Schalter /TH erfolgen, oder indirekt über eine Jobdatei (siehe Schalter /J). Eine weitere Möglichkeit besteht darin, im Themen-Editor eine Standardthemendatei festzulegen. Starten Sie dazu den Themen-Editor. Laden Sie die gewünschte Themen-Datei und betätigen Sie die Schaltfläche Standard. Von jetzt ab, wird dieses Thema verwendet, sofern Sie nicht explizit über den Schalter /TH oder /J ein anderes Thema festlegen!

Schalter Passwort (Password):

/P {Passwort} oder **-P** {Passwort}

Wirkung:

Der Parameter dient als Passwort für das zu erstellende Paket. Schließen Sie das Passwort ebenfalls in Hochkommata ein, wenn es die Zeichen / und - enthält!

Beispiel:

SXC2.exe -P "Gz77-KL90-gZz" -J "c:\Jobs\Katalog.jsd"

Schalter Passwortliste (Passwordlist):

/PL {Passwortdatei} oder **-PL** {Passwortdatei}

Wirkung:

ArchiCryptX Change lädt die hinter dem Schalter PL angegebene Textdatei. Jede Textzeile wird dabei als ein Passwort angesehen. Das zu erstellende Paket wird mit jedem dieser Passwörter erstellt. Dabei wird der Name der Zieldatei (des Paketes) mit der Nummer der Zeile erweitert, in der das zugehörige Passwort steht.

Beispiel:

SXC2.exe -PL "c:\Dokumente und Einstellungen\Passwortlisten\Passworte.txt" -J "c:\Jobs\Katalog.jsd"

Schalter Passwortliste mit Reportdatei (Passwordlist with Report):

/PLL {Passwortdatei} oder **-PLL** {Passwortdatei}

Wirkung:

Wie /PL zusätzlich wird eine Datei erstellt, in der die Paketnamen den zugehörigen Passwörtern gegenübergestellt sind.
Die Datei trägt den Namen des Pakets mit der Endung .PLL

Beispiel:

SXC2.exe -PLL "c:\Dokumente und Einstellungen\Passwortlisten\Passworte.txt" -J "c:\Jobs\Katalog.jsd"

Schalter Passwortliste, Einzeldatei (Passwordlist, single file):

/PLS {Passwortdatei} oder **-PLS** {Passwortdatei}

Wirkung:

ArchiCryptX Change lädt die hinter dem Schalter PLS angegebene Textdatei. Jede Textzeile wird dabei als ein Passwort angesehen. Es wird genau ein Paket so erstellt, dass es mit jedem in der Liste enthaltenen Passwort entschlüsselt werden kann. Es werden maximal 100 Passwörter berücksichtigt.

Beispiel:

SXC2.exe -PLS "c:\Dokumente und Einstellungen\Passwortlisten\Passworte.txt" -J "c:\Jobs\Katalog.jsd"

Schalter Generator (Generator):

/GEN {Passwortschalter} oder -GEN {Passwortschalter}

Der Parameter Passwortschalter selbst ist wieder aus einzelnen Schaltern aufgebaut. Zwischen den einzelnen Anteilen muss ein Komma (,) eingefügt werden!

N={Zahl} Anzahl an zu generierenden Passwörtern

C={Zahl} Aus wie vielen Zeichen soll das Passwort aufgebaut sein?

SA={Zahl} Angabe, alle wie viele Zeichen der Separator - in das Passwort eingefügt werden soll

UD={Zeichenvorrat} Zeichen aus denen das oder die Passwörter aufgebaut werden sollen

P= [n|B|b|S|u] legt den Aufbau des Passwortes fest.

n gibt an, dass das Passwort Zahlen enthalten soll

B Großbuchstaben

b Kleinbuchstaben

S Sonderzeichen

u gibt an, dass das Passwort aus den mittels UD übergebenen Zeichen aufgebaut werden soll.

APP={Pfad} Qualifizierter Pfad einer Datei zur Aufnahme der erzeugten Passwörter; der Schalter ist optional

Mit dem Schalter APP ist es möglich, alle erzeugten Passwortdaten in einer zentralen Datei abzulegen.

Geben Sie dazu in der Parameterfolge für /gen das Schlüsselwort APP= an und fügen Sie den Dateinamen an, in dem die Passwortdaten abgelegt werden sollen. Existiert die Datei noch nicht, wird sie erstellt. Ist sie bereits vorhanden, werden die neuen Daten an die Datei angehängt. Wird der Parameter n mit 1 angegeben, erhält die Zieldatei den im Schalter /T angegebenen Dateinamen. Ist n > 1, werden die resultierenden Dateien nach dem Muster Name1.exe, Name2.exe, Name3.exe usw. benannt. Existieren gleichnamige Dateien, werden diese ohne Rückfrage überschrieben! Wenn Sie den Schalter weglassen, wird eine Datei mit dem Paketnamen und der Endung pll erstellt.

Wirkung:

SmallXChange generiert nach Ihren Vorgaben entsprechende Passwörter. Die Anzahl richtet sich nach der hinter N= angegebenen Zahl. Diese Zahl legt gleichzeitig fest, wie viele Pakete erstellt werden sollen. Die Pakete werden nach Ihren Vorgaben benannt, erhalten jedoch zusätzlich eine Zahl hinter dem Namen (z.B. Katalog1.exe). Beim Erstellen wird eine Liste mit dem Namen des Paketes und der Endung pll erstellt, in der jedem Paket das zugehörige Passwort gegenübergestellt ist. Eine andere Art der Passwortverwaltung entsteht, wenn der Schalter APP= genutzt wird.

Beispiel:Beispiele für den /gen Schalter

Sie möchten 5 Pakete erstellen, die alle mit einem Passwort verschlüsselt werden sollen,

welches aus 12 Ziffern besteht. Um bessere Lesbarkeit zu gewährleisten, soll alle 4 Ziffern ein Bindestrich (-) eingefügt werden.

-gen n=5,c=12,SA=4,P=n

Als Resultat werden Passwörter der folgenden Art erzeugt.

```
1737-9391-7784
2723-4119-2882
8099-9878-1003
3204-2527-0927
4920-8924-3548
```

Beispiel für APP= Schalter

/S "C:\Dokument.txt" /T "C:\Secret.exe" /gen n=1,C=12,SA=4,P=n,App=C:\Passwords.txt

Die Quelldatei C:\Dokument.txt wird mit einem automatisch generierten Passwort verschlüsselt. Die resultierende Datei wird als C:\Secret.exe abgelegt. Das generierte Passwort wird in die Datei Passwords.txt geschrieben. Bereits enthaltene Passwörter bleiben dabei erhalten.

Beispiel für nutzerdefinierten Zeichenvorrat:

Sie möchten 5 Pakete erstellen, die mit Passwörtern entschlüsselbar sind, die ausschließlich aus dem Zeichenvorrat ABCDEFGHIJKLMNOPQRSTUVWXYZ aufgebaut sind.

**/S "C:\Dokument.txt" /T "C:\Secret.exe" /gen n=5,C=12,SA=4,P=u,
UD=ABCDEFGHIJKLMNOPQRSTUVWXYZ,App=C:\Passwords.txt**

Als Resultat werden Passwörter der folgenden Art erzeugt:
CFFG-VAQQ-HIKL

...
...
...

Schalter Generator, Einzeldatei (Generator, Single File):

/GENS {Passwortschalter} oder **-GENS** {Passwortschalter}

Wie Schalter GEN, jedoch wird nur 1 ArchiCryptX Change Paket erstellt, welches mit den erzeugten Passwörtern entschlüsselt werden kann. Maximal werden 100 Passwörter genutzt. Die Passwörter werden im Zielverzeichnis des Pakets als Datei mit dem Namen des Pakets und der Dateiendung pwl abgelegt.

Beispiel:

-gens n=150,c=12,SA=4,P=u,UD=ABCDEFG -T "I:\Wumpel.exe" -S "I:\280506.txt"

Erzeugt trotz n=150 nur 100 Passwörter der Länge 12 Zeichen aus dem Zeichenvorrat ABCDEFG, trennt die Zeichen mit - in 4er Blöcke.

Resultierende Passwörter sehen wie folgt aus:

```
BEEG-FFBC-BFDE
FCAD-ACAC-AFAC
DBCF-ECCD-CAEC
FAED-EADF-EEAC
```

Die erzeugten Passwörter werden in der Datei I:\Wumpel.pwl abgelegt und können nach dem Erstellen weiter verwendet werden.

Schalter Ziel (Target):

/T {Paketname} oder **-T** {Paketname}

Wirkung:

Der Parameter gibt an, wo und unter welchem Namen SmallXChange das Paket ablegen soll.

Beispiel:

```
SXC2.exe -P "Gz77-KL90-gZz" -T "c:\Pakete\Katalog.exe" -S "c:\Archive\Katalog.zip"
```

Schalter Quelle (Source):

/S {Quelldateien oder Verzeichnisse} oder **-S** {Quelldateien oder Verzeichnisse}

Wirkung:

Der Parameter gibt an, welche Dateien in das Paket eingefügt werden sollen. Falls mehrere Dateien in das Paket sollen, trennen Sie die einzelnen Einträge durch einen Strichpunkt (Semikolon) ;

Um ganze Verzeichnisse in das Paket zu übernehmen, geben Sie einfach den Verzeichnisnamen an. Dateien aus Unterverzeichnissen bleiben unberücksichtigt. siehe Schalter SR und SRL

Beispiel:

```
SXC2.exe -P "Gz77-KL90-gZz" -T "c:\Pakete\Katalog.exe" -S "c:\Archive\Katalog.zip;C:\Beschreibungen\KatalogReadme.txt"
```

Schalter Quelle rekursiv (Source, recursive):

/SR {Quelldateien oder Verzeichnisse} oder **-SR** {Quelldateien oder Verzeichnisse}

Wirkung:

Wie Schalter /S allerdings werden bei Verzeichnissen auch alle Dateien aus Unterverzeichnissen rekursiv in das Paket eingefügt.

Beispiel:

```
SXC2.exe -P "Gz77-KL90-gZz" -T "c:\Pakete\Katalog.exe" -SR "c:\Archive\Kataloge"
```

Schalter Quellliste (Sourcelist):

/SL {Datei mit Quelldateien oder Verzeichnissen} oder **-SL** {Datei mit Quelldateien oder Verzeichnissen}

Wirkung:

Es wird die angegebene Textdatei geladen, die in den einzelnen Zeilen die Quelldateien und Verzeichnisse enthält. Inhalte von Unterverzeichnissen werden nicht übernommen. siehe Schalter SLR

Beispiel:

```
SXC2.exe -P "Gz77-KL90-gZz" -T "c:\Pakete\Katalog.exe" -SL "c:\Archive\Kataloge\Katalogliste.txt"
```

Schalter Quellliste rekursiv (Sourcelist, recursive):

/SLR {Datei mit Quelldateien oder Verzeichnissen} oder **-SLR** {Datei mit Quelldateien oder Verzeichnissen}

Wirkung:

Wie /SL jedoch werden bei Verzeichnissen auch Inhalte der Unterverzeichnisse berücksichtigt (rekursiv).

Beispiel:

```
SXC2.exe -P "Gz77-KL90-gZz" -T "c:\Pakete\Katalog.exe" -SLR "c:\Archive\Kataloge\Katalogliste.txt"
```

Schalter Kompression (Compression):

/C {Kompressionsart} oder **-C** {Kompressionsart} [zip|cab]

Wirkung:

Das Paket wird nach dem Erstellen in ein Zip- oder Cab-Archiv gepackt. Dies hat keine Auswirkung auf die Größe der Datei, da SmallXChange die Daten selbst bereits komprimiert. Das zusätzliche "Einpacken" dient lediglich dazu, einem Empfänger das Programm zustellen zu können, ohne dass ggf. Virenprogramme Alarm schlagen.

Beispiel:

SXC2.exe -P "Gz77-KL90-gZz" -T "c:\Pakete\Katalog.exe" -SLR "c:\Archive\Kataloge\Katalogliste.txt" **/C zip**

Schalter Abfrage (Text):

/TXT {Textdatei} oder **-TXT** {Textdatei}

Wirkung:

Die angegebene Textdatei wird als Nachricht eingebunden, die dem Benutzer vor dem eigentlichen Dialog angezeigt wird. Der Paketnutzer muss die Nachricht/Frage positiv beantworten (JA) um zum eigentlichen Paketdialog zu gelangen.

Beispiel:

SXC2.exe -P "Gz77-KL90-gZz" -T "c:\Pakete\Katalog.exe" -SLR "c:\Archive\Kataloge\Katalogliste.txt" -C zip **/TXT "C:\Abfrage.txt"**

Schalter Information (Richtext):

/RTF {Informationstextdatei} oder **-RTF** {Informationstextdatei}

Wirkung:

Die angegebene Textdatei wird im Dialog des Paketes selbst angezeigt. Die Datei muss dabei im RTF-Textformat (Richtext) vorliegen. Die RTF-Datei darf keine Bilder oder OLE-Objekte enthalten, da die Datei sonst nicht auf allen MS-Betriebssystemen angezeigt werden kann!

Beispiel:

SXC2.exe -P "Gz77-KL90-gZz" -T "c:\Pakete\Katalog.exe" -SLR "c:\Archive\Kataloge\Katalogliste.txt" -C zip **-RTF "C:\Hinweise.rtf"**

Schalter Vertrauliche Nachricht (Encrypted Richtext)

/ERTF {Richtextdatei} oder **-ERTF** {Richtextdatei}

Wirkung:

Die angegebene Textdatei wird im Dialog des Paketes angezeigt, nachdem die Daten mit Hilfe des eingegebenen Schlüssels entschlüsselt wurden. Die Datei muss dabei im RTF-Textformat (Richtext) vorliegen. Die RTF-Datei darf keine Bilder oder OLE-Objekte enthalten, da die Datei sonst nicht auf allen MS-Betriebssystemen angezeigt werden kann!

Beispiel:

SXC2.exe -P "Gz77-KL90-gZz" -T "c:\Pakete\Katalog.exe" -SLR "c:\Archive\Kataloge\Katalogliste.txt" -C zip -RTF "C:\Hinweise.rtf" **-ERTF "C:\VertraulicherText.rtf"**

Schalter Sprachnotiz (Wav-Datei)

/WAV {WAV-Datei} oder **-WAV** {WAV-Datei}

Wirkung:

Die angegebene WAV-Datei wird mit in das ArchiCryptX Change Paket übernommen. Im Dialog wird dem Nutzer eine Schaltfläche mit Lautsprecher angezeigt.

Beispiel:

SXC2.exe -P "Gz77-KL90-gZz" -T "c:\Pakete\Katalog.exe" -SLR "c:\Archive\Kataloge

`\Katalogliste.txt" /WAV "C:\Waves\Info_10.wav"`

Schalter Speichere Pfadangaben (Save Path-Info):

`/SP +` oder `-SP +`

Wirkung:

Bei allen Dateien werden die Pfadinformationen gespeichert und auf der Empfängerseite rekonstruiert.

Fehlt Schalter `/REL`, werden absolute Pfadangaben gespeichert.
siehe Schalter `/REL`

Beispiel:

`SXC2.exe -P "Gz77-KL90-gZz" -T "c:\Pakete\Katalog.exe" -SLR "c:\Archive\Kataloge\Katalogliste.txt" -C zip -TXT "C:\Abfrage.txt" -SP +`

Schalter Speichere Pfadangaben, relativ (Save Path-Info, relative):

`/REL +` oder `-REL +`

Nur Zusammen mit Schalter `SP`

Wirkung:

Bei allen Dateien werden die relativen Pfadinformationen gespeichert und auf der Empfängerseite rekonstruiert.

Beispiel:

`SXC2.exe -P "Gz77-KL90-gZz" -J "c:\Pakete\Katalog.jsd" -SP + -REL +`

Schalter Installationsmodus (Is Installer):

`/II +` oder `-II +` (I wie Igel)

Wirkung:

Nur zusammen mit dem Schalter `/EX` nutzbar (siehe unten). Die bei `/EX` angegebene Datei muss eine ausführbare Datei vom Typ Exe, Com oder Bat sein! Die angegebene Anwendung wird nach dem Entschlüsseln gestartet. Im Dialog besteht für den Nutzer keine Möglichkeit, einen Zielpfad zu wählen (Elemente sind ausgeblendet). Alle Dateien werden in das temporäre Verzeichnis entschlüsselt.

Beispiel:

`SXC2.exe -P "Gz77-KL90-gZz" -T "c:\Pakete\Katalog.exe" -SLR "c:\Archive\Kataloge\Katalogliste.txt" -II + -EX "C:\Installer.exe"`

Schalter Ausführen (Execute):

`/EX {Dateiname}` oder `-EX {Dateiname}`

Wirkung:

Dateiname muss eine Datei sein, die sich im Paket befindet und auf dem Zielrechner nach dem Entschlüsseln ausgeführt werden soll. Geben Sie als Dateiname den Pfad und Namen auf Ihrem System an. Dabei muss es sich nicht zwingend um eine ausführbare Datei handeln. Existiert auf dem Zielrechner eine Anwendung, die für die Bearbeitung der angegebenen Datei zuständig ist, wird diese Anwendung mit der Datei gestartet.

Beispiel:

`SXC2.exe -P "Gz77-KL90-gZz" -T "c:\Pakete\Katalog.exe" -SLR "c:\Archive\Kataloge\Katalogliste.txt" -EX "C:\Katalog\KatalogIndex.htm"`

Schalter Keine Kompression (No Compression):

`/NC {Dateiname}` oder `-NC {Dateiname}`

Wirkung:

Der Parameter muss auf eine Datei verweisen, die eine Liste mit Dateierendungen enthält. Dateien mit diesen Endungen werden beim Erstellvorgang nicht komprimiert. In jeder Zeile der Datei kann eine Datei benannt werden.

Z.B.

*.zip
*.rar
*.jpg

Beispiel:

```
SXC2.exe -P "Gz77-KL90-gZz" -T "c:\Pakete\Katalog.exe" -SLR "c:\Archive\Kataloge\Katalogliste.txt" -EX "C:\Katalog\KatalogIndex.htm" -NC "C:\Options\nocompress.txt"
```

Schalter Kein Dialog (Silent):

/SI + oder **-SI** +

Wirkung:

Es werden keine Meldungen und kein Dialog mehr angezeigt

Beispiel:

```
SXC2.exe -P "Gz77-KL90-gZz" -T "c:\Pakete\Katalog.exe" -SLR "c:\Archive\Kataloge\Katalogliste.txt" -EX "C:\Katalog\KatalogIndex.htm" -NC "C:\Options\nocompress.txt" -SI +
```

Schalter PHP Kontrolldatei (PHP)

/PHP {URL der PHP Kontrolldatei} oder **-PHP** {URL der PHP Kontrolldatei}

Wirkung:

Kontrolle des Entschlüsselungsvorgangs über das PHP Kontrollskript unter der angegebenen URL. Beachten Sie bitte, dass die Kontrolle via Internet nur mit der Enterprise Version möglich ist. Setzt Internet Schablone bei Thema voraus!

Beispiel:

```
SXC2.exe -P "Gz77-KL90-gZz" -T "c:\Pakete\Katalog.exe" -SLR "c:\Archive\Kataloge\Katalogliste.txt" -EX "C:\Katalog\KatalogIndex.htm" -NC "C:\Options\nocompress.txt" -SI + -PHP "http://www.MyDomain.com/control/MyControl.php"
```

Schalter Kommandodatei (Command File)

/COF {Dateiname Kommandodatei} oder **-COF** {Dateiname Kommandodatei}

Die Länge der Kommandozeile, die man an eine Anwendung übergeben kann ist auf einigen Systemen begrenzt, zudem lässt sich eine Kommandozeile wegen der Unübersichtlichkeit sehr schlecht bearbeiten und pflegen. SmallXChange unterstützt daher s.g. Kommandodateien. Eine Kommandodatei orientiert sich hinsichtlich Aufbau und Logik an der Kommandozeile.

Aufbau einer Kommandodatei

Kommandodateien sind Textdateien, die folgenden Aufbau haben (Angaben in spitzen Klammern sind Anmerkungen, die durch entsprechende Angaben zu ersetzen sind; Das Zeichen | steht für ODER):

[Job]

Name= <Pfad und Name der Job-Datei>

[Theme]

Name= <Pfad und Name der Themendatei oder nur Name, falls sich das Thema im Standardverzeichnis befindet>

[Password]
 Type=<P|PL|PLS|PLL|GEN|GENS>
 Specific=<Passwort selbst(P), Pfad zur Liste (PL, PLS, PLL) oder Generatoranweisung (GEN, GENS)>
 ;Beispiel:
 ;Type=gens
 ;Specific=n=150,c=12,SA=4,P=u,UD=ABCDEFG

[Source]
 Type=<S|SR|SL|SLR>
 Specific=<Pfad und oder Dateiname der Quelle oder einer Datei mit entsprechender Liste>
 ;Beispiel:
 ;Type=S
 ;Specific=l:\280506.txt

[Target]
 Name=<Pfad und Dateiname des zu erstellenden ArchiCrypX Change Pakets>

[ADDS]
 TXT= <Pfad + Name Textdatei mit Abfrage vor Anzeigen des Dialogs>
 RTF= <Pfad + Name Richtextdatei mit Informationen (unverschlüsselt)>
 ERTF= <Pfad + Name Richtextdatei mit Informationen (verschlüsselt)>
 WAV= <Pfad + Name Wave Datei (Sprachnotiz/Aufnahme)>

[PHP]
 URL=<Internetadresse des PHP Kontroll Skripts>
 ;ACHTUNG: Nur falls Themendatei= Internetschablone; Enterprise Version

[NC]
 Name=<Pfad zu Datei mit Liste nicht zu komprimierender Dateien>

[C]
 Type=<ZIP|CAB>
 ;Beispiel
 ;Type=CAB

[MISC]
 SI=+;Silent zeigt keinen Dialog
 SP=+;Speichert Pfadinformationen
 Rel=+;Speichert relative Pfadinformationen

[I]
 Ex=;Pfad + Name der auf dem Zielsystem auszuführenden Datei
 Il=+;Is Installer Datei hinter Ex muss Dateieindung Exe, com oder bat haben

➔Hinweis: *Löschen Sie jeweils die Anteile aus der jeweiligen Kommandodatei, die Sie nicht benötigen!*

Eine gültige Kommandodatei könnte wie folgt aussehen:

[Theme]
 Name=My Theme.tsd

[Password]
 Type=P
 Specific=Mein Super Passwort 1567521 hjialhd

[Source]
Type=S
Specific=C:\Meine zu übermittelnde Datei.dat

[Target]
Name=C:\Ziel\Paket.exe

[ADDS]
TXT= Sind Sie im Besitz des Passworts?
ERTF= C:\GeheimeBotschaft.rtf
WAV=C:\MeineSprachnachricht.wav

[MISC]
SP=+
Rel=+

[II]
Ex=C:\Meine zu übermittelnde Datei.dat

8.3.4 WEB Access Kommandozeilentool

Kommandozeilentool von ArchiCrypt WEB Access Manager

Das **Kommandozeilentool** erlaubt das Einbinden der WEB Access Manager Funktionen in eigene Arbeitsabläufe. Das Tool setzt eine bestehende Lizenzdatenbank voraus. Es muss mindestens der Schlüssel/das Passwort für das mit der Datenbank verwaltete XChange Paket vorhanden sein. Um die FTP-Upload Funktionen nutzen zu können, müssen Sie die Angaben zur [Lizenzkontrolldatenbank](#) gemacht haben.

Mit dem Tool können Sie aus eigenen oder vorhandenen Werten für Nutzerkennung und Nutzerschlüssel einen Notschlüssel erzeugen lassen, einen Eintrag mit sämtlichen Angaben in der Lizenzdatenbank erzeugen lassen und die zugehörige Lizenzkontrolldatenbank auf Ihrem WEB Server aktualisieren lassen.

Allgemeines

Schalter werden durch das Zeichen / oder das **Minuszeichen -** eingeleitet. Unter manchen Systemen führt das Zeichen / dazu, dass die Kommandozeile nicht erkannt wird. **Nutzen Sie daher das Minuszeichen!**

Bei Schaltern die einen zugehörigen Wert haben, ist der Wert durch ein = vom eigentlichen Schalter getrennt. Also **/Schalter=Wert**. Der Wert kann jeweils in Hochkommata eingeschlossen werden (**/Schalter="Mein Wert"**)

Fehlerprotokoll

Tritt bei einer Aktion ein Fehler auf, wird eine Logdatei **Error.log** (Textformat) angelegt. Die Datei ist, sofern Sie mit Hilfe des Schalters /T ein Zielverzeichnis angegeben haben in diesem Verzeichnis abgelegt, andernfalls im aktuellen Verzeichnis.

Schalter Masterkey

/MKEY=Masterkey

Der Schlüssel, mit dem das XChange Paket erstellt wurde.

Muss angegeben sein

Schalter User-ID

/UID=User-ID

Übergeben Sie hier eine User-ID. Diese User-ID kann bereits in der Datenbank (siehe Schalter DB) enthalten sein, Sie dürfen aber auch eine selbst generierte User-ID übergeben. Übergeben Sie eine User-ID, die bereits in der Lizenzdatenbank enthalten ist, werden die Daten überschrieben, ansonsten wird ein neuer Lizenzdatensatz erzeugt.

Muss angegeben sein

Schalter User-Key

/UKEY=Userkey

Der Nutzerschlüssel. Dieser Schlüssel kann selbst generiert sein.

Muss angegeben sein

Schalter Notschlüssel (Emergency)

/E

Es wird ein Notfallschlüssel erzeugt, mit dem ein entsprechendes XChange Paket auch ohne Verbindung zum Internet entschlüsselt werden kann. Der Notfallschlüssel in der mit /ET festgelegten Datei abgelegt. Wurde keine Zieldatei angegeben, wird der Notfallschlüssel im mit /T festgelegten Verzeichnis als Emergency.waf abgelegt. Falls Sie kein Zielverzeichnis angegeben haben, wird die Datei im aktuellen Verzeichnis erstellt. Der erzeugte Notschlüssel ist 1 Jahr gültig. Möchten Sie einen anderen Termin festlegen, nutzen Sie den Schalter /Exp

Eine so erzeugte Datei kann direkt an den Nutzer weitergegeben werden, der so mit Hilfe der Importfunktion des ArchiCryptX Change Pakets die Daten importieren kann.

Schalter Notschlüssel anhängen (Emergency Append)

/EA

Wie /E, existiert eine Datei bereits, wird der Notfallschlüssel angehängt.

Schalter kein Kopiermodus (no copy-mode)

/NC

Beim Speichern eines Notfallschlüssels, der aus User-ID und einem Nutzerschlüssel besteht, werden beide Werte in einer eigenen Zeile abgelegt. Der Nutzer muss diese Zeichen in die entsprechenden Eingabefelder des XChange Pakets eingeben. Die Importfunktion ist damit nicht möglich.

Anmerkung zu /E und /EA

Der erzeugte Notfallschlüssel wird in die Zeichen **[luid]/[luid][luk]/[luk]** eingebettet und kann so über die Importfunktion des ArchiCryptX Change Pakets importiert werden. Dieses Format ist auch dann nötig, wenn die Daten aus einer Lizenzdatei gelesen werden sollen.

Falls dies nicht gewünscht ist, nutzen Sie den Schalter /NC.

Schalter Notschlüssel Zieldatei

/ET=Zieldatei

Geben Sie hier den Dateinamen für die zu erzeugende Datei in der der Notschlüssel abgelegt wird.

Schalter Verfallsdatum (Expiration)

/Exp=Datum in der Form TT.MM.JJJJ

Beispiel:

/EXP=11.11.2010

Der erzeugte Lizenzdatensatz verfällt zum angegebenen Termin.

Die oben angeführten Schalter genügen, sofern Sie einen Notschlüssel erstellen möchten.

Beispiel:

/UID="Gulpi" /UKEY="Blinde Kuh" /MKEY="oluhaUZUZUGhgas" /T=I:\ /ET="I:\em.waf" /EA /EXP=11.11.2010

Erzeugt aus der User-ID (**/UID**) Gulpi, dem Nutzerschlüssel (**/UKEY**) Blinde Kuh und dem Masterkey (**/MKEY**) oluhaUZUZUGhgas ein Notfallpasswort(**/EA**).

Diese Daten werden in der Datei (**/ET**) I:\em.waf abgelegt. Existiert die Datei bereits, wird eine neue Zeile angehängt(**/EA**). Das Notfallpasswort ist bis 11.11.2010 gültig (**/EXP**). Ein Fehlerprotokoll wird ggf. im Verzeichnis I:\ mit Name error.log (**/T**) abgelegt.

Schalter Lizenzdatenbank

/DB=Dateiname der Lizenzdatenbank

Beispiel:

/DB="C:\DB für Internet\MeineDB.all"

Es wird ein Lizenzdatensatz für die übergebenen Daten UKEY, UID und MKEY erzeugt und in der Lizenzdatenbank abgelegt.

ACHTUNG: Benötigt immer Schalter /DBP

Schalter Passwort Lizenzdatenbank

/DBP=Passwort

Beispiel:

/DBP="Mein DB Passwort"

Beispiel:

/UID="Gulpi" /UKEY="Blinde Kuh" /MKEY="oluhaUZUZUGhgas" /DBP="123" /DB="C:\DB für Internet\MeineDB.all" /T=I:\ /EXP=11.11.2010

Erzeugt aus der User-ID (**/UID**) Gulpi, dem Nutzerschlüssel (**/UKEY**) Blinde Kuh und dem Masterkey (**/MKEY**) oluhaUZUZUGhgas einen Lizenzdatensatz und fügt diesen in die Datenbank (**/DB**) C:\DB für Internet\MeineDB.all, die mit dem Passwort 123 (**/DBP**)

"geschützt" ist ein. Die Lizenz ist bis 11.11.2010 gültig (**/EXP**). Die Lizenz ist nicht bockiert, das XChange Paket kann 2 Mal entschlüsselt werden. Ein Fehlerprotokoll wird ggf. im Verzeichnis I:\ mit Name error.log (**/T**) abgelegt.

Schalter Blocked

/B=Y oder **/B=N**

Falls Wert = Y, wird die Lizenz geblockt, falls N, nicht.

Schalter Anzahl Entschlüsselungen (Limit)

/L=Zahl

Mit dem Lizenzdatensatz kann das XChange Paket Zahl Mal entschlüsselt werden.

FTP spezifisch setzt Voraus, dass die Lizenzdatenbank entsprechende Einträge für [Lizenzkontrolldatenbank](#) enthält.

Schalter FTP Upload

/FTP

Benötigt mindestens die Schalter /Host, /FTPU, /FTPP

Upload der Lizenzkontrolldatenbank auf den WEB Server.

Schalter Host

/Host=Hostname

Schalter FTP Username

/FTPU=Username

Schalter FTP Passwort

/FTPP=Passwort

Beispiel:

/UID="Gulpi" /UKEY="Blinde Kuh" /MKEY="oluhaUZUZUGhgas" /DBP="123" /DB="C:\DB für Internet\MeineDB.all" /T=I:\ /EXP=11.11.2010 /FTP /Host=www.IhreDomain.com /FTPU=MeinUsername /FTPP=MeinPasswort

Erzeugt aus der User-ID (**/UID**) Gulpi, dem Nutzerschlüssel (**/UKEY**) Blinde Kuh und dem Masterkey (**/MKEY**) oluhaUZUZUGhgas einen Lizenzdatensatz und fügt diesen in die Datenbank (**/DB**) C:\DB für Internet\MeineDB.all, die mit dem Passwort 123 (**/DBP**) "geschützt" ist ein. Die Lizenz ist bis 11.11.2010 gültig (**/EXP**). Die Lizenz ist nicht bockiert, das XChange Paket kann 2 Mal entschlüsselt werden.

Die Lizenzkontrolldatenbank wird erzeugt und per FTP (**/FTP**) in das durch die Lizenzdatenbank festgelegte Verzeichnis und mit dem festgelegten Namen auf dem WEB Server gespeichert. Ein Fehlerprotokoll wird ggf. im Verzeichnis I:\ mit Name (**/T**) error.log abgelegt.

Nachfolgende Schalter hängen dem Lizenzdatensatz den entsprechenden Wert an!

Schalter Identifizierer

/ID=Identifizierer

Schalter Anrede

/Anr=Anrede

Schalter Firma

/Frm=Firma

Schalter Nachname

/Nn=Nachname

Schalter Vorname

/Vn=Vorname

Schalter Strasse

/Str=Strasse

Schalter Hausnummer

/HN=Hausnummer

Schalter PLZ

/PLZ=PLZ

Schalter Ort

/Ort=Ort

Schalter Email

/eml=Email

Schalter Telefon

/Tel=Telefonnummer

Schalter FAX

/Fax=Faxnummer

Schalter Titel

/ttl=Titel

Schalter Produkt

/Prd=Produkt

Schalter Anmerkung

/Anm=Anmerkung

Teil



9 Einstellungen ArchiCryptX Change

9.1 Allgemeines

siehe auch

[Einstellung Kompression](#)

[Einstellung Passworteigenschaften und Passwortgenerator](#)

[Einstellung Administrator](#)

Einstellungen Allgemeines

Start der Anwendung

Sie können nur genau eine oder keine der beiden Optionen "**Automatisch zuletzt aktiven Job laden**" oder "**Automatisch zuletzt aktive Themendatei**" laden auswählen.

Bei ausgewählter Option lädt ArchiCryptX Change beim Start die entsprechende Datei. Meist ist die Einstellung **Automatisch zuletzt aktive Themendatei laden** sinnvoll.

Beim Laden eines Jobs

Ein Job enthält viele Angaben, die ArchiCryptX Change zum Erstellen eines Pakets benötigt. Sofern Sie den Job inkl. Passwortdaten gespeichert haben, kann das Paket sofort erstellt werden. Oft möchte man jedoch bestimmte Angaben wie zum Beispiel die Vertrauliche Nachricht ändern. Hier können Sie XChange veranlassen, direkt zum jeweiligen Punkt zu springen.

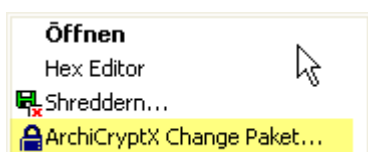
➔ **Wichtig: Eine Job-Datei enthält auch das Thema. Haben Sie mit Hilfe des Themen-Editors Änderungen an einem Thema vorgenommen, wirkt sich dies nicht auf ein Thema in einer Jobdatei aus. Sie müssen das geänderte Thema gesondert "nachladen"**

Aussehen:

Über Aussehen, **Gitternetzlinie bei Dateiliste anzeigen**, schalten Sie in der Liste bei Schritt 1 Gitternetzlinien ein bzw. aus.

Kontextmenü:

Mit dem Schalter **Kontextmenü im Windows Explorer anbieten**, machen Sie die Funktion ArchiCryptX Change Paket... im Windows Explorer verfügbar bzw. schalten diese ab.



Hilfe Anzeigedauer:

Hier können Sie die Anzeigedauer der Hilfe in ArchiCryptX Change ändern.

Dateien Speichern in (XChange Zentrale)

Geben Sie hier das Verzeichnis an, in dem ArchiCrypt X Change Job-Dateien, Passwortdateien, WAV-Dateien, Vertrauliche Nachrichten und Informationsdateien speichern soll.

➔ **ACHTUNG:** Falls Sie als keine Vorgabe machen, wird ein Unterverzeichnis XChange Zentrale im Verzeichnis Eigene Dateien des aktuellen Nutzers eingerichtet. Als Administrator sollten Sie bei einer Vorgabe bedenken, dass alle Nutzer auf diesen Pfad Zugriff haben müssen!

Über:

Informationen über ArchiCryptX Change

Auf Update prüfen:

Prüft, ob eine neuere Version verfügbar ist, lädt diese auf Wunsch.

9.2 Kompression

siehe auch

[Einstellung Allgemeines](#)

[Einstellung Passwortheigenschaften und Passwortgenerator](#)

[Einstellung Administrator](#)

[Schritt 3 Namen Mail Kompression](#)

Einstellungen Kompression

---->>> **Einstellungen Kompression**

Nachfolgende Dateien nicht komprimieren

(Einzelne Einträge durch Leerzeichen Trennen)

Hier können Sie festlegen, welche Dateien nicht komprimiert werden sollen. Viele Dateien liegen bereits in einem Format vor, welches kaum eine weitere Kompression zulässt. In diesem Fall entsteht sowohl bei der Erstellung des Pakets, als auch beim Entschlüsseln des Pakets unnötiger Zeitaufwand. Tragen Sie die Dateiendungen in das Eingabefeld getrennt durch LEERZEICHEN ein und aktivieren Sie die Option **Nachfolgende Dateien nicht komprimieren**.

9.3 Passwortheigenschaften und Passwortgenerator

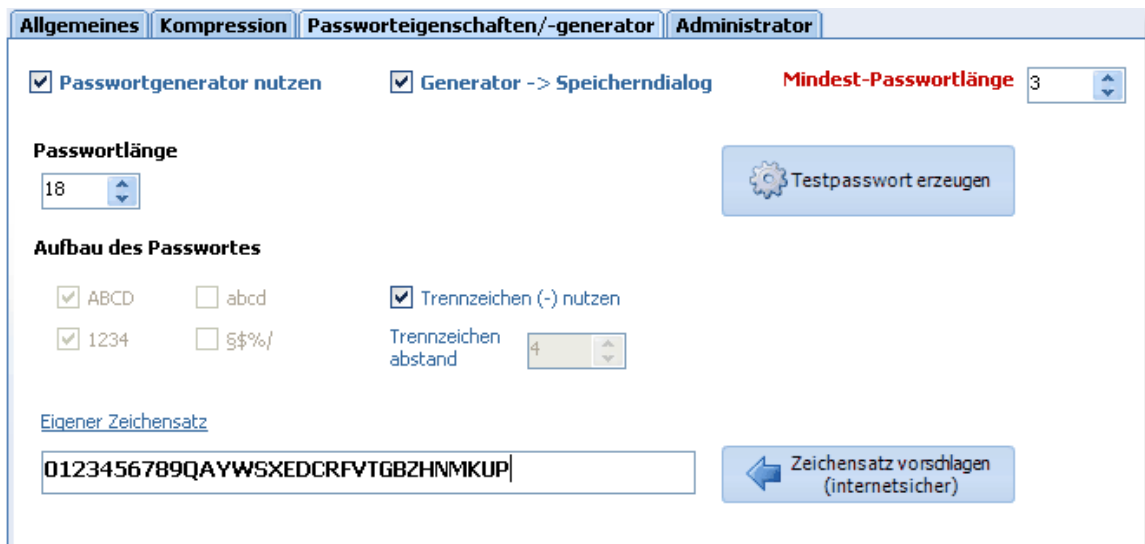
siehe auch

[Einstellung Allgemeines](#)

[Einstellung Kompression](#)

[Einstellung Administrator](#)

Der Passwortgenerator



Passwortgenerator nutzen

Der Generator erzeugt automatisch oder auf Anfrage Passwörter gemäß Ihren Vorgaben. siehe [Schritt 5 Passwort](#)

Zunächst können Sie die gewünschte Passwortlänge (**Mindest-Passwortlänge**) einstellen. Je länger das Passwort, desto sicherer.

Anschließend können Sie festlegen, wie das Passwort aufgebaut sein soll. Mit Hilfe des Trennzeichens (**Trennzeichen nutzen**) können Sie die **Lesbarkeit des Passworts** deutlich erhöhen. Sie machen damit demjenigen, der das Passwort ablesen/ eingeben muss, das Leben leichter.

Gerne können Sie die Passwörter auch aus den Elementen einer selbst definierten Zeichenmenge (**eigener Zeichensatz**) erstellen lassen.

→ Warnung: **Vorsicht, Sie erleichtern Angreifern das Leben erheblich, wenn Sie den Zeichenvorrat verringern, der für den Aufbau eines Passwortes herangezogen wird. Das gilt ausdrücklich auch für die Einschränkung durch Festlegung auf z.B. nur Großbuchstaben und Kleinbuchstaben!**

In obiger Abbildung ist ein Zeichensatz mit 32 Zeichen vorgegeben. Im ASCII Zeichensatz gibt es 256 Zeichen.

Angenommen, Sie haben ein 8 Zeichen langes Passwort mit dem ASCII Zeichensatz erstellt.

Es gibt dann

$$256 * 256 * 256 * 256 * 256 * 256 * 256 * 256 = 2^{64} =$$

$$18.446.744.073.709.551.616$$

verschiedene Passwörter der Länge 8 Zeichen, die man mit diesem Vorrat aufbauen kann.

Mit unserem auf 32 Zeichen begrenzten Vorrat können wir nur

$$32 * 32 * 32 * 32 * 32 * 32 * 32 * 32 = 2^{40}$$

$$1.099.511.627.776$$

verschiedene Passwörter erzeugen.

Die Anzahl möglicher Schlüssel ist anders ausgedrückt, bei der vollen Ausnutzung

der 256 Zeichen um den Faktor 16.777.216 (17 Millionen Mal mehr Passwörter) größer.

Viele Verschlüsselungsprogramme namhafter Hersteller haben in der Vergangenheit solche Verfahren angewandt. Einige wandelten Kleinbuchstaben grundsätzlich in Großbuchstaben, einige filterten Sonderzeichen oder kürzten das Passwort gar. Dies alles ohne Wissen des Nutzers.

➔ **Daher:**

Falls Sie einen eingeschränkten Zeichenvorrat nutzen, muss das Passwort mehr Zeichen umfassen, um annähernd die gleiche Sicherheit zu bieten, wie bei Nutzung des kompletten 256 Zeichen umfassenden Gesamtvorrats.

Nutzen wir z.B. nur 32 Zeichen, muss das Passwort statt 8 Zeichen, ca. 13 Zeichen umfassen. Nutzen wir nur Großbuchstaben, muss das Passwort ca. 14 Zeichen lang sein.

Generator -> Speicherdialog

Das vom Generator erzeugte Passwort müssen Sie sich merken. Bei ausgewählter Option bietet ArchiCryptX Change die Möglichkeit, nach dem Generieren sofort den Dialog für das Speichern des Passworts/der Passwortliste als Textdatei an.

Mindestpasswortlänge

Ein Passwort, welches den kompletten Zeichenvorrat des ASCII Zeichensatzes nutzt, sollte mindestens 8 Zeichen lang sein. Insbesondere Administratoren können durch diese Einstellung sicherstellen, dass ArchiCryptX Change Pakete mit Passwörtern einer vorgegebenen Mindestlänge erstellt werden.

siehe auch [Einstellungen Administrator](#)

9.4 Administrator

siehe auch

[Einstellung Allgemeines](#)

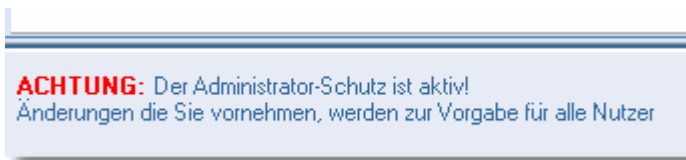
[Einstellung Kompression](#)

[Einstellung Passwortheigenschaften und Passwortgenerator](#)

Administrator-Schutz



Ab Professionalversion können Sie die Software rasch auf verschiedenen Client-Rechnern installieren und einrichten. Sobald er **Administrator-Schutz** aktiviert ist, können Nichtadministratoren keine Einstellungen mehr vornehmen. Die Einstellungen, die Sie als Administrator gemacht haben, gelten dann für alle Nutzer.



Sofern Sie unter [Einstellungen - Allgemeines](#) die Option "**Automatisch zuletzt aktive Themendatei laden**" aktiviert haben, wird das zuletzt durch den Nutzer geladene Thema herangezogen. Wenn Sie jedoch möchten, dass das von Ihnen aktuell vorgegebene Thema für alle Nutzer verbindlich ist, aktivieren Sie die Option "**Aktuelle Themen-Vorgabe überschreibt Nutzerauswahl**"

Import und Export von Einstellungen

Wenn Sie ArchiCryptX Change auf mehreren Rechnern mit gleichen Einstellung installieren müssen, nutzen Sie die **Import-** und **Exportfunktionen** für die Einstellungen. Richten Sie ArchiCryptX Change zunächst auf einem Rechner komplett ein und exportieren Sie diese Daten anschließend. Auf den weiteren Clients können Sie diese Einstellungen dann importieren.

➔WICHTIG:

Die Einstellungen und der Administratorschutz werden bei Verwendung der SmallXChange Version (Kommandozeilenversion) nicht berücksichtigt!!!



TIPP:

Wenn Sie nicht möchten, dass der Nutzer Themendateien editiert, entfernen Sie die Datei ACXEditor.exe aus dem Anwendungsverzeichnis von ArchiCryptX Change. Die Schaltfläche für den Themen-Editor wird dann nicht angezeigt.

Teil



10 Bedienung Themen-Editor

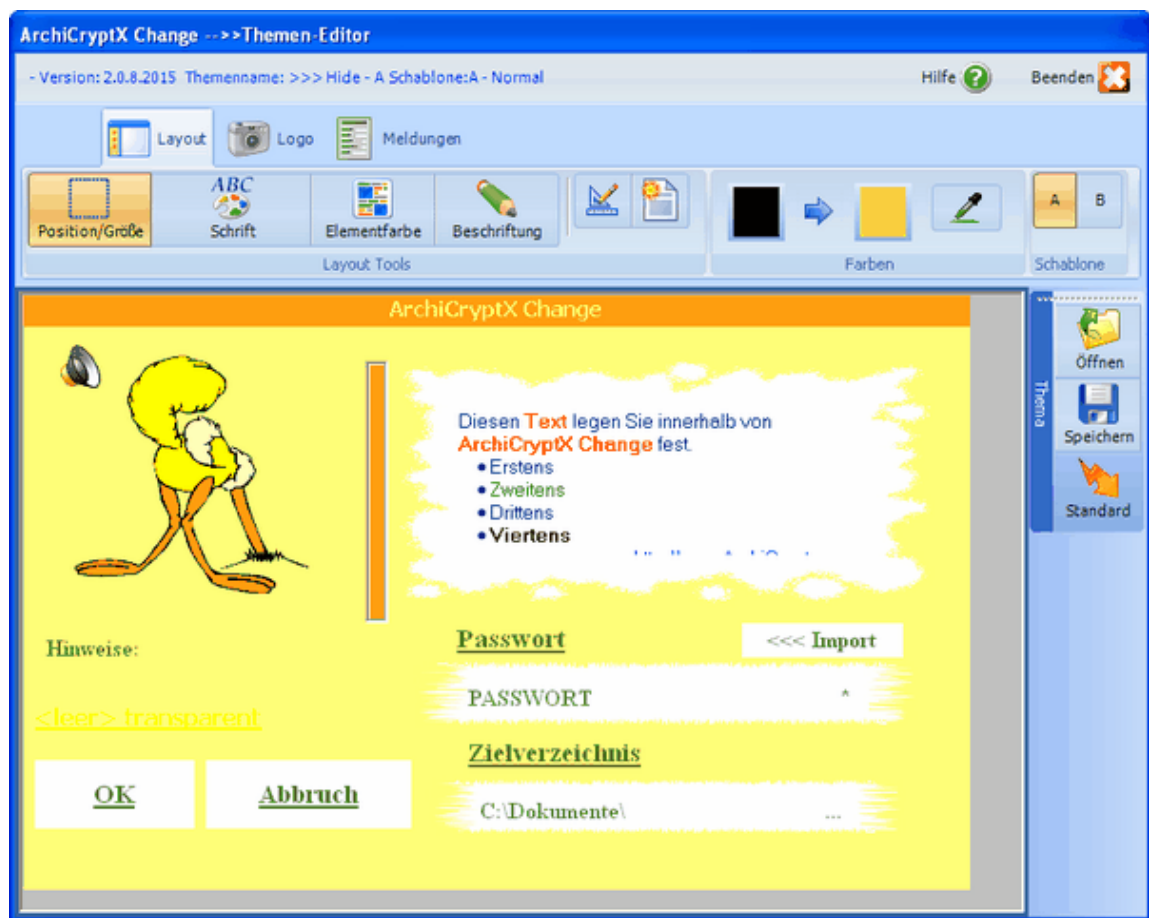
10.1 Übersicht

Der Themen Editor



[Demo Video ArchiCryptX Change](#)

Mit Hilfe des Themen-Editors können vorhandene Themen bearbeitet und neue Themen erstellt werden.

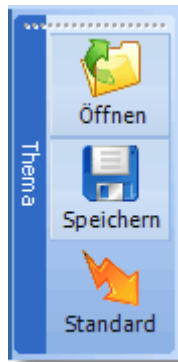


Der Themen-Editor ist in die 3 Rubriken

- [Layout](#)
- [Logo](#)
- [Meldungen](#)

unterteilt.

Die Menüleiste links bezieht sich auf das Thema.



Thema im Editor laden

Laden Sie ein vorhandenes Thema um darauf aufbauend ein neues Thema zu erstellen.



Thema speichern

Nachdem Sie ein Thema bearbeitet haben, speichern Sie es ab.



→ Anmerkung: Falls Sie die Professional oder die Enterprise Version nutzen, beachten Sie Folgendes:

Bei der Benennung sollten Sie das vorgegebene Schema beibehalten. Normale Schablonen (Typ A, nur Passwortabfrage, keine Nutzerkennung) sollten vor dem eigentlichen Namen die Bezeichnung A - tragen. Internet Kontrollschablonen (Abfrage der Nutzerkennung) sollten mit B - beginnen.

Thema als Standard definieren

An verschiedenen Stellen in ArchiCryptX Change, insbesondere bei SmallXChange (Bestandteil der Professional und Enterprise Version) kommt ein **Standard Thema** zum Einsatz, sofern nicht explizit ein anderes Thema angegeben/ausgewählt wurde. Mit dem Betätigen der Schaltfläche **Standard**



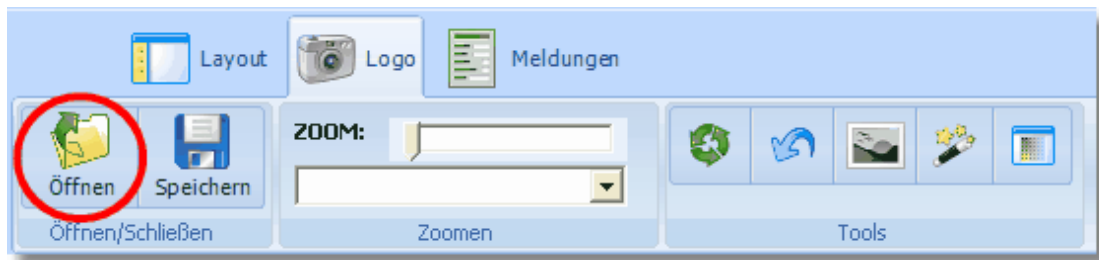
machen Sie das gerade aktive Thema im Editor zum Standard-Thema.

10.2 Erstellen eines Themas-Logo

Logo / Grafik für Thema wählen

Sofern Sie ein neues Thema erstellen möchten, empfiehlt es sich zumeist, ein bereits vorhandenes Thema zu laden und dies anzupassen.

Im ersten Schritt sollten Sie **ein Logo / eine Grafik laden**. Neben dem Laden sind keine weiteren Schritte notwendig.



Die Grafik sollte dabei nicht zu sehr von der Größe abweichen, die Sie im Thema haben soll.

Wechseln Sie jetzt zum [Layout](#)

Weitere Funktionen Logo / Grafik

Grafik speichern



An der Grafik vorgenommene Änderungen können Sie über die Schaltfläche Speichern sichern.

Größe der Grafik anpassen



Die Größe der Grafik können Sie an die vorgesehene Größe im Thema anpassen. Achten Sie darauf, dass die Originalgröße nicht zu sehr von der Größe im Thema abweicht.

Änderung rückgängig machen



Macht letzte Aktion rückgängig

Graustufenbild erzeugen

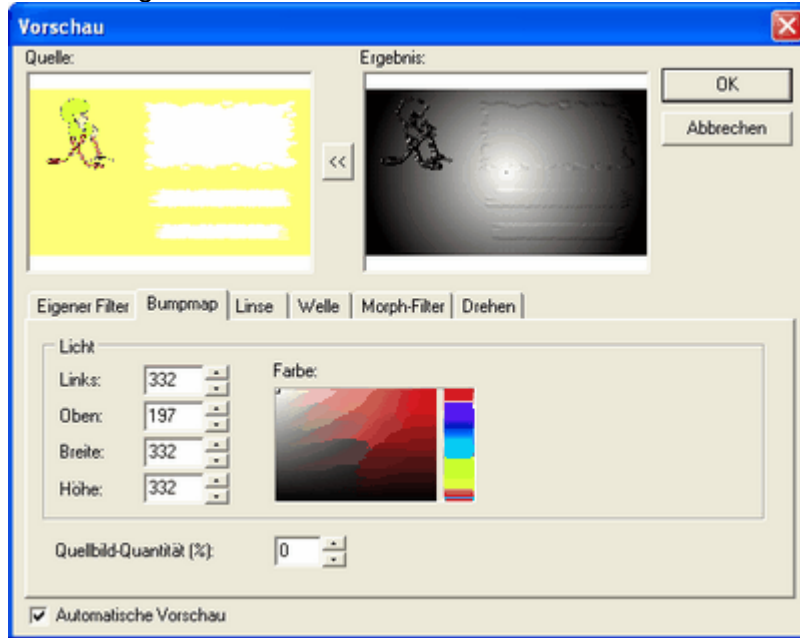


Wandelt die Grafik in ein Graustufenbild um

Effekte Dialog aufrufen



Ruft Dialog zur Auswahl verschiedener Effekte auf



Farbe / Sättigung ändern



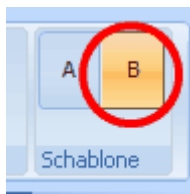
Ruft Dialog zur Auswahl von Farbe und Sättigung auf

10.3 Erstellen eines Themas-Layout

Nachdem Sie ein Logo/eine Grafik geladen haben, können Sie die Gestaltung des Dialogs angehen.

Schablone (nur Enterprise Version)

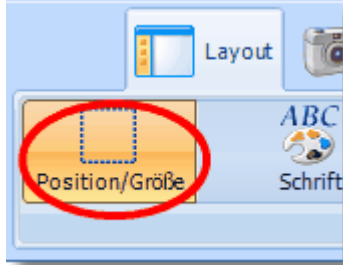
Falls Sie die Enterprise-Version einsetzen und das Entschlüsseln durch ein [Internet Kontrollskript](#) gesteuert werden soll, wählen Sie bitte die Schablone B aus:



Die nachfolgende Reihenfolge beim Erstellen oder Bearbeiten eines Layouts ist lediglich ein Vorschlag. Sie können die Arbeitsschritte in beliebiger Reihenfolge beliebig oft durchführen.

Position und Größe der Elemente

Jetzt sollten Sie **Position und Größe** der einzelnen Elemente festlegen.



Markieren Sie das gewünscht Element bis Sie die blauen Kästchen am Rand des Elements erkennen.



Um die Position des gewählten Elements zu ändern, klicken Sie mit der linken Maustaste auf eine Stelle innerhalb des durch die Kästchen festgelegten Rechtecks und halten Sie die Maustaste gedrückt. Ziehen Sie das Element jetzt mit gedrückter linker Maustaste an die gewünschte Position.

Um die Größe des gewählten Elements zu ändern, bewegen Sie den Mauszeiger über eines der Kästchen, bis sich dieser in ein Pfeilsymbol verwandelt. Drücken Sie dann die linke Maustaste und ändern Sie die Größe durch Ziehen bei gedrückter Maustaste.



TIPP- Auswahl aufheben: *Gelegentlich, insbesondere dann, wenn Sie eine große Grafik im Hintergrund haben, lässt sich die Auswahl nicht mehr auf ein Element im Vordergrund umschalten. Betätigen Sie dann die **ESC-Taste** um die Auswahl des aktiven Elements aufzuheben.*



TIPP - Feinpositionierung: *Um Elemente pixelgenau zu positionieren, markieren Sie das entsprechende Element, wie oben beschrieben. Betätigen Sie anschließend die **Pfeiltasten** auf Ihrer Tastatur um das Element zu bewegen.*

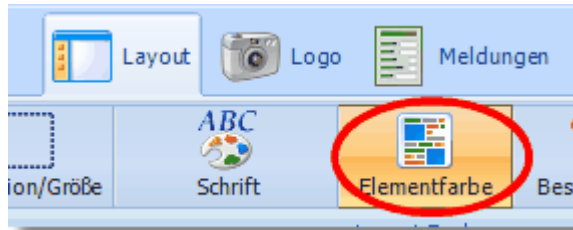


TIPP - Schnellanpassung der Grafikgröße: *Sobald Sie Größe und Position der Grafik festgelegt haben, sollten Sie die Grafik so optimieren lassen, dass der Platz optimal genutzt wird. Mit Hilfe der **Optimieren-Funktion** können Sie sich die Grafik an die gewünschte Größe anpassen lassen.*



Farbe der Elemente

Wenn Sie die Position festgelegt haben, sollten Sie die **Elementfarben festlegen**



Sobald Sie die Funktion Elementfarbe aktiviert haben, ändert jedes Klicken auf ein Element dessen Farbe.

Die Leiste Farben bietet 2 Farbflächen.



Farbflächen und Pipette

Die linke Farbfläche (1) kommt zum Einsatz, wenn Sie mit der linken Maustaste auf ein Element klicken, die rechte Farbe (2) beim Klicken mit der rechten Maustaste. Um den Flächen Farben zuzuweisen, klicken Sie mit der linken Maustaste darauf und wählen die gewünschte Farbe aus. Alternativ können Sie die Farbe mit Hilfe der **Pipette** zuweisen.

Siehe dazu [TIPP - Harmonische Farben](#).



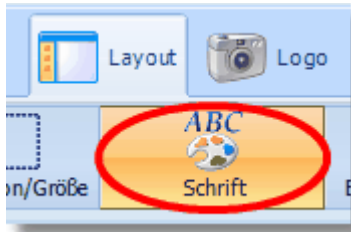
TIPP - Hintergrund: Sie können dem Hintergrund des Dialogs einen Farbverlauf zuweisen, indem Sie zunächst mit der linken, dann mit der rechten Maustaste auf ihn klicken. Soll der Hintergrund einfarbig sein, kopieren Sie die Farbe von Farbfläche 1 zu Farbfläche 2 mit Hilfe der Pfeiltaste zwischen den Schaltflächen. Betätigen Sie jetzt auf dem Hintergrund die linke und dann die rechte Maustaste.



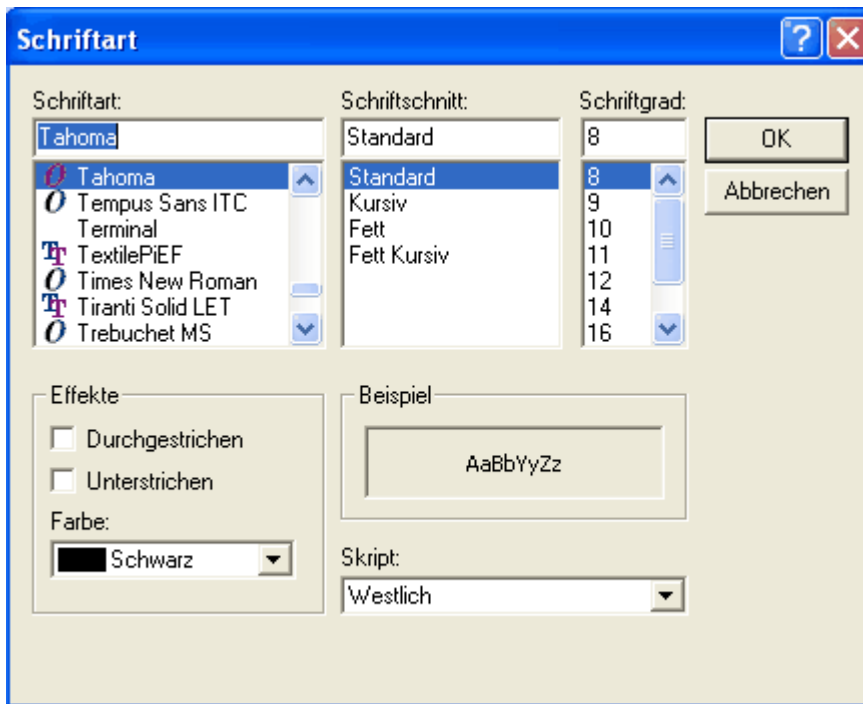
TIPP - Harmonische Farben: Sehr gute Ergebnisse erzielt man, indem man die Farben für Schrift und Elemente auf die Grafik/das Logo abstimmt. Die Pipette leistet hierbei wertvolle Dienste. Mit ihr können Sie die Farbe von Elementen des Dialogs abgreifen. Links auf die Pipette klicken, Maus über die abzutastende Stelle bewegen und Maustaste betätigen. Linke Farbfläche hat jetzt die gewünschte Farbe. Rechts auf die Pipette klicken, Maus über die abzutastende Stelle bewegen und Maustaste betätigen. Rechte Farbfläche hat jetzt die gewünschte Farbe.

Schrifteigenschaften

Passen Sie jetzt die **Schrifteigenschaften** an Ihre Vorstellungen an.



Klicken Sie auf das Element, dessen Schrifteigenschaften Sie ändern möchten. Es erscheint ein Dialog, in dem Sie verschiedene Werte für die Schrift festlegen können.



Hinweis: Beim Festlegen der Schriftart sollten Sie darauf achten, dass nicht alle Schriftarten auf jedem Computer vorhanden sind. Lassen Sie sich die unterstützten Schriftarten der verschiedenen Betriebssysteme einfach auflisten.

Schriftarten



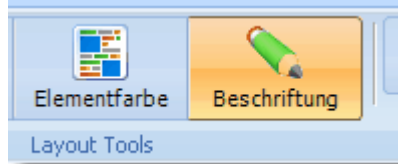
TIPP - Schnelles Ändern der Schriftfarbe: Oft möchte man nur die Farbe der Schrift ändern. Halten Sie dazu die STRG-Taste (für Steuerung; auch CTRL-Taste genannt) gedrückt, während Sie mit der linken (Farbfläche 1) oder der rechten (Farbfläche 2) Maustaste auf das Element klicken.

Es ist durchaus normal, dass man mehrere Male die verschiedenen Funktionen (Position/Größe, Elementfarbe, Schrift) aufrufen muss, bis man ein zufriedenstellendes Ergebnis erzielt hat.

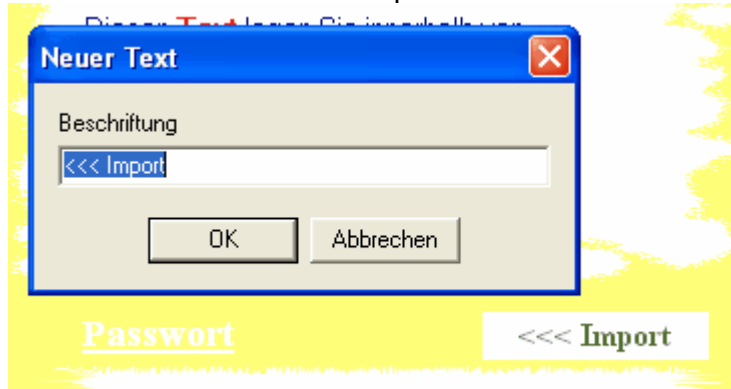
Beschriftung

(siehe auch [Meldungen](#))

Legen Sie jetzt ggf. fest, wie die verschiedenen Elemente beschriftet werden sollen.



Klicken Sie dazu auf das entsprechende Element.

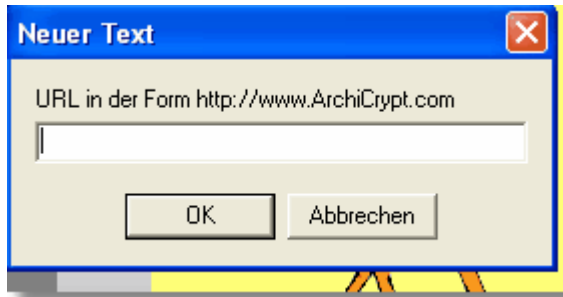


Geben Sie anschließend den gewünschten Text ein.

Einige Elemente haben neben der eigentlichen Beschriftung eine **Link-Eigenschaft**.



Geben Sie, sofern gewünscht, in der zweiten Eingabeaufforderung die URL an.



Klickt der Nutzer dann auf dieses Element, wird ein Browserfenster geöffnet.



TIPP - E-Mail: *Sie können nicht nur eine Internetadresse für eine Seite angeben, sondern auch eine Mailadresse angeben.*

Bauen Sie die Adresse wie folgt auf:

<mailto:IhreAdresse@MyDomain.com>

Sie können sogar Betreff und Text vorgeben.

<mailto:IhreAdresse@MyDomain.com?subject=DerBetreff&body=Der Text>



TIPP - Elemente verstecken 1: *Wenn Sie bestimmte Elemente nicht anzeigen möchten (z.B. Schriftzug Passwort oder Zielverzeichnis), weil diese zum Beispiel Teil der Grafik sind, leeren Sie das Feld bei Eingabe der Beschriftung. Das Element wird im Editor dann mit der Bezeichnung `<leer>` transparent angezeigt. Im Dialog sind diese Elemente später nicht sichtbar.*



TIPP - Elemente verstecken 2: *Die Elemente haben eine bestimmte räumliche Anordnung. Zum Beispiel liegt die Grafik hinter allen anderen Elementen. Das Textfeld für den Informationstext liegt im Vordergrund. Alle Elemente, die Sie hinter das Textfeld legen, werden im Dialog später nicht sichtbar sein.*

Im nächsten Schritt ([Meldungen](#)) können Sie verschiedene Texte festlegen.

10.4 Erstellen eines Themas-Meldungen

Das ArchiCryptX Change Paket gibt dem Nutzer in verschiedenen Situationen Rückmeldungen. Zum Beispiel wird eine kurze Hilfe angezeigt, sobald der Nutzer die Maus über ein Element bewegt, oder es wird ein Statustext angezeigt, der mitteilt, welche Aufgabe das ArchiCryptX Change Paket gerade verrichtet.

Sie haben hier die Möglichkeit, für jede dieser Meldungen eigenen Text anzugeben. Dies ist nicht nur dann sinnvoll, wenn Sie ein ArchiCryptX Change Paket für den Einsatz in einer anderen Sprache vorbereiten.

	Erläuterung	Original	Übersetzung (Ihr Text)
1	Wird als Titel des Dialogs angezeigt	ArchiCryptX Change	
2	Hilfetext Maus über Passworteingabe	Geben Sie hier Ihr Passwort ein	
3	Hilfetext Maus über Schaltfläche für das Umschalten der	Schaltet zwischen Klartext und verdeckter Ansicht um	

Nachrichten Tabelle laden

Sie können bereits vorhandene Nachrichten Tabellen laden.



Öffnen

oder die aktuelle Tabelle für eine spätere Verwendung mit anderen Themen speichern.

Nachrichtentabelle speichern



Speichern

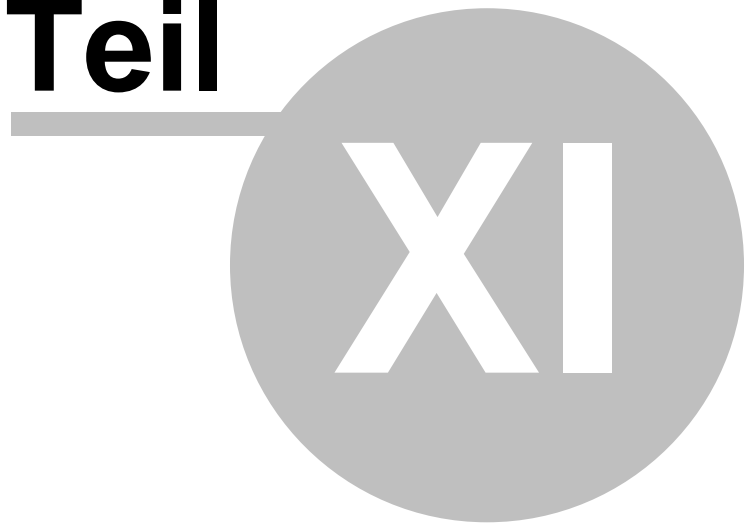
Anpassen der Meldungen und Hilfetexte

In der Spalte **Erläuterung** erhalten Sie Informationen über den Zweck des Textes (wann wird dieser Text angezeigt). In der Spalte **Original** sehen Sie den Text, der angezeigt wird, sofern Sie selbst keine "Übersetzung" angeben.

In der Spalte **Übersetzung** können Sie den Text eingeben, der statt des Originaltextes angezeigt werden soll. Klicken Sie dazu doppelt in das entsprechende Feld in der Spalte Übersetzung und geben Sie Ihren Text ein.

Achten Sie darauf, dass der Text hinsichtlich der Länge nicht zu sehr vom Originaltext abweicht.

Teil



11 ArchiCrypt WEB Access Manager (WAM)

11.1 Überblick

siehe auch: [Wichtige Begriffe - Begriffserläuterungen](#)

[Lizenzverwaltung](#)

[Einstellungen](#)

[PHP-Editor](#)

Kommandozeilentool des WEB Access Managers

Zweck / Funktion des ArchiCrypt WEB Access Managers

ArchiCrypt WEB Access Manager ist die Zentrale zur Verwaltung von Lizenzinformationen. Der WEB Access Manager ist Bestandteil der Enterprise Version von ArchiCryptX Change.

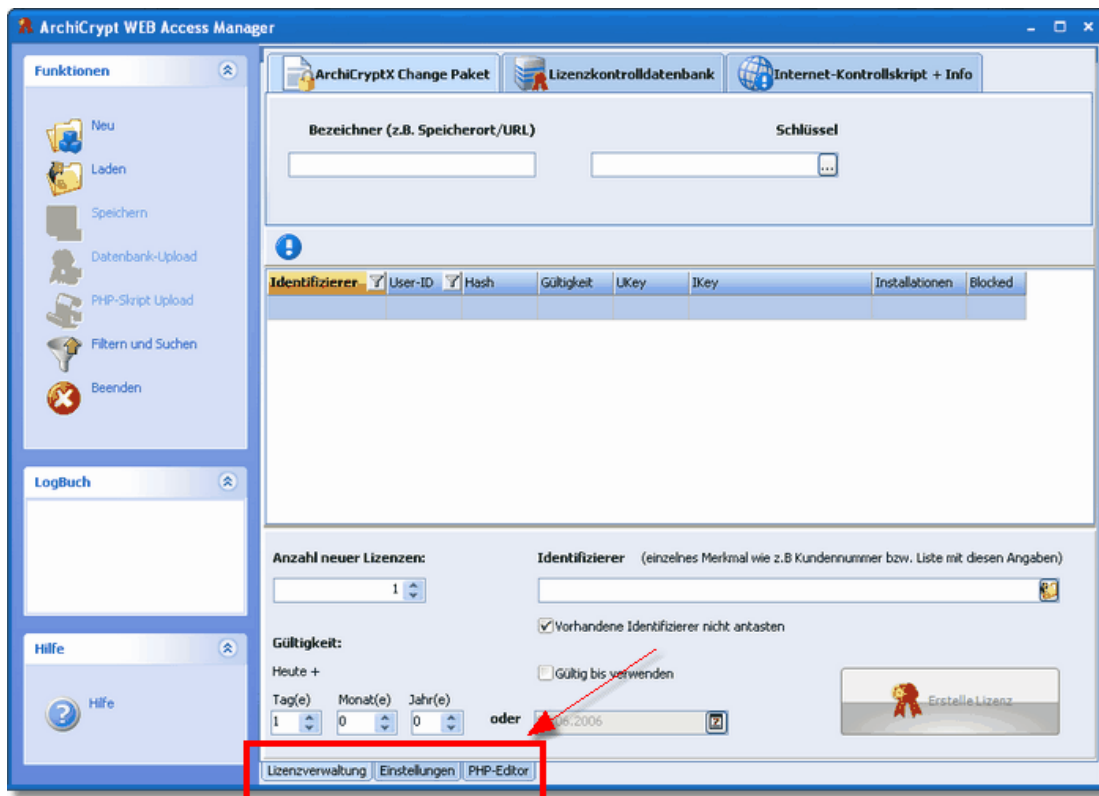
Mit Hilfe des WEB Access Managers können Sie für ein ArchiCryptX Change Paket eine "**Lizenzkontrolldatenbank**" erstellen die den Zugriff auf die Inhalte in einem ArchiCryptX Change Paket zusammen mit dem **Internet-Kontrollskript** steuert.

Zunächst sollten Sie sich mit einigen für den **WEB Access Manager (WAM)** [wichtigen Begriffen](#) vertraut machen!

Wie funktioniert die Kontrolle via Internet

Das ArchiCryptX Change Paket wird wie gewohnt mit einem Passwort, dem s.g. **Masterkey** verschlüsselt. Der WEB Access Manager spaltet diesen Schlüssel so auf, dass mehrere Teilschlüssel entstehen (**UserKey** und **InternetKey**). Der Empfänger des ArchiCryptX Change Pakets erhält seinen Teilschlüssel (**Nutzerschlüssel** und eine **Nutzerkennung**) auf sicherem Wege.

Gibt der Nutzer seine Daten in das ArchiCryptX Change Paket ein, sendet dieses eine Anfrage an das Internet-Kontrollskript. Das Kontrollskript liest verschiedene Werte aus der Lizenzkontrolldatenbank. Handelt es sich um eine gültige Lizenz (**nicht abgelaufen oder gesperrt, maximale Anzahl an Installationen nicht überschritten**), überträgt das Skript den zweiten Teilschlüssel (**InternetKey**) über das Internet. Das ArchiCryptX Change Paket berechnet jetzt aus den Teilschlüsseln den Originalschlüssel und entschlüsselt die Daten im Paket.



Am unteren Rand können Sie zwischen den Registern

- [Lizenzverwaltung](#)
- [Einstellungen](#)
- [PHP-Editor](#)

wechseln.

Wenn Sie den WEB Access Manager starten, wird die [Lizenzverwaltung](#) angezeigt. Hier können Sie bestehende Lizenzen verwalten und neue einrichten.

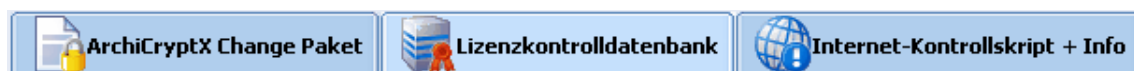
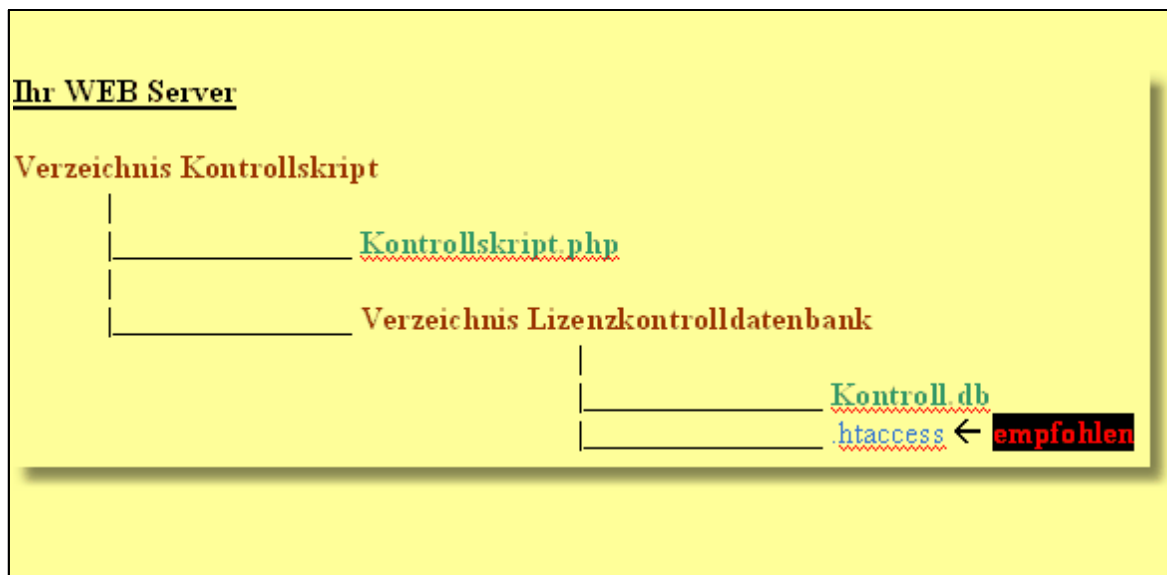
11.2 Schritt 1 Dateinamen und Passwort

siehe auch: [Wichtige Begriffe - Begriffserläuterungen](#)
[Lizenzen erstellen und bearbeiten](#)

Benennung, Speicherorte und Passwort

Die [Lizenzverwaltung](#) dient dem Verwalten vorhandener und Erstellen neuer Lizenzen. Sie sollten zunächst verschiedene Dateinamen und Internetadressen festlegen, bevor Sie Lizenzen erstellen.

WICHTIG Verzeichnisse auf WEB Server vorbereiten: Das **Internet-Kontrollskript** sollte in einem eigenen Verzeichnis auf Ihrem Server abgelegt werden. Legen Sie dieses Verzeichnis mit Ihrem FTP Programm an. Legen Sie zeitgleich ein Unterverzeichnis für die **Lizenzkontrolldatenbank** an.



Im oberen Bereich der Lizenzverwaltung sehen Sie die 3 Registerseiten

- [ArchiCryptX Change Paket](#)
- [Lizenzkontrolldatenbank](#)
- [Internet-Kontrollskript + Info](#)

ArchiCryptX Change Paket

Bezeichner:

Geben Sie hier einen möglichst eindeutigen Bezeichner für das Paket an. Dies kann ein von Ihnen frei gewählter Text sein. Es empfiehlt sich zumeist, die Internetadresse (sofern Sie die Datei als Download bereitstellen) oder der lokale Name (inkl. Pfad) anzugeben. Der Bezeichner soll Sie dabei unterstützen, das mit der Lizenzdatenbank verknüpfte Paket zu erkennen.

Schlüssel / Passwort:

Geben Sie hier das Passwort an, mit dem Sie das ArchiCryptX Change Paket erstellt haben. Handelt es sich um ein Paket, welches mit mehreren Passwörtern verschlüsselt wurde, wählen Sie eines aus. (siehe [Schritt 5 Passwort](#)).

Durch Betätigen der Schaltfläche  können Sie auch eine Schlüsseldatei einlesen ([Exportiert aus ArchiCryptX Change](#)).

➔ **WICHTIG:** *Unterlaufen Sie die hohe Sicherheit, die Ihnen der Advanced Encryption Standard (AES; 256 BIT Version) bietet, nicht dadurch, dass Sie ein zu kurzes und ungeeignetes Passwort wählen. Falls Sie den Zugriff mit WAM über das Internet (nur Enterprise Version) steuern möchten, sollten Sie ein generiertes Passwort der Mindestlänge 20 Byte verwenden.*

Lizenzkontrolldatenbank

ArchiCryptX Change Paket	Lizenzkontrolldatenbank	Internet-Kontrollskript + Info
Dateiname auf Webserver <input type="text" value="access.db"/> ersetzt <%DataBaseName%> im Skript	Zielverzeichnis auf Webserver <input type="text" value="controll/1access"/> muss bereits existieren	Relativer Pfad zu Kontrollskript <input type="text" value="1access"/> ersetzt <%RelPath%> im Skript

Dateiname der Lizenzkontrolldatenbank auf Webserver

Geben Sie hier den Namen ein, den die Lizenzkontrolldatenbank auf Ihrem WEB Server haben soll. Bei der Benennung orientieren Sie sich an der Namenskonvention für Dateien auf Ihrem System.

Der Name könnte zum Beispiel lauten:

me12388x.dat

oder

access.db

oder gemäß [Grafik](#)

Kontroll.db

Der hier festgelegte Name wird in das Internet-Kontrollskript eingefügt ([\\$tablefile](#)).

Ersetzt die Zeichenfolge

<%DataBaseName%>

Zielverzeichnis für Lizenzkontrolldatei auf Webserver

Geben Sie hier den Namen des Zielverzeichnisses auf Ihrem WEB Server an. Stellen Sie dem Verzeichnisnamen einen Slash voran.

Ein möglicher Verzeichnisname könnte lauten:

/1Access5

oder

/controll/1access

oder gemäß [Grafik](#)

/Verzeichnis Kontrollskript/Verzeichnis Lizenzkontrolldatenbank

➔ **WICHTIG:** Das Verzeichnis, welches Sie als Ziel angeben, muss auf dem Server bereits existieren!

Relativer Pfad zu Kontrollskript

Geben Sie hier den Namen des Pfades bezogen auf den Pfad zum Kontrollskript an (relativ). Liegt das Kontrollskript zum Beispiel in

/controll

und

die Lizenzdatenbank in

/controll/1access

so ist der relative Pfad

1access

oder gemäß [Grafik](#)

Verzeichnis Lizenzkontrolldatenbank

➔ **WICHTIG:** Das Verzeichnis muss auf dem Server bereits existieren!

Der hier festgelegte Name wird in das Internet-Kontrollskript eingefügt ([\\$tablefile](#)).

Ersetzt die Zeichenfolge

`<%RelPath%>`

➔ **Hinweis Sicherheit:** Sie sollten den direkten Zugriff auf die Lizenzkontrolldatei unbedingt unterbinden. Legen Sie dazu eine `.htaccess` Datei im Zielverzeichnis für die Lizenzkontrolldatei an. Der Inhalt der Lizenzkontrolldatei kann dann nicht mehr mit dem Browser angezeigt werden. Testen Sie dies, indem Sie die Internetadresse der Lizenzkontrolldatei als Adresse in Ihrem Browser eingeben.

Internet-Kontrollskript + Info

ArchiCryptX Change Paket	Lizenzkontrolldatenbank	Internet-Kontrollskript + Info
Adresse des Internet-Kontrollskripts (URL)	Info Zugang gesperrt (URL)	Info Zugang abgelaufen (URL)
<input type="text"/>	<input type="text"/>	<input type="text"/>
Info Installationszahl überschritten (URL)		
<input type="text"/>		

Adresse des Internet-Kontrollskripts

Das Internet-Kontrollskript ist eine PHP Datei, die die Kommunikation mit einem ArchiCryptX Change Paket übernimmt. Die Adresse, die Sie hier eingeben, müssen Sie beim Erstellen des ArchiCryptX Change Pakets ebenfalls angeben! (siehe [Schritt 5 Passwort](#))

Eine mögliche Adresse könnte wie folgt aussehen:

<http://www.MyDomain.com/MyAccessDB/MyControl.php>

oder gemäß [Grafik](#)

http://www.MyDomain.com/Verzeichnis_Kontrollskript/Kontrollskript.php

➔ **WICHTIG:**

- **Das Verzeichnis, im Beispiel /MyAccessDB muss auf dem Server bereits existieren.**
- **Die Datei muss die Endung PHP haben.**
- **Falls Sie hier Änderungen vornehmen, müssen Sie das PHP Skript neu generieren und auf Ihrem Server ablegen lassen!**

Sie können das Skript durch Betätigen der **Schaltfläche U (Upload)** auf Ihre Internetpräsenz laden, vorausgesetzt, Sie haben unter [Einstellungen](#) bereits die Daten für Ihren FTP Zugang angegeben.

Informationsseiten

- **Info Zugang gesperrt** (Sie haben den Zugriff gesperrt)
- **Info Zugang abgelaufen** (Das von Ihnen festgelegte Datum wurde überschritten)
- **Info Installationszahl überschritten** (Die durch Sie festgelegte maximale Anzahl an Installationen wurde überschritten)

Geben Sie hier jeweils die URL (Internetadresse) an, die dem Nutzer beim Vorhandensein der entsprechenden Voraussetzung angezeigt werden soll. Eine mögliche Adresse für eine Informationsseite könnte wie folgt aussehen:

<http://www.MyDomain.com/Expired.htm>

weiter zu [Lizenzen erstellen und bearbeiten](#)

11.3 Schritt 2 Lizenzen erstellen und bearbeiten

siehe auch: [Wichtige Begriffe - Begriffserläuterungen Erzeugen und Upload der Lizenzkontrolldatei](#)

Neue Lizenzen erstellen und Lizenzen bearbeiten

Nachdem Sie zumindest das [Passwort](#) für das ArchiCryptX Change Paket angegeben haben, können Sie Lizenzen erstellen.

The screenshot shows a web form for creating licenses. The 'Anzahl neuer Lizenzen:' field is highlighted with a red box and contains the value '1'. A red arrow points to this field. Other fields include 'Identifizierer' (with a text input and a small icon), 'Gültigkeit:' (with 'Heute +' and 'Gültig bis verwenden' options), and date pickers for 'Tag(e)', 'Monat(e)', and 'Jahr(e)', along with a date field containing '07.06.2006'. A 'Erstelle Lizenz' button is visible on the right. At the bottom, there are navigation tabs for 'Lizenzverwaltung', 'Einstellungen', and 'PHP-Editor'.

Anzahl neuer Lizenzen

Legen Sie zunächst fest, wie viele Lizenzen erstellt werden sollen (nicht identisch, mit Anzahl erlaubter Installationen!).

Identifizierer

Sie können bei Bedarf einen s.g. Identifizierer angeben. Wie der Name vermuten lässt, soll er Ihnen helfen, eine Lizenz einem bestimmten Objekt (Person, Firma, Institution, etc.) zuzuordnen. Der hier angegebene Wert spielt keine Rolle bei der Berechnung von Schlüsselwerten. Falls Sie hier einen Wert direkt in das Eingabefeld eingeben, kann nur 1 Lizenz erstellt werden. Falls Sie eine Textdatei mit Identifizierern (ein Identifizierer pro Zeile) haben, können Sie den Dateinamen auswählen. Es wird dann für jeden Identifizierer eine Lizenz erstellt. Zusammen mit der Option "**Vorhandene Identifizierer nicht antasten**" können Sie sicherstellen, dass nur für neu in einer solchen Liste aufgeführte Identifizierer neue Lizenzen erstellt werden.

Gültigkeit

Die neu erstellten Lizenzen können entweder mit einem konkreten Verfalldatum (Gültig bis verwenden aktiv) versehen werden oder mit einer frei wählbaren Zeitspanne ab Erstelldatum der Lizenz.

Hinweis: Bei der Prüfung durch das ArchiCryptX Change Paket zählt das Datum auf Ihrem WEB Server und nicht das lokale Datum des Nutzers.

Durch das Betätigen der Schaltfläche **Erstelle Lizenz**, starten Sie den Erstellprozess. Sie können den Vorgang abbrechen, indem Sie die ESC-Taste betätigen.

→Wichtig: Unter Einstellungen - Schlüssel und Datenbank können Sie festlegen, wie viele Installationen beim Erzeugen neuer Lizenzen vorgegeben werden sollen.

Identifizierer	User-ID	Hash	Gültigkeit	UKey	IKey	Installationen	Blocked
W5TMRPS	B38BE2B8C	08.06.200	90EB4F832	40E316FFCB5BCF9E53F2AC8D	2	N	
ECYJY94E	74F7F34D6	08.06.200	09783808B	AE56CC7B8CC0AB324E12F8D	2	N	
P7Z9D6LQ	976576045	08.06.200	62E9E77BF	25864D09865F9851688DF0C9	2	N	
F01WBYB	F66065E64	08.06.200	B816314B9	81F16D68BF559CC1EC5E7CA	2	N	
1YICKLZ3	6C3EC04CF	08.06.200	3C3764045	7081BBDE8BEC3EFC9C1398D9	2	N	
9TCDDZP	10153F4AA	08.06.200	47E8B8823	2B2BFADB9637F7DDA92E7676	2	N	
8RGXKER	3E3340856	08.06.200	AD6602209	870B76F459C60A2AB4124BCD	2	N	
S13UYXH	773FDF20D	08.06.200	37D3B9167	686B23C56E174EE57ECC9086	2	N	
AKTJDUU	80A612F67	08.06.200	6F8EFB25D	6CF3E8D286676B04DB211F70	2	N	

Die Tabelle enthält jetzt in jeder Zeile einen Datensatz für eine Lizenz. Eine mit Hilfe dieser Daten erzeugte Lizenzkontrolldatei ist bereits funktionsfähig.



TIPP: Unter Einstellungen - Tabellenansicht können Sie festlegen, welche Spalten in der Tabelle sichtbar sein sollen. Sie können die Reihenfolge der Spalten ändern, indem Sie die Spaltenüberschriften per Drag&Drop an die gewünschte Position ziehen.

Lizenzinformationen zuordnen

Sicher möchten Sie den Lizenzen jedoch weitere Informationen zuordnen. Doppelklicken Sie dazu mit der linken Maustaste auf die entsprechende Zeile.

Die Registerseite Schlüssel bietet dabei Zugriff auf die grundsätzlichen Lizenzinformationen. Hier können Sie **Lizenzen sperren** (Option **Lizenz gesperrt** auswählen), den Identifizierer ändern oder festlegen, einen Lizenznehmer eintragen (**Lizenz für**) und die Gültigkeit ändern.



TIPP: Soll der Lizenznehmer so viele Installationen/Entschlüsselungen vornehmen dürfen, wie er möchte, geben Sie bei Anzahl Installationen den Wert 0 an.

Auf der Registerseite Lizenznehmer können Sie bei Bedarf weitergehende Informationen zum Lizenznehmer machen.

Die hier eingegebenen Informationen können Sie mit Hilfe der [Platzhalter in den Schablonen](#) nutzen.

weiter zu [Erzeugen und Upload der Lizenzkontrolldatei](#)

11.4 Schritt 3 Erzeugen und Upload der Lizenzkontrolldatei

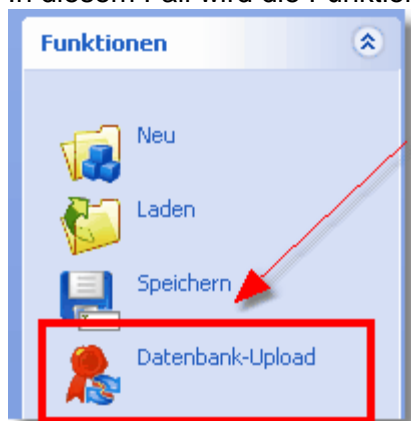
siehe auch: [Wichtige Begriffe - Begriffserläuterungen Anpassen und Upload der Kontrollskript Lizenzdaten verteilen](#)

Erzeugen und Upload der Lizenzkontrolldatei

Sie haben in [Schritt 2](#) bereits Lizenzen erzeugt und diesen ggf. weitergehende Informationen zugeordnet.

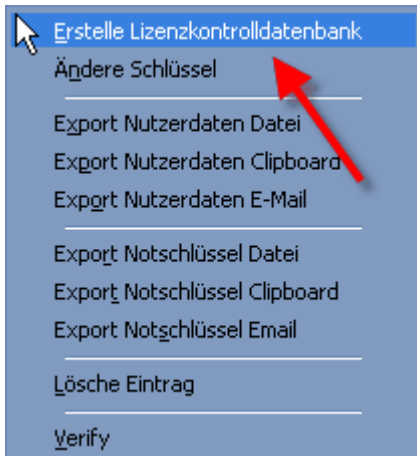
Sie sollten auf jeden Fall die in [Schritt 1](#) notwendigen Angaben gemacht und unter [Einstellungen - FTP](#) die Daten für den FTP Upload eingegeben haben.

In diesem Fall wird die Funktion **Datenbank-Upload** verfügbar.



Sobald Sie die Funktion aufrufen, wird die Lizenzkontrolldatei erzeugt und auf Ihre Internetpräsenz geladen.

Wenn Sie die Datei selbst auf Ihrem Server ablegen möchten, oder eine lokale Kopie verfügbar haben möchten, rufen Sie im Kontextmenü der Tabelle den Eintrag **Erstelle Lizenzkontrolldatenbank** auf.



Die erzeugte Datei ist eine Textdatei und enthält Einträge der Art:

```
B38E2B8C57380A0D111AB6ED3431D2E24163C19|20060608|0|40E316FFCB5BCF9E53F2AC8D781D6E71A3D833B35D0D3F6F8F90CFF5745F0A27|none|2
74F7F34D632CC402FA54BA10EA8F726ACCF29068|20060608|0|AE56CC7B8CC0AB324E12F8D0994E48C3173C966B26B89AFB37AAAB54E6D6FC14|none|2
9765760450FF2932411F96357E3130F66FB7391B|20060608|0|25864D09865F9851688DF0C92AC4DD13C053FCF216270C8F338B9C1DE42A8E10|none|2
F66065E641816338235D67FCD826651F10D583EC|20060608|0|81F16D6BBF559CC1ECSE7CA8AA113FAE7A8171A643149C7BBA3568240F9D0969|none|2
6C3EC04CF4E94FB643FAB847B3EA1D024CD4559E|20060608|0|7081BBDE8BEC3EFC9C1398D928C4E3A53CCC06619B88D642D8499E207CB47578|none|2
10153F4AABC439FD570A106F4240C9EAF7D9E59B|20060608|0|2B2BFAD89637F7DDA92E7676DC62C4162C026630C2F4C1CE8A94D6CFF8275B37|none|2
3E33408563FF05D31148F860ED67DCBB2C86409|20060608|0|870B76F459C60A2AB4124BCD5764673AAF682F4BB0C09F4A7CE2629AB7838338|none|2
```

Bitte editieren Sie unter keinen Umständen diese Datei!

weiter zu [Anpassen und Upload der Kontrollskript](#)

11.5 Schritt 4 Anpassen und Upload Kontrollskript

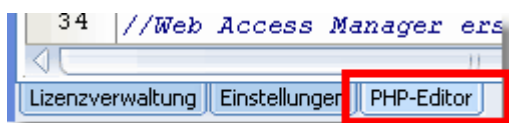
siehe auch: [Wichtige Begriffe - Begriffserläuterungen](#)
[Lizenzdatenbank lokal speichern](#)

Anpassen und Upload des Internet Kontrollskripts

Das **Kontrollskript** übernimmt auf Ihrem WEB Server die Kommunikation mit dem entsprechenden ArchiCryptX Change Paket. Damit das Kontrollskript diese Funktion übernehmen kann, muss es an einigen Stellen angepasst werden. Das Skript enthält bestimmte Platzhalter, die durch Ihre Angaben in [Schritt 1](#) ersetzt werden. Sie müssen keine direkten manuellen Anpassungen am Skript vornehmen.

Sofern Sie wünschen, können Sie bestimmte Parameter im PHP Skript manuell ändern.

Wechseln Sie dann zum [PHP-Editor](#).



Im Skript finden Sie zahlreiche Anmerkungen und Hinweise. Diese Hinweise sind mit **//--->>> ÄNDERN???** gekennzeichnet.

➡ WARNUNG: ÄNDERUNGEN am Skript GEHEN VERLOREN, wenn Sie das Skript vor dem Beenden nicht explizit speichern.

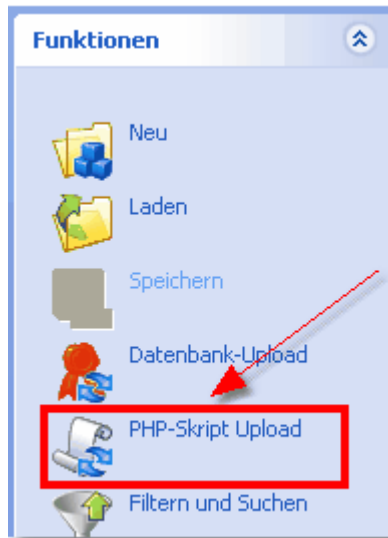


HINWEIS: Sie können gerne das komplette Skript abändern (z.B. Realisierung

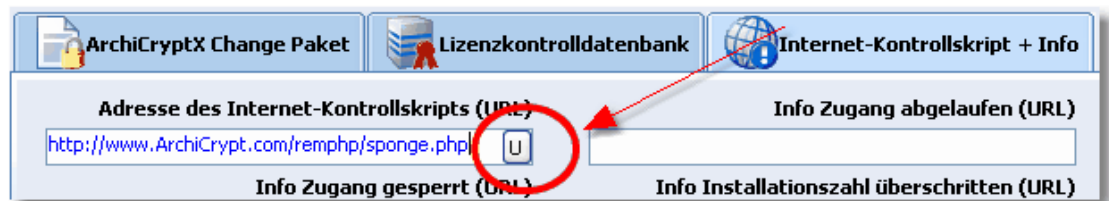
mittels MySQL Datenbank). Wichtig ist lediglich, dass die Auswertung des durch das ArchiCryptX Change Paket übergebenen Parameters (der Prüfwert oder Hashwert) und die Art der Übergabe der Werte durch das Skript an das ArchiCryptX Change Paket nicht geändert wird.

PHP-Skript Upload

Wenn Sie die Anpassungen vorgenommen haben, können Sie das Skript auf Ihren WEB Server laden lassen.



oder



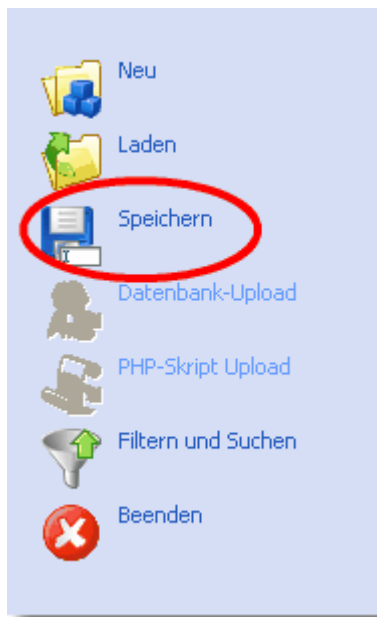
weiter zu [Lizenzdatenbank lokal speichern](#)

11.6 Schritt 5 Lizenzdatenbank lokal speichern

siehe auch: [Wichtige Begriffe - Begriffserläuterungen](#)

Lizenzdatenbank lokal speichern

Nachdem Sie das **Kontrollskript** und die **Lizenzkontrolldatenbank** auf Ihrem WEB Server abgelegt haben, sollten Sie die **Lizenzdatenbank** speichern.



Betätigen Sie dazu die Schaltfläche **Speichern**. Legen Sie dann den Namen und das Verzeichnis für die Lizenzdatenbank fest. Sie müssen jetzt ein Passwort eingeben, mit dem die Lizenzdatenbank verschlüsselt werden soll. Merken Sie sich das Passwort gut!

➔ **WICHTIG** Sichern der Datenbank: *Sichern Sie unbedingt die Lizenzdatenbanken regelmäßig (notfalls nach jeder Änderung!). Diese Datenbanken enthalten alle Daten, mit denen Lizenzen verwaltet (ändern, neu erstellen) werden können.*



TIPP Passwort für Lizenzdatenbank ändern: *Um eine Lizenzdatenbank mit einem anderen Passwort zu schützen, geben Sie beim Speichern einen anderen Namen oder ein anderes Zielverzeichnis an.*

11.7 Lizenzdaten verteilen und exportieren

siehe auch: [Wichtige Begriffe - Begriffserläuterungen](#)
[Kontextmenü Lizenztabelle](#)

Lizenzdaten verteilen und exportieren

Der Übertragungsweg für **Nutzerkennung** (User-ID) und **Nutzerschlüssel** (User-Key) sollte sich nach dem Sicherheitsbedürfnis richten.

Weitergabe von Lizenzdaten via E-Mail

Sie sollten sich darüber im Klaren sein, dass die unverschlüsselte Weitergabe dieser Daten via Internet (E-Mail/Download) die Gefahr birgt, dass die Daten abgefangen und gestohlen werden. Für hochbrisante Daten also sicher die falsche Art der Weitergabe.

Für viele Situationen (insbesondere Weitergabe von Softwarevollversionen) dürfte die Verteilung via E-Mail jedoch ausreichend sicher sein. Bitte senden Sie die

Lizenzdaten nicht mit dem ArchiCryptX Change Paket!

Persönliche Weitergabe von Lizenzdaten

Sind die Inhalte des XChange Pakets hochsensibel, sollten Sie Nutzerkennung und Nutzerschlüssel persönlich übergeben.

Um die für den Nutzer wichtigen Lizenzdaten weiter zu geben, bietet die Tabelle ein Kontextmenü an. Betätigen Sie über einer der Tabelleneinträge die rechte Maustaste:



Sie haben grundsätzlich 3 Möglichkeiten:

Export Nutzerdaten Datei

Erzeugt eine Datei, die der Nutzer über die Importfunktion im ArchiCryptX Change Paket einfach importieren kann. Die Datei ist damit erste Wahl, wenn man die Daten per Datenträger oder als Anhang einer E-Mail verteilen möchte. ArchiCrypt WEB Access Manager nutzt dazu die [Textschablone](#).

Export Nutzerdaten Clipboard

Kopiert die Daten in die Zwischenablage. Von dort können Sie die Daten in andere Anwendungen als Text übernehmen. ArchiCrypt WEB Access Manager nutzt dazu die [Textschablone](#).

Export Nutzerdaten E-Mail

Erzeugt eine E-Mail und nutzt dabei die [Textschablone](#).

Notschlüssel

Neben der normalen Weitergabe der Daten für die Nutzer, bietet ArchiCryptX Change an, einen s.g. **Notschlüssel** zu erzeugen. Ein Notschlüssel kann dann notwendig werden, wenn der Nutzer zwingend Zugriff auf die Daten in einem ArchiCryptX Change Paket benötigt, er jedoch keine Verbindung zum Internet herstellen kann. ArchiCrypt WEB Access Manager nutzt dazu die [Textschablone](#).



Sie haben die Wahl zwischen:

[Export Notschlüssel Datei](#)

[Export Notschlüssel Clipboard](#)

[Export Notschlüssel E-Mail](#)

➔ WARNUNG: Ein Notschlüssel unterläuft die Kontrolle im Internet. Wer den Notschlüssel besitzt, kann ohne Einschränkung auf das ArchiCryptX Change Paket zugreifen. Das angegebene Verfallsdatum für den Notschlüssel kann sehr leicht manipuliert und unterlaufen werden!

Was tun, wenn ein Notschlüssel herausgegeben wurde?

Wenn es sich um Inhalte handelt, die sich ändern und in der jetzigen Form für den Besitzer des Notschlüssels bald veraltet sind, sollten Sie unmittelbar nach Herausgabe des Notschlüssels zunächst das ArchiCryptX Change Paket mit einem neuen Passwort erzeugen. Anschließend nutzen Sie bitte die Funktion "[Ändere Schlüssel](#)", geben als neuen Schlüssel das für das neue Paket verwendete Passwort an und laden die geänderte Lizenzkontrolldatenbank auf Ihren WEB Server. Das alte ArchiCryptX Change Paket ersetzen Sie bitte ebenfalls.

Export Datenbank

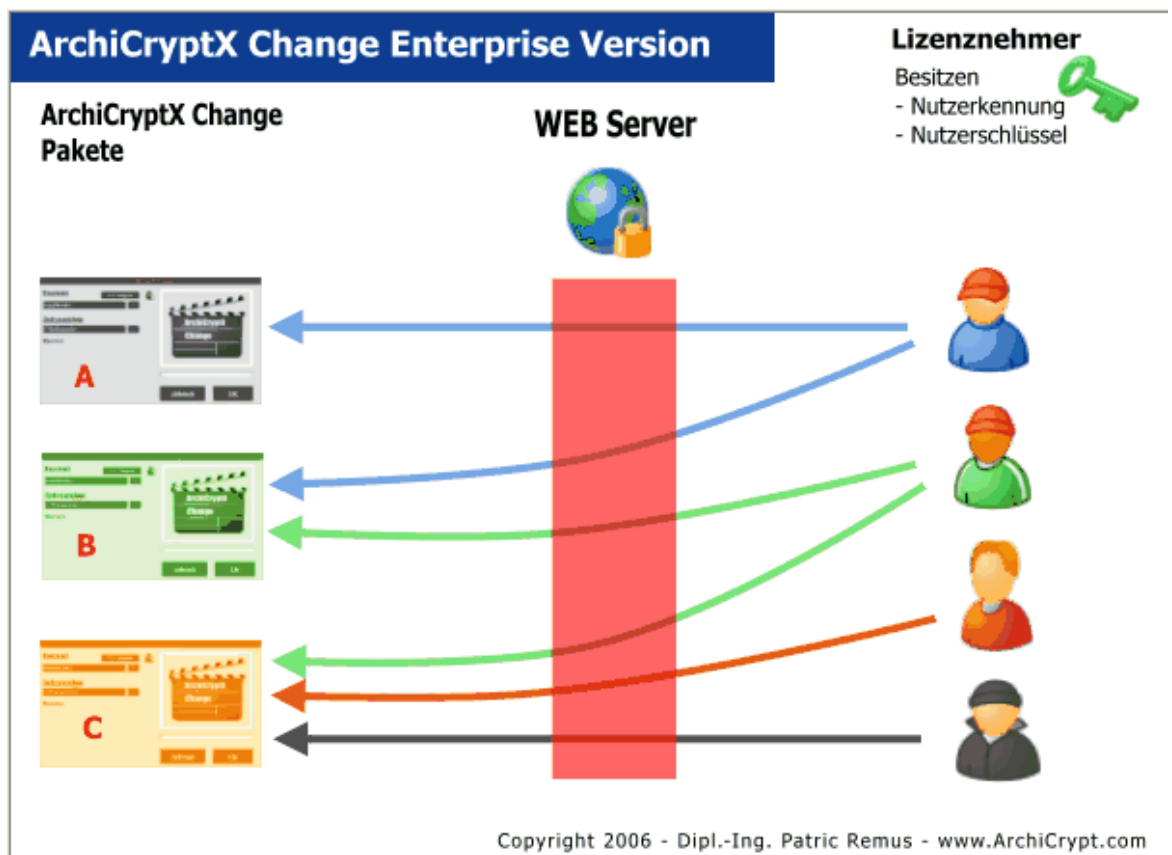
Oft ist es nötig, Lizenzdaten in anderen Anwendungen weiter zu verarbeiten oder in einem bestimmten Format weiterzugeben.

WAM stellt hierfür die Funktion [Export Datenbank](#) zur Verfügung.

Als Schablone wird [Schablone Export Lizenzdaten](#) verwendet. Jeder Eintrag der Lizenzdatenbank erzeugt genau einen Eintrag gemäß Schablone in der Zieldatei.

siehe [Einstellungen Schablonen E-Mail und Export Nutzerdaten](#)

11.8 Ein Lizenznehmer - mehrere ArchiCryptX Change Pakete



Angenommen, Sie bieten mehrere ArchiCryptX Change Pakete an. Ein Lizenznehmer kann mehrere dieser Pakete lizenziert haben.

Die klassische Variante sieht so aus, dass Sie dem Lizenznehmer für jede der lizenzierten Pakete eigene Lizenzdaten überstellen.

Für den Lizenznehmer wird in jeder der Lizenzdatenbanken eine eigene Lizenz erzeugt.

Ein Lizenznehmer - mehrere XChange Pakete - ein Lizenzdatensatz

Um dem Lizenznehmer nicht für jedes Paket eine andere Nutzererkennung und einen anderen Nutzerschlüssel übersenden zu müssen, bietet ArchiCrypt WEB Access Manager eine Export- und Importfunktion für Kenndaten an.

Mit Hilfe dieser Funktion ist es möglich, einem Lizenznehmer den Zugriff auf verschiedene ArchiCryptX Change Pakete mit gleichen Kenndaten (Nutzerschlüssel und Nutzererkennung) zu ermöglichen.

Nachfolgend finden Sie verschiedene Vorgehensweisen um einem Lizenznehmer mit einem einzigen Lizenzdatensatz Zugang zu mehreren ArchiCrypt XChange Paketen zu gewähren.

Nachfolgende Vorgehensweise hat sich bewährt

ArchiCryptX Change Pakete

Erzeugen Sie die ArchiCryptX Change Pakete wie gewohnt unter Nutzung eines B-Themas (Internetschablone; Schablone B - ...). Als Kontrollskript geben Sie unbedingt unterschiedliche Adressen an.

Die Adressen der Kontrollskripte für unser Beispiel könnten wie folgt aussehen:

<http://www.MeineDomain/Kontroll/controlA.php>

<http://www.MeineDomain/Kontroll/controlB.php>

<http://www.MeineDomain/Kontroll/controlC.php>

Lizenzdatenbanken

Erzeugen Sie für die Pakete, im Beispiel A,B und C jeweils eine eigene **Lizenzdatenbank**. Machen Sie alle Angaben, **erzeugen Sie jedoch keine Lizenzen**. Berücksichtigen Sie die Namen der Kontrollskripte in der jeweiligen Lizenzdatenbank.



Dummy-Lizenzdatenbank:

Legen Sie eine Dummy-Lizenzdatenbank an, die lediglich ein Passwort/Schlüssel (beliebig wählbar) enthält. Generieren Sie hier Ihre Lizenzen und fügen Sie den Lizenzen bei Bedarf Lizenzinformationen an. Für diese Lizenzdatenbank bitte **keine Lizenzkontrolldatenbank** und **kein Lizenzkontrollskript** erzeugen und auf Ihrem WEB Server speichern. Sie dient lediglich der Verwaltung von Lizenznehmern.

Legen Sie für Lizenznehmer, die gleiche Pakete lizenziert haben, **gleiche Identifizierer** fest. Dazu vor dem Erstellen einen entsprechenden Identifizierer festlegen, der Auskunft darüber gibt, auf welche Pakete dieser Lizenznehmer zugreifen darf.

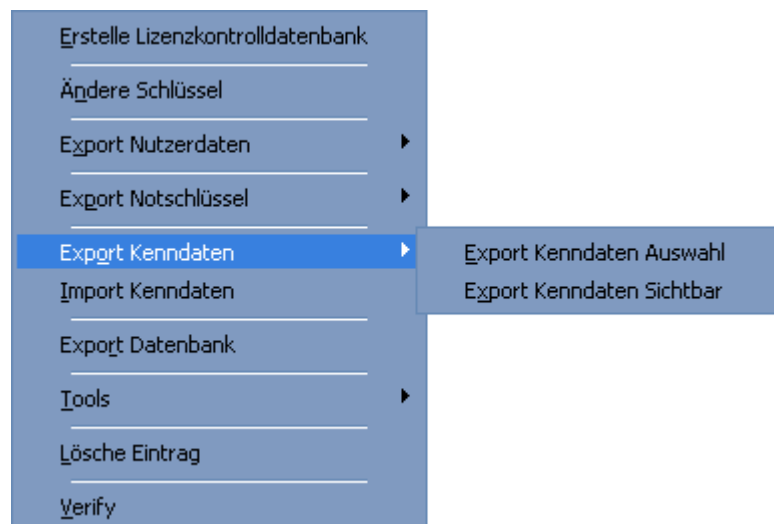
Für unser Beispiel zeigt das folgende Bild, wie 2 Lizenzen erzeugt werden, die auf Paket A und B zugreifen können.



Die Dummydatenbank sieht dann zum Beispiel wie folgt aus:

Identifiziere	User-ID	Hash	Gültigkeit	UKey	Blocked
BC	ENTSISBV	9E55B4AD9	07.07.2006	33CBFECE7	N
BC	SKDQ5X8K	630F863F0	07.07.2006	3761631DD	N
AB	5NX5NJE1	7526CCE46	07.07.2006	47823FDBC	N
AB	245EJJKP	01D15B98D	07.07.2006	D5A946CCE	N
A	OCWMDA	B03C333D0	07.07.2006	D618383F3	N
A	82AL716D	E787427204	07.07.2006	269498D8B	N
A	LA6SIG95	EB0983A7F	07.07.2006	E54191C2B	N
A	JM9PW85	6E5A2F1E7	07.07.2006	BE11A978E	N

Exportieren Sie jetzt die Kenndaten mit [Export Kenndaten Sichtbar](#).



wechsel zur jeweiligen Lizenzdatenbank:

Lizenzdatenbanken

Importieren Sie jetzt diese Daten in die jeweilige [Lizenzdatenbank](#) ([Import Kenndaten](#)).

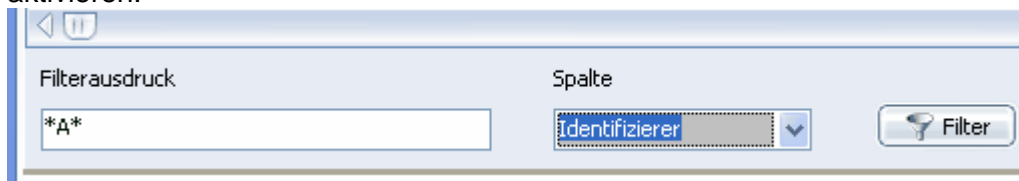


Filtern Sie die Lizenzdatenbank jetzt so, dass nur noch Datensätze angezeigt werden, die zum aktuellen Paket gehören.

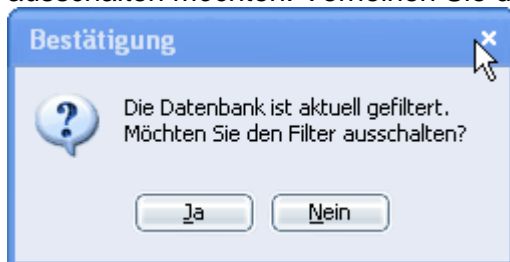
Für die Lizenzdatenbank A hieße das, dass wir einen Filter

A

aktivieren.



Speichern Sie jetzt die Lizenzdatenbank. Sie werden gefragt, ob Sie den Filter ausschalten möchten. Verneinen Sie die Frage!



Jetzt werden nur die Einträge gespeichert, die für das Paket auch eine Lizenz enthalten. Zugehörige Kontrollskript und Lizenzdatenbank können jetzt wie gewohnt eingerichtet werden.

Für die weiteren Pakete verfahren Sie entsprechend. Also Import der Daten, filtern nach B (mit ***B***) bzw. C (mit ***C***) und speichern, ohne den Filter vor dem Speichern jeweils aufzuheben.

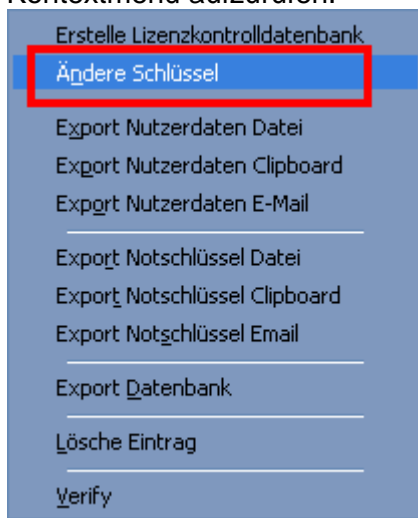
11.9 Schlüssel / Passwort ändern

siehe auch: [Wichtige Begriffe - Begriffserläuterungen](#)
[Notschlüssel](#) und [Sicherheit](#)
[Kontextmenü Lizenzteballe](#)

Ändern des Passworts / Schlüssels bei einem ArchiCryptX Change Paket

Von Zeit zu Zeit sollten Sie das Passwort für das ArchiCryptX Change Paket ändern. Wenn das Passwort für ein ArchiCryptX Change Paket geändert wurde, müssen Sie die **Lizenzdatenbank** anpassen, die **Lizenzkontrolldatei** neu erstellen und auf Ihrem WEB Server speichern.

Laden Sie die Lizenzdatenbank für das betroffene ArchiCryptX Change Paket. Klicken Sie in der Tabelle mit der rechten Maustaste auf einen beliebigen Eintrag um das Kontextmenü aufzurufen.



Wählen Sie die Funktion **Ändere Schlüssel** aus. Sie werden jetzt 2 Mal aufgefordert, das neue Passwort einzugeben (*Typfehler werden so vermieden*). ArchiCrypt WEB Access Manager berechnet jetzt die Internetschlüssel (IKKey) neu.

Nach der Neuberechnung sollten Sie die Lizenzdatenbank sichern (ggf. unter neuem Namen um eine Sicherungskopie verfügbar zu haben) und die geänderte [Lizenzkontrolldatei auf Ihren WEB Server laden](#).

➔ **WICHTIG:** Die Nutzerdaten bleiben erhalten, müssen den Lizenznehmern also nicht erneut zugesandt werden.

11.10 Kontextmenü Lizenztabelle

siehe auch: [Wichtige Begriffe - Begriffserläuterungen](#)

Kontextmenü der Lizenztabelle

Das Kontextmenü der Lizenztabelle bietet zahlreiche Funktionen.



Erstelle Lizenzkontrolldatenbank

Sie können die **Lizenzkontrolldatenbank** lokal speichern.

siehe auch [Schritt 3 Erzeugen und Upload der Lizenzkontrolldatei](#)

Ändere Schlüssel

Passt die Lizenzdatenbank an ein geändertes Passwort für ein ArchiCryptX Change Paket an.

siehe auch [Schlüssel / Passwort ändern](#)

Export von Nutzerdaten

siehe [Lizenzdaten verteilen](#)

Export von Notschlüssel

siehe [Lizenzdaten verteilen](#)

Export Kenndaten

siehe [Ein Lizenznehmer - mehrere ArchiCryptX Change Pakete](#)

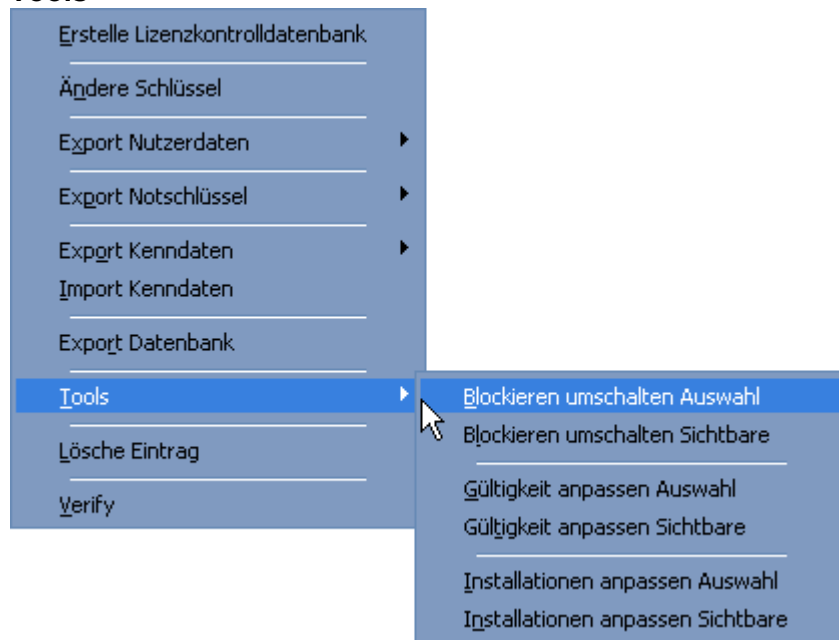
Import Kenndaten

siehe [Ein Lizenznehmer - mehrere ArchiCryptX Change Pakete](#)

Export Datenbank

siehe [Lizenzdaten verteilen](#)

Tools



Blockieren umschalten Auswahl

Schaltet den aktuellen Status von Blocked für die aktuell markierte Zeile um (Von Ja auf Nein und umgekehrt)

Blockieren umschalten Sichtbare

Schaltet den aktuellen Status von Blocked für die aktuell in der Tabelle angezeigten Werte um (Von Ja auf Nein und umgekehrt). Durch einen Filter ausgeblendete Zeilen bleiben unberührt.

Gültigkeit anpassen Auswahl

Setzt die Gültigkeit für die aktuell markierte Zeile auf den eingestellten Wert.

Gültigkeit anpassen Sichtbare

Setzt die Gültigkeit für die aktuell in der Tabelle angezeigten Werte neu. Durch einen Filter ausgeblendete Zeilen bleiben unberührt.

Installationen anpassen Auswahl

Setzt Anzahl möglicher Verschlüsselungen/Installationen für die aktuell ausgewählte Zeile neu.

Installationen anpassen Sichtbare

Setzt Anzahl möglicher Verschlüsselungen/Installationen für die aktuell in der Tabelle angezeigten Werte neu. Durch einen Filter ausgeblendete Zeilen bleiben unberührt.

Lösche Eintrag

Löscht den markierten Eintrag aus der Lizenzdatenbank

Verify

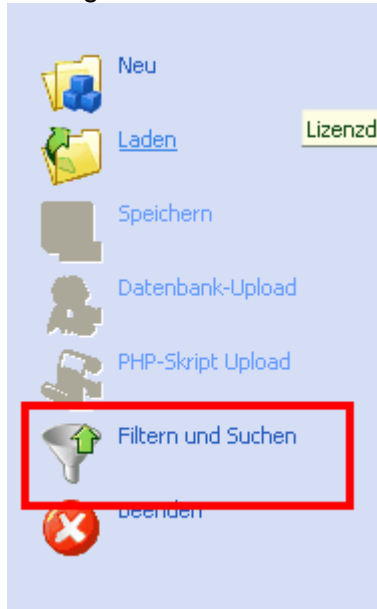
Prüft, ob die markierte Lizenz den Schlüssel für das ArchiCryptX Change Paket erzeugen kann

11.11 Suchen und Filtern von Lizenzen

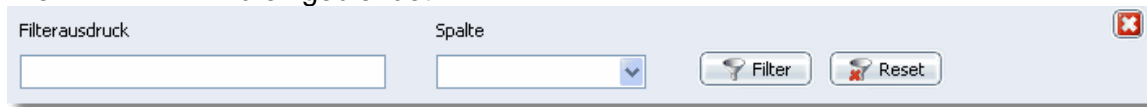
Suchen und Filtern von Lizenzen

Wenn Sie sehr viele Lizenzen zu verwalten haben, kann es äußerst hilfreich sein, die Tabelle mit Lizenzeinträgen nach bestimmten Kriterien zu filtern.

Betätigen Sie die Schaltfläche **Filtern und Suchen**.



Die **Filterleiste** wird eingeblendet.



Wählen Sie zunächst die **Spalte** aus, die gefiltert werden soll.

Geben Sie jetzt den **Filterausdruck** ein. Sie können s.g. Jokerzeichen (Platzhalter) nutzen.

*,?

Auch Größenvergleiche sind zulässig.

>, <, >=, <=, =, ! (! bedeutet nicht)

Sie können verschiedene Ausdrücke mit Logikoperatoren verknüpfen

&, ^ (logisches UND, logisches ODER)

Sie sehen jetzt in der **Statusleiste** ein Filtersymbol.



Um den Filter wieder zurückzusetzen, betätigen Sie bitte die Schaltfläche **Reset**.



Um die Filterleiste zu schließen, betätigen Sie die **Schließen** Schaltfläche

**Beispielfilter:**

>= W ^ <= 9

Wirkung:

Listet alle Einträge der gewählten Spalte, deren erster Buchstabe mit W,X,Y oder Z oder mit den Ziffern 9,8,7,6,5,4,3,2,1,0 beginnt.

Identifiziere	User-ID
	WIOT21Y
	YH19SY99
	8RGXKER

Beispielfilter:

Spalte Nachname und Filterausdruck A*

Listet alle Lizenznehmer mit Nachname beginnend mit A auf.

Sie können die Datenbank nach mehreren Spalten gleichzeitig filtern.

Spalte Nachname und Filterausdruck A*

Listet alle Lizenznehmer mit Nachname beginnend mit A auf.

Jetzt Spalte Installationen auswählen und Filterausdruck >=100

Wirkung:

Listet alle Lizenznehmer mit Nachname beginnend mit A auf, die mindestens 100 Installationen durchführen dürfen.

11.12 Einstellungen

Schlüssel und Datenbank

Länge Nutzerkennung

Geben Sie hier an, wie lange die von WAM erzeugten **USER-ID** s sein sollen.
Minimal 10, maximal 20

➡**Hinweis:** Da die User-ID als SALT Wert verwendet wird, sollte die Länge ausreichend groß sein. Da ein ArchiCryptX Change Paket die Möglichkeit bietet, Nutzerkennung und Nutzerschlüssel aus einer Datei oder der Zwischenablage zu importieren, sollte die Länge eine untergeordnete Rolle spielen. Empfohlen wird eine Länge von mindestens 10 Zeichen (10 Byte).

Länge Nutzerschlüssel

Der Wert gibt an, wie lange der zu erzeugende **Nutzerschlüssel** sein soll.
Minimal 16, maximal 128 Byte (= 1024 BIT)

➡**Hinweis:** Da ein ArchiCryptX Change Paket die Möglichkeit bietet, Nutzerkennung und Nutzerschlüssel aus einer Datei oder der Zwischenablage zu importieren, sollte die Länge eine untergeordnete Rolle spielen. Empfohlen wird eine Länge von mindestens 16 Zeichen (16 Byte). Das zur Verschlüsselung des XChange Pakets genutzte Passwort sollte mindestens gleiche Länge aufweisen.

Tabellenzeile für Lizenzkontrolldatei

WARNUNG: Diese Schablone bestimmt die Struktur eines Datensatzes in der Lizenzkontrolldatei.
Nehmen Sie an dieser Stelle nur nach vorheriger Rücksprache mit unserer Entwicklungsabteilung auf!

FTP

Diese Angaben werden benötigt, damit WAM Lizenzkontrolldatei und Internet Kontrollskript auf Ihrem WEB Server ablegen kann.

Hostname

Hostname Ihres WEB Servers.
Z.B.: **www.ArchiCrypt.com**

Port

Port des FTP Servers.
Z.B.:
FTP
oder
21

Nutzername

Ihr Nutzername für den FTP Server
Z.B.:
WalterEftepe

Passwort

Ihr Passwort für den FTP Server

Modi

Passiv kann bei Einsatz einer Firewall sinnvoll sein.

Synchron Modus wartet jeweils auf die Antwort des FTP Servers bis zum Ausführen des nächsten Befehls.

Binärmodus überträgt die Daten als Binärdaten. Sonst als Textdaten.

Test

Sobald Sie alle Werte eingegeben haben, können Sie versuchen, eine Testverbindung zum FTP Server aufzubauen. Das Ergebnis des Tests sehen Sie im LogBuch

Abbruch

Sie können einen Test abbrechen.

Schablonen E-Mail und Export Nutzerdaten

siehe auch [Lizenzdaten verteilen und exportieren](#)

Absender

Tragen Sie hier ggf. eine Absenderadresse ein, die beim Versand von Nutzerdaten oder Notschlüssel als E-Mail genutzt werden soll.

siehe auch [Lizenzdaten verteilen](#)

Betreff

Tragen Sie hier ggf. die Betreffzeile ein, die beim Versand von Nutzerdaten oder Notschlüssel als E-Mail genutzt werden soll.

siehe auch [Lizenzdaten verteilen](#)

Platzhalter für Schablonen

<%Anmerkung%>
<%Anrede%>
<%Bezeichner%>
<%Blocked%>
<%Email%>
<%FAX%>
<%Firma%>
<%Gültigkeit%>
<%Hash%>
<%Hausnummer%>
<%Identifizierer%>
<%IKey%>
<%Installationen%>
<%Name%>
<%Ort%>

<%PLZ%>
 <%Produkt%>
 <%Straße%>
 <%Tel%>
 ArchiCryptX Change
 <%UKey%>
 <%User-ID%>
 <%Vorname%>

Um einen Platzhalter einzufügen, betätigen Sie bitte die Space oder LEERTASTE bei gedrückter STRG-Taste. Die Bezeichnung entspricht dabei der Spaltenüberschrift in der Lizenztablelle.



Schablone Export Nutzerdaten

Tragen Sie hier den Text ein, der beim Export der Nutzerdaten als Schablone genutzt werden soll. In den Text können Sie an beliebiger Stelle (gerne auch mehrfach) bestimmte Platzhalter eintragen, die beim Erstellen durch entsprechende Werte der Lizenzdatenbank ersetzt werden.

Um dem Nutzer dieser Daten das Übertragen der Lizenzdaten (Nutzerkennung und Nutzerschlüssel) in die entsprechenden Eingabefelder des ArchiCryptX Change Pakets zu vereinfachen, setzen Sie bitte den Schlüssel zwischen die Tags

[luk]/[luk]

und die Nutzerkennung zwischen

[luid]/[luid].

Beispiel:

Mit Platzhalter sollte dies so aussehen:

[luid]<%User-ID%>/[luid]

[luk]<%UKey%>/[luk]

Der Nutzer kann jetzt beliebigen Text markieren, der diese Daten enthält, in die Zwischenablage kopieren und von dort in das XChange Paket importieren.

Schablone Notfallschlüssel

Wie Schablone Export Nutzerdaten

Dient jedoch als Vorlage für den Export von Notfallschlüsseln.

Schablone Export Lizenzdaten

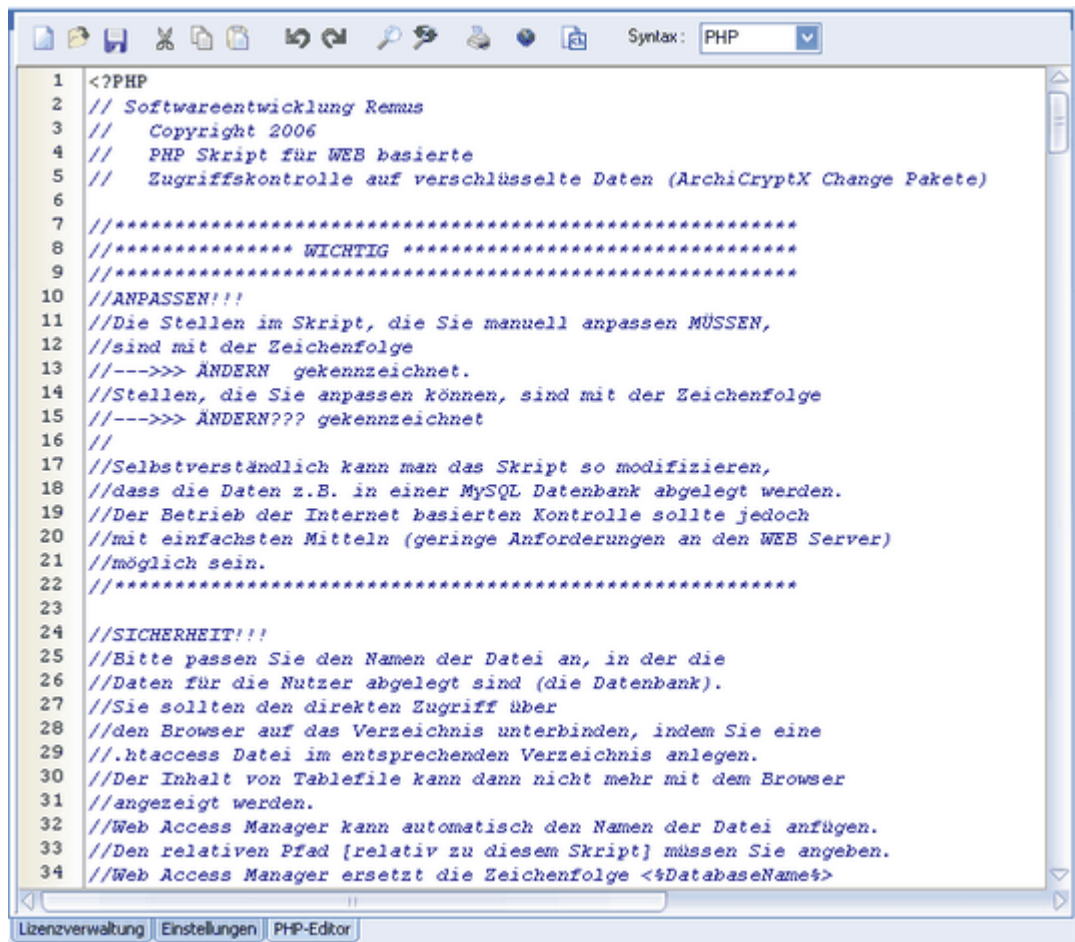
Wie Schablone Export Nutzerdaten. Die Schablone dient jedoch als Vorlage für den Export der kompletten Datenbank. Für jede Lizenz in der Datenbank wird also in der Zielfeile genau ein Eintrag mit der Schablone erzeugt.

Tabellenansicht

Hier können Sie einzelne Spalten der Tabelle sichtbar und unsichtbar schalten.

11.13 PHP-Editor

Der PHP Editor



```

1  <?PHP
2  // Softwareentwicklung Remus
3  // Copyright 2006
4  // PHP Skript für WEB basierte
5  // Zugriffskontrolle auf verschlüsselte Daten (ArchiCryptX Change Pakete)
6
7  //*****
8  //***** WICHTIG *****
9  //*****
10 //ANPASSEN!!!
11 //Die Stellen im Skript, die Sie manuell anpassen MÜSSEN,
12 //sind mit der Zeichenfolge
13 //--->>> ÄNDERN gekennzeichnet.
14 //Stellen, die Sie anpassen können, sind mit der Zeichenfolge
15 //--->>> ÄNDERN??? gekennzeichnet
16 //
17 //Selbstverständlich kann man das Skript so modifizieren,
18 //dass die Daten z.B. in einer MySQL Datenbank abgelegt werden.
19 //Der Betrieb der Internet basierten Kontrolle sollte jedoch
20 //mit einfachsten Mitteln (geringe Anforderungen an den WEB Server)
21 //möglich sein.
22 //*****
23
24 //SICHERHEIT!!!
25 //Bitte passen Sie den Namen der Datei an, in der die
26 //Daten für die Nutzer abgelegt sind (die Datenbank).
27 //Sie sollten den direkten Zugriff über
28 //den Browser auf das Verzeichnis unterbinden, indem Sie eine
29 //.htaccess Datei im entsprechenden Verzeichnis anlegen.
30 //Der Inhalt von Tablefile kann dann nicht mehr mit dem Browser
31 //angezeigt werden.
32 //Web Access Manager kann automatisch den Namen der Datei anfügen.
33 //Den relativen Pfad [relativ zu diesem Skript] müssen Sie angeben.
34 //Web Access Manager ersetzt die Zeichenfolge <%DatabaseName%>

```

Gehen Sie das **Kontrollskript** durch und lesen Sie die Anmerkungen sorgfältig. Um die nötigen Anpassungen vorzunehmen, müssen Sie keine besonderen PHP Kenntnisse besitzen. Es wird lediglich erwartet, dass Sie mit Ihrem FTP Programm ein Verzeichnis erstellen und ggf. eine Zugriffskontrolle mit einer htaccess Datei erstellen können.

11.14 Sicherheit

siehe auch: [Wichtige Begriffe - Begriffserläuterungen](#)

Informationen über die Sicherheit der Lösung mit Internetkontrolle

Die im Zusammenhang mit der Verschlüsselung verwendeten Verfahren sind standardisiert. Es gelten die folgenden Rahmenbedingungen.

Rahmenbedingungen

- Mit einem **Teilschlüssel** (**Nutzerschlüssel** oder **Internetschlüssel**) alleine ist es nicht möglich die Daten zu entschlüsseln.
- Der Nutzerschlüssel wird nicht über das Internet übertragen.
- Aus dem **Hashwert** lässt sich der Nutzerschlüssel nicht berechnen.
- Der Internetschlüssel wird offen über das Internet übertragen. Es wird das HTTP Protokoll verwendet.
- Mit nicht unerheblichem technischem Aufwand ist es für einen Nutzer, der gültige Daten (**UserKey**, **User-ID** und aktiven und gültigen Eintrag in der Lizenzdatenbank) besitzt, möglich aus seinem Nutzerschlüssel, der User-ID und dem übertragenen **Internet-Schlüssel** den Originalschlüssel (**MasterKey**) zu berechnen. Mit Hilfe des MasterKeys kann man die unverschlüsselten Daten herstellen.

Die mit der internetbasierten Methode **erreichbare Sicherheit** ist also wesentlich davon abhängig, wie zuverlässig die Besitzer der Nutzerdaten (Nutzerschlüssel und User-ID) sind.

Die Sicherheit ist gewährleistet, sofern der Nutzer nicht dazu beiträgt, dass seine Daten (insbesondere der Nutzerschlüssel) in falsche Hände geraten und, dass das System, auf dem das ArchiCryptX Change Paket gestartet wird, nicht durch Schadsoftware ausspioniert wird.

Daher:

Falls Sie Missbrauch feststellen, verschlüsseln Sie das ArchiCrypt XChange Paket neu und lassen Sie die Datenbank neu berechnen, nachdem Sie den missbrauchten Lizenzeintrag entfernt haben.

Handelt es sich um hochsensible Daten, auf die wenig zuverlässige Personen zugreifen, sei es auch nur, weil diese auf einem völlig unzuverlässigen System arbeiten (z.B. Rechner im Internet Café), wird der Einsatz der internetbasierten Lösung nicht empfohlen. Diese Konstellation dürfte jedoch der Ausnahmefall sein.

Wenn Sie einen Notschlüssel für einen Nutzer erzeugt und weitergeleitet haben, müssen Sie zwingend das ArchiCryptX Change Paket neu verschlüsseln und die neue Lizenzkontrolldatei (siehe auch: [Schlüssel ändern](#)) erzeugen und auf Ihre Internetpräsenz laden.

Teil

XII

12 Technischer Teil

12.1 Warum Verschlüsselung?

Ist Verschlüsselung sinnvoll?

"Ich habe nichts zu verbergen, ich habe keine Geheimnisse!"

Während man Menschen, die beruflich mit dem Computer arbeiten inzwischen Gott sei Dank nicht mehr erläutern muss, warum der Schutz bestimmter Daten Pflicht ist, sind viele Privatanwender immer noch der Meinung, Verschlüsselung sei nicht notwendig. Schließlich mache man nichts Illegales am Rechner, weswegen man auch nichts verbergen müsse. In dieser Aussage steckt implizit die Annahme, die Angreifer auf die Daten im Rechner seien Justiz- und Polizeibehörden. Doch genau hier irrt man. Die "Dunklen Seiten des Internet" lassen erahnen, wer es auf die Daten in Ihrem Rechner abgesehen hat. Es geht um Identitätsdiebstahl, Diebstahl von Passwörtern, Ausspähen, Erpressen, Fernsteuern und Missbrauch von Rechnern. Also um all die Dinge, die man noch vor wenigen Jahren nur aus Science Fiction Filmen kannte. Heute ist dies traurige Realität. Weiterhin ist es zu einer Art Volkssport geworden, sich in einschlägigen Foren im Internet Codes, Schlüssel und Passwörter zu besorgen, mit denen man dann "kostenlos" auf kostenpflichtige Inhalte zugreift.

Der Verlust vertraulicher Daten kann zum Ruin führen.

Im privaten Bereich kann es um die eigene Existenz gehen, im beruflichen Alltag um ein Unternehmen. In meinem Berufsleben habe ich viele Mitarbeiter und Kollegen gesehen, die, falls überhaupt, die eingebaute Möglichkeit von Kompressions- oder Office-Produkten nutzten um selbst eingestufte Informationen abzulegen und zu versenden. Eine trügerische Sicherheit! Selbst die Hersteller solcher Produkte verweisen in Ihren Hilfetexten auf die Unsicherheit der integrierten Verfahren. Jedoch dringt dies meist nicht bis zum Nutzer durch, da dieser bei dem Menüpunkt Verschlüsselung oder bei dem Reizwort Passwort direkt davon ausgeht, behandelte Daten seien gut geschützt.

Informationen haben sich zu einem der wichtigsten Wirtschaftsgüter entwickelt. Der Schutz dieser Daten ist die Herausforderung des 21 ten Jahrhunderts. In den letzten Jahren ist folgender Umstand hinzugekommen. Zahlreiche Rechner mit sensiblen Informationen (Kundendaten/Verträge/Urkunden/etc.) sind Bestandteil eines Netzwerks. Oft kennen Nutzer die Gefahr nicht, die droht, wenn Sie sich in das Internet einwählen oder im Falle eines DSL Zugangs ständig mit dem Internet verbunden sind. Die Software Firewall Systeme, die eine trügerische Sicherheit vermitteln, verleiten viele Nutzer zu einem sehr arglosen Umgang mit Daten auf Rechnern mit Verbindung zum Internet. Auch bei Verwendung des hervorragenden Mediums E-Mail, wird meist übersehen, dass die verschickten Daten völlig unverschlüsselt über eine Vielzahl gänzlich unbekannter Rechner im Internet geleitet werden.

Man sollte sich allerdings darüber im Klaren sein, dass es eine absolute Sicherheit nicht gibt. Auch die besten und ausgefeiltesten Tools können an diesem Umstand nichts ändern. Ziel jedoch muss es sein, das Risiko, sensible Daten zu verlieren, zu minimieren. Hierbei spielt die eingesetzte Software eine entscheidende Rolle.

"Verschlüsselung ist mir zu kompliziert"

Viele Menschen denken bei dem Thema Verschlüsselung an hochkomplizierte Vorgänge und Anwendungen. Viele Hersteller tragen diesem Vorurteil Rechnung und liefern entsprechende Anwendungen aus. Wer aber sagt, dass man die zugrundeliegende Komplexität von Verschlüsselung an den Anwender weiter geben muss? ArchiCryptX Change ist unkompliziert und verknüpft auf geniale Weise Datensicherheit mit marketingwirksamen Elementen. Wird E-Mail als Transportmedium für sensible Daten genutzt, hat ArchiCryptX Change den großen Vorteil, dass ein Empfänger keinerlei spezielle Software installiert haben muss. Der Empfänger benötigt ausschließlich das Passwort.

12.2 Verschlüsselung was ist das?

Was versteht man unter Verschlüsselung?

Verschlüsselungsverfahren sind immer dann gefordert, wenn es darum geht, vertrauliche Informationen über **unsichere Informationskanäle** zu übertragen oder allgemein, Daten vor dem Zugriff unbefugter zu schützen.

Man unterscheidet dabei grundsätzlich zwei Verfahren. Das **symmetrische Verfahren**, bei welchem zur Verschlüsselung und Entschlüsselung der gleiche Schlüssel zum Einsatz kommt und das **asymmetrische Verfahren**, bei dem man für das Ver- und Entschlüsseln unterschiedliche Schlüssel nutzt.

Bei asymmetrischen Kryptographie-Techniken wird mit einem öffentlich zugänglichen, nicht geheimen Code, dem so genannten Öffentlichen Schlüssel („**public key**“) und einem Privaten Schlüssel („**private key**“, Secret Key) gearbeitet. Eine Kombination aus beiden Verfahren wird als **Hybrid-Codierung** bezeichnet. Reine asymmetrische Verfahren kommen sehr selten vor und wenn, dann nur, wenn es um geringe Datenmengen geht. In Echtzeitumgebungen werden hingegen Hybride Verfahren genutzt, wobei die tatsächliche Datenverschlüsselung mit einem symmetrischen Verfahren durchgeführt wird.

ArchiCryptX Change nutzt reine symmetrische Verfahren.

Mein Verschlüsselungsprogramm hat aber eine 4096 BIT Verschlüsselung!

Im Zusammenhang mit der Sicherheit eines Verfahrens wird sehr gerne die s.g. Schlüssellänge in BIT herangezogen. Dabei können asymmetrische Verfahren mit sehr großen Schlüssellängen auf sich aufmerksam machen. Während **AES** mit vergleichsweise kleinen **256 BIT** aufwartet, bietet das berühmte **RSA** Verfahren (benannt nach seinen Erfindern Ron Rivest, Adi Shamir, and Leonard Adleman.) bis zu **4096 BIT** lange Schlüssel. Auf den ersten Blick ein überwältigender Vorteil des RSA Verfahrens. In Wahrheit handelt es sich hier jedoch um Äpfel und Birnen, die man bekanntermaßen nicht miteinander vergleichen kann. Dies ist durch die unterschiedliche mathematische Basis begründet, die den jeweiligen Verfahren zu Grunde liegt. Bei symmetrischen Verfahren werden 128 BIT als sicher angesehen,

bei asymmetrischen 1024 BIT; immer unter bestimmten Rahmenbedingungen!
In diesem Zusammenhang tritt eine weitere Unart auf. Bestimmte Verfahren expandieren (erweitern) Schlüssel während des eigentlichen Verschlüsselungsvorgangs. Bestimmte Hersteller nutzen diesen Wert in Ihrer Werbung. Gelegentlich erfinden Sie auch neue Verfahren und warten mit gigantischen Schlüssellängen auf. Hüten Sie sich vor solchen Produkten, es könnte sich um Snake Oil ([Snake Oil bei Wikipedia](#)) handeln!

Was ist Kryptologie

Kryptologie ist wörtlich die „**Wissenschaft der Verschlüsselung**“ und basiert auf mathematischen Algorithmen, die man heutzutage in Software umsetzt. Im alten Rom wurde ein extrem simples Verfahren verwendet, welches darin bestand, jeden Buchstaben „X“ der Nachricht durch einen anderen Buchstaben zu ersetzen, der sich aus einem bestimmten Abstand „X+n“ zu dem Original ergibt. So wurde z. B. aus einem „A“ ein „C“, aus „B“ ein „D“, aus „C“ ein „E“, usw. Diese Methoden sind noch schwächer als die s.g. [XOR-Verschlüsselung](#).

Die Sicherheit solcher Verfahren beruht auf der Schwierigkeit, aus den umgewandelten Daten ohne Kenntnis des Schlüssels, die Originaldaten wieder herzustellen.

Die Wahl des Verfahrens ist daher mit entscheidend für die Sicherheit eines Produktes! (siehe [Eingesetzte Verfahren](#))

12.3 Eingesetzte Verfahren

Welche Verfahren nutzt ArchiCryptX Change

ArchiCryptX Change setzt [AES \(Advanced Encryption Standard\)](#) ein. Dieser Algorithmus ging aus einem Wettbewerb als Sieger hervor, der 3 Jahre andauerte und in dem die vorgestellten Methoden strengsten Untersuchungen unterzogen wurden. Das Verfahren hat die Eigenschaft, dass die einzige Möglichkeit, unbefugt an Daten zu gelangen der s.g. Brute-Force Angriff ist. ArchiCryptX Change setzt die besonders sichere Variante mit einer Schlüssellänge von 256 BIT ein. Das von Ihnen eingegebene Passwort wird dabei nicht direkt eingesetzt, sondern dient als Eingangsgröße für eine s.g. kryptografische Einweg-Hash-Funktion. Die Umsetzung in ArchiCryptX Change orientiert sich dabei am SHS ([Secure Hash Standard](#)) des NIST (National Institut of Standards and Technology) und setzt das Verfahren SHA ein. (siehe auch [Secure Hash Standard](#) im Internet)

ArchiCryptX Change setzt gleichzeitig eine s.g. KDF (Key-Derivation-Function) ein. Grundlage für dieses Verfahren war der [PKCS #5 Password-Based Cryptography Standard](#), welcher klare Vorgaben macht.

In der Endausscheidung waren von den anfänglich 15 Verfahren noch 5 Kandidaten im Rennen.

Obwohl die Verfahren von zum Teil äußerst renommierten Firmen eingebracht wurden, waren bei einigen Methoden schnell Schwachstellen und Lücken entdeckt. Dies sollte uns einmal mehr davor warnen, ein Verfahren unter Ausschluss der Öffentlichkeit zu entwickeln. Glauben Sie auch keinem Unternehmen, welches Ihnen einen neuen

selbstentwickelten Algorithmus verkaufen will. Die Versuchung dies doch zu tun, ist aber offensichtlich sehr hoch.

Die Methoden der Endrunde lieferten sich hinsichtlich der Leistungen ein Kopf an Kopf Rennen. Letztlich fiel folgende Entscheidung:

Rijndael:	86 Stimmen
Serpent:	59 Stimmen
Twofish:	31 Stimmen
RC6:	23 Stimmen
MARS:	13 Stimmen

Die Entscheidung zu Gunsten von Rijndael kam letztlich dadurch zu Stande, dass er die Anforderungen (siehe [AES](#)), die unterschiedlich gewichtet wurden, am besten erfüllte. Gleichzeitig bedeutet dies jedoch, dass die anderen Verfahren durchaus in bestimmten Einsatzgebieten bessere Eigenschaften aufweisen, als der Gewinner. Sicher, nach heutigem Verständnis, sind alle der oben aufgeführten Methoden.

Sicher bedeutet in diesem Zusammenhang, dass die beste Methode ohne Passwort an die Klartextdaten zu gelangen die s.g. Brute-Force Methode ist. Man geht den Daten sozusagen mit roher Gewalt an den Kragen und testet alle möglichen Passwörter durch, bis man das korrekte Passwort erwischt hat.

Informationen über die Verfahren erhalten Sie unter den angegebenen Internetadressen:

- [MARS](#) - IBM
- [RC6](#) - RSA Laboratories
- [RIJNDAEL](#) - Joan Daemen, Vincent Rijmen
- [Serpent](#) - Ross Anderson, Eli Biham, Lars Knudsen
- [Twofish](#) - Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson
- [Blowfish](#) - Bruce Schneier

12.4 Passwörter

Regeln zur Passwortgestaltung

Passwörter werden meist als **Schlüssel** oder als Ausgangspunkt für eine Schlüsselberechnung genutzt (siehe [Eingesetzte Verfahren](#)). Sie sind quasi der Schlüssel zum Schloss, welches unsere Daten vor unbefugtem Zugriff schützt. Es ist sicher einleuchtend, dass es auf zwei Dinge ankommt. Die Methode (der Algorithmus) die zur Ver- und Entschlüsselung genutzt wird und das Passwort müssen sicher sein. Was nutzt die beste Methode wenn Sie als Passwort den Buchstaben A wählen. Was nutzt das beste Passwort, wenn Sie als Methode eine [XOR-Verknüpfung](#) wählen.

Keine Begriffe aus Ihrem sozialen Umfeld

Sie sollten keinesfalls Geburtsdaten, Namen, Hobbys, Lieblingsverein, usw. nutzen. Die Passwörter entstammen Ihrem sozialen Umfeld. Einem Angreifer der sich über

Ihre Lebensumstände, Ihre Vorlieben etc. informiert, fällt es leicht, auf die Lösung zu kommen.

Vor diesem Fehler kann die Passwortbewertung von ArchiCryptX Change Sie nicht bewahren!

Keine lexikalischen Begriffe

Vermeiden sollten Sie auch lexikalische Begriffe. Ein Wörterbuch enthält um die 120.000 Einträge. Für einen Angreifer ist es leicht die 120.000 Wörter mit Hilfe eines Computers in wenigen Sekunden zu testen. Um aus diesem Fundus dennoch zu schöpfen, müssten Sie ein Passwort bilden, welches aus ca. acht Einzelworten mittlerer Länge besteht (siehe auch [Bewertung von Passwörtern](#)).

Vor diesem Fehler kann die Passwortbewertung von ArchiCryptX Change Sie nicht bewahren!

Regel

Beachten Sie auch die Anmerkungen unter [Passworteigenschaften und Passwortgenerator](#). Als Faustregel gilt, je kleiner der Vorrat an Zeichen, aus dem ein Passwort gebildet werden kann, desto länger muss es sein!

12.5 Bewertung von Passwörtern

siehe auch [Angriff auf Verschlüsseltes](#)

Wie wird das Passwort bewertet

➡ACHTUNG: ArchiCryptX Change kann nicht beurteilen, ob ihr Passwort trotz ausreichender Länge für einen Angreifer leicht zu erraten ist. Beachten Sie unbedingt die Hinweise im Kapitel [Passwörter](#). Die Bewertung arbeitet stupide und rein mathematisch, eine Wortsinnanalyse ist nicht integriert. Sprich, ArchiCryptX Change weiß nicht, ob Bernhard ein Name ist, er bewertet Bernhard genau so, wie zum Beispiel jkiaSerp.

Das Passwort kann Zeichen aus einem bestimmten Zeichenvorrat nutzen. Der Vorrat ist begrenzt. Die Bewertung des Passwortes folgt dabei dem folgenden Schema:

Länge des Passwortes * log(Anzahl Möglicher Werte)

wobei Log der Logarithmus zur Basis 10 ist.

Wählen Sie zum Beispiel ein Passwort der Länge 10, welches lediglich aus Ziffern besteht, erhalten Sie einen Wert von

$$10 * \log(10) = 10$$

ArchiCrypt Live hat die verfügbaren Zeichen in Gruppen aufgeteilt:

- Gruppe Großbuchstaben
- Gruppe Kleinbuchstaben
- Gruppe Ziffern
- Gruppe Sonderzeichen (auf Tastatur verfügbar)
- Gruppe ASCII Zeichen (nicht auf Tastatur) (hierzu siehe auch ASCII-Tabelle und Passwörter)

Während Ihrer Eingabe wird jetzt geprüft, aus welcher Menge Ihre Zeichen stammen und wie lange das eingegebene Passwort ist. Die Texte, die Sie als Bewertung vorfinden, stammen aus

["Angewandte Kryptographie" von Bruce Schneier](#)

Die Aussagen beziehen sich auf Informationstypen, Informationen, die nach einem bestimmten Zeitraum Ihre Geheimhaltungsbedürftigkeit verlieren. Für die unterschiedlichen Informationstypen, werden jetzt Mindestschlüssellängen gefordert. Das Ergebnis obiger Gleichung wird nun mit genau dieser Mindestforderung verglichen. Die Schlüssellänge ist nur dann ein Maß, mit dem man verschiedene Verschlüsselungsalgorithmen vergleichen kann, wenn alle Methoden optimale Methoden sind. D.h. die beste Variante die Methode zu knacken muss die **Brute Force** Methode sein.

12.6 AES

siehe auch [Eingesetzte Verfahren](#)

Der Advanced Encryption Standard

Das NIST ([National Institute of Standards and Technology](#)) rief 1997 weltweit dazu auf, ein neues symmetrisches Verschlüsselungsverfahren zu entwickeln.

Am 02.10.2000 erklärte der amerikanische Staatssekretär Norman Mineta den Algorithmus der beiden belgischen Kryptographen Joan Daemen von der Firma Proton-Welt International und Vincent Rijmen Mitglied von der Katholischen Universität Leuven zum neuen Standard der Nation.

Der Rijndael Algorithmus ist damit der Gewinner eines dreijährigen Wettbewerbes, an denen sich einige der führenden Kryptographen der Welt beteiligten.

Der Wettbewerb selbst wurde mit großer Begeisterung aufgenommen. Auf der 2. AES-Konferenz am 22./23. März 1999 in Rom wurden die zur Diskussion stehenden Algorithmen sowie die dazu durchgeführten Analysen vorgestellt und diskutiert. Die Konferenz hatte ca. 180 Teilnehmer aus 23 Ländern und es wurden 21 White-Papers vorgestellt. In der ersten Runde gab es hierzu 15 Vorschläge, aus welchen in mehreren Schritten der endgültige AES Algorithmus ausgewählt werden sollte. Informationen hierzu finden Sie unter <http://www.nist.gov/aes>.

In der zweiten Runde gab es noch die Kandidaten: **MARS**, **RC6**, **Rijndael**, **Serpent** und **Twofish**.

Der Gewinner sollte folgenden Anforderungen genüge leisten:

Aufruf des NIST vom 12.09.1997

Symmetrische Blockchiffre

- Unterstützt mindestens die Schlüssellängen 128, 192 und 256 bits und eine Blocklänge von 128 bits
- Besser als derzeitige Verfahren: Sicherer und effizienter (hinsichtlich Laufzeit,

Platzbedarf auf Chip) als Triple-DES

- Einsetzbar in verschiedenen Anwendungsumgebungen
- Verwendbar für Stream Cipher, Message Authentication Code (MAC) Generator, Pseudozufallszahlen-Generator, Hashfunktion etc.
- Implementierbar in Hard- und Software
- Weltweit lizenzfrei verfügbar
- Sicherheit soll für 20-30 Jahre gewährleistet sein
- Der Algorithmus soll öffentlich definiert und evaluiert sein.

War es bisher ein Privileg von Regierungen und Militärs, sensible Daten mit kryptographischen Mitteln zu schützen, verwendet heute fast jeder solche Mittel, ohne es zu merken. Beim Surfen im Internet, bei der Nutzung von Pay-TV, beim Gebrauch der EC-Karte, beim Telefonieren usw.

Das neue AES-Verfahren wird sich auf unseren gesamten Lebensbereich ausdehnen. Alle Unternehmen und Dienstleister werden das Verfahren einsetzen.

12.7 Angriff auf Verschlüsseltes

Verschlüsselung knacken

Zuverlässige Kryptographie-Verfahren sollten fast unmöglich zu knacken sein. Der Aufwand für einen hochwertigen Algorithmus muss im Übrigen nicht unbedingt höher sein als für eine weniger effektive Lösung. Verfolgt man keine besondere Strategie, um einen Code zu knacken, muss man notfalls jede erdenkliche Kombinationen durchprobieren, bis man zufällig (siehe auch [Entropie](#))- irgendwann die Lösung findet. Mit steigender Codelänge wächst zwar die benötigte Rechenzeit exponentiell, doch alle 18 Monate verdoppelt sich gemäß **Moore'schen Gesetz** die Performance der jeweils aktuellen Rechner. Für einen 56-Bit-Schlüssel benötigt man bereits ein Computernetzwerk. 64- bis 80-Bit-Schlüssel sind vorerst nur von wenigen Staaten und Institutionen zu knacken, so dass man einen 128-Bit-Schlüssel zurzeit als sicher einstuft.

ArchiCrypt Live setzt 256 BIT ein und ist nach heutigen Gesichtspunkten auf der absolut sicheren Seite.

Aus der Länge des Schlüssels kann man nur ableiten, wie viele Versuche ein potentieller Angreifer im ungünstigsten Fall unternehmen muss um den Code zu brechen. In der Regel werden sehr viele solche Kombinationen durchgerechnet, bevor der Code gebrochen ist. Eine Methode, die sich mittels Brute-Force innerhalb einer Woche knacken lässt, kann auch schon zufällig nach drei oder vier Tagen, in Ausnahmefällen auch innerhalb eines Tages - aber nur mit sehr sehr niedriger Wahrscheinlichkeit - entschlüsselt sein. Wie man sieht, ist die bloße Länge des Schlüssels nicht der einzige Garant für hohe Sicherheit. Wurde der Schlüssel aus einer Zufallssequenz abgeleitet und wurde diese Sequenz nur „pseudo“-zufällig erzeugt, so kann auch ein vergleichsweise langer Schlüssel brechbar sein, wenn sich die Regel, nach der er errechnet wurde, ermitteln lässt. ArchiCrypt Live nutzt daher Ihre Mausbewegungen zur Erzeugung eines **Zufallszahlenpools**.

Ein kryptografisches Verfahren gilt als sicher, wenn die beste Methode ohne Schlüssel an die Daten zu gelangen die s.g. Brute-Force-Methode ist. D.h. man testet jeden möglichen Schlüssel.

Im Falle von ArchiCrypt Live wird die besonders sichere AES Implementierung mit einer 256 BIT Schlüssellänge. Im schlechtesten Fall muss ein Angreifer 2^{256} verschiedene Schlüssel testen, bis er den richtigen Schlüssel findet.

Dies ergibt ca. $1,1579208923731619542357098500869e+77$ verschiedene Schlüssel. Geht man davon aus dass ein Rechner 1000000 (1 Million) Schlüssel pro Sekunde durchtesten kann, bleiben

$1,1579208923731619542357098500869e+71$ Sekunden

$1,9298681539552699237261830834781e+69$ Minuten

$3,2164469232587832062103051391302e+67$ Stunden

$1,3401862180244930025876271413043e+66$ Tage

$3,6717430630808027468154168254911e+63$ Jahre

Sie sehen also, dass es recht lange dauern kann, bis man auf diese Art an die geheimen Informationen kommt.

Es gibt auch interessante Berechnungen darüber, ob die Masse der Erde ausreicht ($E=m \cdot C^2$), um die bei den Berechnungen nötigen Energiemengen aufzubringen.

Rainbow Tables

Man könnte eine Software schreiben, die den gerade angegebenen Schlüssel nutzt, gleich ob korrekt oder nicht, um verschlüsselte Daten zu entschlüsselt. Ist der Schlüssel nicht korrekt, entsteht reiner Datenmüll.

Dies ist oft wenig sinnvoll. Als äußerst wertvoll haben sich in diesem Zusammenhang die s.g. kryptografischen Hashfunktionen erwiesen. Es handelt sich um eine Art eindeutige Prüfsumme oder einen Fingerabdruck. Beim Verschlüsseln wird ein solcher Fingerabdruck Ihres Passwortes gespeichert, beim Entschlüsseln wird der Fingerabdrucke des eingegeben Passwortes berechnet und mit dem gespeicherten Wert verglichen. Stimmen beide Werte überein, ist dass Passwort korrekt und es kann entschlüsselt werden.

Rainbow Tables sind Tabellen, die zu jedem Eintrag aus einem Wörterbuch (enthält alle möglichen Kombinationen eines bestimmten Zeichenvorrats) den zugehörigen Hashwert/Prüfwert speichern. Hat man den Prüfwert, der ja offen gespeichert ist, kann man in der Tabelle den passenden Eintrag suchen und das zugehörige Passwort auslesen. Die Berechnung einer solchen Tabelle ist langwierig und speicherintensiv. Einmal berechnet, kann jedoch ohne großen Aufwand mit ihr gearbeitet werden.

Gegen diese Art des Angriffs gibt es eine lange bekannte Waffe. S.g. Salted Hashwerte. Man fügt dem Passwort vor der Berechnung eine bestimmte Anzahl zufälliger Zeichen hinzu. Berechnet also Hash(Passwort + SALT). Die vorberechneten Tabellen sind dadurch jetzt völlig wertlos. Die Neuberechnung entspricht dem Aufwand her in etwa einem Brute Force Angriff, bringt also keinen Vorteil mehr.

ArchiCryptX Change Pakete setzt selbstverständlich die Salted Hash Methode ein!

12.8 Hashfunktionen

Eindeutige Prüfsummen

Eine **Hashfunktion** ist eine Funktion, die eine Eingabe beliebiger Länge erhält und einen Funktionswert, den so genannten Hashwert liefert. Dieser Hashwert hat eine vorgegebene Länge. ArchiCryptX Change setzt SHA 1 ein. SHA1 (Secure Hash Algorithm 1) liefert einen Hashwert der Länge 160 Bit.

Im kryptografischen Umfeld kommen nur Hashfunktionen zum Einsatz mit denen es möglich ist, einen Hashwert zu einer Eingabe zu ermitteln. Eine Berechnung der Eingabe aus dem Hashwert hingegen ist unmöglich. (Diese Eigenschaft wird auch als **Einweg-Eigenschaft** bezeichnet, Funktionen mit dieser Eigenschaft als **Einweg-Hashfunktionen**.)

Die Anforderungen reichen weiter: Die Funktion muss öffentlich sein, d.h. jeder muss Zugriff auf die Funktion haben. Weiterhin soll es unmöglich sein, 2 unterschiedliche Eingabewerte zu finden, die den gleichen Hashwert liefern (Kollisionsfreiheit; wegen Kollisionsattacken). Da die Hashwerte genutzt werden, um Identitäten zu überprüfen, wäre es sonst nicht mehr möglich, eindeutig zu identifizieren.

ArchiCryptX Change setzt diese Funktion für verschiedene Zwecke ein. Der erste Einsatzfall ist die Aufbereitung der Zufallsdaten die bei der Generierung von Passwörtern und Schlüsseldaten gesammelt werden. Der zweite Einsatz kommt bei der Identifikation von Passwörtern und der Ableitung von Schlüsseln aus Passwörtern zum Einsatz.

12.9 Entropie

Informationsgehalt

Die Entropie einer Datei ist ein Maß für den Informationsgehalt. Die Entropie wird in bit/char (sprich Bit pro Zeichen) angegeben.

Informationsgehalt:

Für die Berechnung des Informationsgehaltes betrachtet man die Wahrscheinlichkeitsverteilung der Zeichen in einer Datei. Man geht davon aus, dass die einzelnen Bytes der Datei stochastisch unabhängig voneinander sind und mit gleicher Wahrscheinlichkeit in der Datei auftreten.

Der Informationsgehalt einer Nachricht $N[I]$ ist definiert:

$$\text{Informationsgehalt}(N[I]) := \log_2(1/P[I]) = -\log_2(P[I]).$$

$P[I]$ ist dabei die Wahrscheinlichkeit, mit der die Nachricht $N[I]$ in der Datei auftritt. \log_2 bezeichnet den Logarithmus zur Basis 2.

Der Informationsgehalt hängt damit ausschließlich von der Wahrscheinlichkeitsverteilung ab. Der semantische Inhalt geht dabei nicht in die Berechnung ein.

Da der Informationsgehalt einer seltenen Nachricht höher als der einer häufigen Nachricht ist, wird in der Definition der Kehrwert der Wahrscheinlichkeit verwendet.

Der Informationsgehalt zweier unabhängig voneinander ausgewählter Nachrichten ist gleich der Summe der Informationsgehalte der einzelnen Nachrichten.

Entropie

Mit der Definition des Informationsgehaltes kann nun die mittlere Information berechnet werden.

Für die Mittelwertbildung werden die einzelnen Nachrichten mit der Wahrscheinlichkeit ihres Auftretens gewichtet.

$$\text{Entropie}(P[1], P[2], \dots, P[r]) := -(P[1] * \log(P[1]) + P[2] * \log(P[2]) + \dots + P[r] * \log(P[r]))$$

Man kann das etwas verständlicher wie folgt beschreiben:

Die Entropie gibt die Unsicherheit als Anzahl der notwendigen Ja / Nein-Fragen zur Klärung einer Nachricht oder eines Zeichens an. Hat ein Zeichen eine sehr hohe Auftrittswahrscheinlichkeit, so hat es einen geringen Informationsgehalt. Dies entspricht etwa einem Gesprächspartner, der regelmäßig mit "ja" antwortet. Antworten, die sehr selten auftreten, haben einen hohen Informationsgehalt.

In diesem Zusammenhang sind die Extremwerte interessant:

Ein Dokument, welches nur Ziffern enthält, kann im schlechtesten Fall 0 bit/char Entropie besitzen, ein Dokument, in welchem alle Ziffern mit gleicher Wahrscheinlichkeit auftreten kann die Entropie (im Höchstfall) $\log_2(10) = 3,3219$ besitzen.

Für uns ist noch von Interesse, welche maximale Entropie in Dateien auftreten kann. Unsere Dateien sind aus Bytes aufgebaut. Also 8 Bit. Mit diesen 8 Bit kann man 256 verschiedene Zeichen darstellen.

Die Entropie für solche Dokumente beträgt mindestens 0 bit/char und höchstens 8 bit/char, falls in der Datei alle Zeichen gleich häufig vorkommen.

Entropie einer Datei

Die Entropie einer vorliegenden Datei kann also relativ leicht ermittelt werden. Man ermittelt für eine gegebene Datei, wie oft jedes Zeichen vorkommt.

das war schon immer so, man glaubt es kaum, aber es stimmt.

a	:= 6
b	:= 2
c	:= 1
d	:= 1
e	:= 4
h	:= 1
i	:= 2
k	:= 1
l	:= 1
m	:= 6
n	:= 2
o	:= 2
r	:= 3
s	:= 6
t	:= 3
u	:= 2

w := 1

Anschließend setzt man die Werte in obige Gleichung ein und erhält einen Entropiewert von 3,2682.

Wobei $P[a] = 6 / 58$, $P[b] = 2 / 58$ usw.

Verschlüsselte Dokumente kann man eventuell am Entropiewert erkennen. Je näher dieser Wert am Maximum liegt, desto größer ist die Wahrscheinlichkeit, dass es sich um eine verschlüsselte Datei handelt. Man kann diese Methode dazu nutzen, abzuschätzen, ob ein Angriff auf eine Datei erfolgreich war. Man testet verschiedene Passworte und nimmt das Ergebnis als Klartext, bei welchem der Entropiewert am geringsten ist.

Auf der anderen Seite sollte ein Verschlüsselungsverfahren immer Daten liefern, die einen fast maximalen **Entropiewert** besitzen. In unserem Fall also bei 7,9 und höher.

12.10 XOR

Das exklusive Oder

Dieses Verfahren können Sie selbst auf einem Blatt Papier nachvollziehen.

Der Schlüssel für dieses Verschlüsselungsverfahren besteht aus einer Folge von Bits (siehe auch [Passwörter](#)).

Der Schlüssel wird bitweise mit den Bits des Klartextes mittels exklusivem Oder (**XOR**) verknüpft.

Der Schlüssel selbst wird dabei zyklisch verwendet. D.h. Sind die Bits des Schlüssels aufgebraucht, beginnt man erneut beim ersten Schlüsselbit.

Die Entschlüsselung geschieht durch erneute Anwendung der Verknüpfung mit XOR. Dies ist eine Eigenschaft der XOR-Verknüpfung, die in der Fachsprache mit Involution bezeichnet wird.

Es gilt $((A \text{ XOR } B) \text{ XOR } B) = A$ für alle Wahrheitswerte A und B.

Das exklusive Oder ermittelt aus zwei Wahrheitswerten (FALSCH=0 und WAHR=1) einen neuen Wahrheitswert.

In der nachfolgenden Wahrheitstabelle ist dies aufgeführt:

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

Falls beide Werte gleich sind, wird also 0 = FALSCH geliefert. Falls genau ein Wert WAHR ist, liefert die Verknüpfung 1 = WAHR.

Beispiel:

Klartext:	1	0	1	1	0	0	1	0
Schlüssel:	1	0	0	0	1	1	1	1

Ergebnis:	0	0	1	1	1	1	0	1

Um aus dem Verschlüsselungsergebnis erneut den Klartext zu erhalten, wenden wir erneut die XOR-Operation unter Verwendung des Schlüssels an.

Ergebnis:	0	0	1	1	1	1	0	1
Schlüssel:	1	0	0	0	1	1	1	1

Klartext:	1	0	1	1	0	0	1	0

Kennt man das am häufigsten vorkommende Zeichen im Klartext, so ist die Ermittlung des Schlüssels und somit auch des Klartextes möglich.

Index

- " -

"Angewandte Kryptographie" von Bruce Schneier
114

"Verschlüsselung ist mir zu kompliziert" 110

- % -

%userprofile%\Anwendungsdaten\ArchiCryptSDF2
47

- / -

/C 49

/COF 49

/ERTF 49

/EX 49

/GEN 49

/GENS 49

/II 49

/J 49

/NC 49

/P 49

/PHP 49

/PL 49

/PLL 49

/PLS 49

/REL 49

/RTF 49

/S 49

/SI 49

/SL 49

/SLR 49

/SP 49

/SR 49

/T 49

/TH 49

/TXT 49

/WAV 49

- < -

<%Anmerkung%> 103

<%Anrede%> 103

<%Bezeichner%> 103

<%Blocked%> 103

<%Email%> 103

<%FAX%> 103

<%Firma%> 103

<%Gültigkeit%> 103

<%Hash%> 103

<%Hausnummer%> 103

<%Identifizierer%> 103

<%IKey%> 103

<%Installationen%> 103

<%Name%> 103

<%Ort%> 103

<%PLZ%> 103

<%Produkt%> 103

<%Straße%> 103

<%Tel%> 103

<%UKey%> 103

<%User-ID%> 103

<%Vorname%> 103

- 4 -

4096 BIT 111

- A -

Abbruch 103

Abfrage 33

Absender 103

absolute Sicherheit 110

Adi Shamir 111

Administratorrechte 20

Administrator-Schutz 67

Adresse des Internet-Kontrollskripts 82

Advanced Encryption Standard 112

Aktuelle Themen-Vorgabe überschreibt
Nutzerauswahl 67

Algorithmus 113

Ändere Schlüssel 99, 100

Ändern des Passworts / Schlüssels bei einem
ArchiCryptX Change Paket 99

Änderung rückgängig machen 72
 Anpassen der Meldungen und Hilfetexte 78
 Anzahl neuer Lizenzen 86
 ArchiCrypt Online 30
 ArchiCryptX Change 103
 ArchiCryptX Change Paket 22, 82
 asymmetrische Verfahren 111
 Auf Update prüfen 64
 Aufbau einer Kommandodatei 49
 Aussehen 64
 Aussehen des Pakets 33
 Auswahl eines Speicherortes 37
 Automatisch zuletzt aktive Themendatei 64
 Automatisch zuletzt aktiven Job laden 64

- B -

Beenden 30
 Beim Laden eines Jobs 64
 Benennung, Speicherorte und Passwort 82
 Beschriftung 73
 Betreff 103
 Bezeichner 82
 Binärmodus 103
 Bitte ein Thema laden 33
 Blockchiffre 115
 Blockieren umschalten Sichtbare 100
 Brute Force 114
 Brute-Force 116

- C -

-C 49
 -COF 49

- D -

Datei ausführen 31
 Dateien für das ArchiCryptX Change Paket festlegen 31
 Dateien Speichern in (XChange Zentrale) 64
 Dateiname der Lizenzkontrolldatenbank auf Webserver 82
 Datenbank-Upload 89
 Der Advanced Encryption Standard 115
 Der PHP Editor 107
 Der Themen Editor 70

Dialog zur Auswahl eines Themes 33
 Dialog zur Eingabe der E-Mail 37
 Dialogsprache 33
 Drag&Drop 31

- E -

Effekte Dialog aufrufen 72
 eigener Zeichensatz 65
 Ein Lizenznehmer - mehrere XChange Pakete - ein Lizenzdatensatz 95
 ein Logo / eine Grafik laden 72
 Eindeutige Prüfsummen 118
 Eingabefeld Passwort 42
 Einstellungen 30
 Einstellungen Allgemeines 64
 Einstellungen Kompression 65
 Einweg-Eigenschaft 118
 Einweg-Hashfunktionen 118
 Elementfarben festlegen 73
 E-Mail 37
 E-Mail bearbeiten 37
 Enterprise Version 26
 Entropie 118
 Entropie einer Datei 118
 Entropiewert 118
 Erstelle Lizenzkontrolldatenbank 89, 100
 -ERTF 49
 -EX 49
 Export Datenbank 92, 100
 Export Kenndaten 100
 Export Notschlüssel Clipboard 92
 Export Notschlüssel Datei 92
 Export Notschlüssel E-Mail 92
 Export Nutzerdaten Clipboard 92
 Export Nutzerdaten Datei 92
 Export Nutzerdaten E-Mail 92
 Export von Notschlüssel 100
 Export von Nutzerdaten 100
 Export von Passwörtern 42
 Extremwerte 118

- F -

Farbe / Sättigung ändern 72
 Farbe der Elemente 73
 Feature Matrix 26

Fertigstellen 45
 Filterausdruck 102
 Filterleiste 102
 FTP 103

- G -

-GEN 49
 Generator -> Speicherndialog 65
 -GENS 49
 Grafik speichern 72
 Graustufenbild erzeugen 72
 Größe der Grafik anpassen 72
 Gültigkeit 86
 Gültigkeit ändern 86
 Gültigkeit anpassen Auswahl 100
 Gültigkeit anpassen Sichtbare 100

- H -

Hash 22
 Hashfunktion 118
 Hilfe Anzeigedauer 64
 Hinweis/Abfrage 33
 Hinzufügen 31
 Hostname 103
 Hybrid-Codierung 111

- I -

Identifizierer 86
 Identifizierer ändern oder festlegen 86
 -II 49
 IKey 22
 Import Kenndaten 100
 Import von Passwörtern 42
 Info Installationszahl überschritten 82
 Info Zugang abgelaufen 82
 Info Zugang gesperrt 82
 Information 33
 Informationen über die Sicherheit der Lösung mit Internetkontrolle 108
 Informationsgehalt 118
 Informationsseiten 82
 Installationen anpassen Auswahl 100
 Installationen anpassen Sichtbare 100
 Installationsroutine 20

Installer erstellen 31
 InternetKey 22
 Internet-Kontrollskript 42, 82
 Internetschlüssel 22
 Ist Verschlüsselung sinnvoll? 110

- J -

-J 49
 Ja/Nein Abfrage 33
 Job 22
 Jobdatei speichern 45
 Job-Datei speichern 45

- K -

Keine Begriffe aus Ihrem sozialen Umfeld 113
 Keine lexikalischen Begriffe 113
 Keine Passwörter nur aus Ziffern 113
 Klartextansicht 42
 Kommandoschaltern 47
 Kommandozeilenversion 49
 Kompression 37, 65
 Kontextmenü 31, 64
 Kontrollskript 22, 90

- L -

Lade Job 31
 Laden Sie ein vorhandenes Thema 70
 Länge des Schlüssels 116
 Länge Nutzerkennung 103
 Länge Nutzerschlüssel 103
 Layout anpassen 30
 Leonard Adleman 111
 Link-Eigenschaft 73
 Lizenz für 86
 Lizenz gesperrt 86
 Lizenzdatenbank 22
 Lizenzdatenbank lokal speichern 91
 Lizenzen sperren 86
 Lizenzinformationen zuordnen 86
 Lizenzkontrolldatenbank 82
 Lizenznehmer eintragen 86
 Lizenzverwaltung 82
 Logo / Grafik für Thema wählen 72
 Lösche Eintrag 100

- M -

- MARS 112, 115
- MasterKey 22
- Mein Verschlüsselungsprogramm hat aber eine 4096 BIT Verschlüsselung 111
- Methode 113
- Mindestpasswortlänge 65
- Mindest-Passwortlänge 65
- Modi 103
- Mögliche Parameter beim Start von ArchiCryptX Change 47
- Mooreschen Gesetz 116
- PHP-Skript Upload 90
- PKCS 112
- PKCS #5 112
- PL 49
- Platzhalter für Schablonen 103
- Platzhalter in den Schablonen 86
- PLL 49
- PLS 49
- Port 103
- Position und Größe der Elemente 73
- Proxy 47
- Prüfwert 22

- R -**- N -**

- Nachfolgende Dateien nicht komprimieren 65
- Nachrichten Tabelle laden 78
- Nachrichtentabelle speichern 78
- Name für das ArchiCryptX Change Paket festlegen 37
- National Institut of Standards and Technology 112
- National Institute of Standards and Technology 115
- NC 49
- Neu in Version 5 7
- Neu starten 45
- NIST 115
- Nutzerkennung 22
- Nutzername 103
- Nutzerschlüssel 22
- Rahmenbedingungen 108
- Rainbow Tables 116
- RC6 112
- Regeln zur Passwortgestaltung 113
- REL 49
- Rijndael 112, 115
- Ron Rivest 111
- RSA 111
- RTF 49

- S -**- P -**

- P 49
- Paket erstellen 30
- Passiv 103
- Password-Based Cryptography Standard 112
- Passwort 103
- Passwort (Wiederholung) 42
- Passwort festlegen 42
- Passwort für Lizenzdatenbank ändern 91
- Passwortgenerator 65
- Passwortgenerator nutzen 65
- Persönliche Weitergabe von Lizenzdaten 92
- Pfadinformation speichern 37
- PHP 49
- S 49
- SALT 22
- Salted Hash Methode 116
- Schablone Export Lizenzdaten 103
- Schablone Export Nutzerdaten 103
- Schablone Notfallschlüssel 103
- Schablonen E-Mail und Export Nutzerdaten 103
- Schalter Abfrage 49
- Schalter Ausführen 49
- Schalter Execute 47
- Schalter Generator 49
- Schalter Generator, Einzeldatei 49
- Schalter Information 49
- Schalter Installationsmodus 49
- Schalter Job 49
- Schalter Kein Dialog 49
- Schalter Keine Kompression 49
- Schalter Kommandodatei 49
- Schalter Kompression 49
- Schalter Kontrolldatei 47

Schalter Nutzerkennung 47
 Schalter Open 47
 Schalter Passwort 47, 49
 Schalter Passwortliste 49
 Schalter Passwortliste mit Reportdatei 49
 Schalter Passwortliste, Einzeldatei 49
 Schalter PHP Kontrolldatei 49
 Schalter Quelle 49
 Schalter Quelle rekursiv 49
 Schalter Quellliste 49
 Schalter Quellliste rekursiv 49
 Schalter Speichere Pfadangaben 49
 Schalter Speichere Pfadangaben, reaktiv 49
 Schalter Sprachnotiz 49
 Schalter Thema 49
 Schalter Vertrauliche Nachricht 49
 Schalter Ziel 49
 Schalter Zielverzeichnis 47
 Schlüssel / Passwort 82
 Schlüssel und Datenbank 103
 Schlüsseldatei einlesen 82
 Schrifteigenschaften 73
 sdfproxy.ini 47
 Secure Hash Standard 112
 Serpent 112
 SHA 112
 -SI 49
 Sichere Passwörter 113
 Sicherheit eines Verfahrens 111
 Sichern der Datenbank 91
 -SL 49
 -SLR 49
 SmallXChange 49
 So könnte Ihr Passwort aussehen 113
 -SP 49
 Speicherort 37
 Sprachnotiz 33
 -SR 49
 Standard Thema 70
 Start der Anwendung 64
 Statusleiste 102
 symmetrische Verfahren 111
 Synchron Modus 103

- T -

-T 49

Tabellenansicht 103
 Tabellenzeile für Lizenzkontrolldatei 103
 Teilschlüssel 22
 Test 103
 Testen 45
 Text bearbeiten 33
 Text editieren 33
 Text Editor 33
 Texte erstellen und laden 33
 -TH 49
 Thema 22
 Thema als Standard definieren 70
 Thema festlegen 33
 Thema im Editor laden 70
 Thema laden 33
 Theme Editor 33
 Theme laden 33
 Themen-Editor starten 33
 TIPP nur vertrauliche Nachricht: 40
 Tools 100
 Trennzeichen nutzen 65
 Twofish 112, 115
 -TXT 49

- U -

Über 64
 Übernehmen 33
 UD 49
 UID 22
 User-ID 22
 UserKey 22

- V -

verdeckten Passwordeingabe 42
 Verify 100
 Verschlüsselung knacken 116
 Verschlüsselungssoftware kann nur Teil eines Sicherheitskonzeptes sein 110
 Verschlüsselungsverfahren 111
 Vertrauliche Nachricht verfassen 40
 Verwalten vorhandener und Erstellen neuer Lizenzen 82

- W -

- WAM 22
- Was tun, wenn ein Notschlüssel herausgegeben wurde? 92
- Was versteht man unter Verschlüsselung? 111
- WAV 49
- WEB Access Manager 22
- Weitere Funktionen Logo / Grafik 72
- Weitergabe erzeugter Passwörter 42
- Weitergabe von Lizenzdaten via E-Mail 92
- Werbetext 33
- WICHTIG Verzeichnisse auf WEB Server vorbereiten 82
- Wie funktioniert die Kontrolle via Internet 81
- Wie wird das Passwort bewertet 114
- Wissenschaft der Verschlüsselung 111
- Wörter
 - die Sie auf keinen Fall als Passwort benutzen sollten 113
- Wörterbücher 113

- X -

- XOR 120

- Z -

- Zahlen als Passwort 113
- Zeichen der Tastatur als Passwort 113
- Zielverzeichnis für Lizenzkontrolldatei auf Webserver 82
- ZIP- und CAB-Archive 37
- Zufallsdaten 118
- Zufallssequenz 116
- Zufallszahlenpool 116
- Zweck / Funktion des ArchiCrypt WEB Access Managers 81

Endnotes 2... (after index)

Back Cover