Dok.-Nr.: ACLB-HB-0007

Ausgabedatum: 08.03.2017

Ausgabe-Nr.: 7.1

Handbuch
ArchiCrypt Passwort Safe

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Alle Rechte vorbehalten Weitergabe sowie Vervielfältigung dieser Unterlage, Verwertung und Mitteilung ihres Inhalts sind nur mit ausdrücklicher Zustimmung von Patric Remus erlaubt. Zuwiderhandlungen verpflichten zum Schadenersatz.

D-85521Ottobrunn
Telefon (089) 66000893
Telefax (089) 66000875
E-Mail Anfrage@ArchiCrypt.com

Inhalt

Teil I ArchiCrypt WEB-Seite 0

Teil II ArchiCrypt Downloads 0

Teil III ArchiCrypt Passwort Zentrale 0

Teil IV Hilfe zur Hilfe 3

Teil V Bestelllen / Freischalten 3

Teil VI Einleitung 6

1 Willkommen 6
2 Neu in dieser Version 9

Teil VII Allgemeine Informationen 15

1 Installationshinweise 15
2 Systemvoraussetzungen 15
3 Credits 16

Teil VIII Bedienung 23

1 Workshop 23
2 Überblick 24
3 Erster Start von ArchiCrypt Passwort Safe 27
4 Safe erstellen und öffnen 30
5 Die Bedienoberfläche 39
6 Übersicht über Menüs 45
7 Passworteintrag 67
8 Überwachung 79
9 Textverschlüsselung 81

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

10 Drag-Drop Verschlüsselung ... 83
11 Einstellungen ... 86
12 Austausch von Passwort Datenbanken ... 120
13 Was ist ein gutes Passwort? ... 126
14 ArchiCrypt Passwort Safe-Online ... 128

Teil IX PassOnPaper 1

1 Bedienung ... 1
2 Sicherheit von PassOnPaper ... 5

Teil X Dialoge 8

1 Safeeintrag erstellen ... 8
2 Dialog zur Suche ... 26
3 Passworteingabe ... 28
4 Virtuelle Tastatur ... 31
5 Schlüsseldateien ... 33

Teil XI Tastaturkürzel 37

Teil XII Mobile Nutzung 38

1 Safe Portable ... 38

Teil XIII Umgang mit der Software 41

1 Datenverlust vorbeugen ... 41
2 Sicherheit ... 42

Index 46

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

4 Hilfe zur Hilfe

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.

Vorgehensweisen

Textstellen, die mit einem solchen Symbol gekennzeichnet sind, enthalten eine Anleitung für ein bestimmtes Vorgehen.

TIPPS und Tricks

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

5 Bestelllen / Freischalten

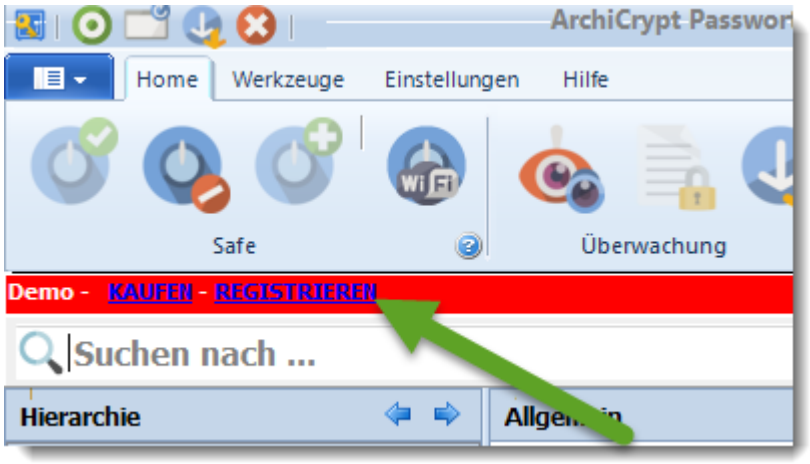
Bestellen bei ArchiCrypt

ArchiCrypt Passwort Safe im Shop

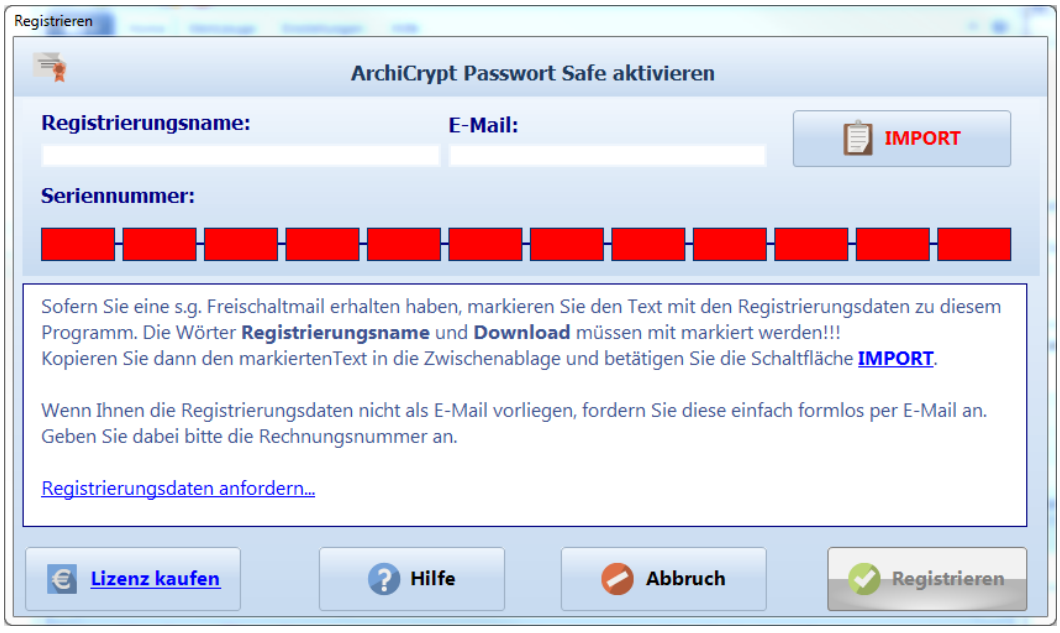
Weitere Bestellmöglichkeiten >>[5]

So schalten Sie ArchiCrypt Passwort Safe frei

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



Es erscheint der folgende Dialog:



© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

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

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

5. Klicken Sie jetzt auf ***IMPORT***

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

➡**HINWEIS: Mit der PC Version können Sie eine portable Version[38] erzeugen. Diese müssen Sie ebenfalls registrieren. Dazu dürfen Sie die gleichen Registrierungsdaten verwenden wie bei der PC Version.**

Weitere Bestellmöglichkeiten

Weitere Bestellmöglichkeiten		
Online-Shop	zum Online-Shop	Sobald Sie den Bestellvorgang starten, wird eine verschlüsselte SSL-Verbindung aufgebaut. Alle Daten, die zwischen Ihrem Rechner und

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

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

6 Einleitung

6.1 Willkommen

Vielen Dank, dass Sie sich für ArchiCrypt Passwort Safe entschieden haben!

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Mangelndes Sicherheitsbewußtsein und Bequemlichkeit

Wahrscheinlich ist Ihnen bewusst, dass die Sicherheit Ihrer Daten nicht zuletzt von der geschickten und klugen Wahl Ihres Passwortes abhängt. Genau an diesem Punkt beginnt jedoch oft das Problem. Sichere Passwörter kann man sich nur schwer merken und einfach zu merkende Passwörter bieten keinerlei Schutz. Haben wir uns dann endlich ein wirklich gutes Passwort erstellt und gemerkt, nutzen wir das Passwort bei jeder sich bietenden Gelegenheit. Es wird als Absicherung des Zugangs zu Foren, zum E-Mail Konto, zu diversen Online-Shops, zum PayPal-, eBay- und Amazon-Konto genutzt. Man muss den Satz nur nochmals lesen und kurz über die Tragweite nachdenken. Die Gefahr sticht ins Auge und wird dennoch in der Praxis kaum wahrgenommen!

Meldungen über den **Diebstahl von Nutzerdaten** sind inzwischen an der Tagesordnung. Kann man den Verlust von Zugangsdaten für ein relativ unwichtiges Forum noch leicht verschmerzen, wird es schnell unangenehm, wenn Sie mit den gleichen Daten auch Ihren eBay Account oder den Zugang zum PayPal Konto schützen. Sie fragen sich jetzt sicher, woher die Datendiebe wissen sollen, dass Sie auch bei eBay und Amazon ein Konto haben, oder?

Die Antwort ist sehr einfach! Die Diebe wissen es nicht, sie probieren es einfach aus. Auch das Bild des vor dem PC sitzenden Hackers, der seinen Browser geöffnet hat und dort verschiedene Passwörter durchprobiert, ist vollkommen falsch und unrealistisch. Es kommen hochspezialisierte Computerprogramme zum Einsatz die innerhalb weniger Minuten Millionen von Passwörtern in allen Varianten auf den begehrtesten Seiten im Internet testen.

Ich erzähle Ihnen das, weil die Ursache für dieses Verhalten **Bequemlichkeit** ist. Eine absolut nachvollziehbare Bequemlichkeit. Denn, wer hat die Zeit, sich bei jeder Internetseite mit Login ein sicheres Passwort zu erzeugen und es dann entweder auf Papier festzuhalten oder es sich zu merken.

Etwas weniger sicherheitskritisch, dafür jedoch äußerst lästig, ist die Aufgabe, die Passwörter auf den Internetseiten einzugeben.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Von Key-Loggern, die jede Eingabe per Tastatur protokollieren und anschließend versenden, ganz zu schweigen.

Uns ist bewusst, dass es durchaus "Lösungen" gibt, die direkt in die jeweiligen Browser integriert sind. Schnell stimmt man zu, dass die Login Daten gespeichert werden. Bei diesen integrierten Lösungen ist man immer auf einen bestimmten Browser festgelegt. Es ist nicht möglich, die Daten, die man in Firefox angelegt hat, im nächsten Moment im Internet Explorer zu nutzen.

Darüber hinaus bietet ArchiCrypt Passwort Safe eine Fülle zusätzlicher Funktionen, die Sie nach kurzer Zeit nicht mehr missen möchten.

ArchiCrypt Passwort Safe kümmert sich um Ihre Daten
Sie müssen sich nur noch **ein** sicheres Passwort erzeugen und merken. Das Passwort nämlich, mit dem der Passwort Safe geschützt wird. Den Rest erledigt der Passwort Safe für Sie. Er generiert sichere Passwörter für jede beliebige Internetseite und überträgt diese per Hotkey in die Eingabefelder, ver- und entschlüsselt Texte und sogar Dateien. Er kann das Starten bestimmter Anwendungen erkennen und zugehörige Daten automatische bereitstellen u.v.m.

Es gibt wenige Anwendungen, die auf **mobilen Endgeräten** wie Tablet und SmartPhone ebenso Sinn machen, wie auf dem PC. Der Passwort Safe gehört jedoch ohne Zweifel zu diesen sinnvollen Programmen. Sie finden daher im Apple AppStore und im Google Play Store Version für die entsprechenden Plattformen. Dabei können Sie die Passwort Datenbank beliebig zwischen den Plattformen austauschen. Die Daten, die Sie auf dem PC Verwenden, können Sie jetzt auch auf SmartPhone und Tablet nutzen.

ArchiCrypt Passwort Safe bietet hohe Sicherheit bei hohem Komfort!

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

Dipl.-Ing. Patric Remus

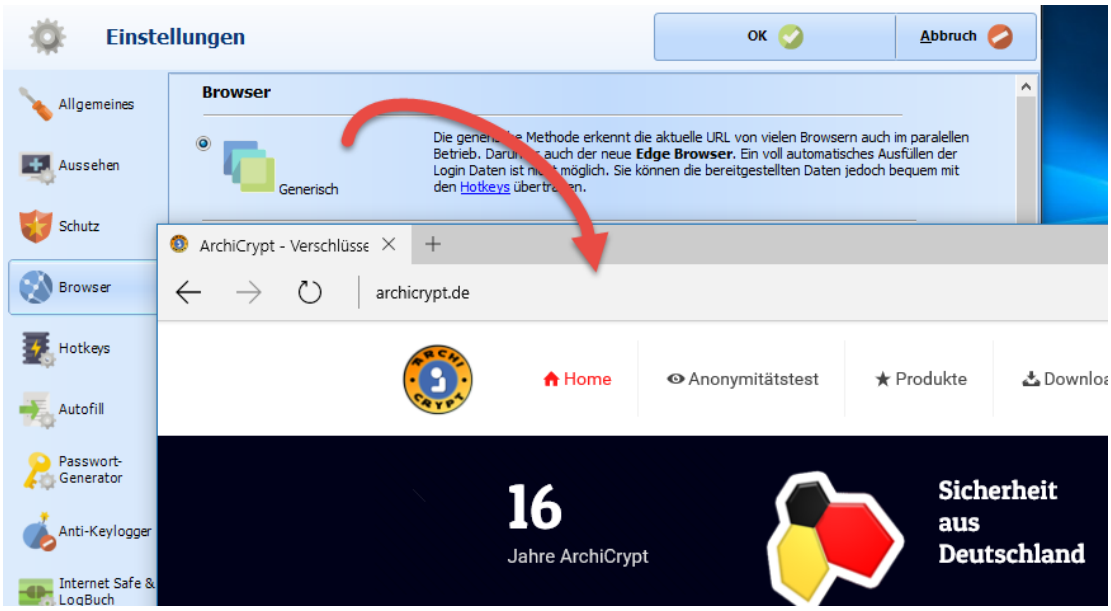
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

6.2 Neu in dieser Version

Welche Neuerungen bietet der ArchiCrypt Passwort Safe 7

Unterstützung für Microsoft Edge

Der mit Windows 10 vorgestellte Browser Edge, steckt noch in den Kinderschuhen. Durch die tiefe Integration in das neue Betriebssystem ist es jedoch unumgänglich eine Unterstützung anzubieten. Version 7.7.1 + führt die generische Browser-Unterstützung ein. Diese erkennt nicht nur den neuen **Edge Browser**, sondern erlaubt auch den parallelen Betrieb verschiedener Browser. Der Passwort Safe erkennt die aktuelle URL des Browsers im Vordergrund und stellt den passenden Eintrag im Safe ein. Die Inhalte können so per Hotkey in den Browser übertragen werden.



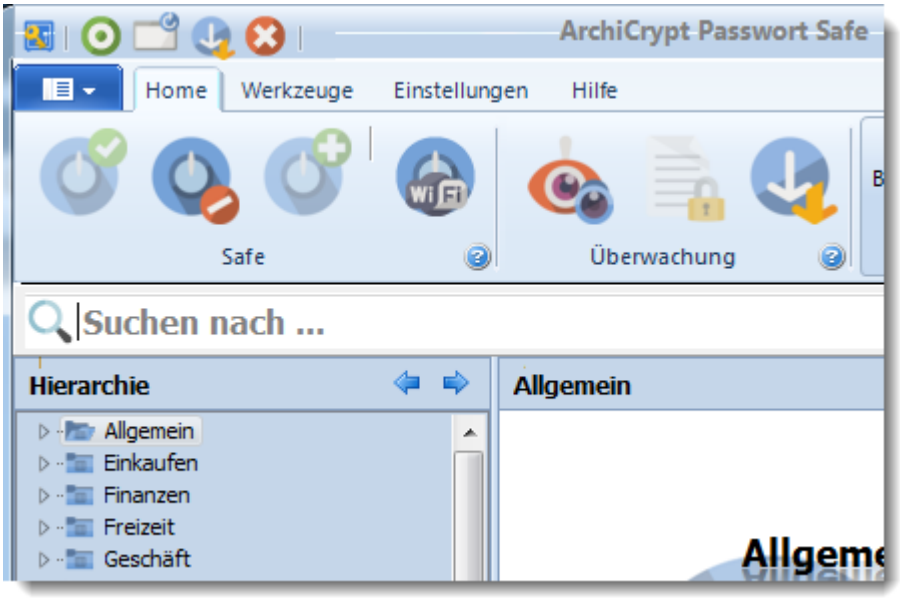
Suche als zentrale Funktion

Viele Anwender nutzen das Programm seit der ersten Stunde. Gleichzeitig steigt die Zahl an Diensten, die ein sicheres Passwort verlangen, immer weiter an. Eine leistungsfähige Suche ist daher von großer Bedeutung.

Wenn Sie ArchiCrypt Passwort Safe in den Vordergrund rufen, können Sie direkt einen Suchbegriff eingeben. Der entsprechende Eintrag wird markiert und Sie können zum Beispiel durch Betätigen der Eingabetasten zur verknüpften Internetseite springen. Befindet sich der Passwort Safe im **Überwachen** Modus, minimiert im

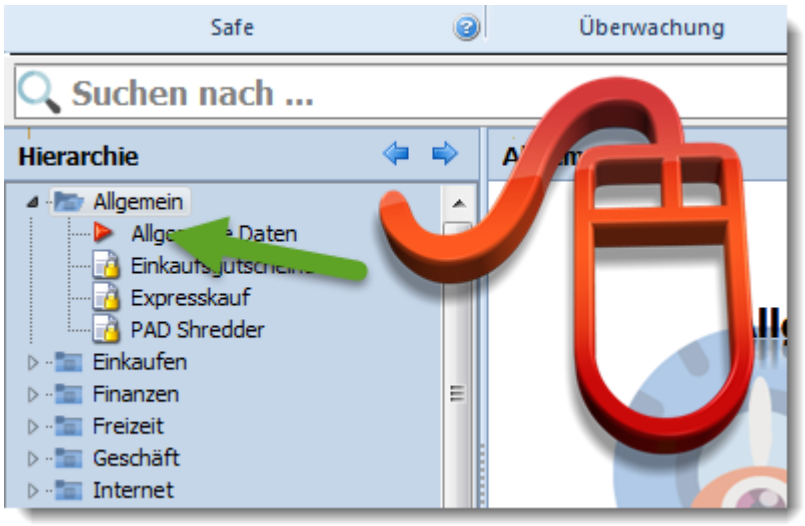
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Systemtray, können Sie die Suche mit Hilfe eines **Hotkeys** aufrufen.



Einfacheres Bearbeiten

In allen Listen, in denen die Passwort Safe Einträge aufgeführt sind, genügt es jetzt, den Eintrag **doppelt anzuklicken**, um den Eintrag zu bearbeiten. Betätigt man die **Entf Taste**, werden Einträge gelöscht.



Sofortiges Speichern

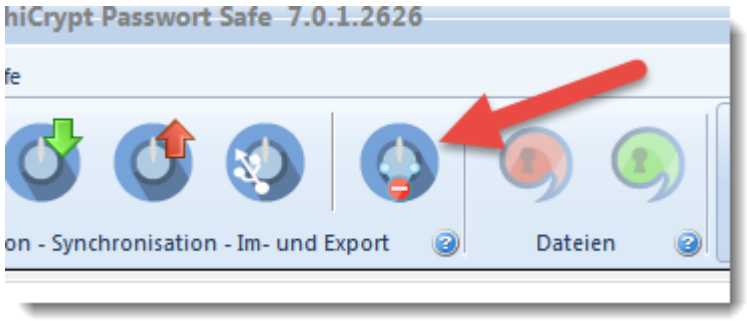
Änderungen an der Passwort Datenbank werden sofort in die Passwortdatenbank geschrieben. Stürzt der Rechner ab, bevor man

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

den Passwort Safe geschlossen hat, gehen neue Passworteinträge nicht verloren.

Passwort Datenbank aufräumen

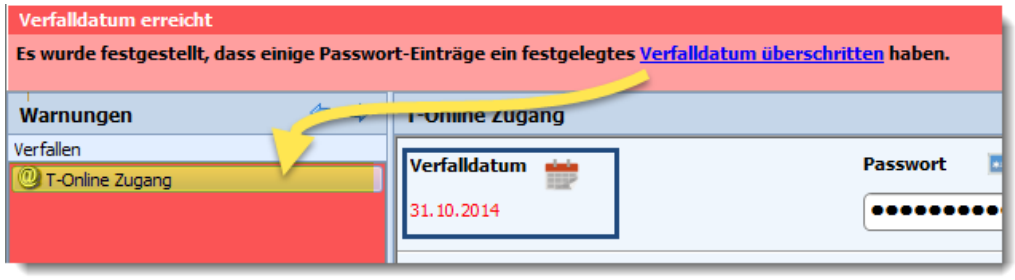
Passwort Einträge werden beim Löschen, ähnlich wie Dateien auf Ihrer Festplatte, nicht wirklich gelöscht, sondern nur als ungültig markiert. Durch das Aufräumen werden diese Einträge tatsächlich aus der Datenbank entfernt. Die Größe der Datenbankdatei schrumpft entsprechend.



Verfalldatum

Insbesondere bei Zugangsdaten zu Online-Diensten macht es Sinn, ein Verfalldatum für ein Passwort festzulegen. Regelmäßiges Ändern schützt davor, dass man bei einem großangelegten Datendiebstahl bei einem Internet Dienstanbieter selbst Opfer wird. Im Allgemeinen dauert es nämlich etwas, bis die entwendeten Daten tatsächlich missbräuchlich verwendet werden.

Gerade Zugangsdaten zu E-Mail Postfächern sind oft der Schlüssel zu allen anderen Zugangsdaten. Wer diese Passwörter regelmäßig ändert, mindert die daraus resultierenden Gefahren deutlich.

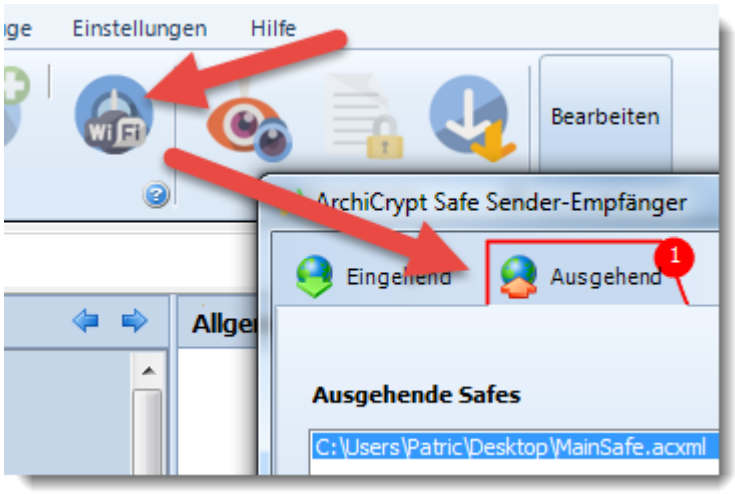


Übertragen von Passwort Safes im LAN

Gerade der Sprung auf die mobilen Geräte macht es erforderlich, die Daten zwischen verschiedenen Plattformen auszutauschen. Im eigenen Netzwerk können Passwort Datenbanken jetzt ohne

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Rückgriff auf einen Drittanbieter (*Dropbox, ArchiCrypt Passwort Zentrale, etc.*)bequem via LAN/WLAN übertragen werden. Dabei spielt es keine Rolle, ob man einen Passwort Safe von einem Windows Rechner zum iPhone, vom iPhone zum Android Tablet oder von einem PC zu einem anderen PC übertragen möchte.



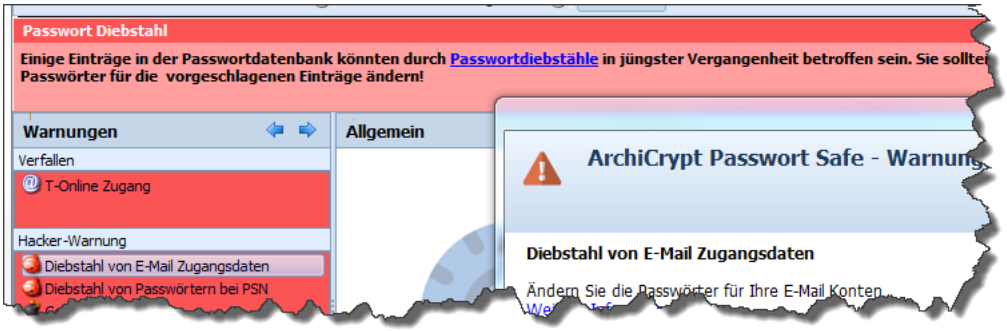
Cloud Anbindung

Beim Öffnen und Anlegen von Passwort Safes erkennt ArchiCrypt Passwort Safe verschiedene Coud Anbieter.
Ein Klick genügt und Sie können einen Safe im Cloud Verzeichnis abgelegen bzw. von dort laden. Sofern Sie *Dropbox* verwenden, stellt ArchiCrypt Passwort Safe sicher, dass die Passwort Datenbank so abgelegt wird, dass sie von den mobilen Versionen für iOS und Android gefunden wird.

Alarm bei Passwort Diebstahl

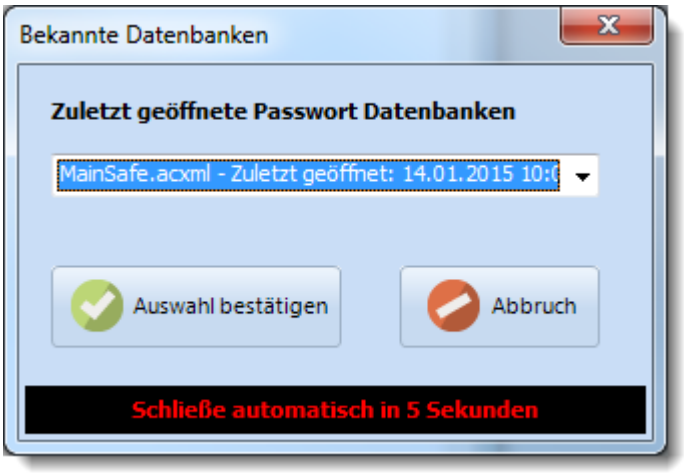
Der Diebstahl von Nutzer- und Passwortdaten ist inzwischen fast alltäglich geworden. Schwer, hier selbst den Überblick zu behalten und schnell zu reagieren. Der **Diebstahl Alarm** informiert über Datendiebstahl bei großen Internetanbietern und gibt Ihnen die Möglichkeit, schnell zu reagieren.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



History Liste

Der Begriff hört sich zunächst unspektakulär an, hat jedoch in der Praxis weitreichende Vorteile. Verwendet man unterschiedliche Passwort Datenbanken oder arbeiten verschiedene Personen an einem Rechner, dann kann man jetzt mit Hilfe der History schnell zwischen verschiedenen Datenbanken wechseln.



Windows 10 Unterstützung

Im Laufe des Jahres 2015 wird Windows 10 erscheinen. Die aktuell verfügbare Technical Preview ist eine frühe Version, die lediglich einen Überblick bietet. Eine unfertige Vorschau eben. Dennoch gibt es ein Gefühl der Sicherheit, wenn man weiß, dass der Passwort Safe für die Zukunft gerüstet ist.

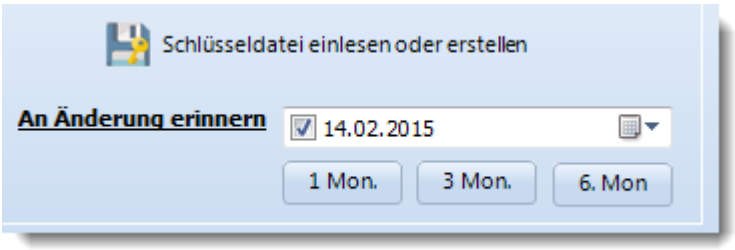
Die Funktionen wurden alle an die neue Windows Version angepasst. Einzig die Anti-KeyLogger Funktionen sind unter Windows 10 nicht verfügbar. Es ist durchaus möglich, dass sich dies mit zunehmender Fertigstellung von Windows 10 noch ändert.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Was müssen Sie beim Umstieg auf die neue Version beachten?

Sie können Ihre vorhandene Passwort Datenbank ohne Änderungen weiter verwenden. Ein Verfalldatum wird bei vorhandenen Einträgen nicht gesetzt. Wenn Sie ein Verfalldatum aktivieren möchten, klicken Sie doppelt auf den Eintrag. Beim Bearbeiten können Sie jetzt ein entsprechendes Datum festlegen.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Lesen Sie weiter bei **So gelingt der Umstieg von der Vorversion**[28]

7 Allgemeine Informationen

7.1 Installationshinweise

Das Programm wird mit einer Installationsroutine geliefert, die Ihnen die Arbeit abnimmt.

Achten Sie darauf, dass Sie unter den Betriebssystemen **Windows 7/8** und **10** zur Installation der Software lokale Administratorrechte besitzen müssen.

7.2 Systemvoraussetzungen

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

Betriebssystem
Windows 7/8 oder Windows 10

Minimale Anforderungen

Microsoft Windows 7
Bildschirmauflösung 1024x768 mit 32k Farben
ca. 30 MB freier Festplattenplatz
Intel Pentium oder AMD K5 Prozessor mit mindestens 200 MHz
512 MB RAM
CD-ROM oder DVD-ROM-Laufwerk (optional)

Empfohlene Systemkonfiguration

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Microsoft Windows 7
Bildschirmauflösung 1024x768, true color
50 MB freier Festplattenplatz
2 GB RAM
CD-ROM oder DVD-ROM-Laufwerk

Bei Installation auf einem Wechselmedium zur mobilen Nutzung, benötigen Sie ca. 50 MB freien Speicherplatz.

➡**WICHTIG: Sie können nur Passwortdaten an Anwendungen übertragen, die mit gleichen oder niedrigeren Rechten laufen, wie ArchiCrypt Passwort Safe. Sie können ArchiCrypt Passwort Safe als Administrator starten, um an alle Anwendungen Daten übertragen zu können.**

➡**WICHTIG: Je nachdem, welchen Browser[93] Sie verwenden, stehen Ihnen andere Funktionen zur Verfügung. Wir Empfehlen den Einsatz von Internet Explorer oder Firefox.**

7.3 Credits

```
  LICENSE ISSUES
  ==============

  The OpenSSL toolkit stays under a dual license, i.e. both the
conditions of
  the OpenSSL License and the original SSLeay license apply to
the toolkit.
  See below for the actual license texts. Actually both licenses
are BSD-style
  Open Source licenses. In case of any license issues related to
OpenSSL
  please contact openssl-core@openssl.org.

  OpenSSL License
  ---------------

/*
=====================================================================
====
 * Copyright (c) 1998-2011 The OpenSSL Project.  All rights
reserved.
 *
 * Redistribution and use in source and binary forms, with or
without
 * modification, are permitted provided that the following
conditions
 * are met:
 *
```

```
 * 1. Redistributions of source code must retain the above
copyright
 *    notice, this list of conditions and the following
disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above
copyright
 *    notice, this list of conditions and the following
disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of
this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL
Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not
be used to
 *    endorse or promote products derived from this software
without
 *    prior written permission. For written permission, please
contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called
"OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior
written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the
following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL
Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS''
AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL
PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
```

```
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 *
================================================================
====
 *
 * This product includes cryptographic software written by Eric
Young
 * (eay@cryptsoft.com).  This product includes software written
by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */

 Original SSLeay License
 -----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with
Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as
long as
 * the following conditions are aheared to.  The following
conditions
 * apply to all code found in this distribution, be it the RC4,
RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL
documentation
 * included with this distribution is covered by the same
copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright
notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be
given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program
startup or
```

```
 * in documentation (online or textual) provided with the
package.
 *
 * Redistribution and use in source and binary forms, with or
without
 * modification, are permitted provided that the following
conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following
disclaimer.
 * 2. Redistributions in binary form must reproduce the above
copyright
 *    notice, this list of conditions and the following
disclaimer in the
 *    documentation and/or other materials provided with the
distribution.
 * 3. All advertising materials mentioning features or use of
this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines
from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative
thereof) from
 *    the apps directory (application code) you must include an
acknowledgement:
 *    "This product includes software written by Tim Hudson
(tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS
BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF
```

```
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically
available version or
 * derivative of this code cannot be changed.  i.e. this code
cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```

ArchiCrypt Passwort Safe is using the libraries to load Password Safe via SSL/TLS
##################################

ArchiCrypt Passwort Safe nutzt für die Übertrag der Login Daten externe Skriptdateien, die mit Autoit Version 3 erzeugt wurden.
http://www.autoitscript.com/site/autoit/

Als Basis für Firefox dient das Script _FF_AutoLogin von Herrn Thorsten Willert, welches wiederum
das Script FF.au nutzt.

```
        * FF.au3
        *
        * This program is free software; you can redistribute it and/or
        * modify it under the terms of the GNU General Public License
        * as published by the Free Software Foundation; either version
2
        * of the License, or any later version.
        *
        * This program is distributed in the hope that it will be useful,
        * but WITHOUT ANY WARRANTY; without even the implied
warranty of
        * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
See the
        * GNU General Public License for more details.
        *
        * You should have received a copy of the GNU General Public
License
        * along with this program; if not, write to the Free Software
        * Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA
02111-1307, USA.

        - Jonathan Bennett and the AutoIt Team for AutoIt v3 the
freeware
        BASIC-like scripting language
        (and thanks John George Kemeny and Thomas Eugene Kurtz for
BASIC)
```

- Dale Hohm, for his great IE.au3, which I've used as base for the
functions-names and the error handling.
- Johannes Schirmer, for some functions and suggestions for the FF.au3
- all others for their suggestions, bug reports ...
- the FireFox-Team for his fantastic browser

- and Massimiliano Mirra, without his work would this UDF impossible,
for MozLab / MozRepl

Das Skript setzt voraus, dass Sie das Firefox Plugin MozLab / MozRepl installiert haben

https://github.com/bard/mozrepl/wiki

Folgende freie Komponenten und Module kommen zum Einsatz:

```
// Project:         Drag and Drop Component Suite
// Module:          DragDrop
// Description:     Implements base classes and utility functions.
// Version:         5.2
// Date:            17-AUG-2010
// Target:          Win32, Delphi 5-2010
// Authors:         Anders Melander, anders@melander.dk, http://melander.dk
// Copyright        © 1997-1999 Angus Johnson & Anders Melander
//                  © 2000-2010 Anders Melander
//
-----------------------------------------------------------------------
-

//
******************************************************************
**********************
// * Export components for Delphi.
//
******************************************************************
**********************
// * Copyright 2001-2005, Bitvadász Kft. All Rights Reserved.
//
******************************************************************
**********************
// * This component can be freely used and distributed in commercial and
```

```
// * private environments, provied this notice is not modified in
any way.
//
**********************************************************
**********************
// * Feel free to contact me if you have any questions,
comments or suggestions
// * at support@maxcomponents.net
//
**********************************************************
**********************
// * Web page: www.maxcomponents.net
//
**********************************************************
**********************
// * Date last modified: 03.03.2005
//
**********************************************************
**********************
// * TmxExport v2.37
//
**********************************************************
**********************
// * Description:
// *
// * The TmxExport is a 100% native VCL component to export
tables, queries,
// * stringlists, etc. to different file formats.
// *
//
**********************************************************
**********************
```

ALMailSlot v1.06

(C)1999-2000 Andrew Leigh
http://www.alphalink.com.au/~leigh/components

Description:
ALMailSlot is a component which allows applications to send messages across
a network using mailslots.

Overbyte ICS InternetComponent Suite

http://www.overbyte.be

8 Bedienung

8.1 Workshop

In einem ca. **einstündigen Video** werden viele Themen rund um den Passwort Safe besprochen. In der nachfolgenden Übersicht finden Sie Links, die Sie direkt zu den entsprechenden Themen im Video bringen.

Video Workshop ArchiCrypt Passwort Safe 23

Inhaltsangabe Workshop

Das **Workshop** Video umfasst die nachfolgend aufgeführten Themen. Ein Klick auf den entsprechenden Link springt direkt zur passenden Stelle im Video bei **Youtube**.

Einführung
Einleitung
Benutzeroberfläche
Menüleisten
Safe erstellen
Passwort Dialog
Tipps zum Passwort
Safeeinträge erstellen
Passwort Diebstahl Warnung
Favoriten
Warnungen

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Detailansicht
Einträge organisieren
Kategorien und Ordner
Bearbeiten Menü
Hilfe
Kategorie erstellen
Ordner erstellen
Passworteintrag erstellen
Bezeichnung
Benutzername
Passwort
Passwort Generator nutzen
Internetseite für Safeeintrag
Tausendsassa
Eintrag verschieben
Erste Zusammenfassung
Eintrag löschen
Einstellungen anpassen
Hotkeys einrichten
Listen mit Hotkeys drucken
Hotkeys verwenden
Passwortgenerator
Passwort Safe schließen
Passwort Safe laden
Passwort Safe im Alltag
Passwort Eintrag suchen
Zusammenarbeit mit Browser sicherstellen
Browser überwachen
Symbol im Systemtray
Standby Modus
Kontextmenü Systemtray
Favorit festlegen
Erkennen einer Internetseite
Automatisches Login
Passwort für Internetseite erzeugen
Austausch von Passwortdatenbanken
WiFi LAN WLAN Modul
Safe Datenbank von PC zu PC
Austausch mit SmartPhone und Tablet

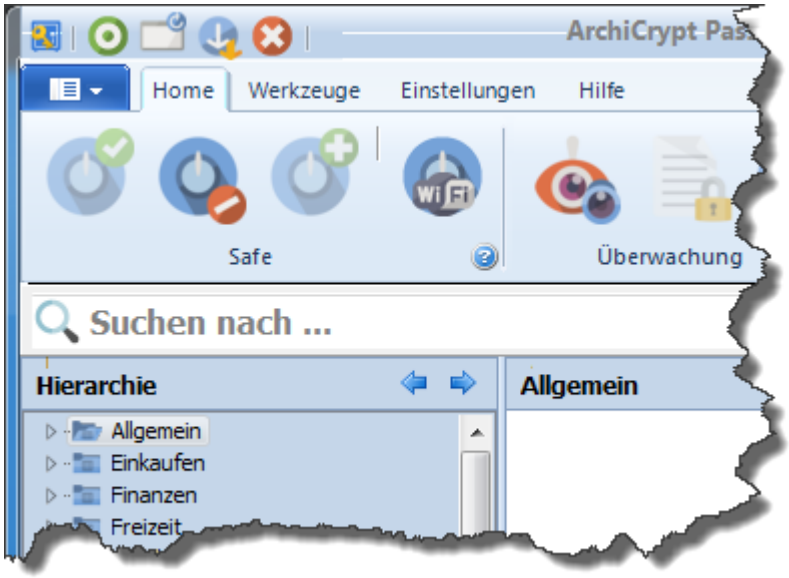
8.2 Überblick

Die Aufgabe, sich ein **gutes Passwort** auszudenken ist nicht so einfach, wie man sich dies vorstellt. Hat man diese Hürde genommen, steht man vor dem Problem, sich das Passwort merken zu müssen.

Ist auch das geschafft, steht man vor der praktisch **unlösbaren** Aufgabe, diesen Vorgang für eine Fülle unterschiedlichster

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Internetseiten, Mailkonten, FTP Zugänge, Anwendungen etc. zu wiederholen.



Im Alltag sieht es daher meist wie folgt aus:

1. Man erzeugt sich einfach zu merkende Passwörter wie **WinterMaus0867**. Passwörter, die man sich einfach merken kann, sind meist auch leicht knackbar. Mit speziellen Verfahren wie Wörterbuchattacken und Social Engineering geht es diesen Passwörtern sehr schnell an den Kragen.

2. Ist ein brauchbares Passwort erst einmal erstellt und man hat es sich gemerkt, dann wird es meist zur Absicherung bei jeder sich bietenden Gelegenheit genutzt. Bei eBay, bei Amazon, für das SmartPhone, den Zugang zum Rechner, für den E-Mail Zugang, das Telefonbanking usw.

   Mehrfachverwendung ist eine riesige Gefahr! Ist erst einmal **einer** der damit geschützten Dienste kompromittiert, besteht Missbrauchsgefahr bei **allen** Diensten. Immer wieder kommt es vor, dass Nutzerdaten bei großen Anbietern gestohlen werden. Diese gestohlenen Daten werden dann genutzt, um mit Hilfe spezieller Computerprogramme zu versuchen,Zugriff auf begehrte Internetdienste zu erhalten. Facebook, Amazon, eBay, Google Dienste, Dropbox etc.

ArchiCrypt Passwort Safe hilft

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

ArchiCrypt Passwort Safe gestattet das bequeme Verwalten von Passwörtern, dient als Zentrale für Schlüssel- und Registrierungsdateien, unterstützt Sie bei der Erzeugung sicherer Passwörter, verschlüsselt Text, verschlüsselt auf Wunsch auch Dateien, bewertet bestehende Passwörter, kann Login Daten automatisch an den jeweiligen Browser übertragen.

Alle sensiblen Daten und nicht nur das Passwort werden dabei mit Hilfe modernster Verschlüsselungsverfahren geschützt. Ab jetzt genügt es, wenn Sie sich **EIN Passwort** für ArchiCrypt Passwort Safe merken.

Wer ArchiCrypt Passwort Safe unterwegs nutzen möchte, kommt mit **Safe Portable (USB)** auf seine Kosten. Diese **portable** Version lässt sich aus der PC Version heraus erzeugen.

Weitere wichtige Gründe, die für ArchiCrypt Passwort Safe sprechen:

- **Vollverschlüsselung** sogar im Hauptspeicher. Alle Daten im Passwort Safe bleiben auch im Hauptspeicher so lange verschlüsselt, bis sie an eine andere Anwendung übertragen werden.
- **Anti-Keylogger** Funktionen die auch Eingaben in anderen Anwendungen schützen.
- Einfache **Verschlüsselung** von Texten und Dateien. Damit können Sie zum Beispiel nicht nur sicher E-Mails und Dateien mit anderen austauschen, sondern auch sensible Informationen auf Ihrem Rechner schützen.
- **Grafiken** und **kleinere Dateien** können direkt in den Safe übernommen werden. Die Daten werden selbstverständlich ebenfalls verschlüsselt direkt im Passwort Safe abgelegt. Nach Eingabe des Passwortes stehen die Daten dann auf Wunsch zur Verfügung.
- **PassOnPaper** ein Passwort Safe auf Papier zum Ausdrucken. Hilft immer dann, wenn man unterwegs keinen Zugriff auf entsprechende Hardware hat.
- Erzeugen von **aussprechbaren Passwörtern**. Herkömmliche Passwörter der Art ZGfcx6Rdi sind nicht zuletzt deshalb schwer merkbar, weil man sie nicht aussprechen kann. Dagegen kann man sich Passwörter wie DaGeSiNaru schon leichter merken.
- **Mobile Versionen** für **iOS** und **Android** stehen optional im Apple AppStore und im Google Play Store zur Verfügung.
- u.v.a.m.

Folgende Themen könnten Sie ebenfalls interessieren:

Erster Start - So richten Sie ArchiCrypt Passwort Safe ein 27

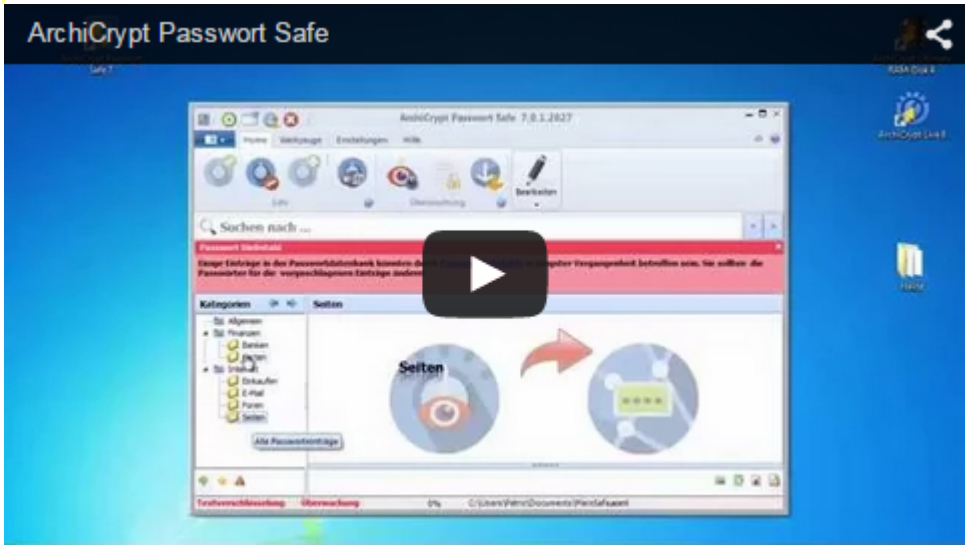
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Safe erstellen 30
Überwachung 79

8.3 Erster Start von ArchiCrypt Passwort Safe

Sehen Sie sich das etwa einstündige Video an, in dem detailliert auf die wichtigsten Themen eingegangen wird.
Sie können aus der Übersicht auch gezielt zu einzelnen Themen springen 23.

Video Workshop ArchiCrypt Passwort Safe 23



HOME-Ansicht

Falls noch kein Passwort Safe erstellt wurde oder ein Passwort Safe geschlossen wird, erscheint die Home Ansicht 47 mit einer Kurzanleitung.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Die Kurzanleitung leitet Sie Schritt für Schritt durch den Erstellprozess und bietet Ihnen die Möglichkeit sich in einem Video durch die Ersteinrichtung von ArchiCrypt Safe leiten zu lassen.

So gelingt der Umstieg von der Vorversion

Sofern Sie von Version 6 umsteigen, müssen Sie nichts spezielles beachten. Merken Sie sich ggf. den Speicherort Ihrer Passwort Safe Datei.

Falls Sie von einer älteren Version (*5 oder früher*) umsteigen, gehen Sie wie folgt vor:

Bevor Sie die alte Passwortdaten umwandeln können, müssen Sie sicherstellen, dass die Passwortdatenbank mit einem Passwort und **nicht** etwa einer **Schlüsseldatei** geschützt wird. Ändern Sie den Schutz gegebenenfalls. Nachdem die Datenbank in das neue Format umgewandelt wurde, können Sie

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

den Schutz in der neuen Version wieder auf eine Schlüsseldiskette umstellen.

Öffnen Sie bitte Ihre alte Safedatenbank mit der neuen Version 6. Die alte Passwort Safe Datei endet auf die **Dateiendung acd**.

HINWEIS: Falls Sie nicht mehr wissen, wo diese Datei liegt, starten Sie Version 5 und klicken in der Statusleiste auf den Dateinamen. Ihnen wird jetzt der genaue Speicherort Ihrer Datei angezeigt.

Jetzt wird der s.g. **Konverter** gestartet, der nach Abfrage Ihres Passwortes (*Schlüsseldatei ist nicht möglich, hier müssen Sie den Schutz auf Passwort mit der alten Anwendung umstellen*) die neue Datenbank erzeugt. Dabei wird das alte Passwort verwendet um die neue Datenbank zu schützen.
Nach Abschluss der "Umwandlung" wird die neue Datenbank sofort gestartet. Die alte Datenbank bleibt unberührt und kann theoretisch weiter verwendet werden.

Wenn Sie mit der Vorversion einen Safe ToGo (*Dateiendung **exe***) erzeugt haben, wählen Sie bitte im Dialog als Dateityp SafeToGo alt aus. Nachdem Sie Ihren Safe ToGo gewählt haben wird das Passwort abgefragt und ein neuer Safe im neuen Format wird erzeugt.

Video Ersteinrichtung von ArchiCrypt Passwort Safe

In der Home Ansicht haben Sie die Möglichkeit

1. einen bestehenden Safe zu öffnen[48]

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

2 einen neuen Safe zu erstellen[30]

3 ArchiCrypt Safe zu beenden[45]

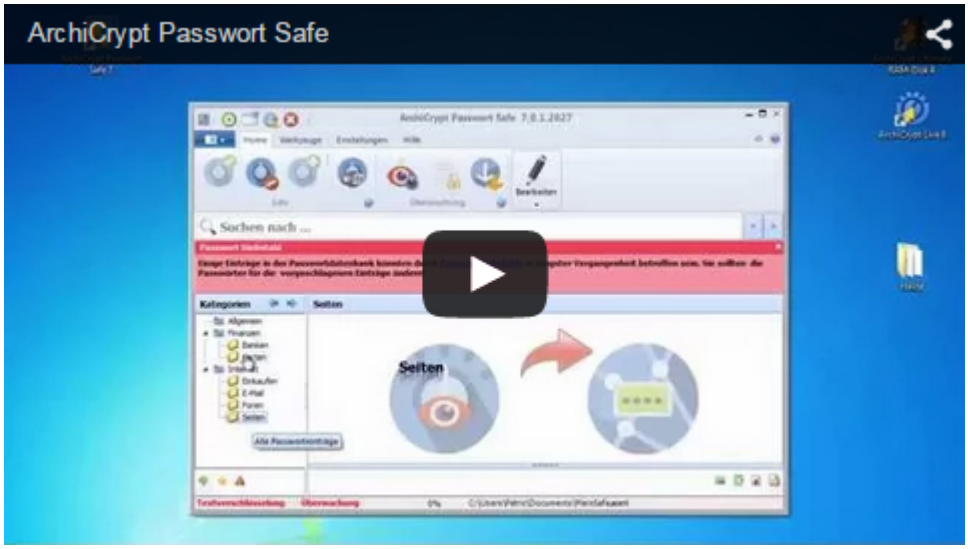
Folgende Themen könnten Sie ebenfalls interessieren:

- Was muss ich beim Umstieg auf die neue Version beachten[14]
- Menüleiste Safe[48]
- Einen Safeeintrag erstellen[8]
- Einstellungen - So legen Sie Hotkeys fest[101]
- Menüleiste Safe[48]
- Dialog für die Passworteingabe[30]
- Passwort Safe Online[128]
- Was ist ein gutes Passwort[126]

8.4 Safe erstellen und öffnen

Video Workshop ArchiCrypt Passwort Safe[23]

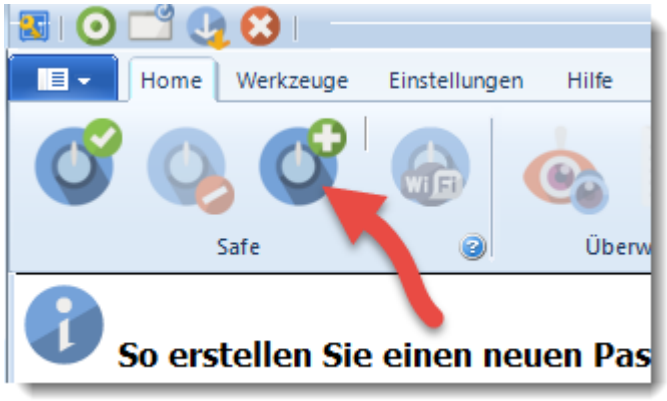
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



So erstellen Sie einen neuen Passwort Safe

Schritt 1:

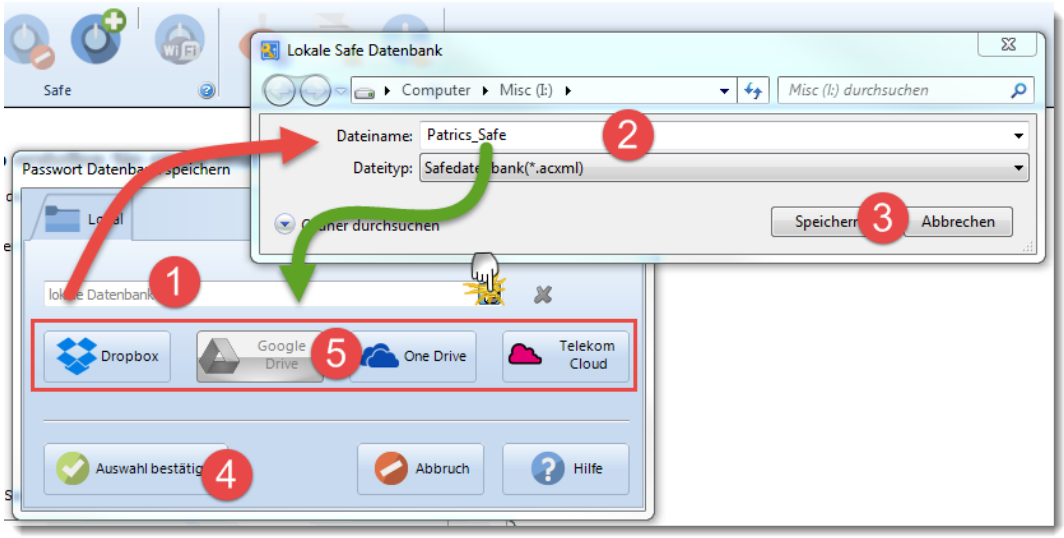
Klicken Sie in der Menüleiste Safe[48] auf das Symbol für einen neuen Passwort Safe.



Schritt 2:

Legen Sie den Speicherort für den Safe fest.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Sie können den **Speicherort** bei (1) manuell festlegen. Der Windows Dialog wird gestartet in dem Sie Verzeichnis und Dateiname (2) wählen können. Nach Ihrer Wahl klicken Sie auf Speichern (3). Die Angaben werden bei (1) übernommen und Sie können den Schritt mit **Auswahl bestätigen** (4) abschließen.

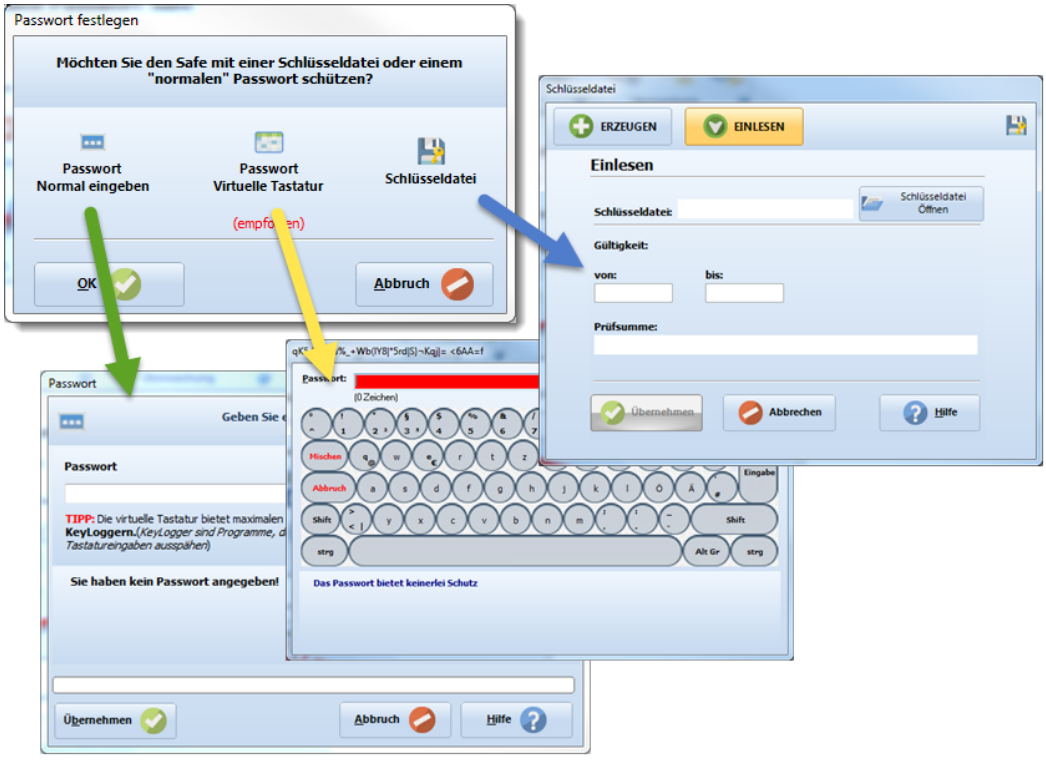
Bei (5) sehen Sie verschiedene **Cloud Dienste** die ArchiCrypt Passwort Safe kennt. Wird der entsprechende Cloud Dienst gefunden, können Sie durch Klick auf die entsprechende Schaltfläche den Speicherort in ein spezielles Verzeichnis in der Cloud legen. Sie werden aufgefordert, einen Namen für die Datei anzugeben. Die **Sicherheit in der Cloud** ist durch die Verschlüsselung der Passwortdatenbank gewährleistet. Diese bleibt in der Cloud zu jedem Zeitpunkt verschlüsselt. Ihr Safe Passwort wird weder in der Cloud noch auf Ihrem Rechner abgelegt.

siehe auch: Sicherheit 42

Schritt 3:

Entscheiden Sie sich, ob Sie den Safe mit einem Passwort oder mit einer Schlüsseldatei schützen möchten.
Mit einem Passwort kommen die meisten Nutzer am besten klar.
Die beste Verschlüsselung nützt nichts, wenn Sie ein schwaches Passwort wählen.
Beachten Sie bitte die Empfehlungen zum Passwort 126 .

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Der Safe ist jetzt erstellt. Sie finden bereits einige Kategorien, die Sie löschen oder auch umbenennen können.

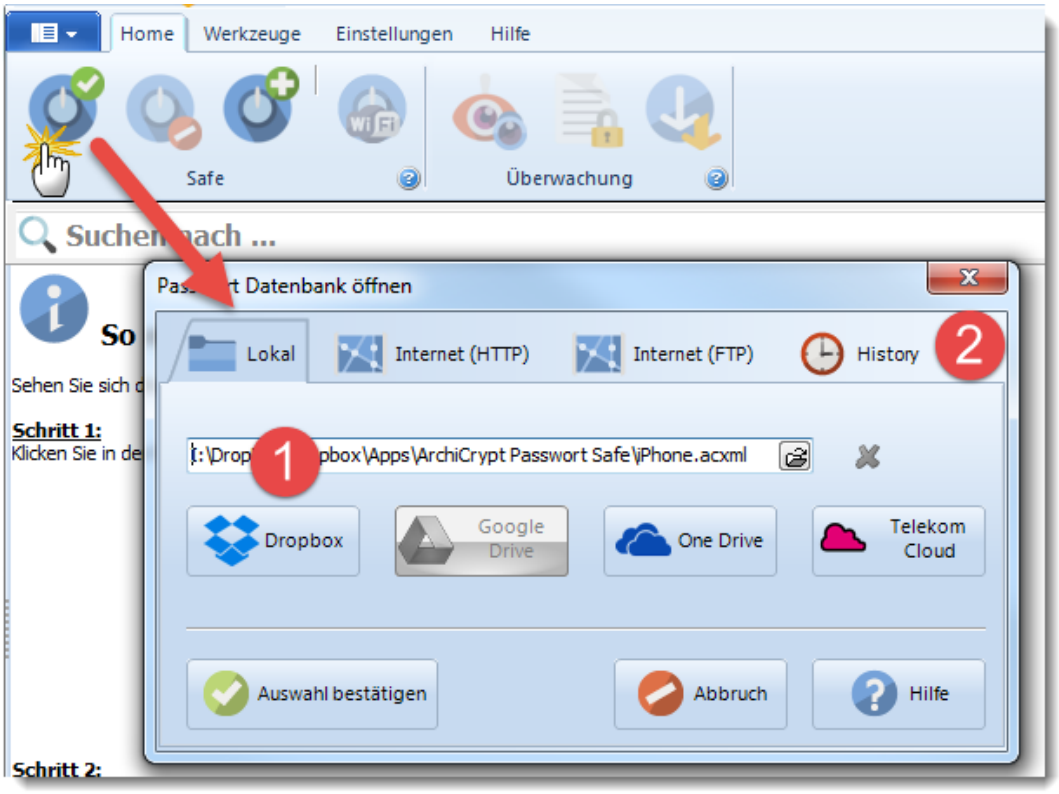
So laden Sie Ihren Passwort Safe

Wenn Sie Ihren Passwort Safe im Internet abgelegt haben, dann lesen Sie bitte "So laden Sie Ihren Passwort Safe aus dem Internet[35]".

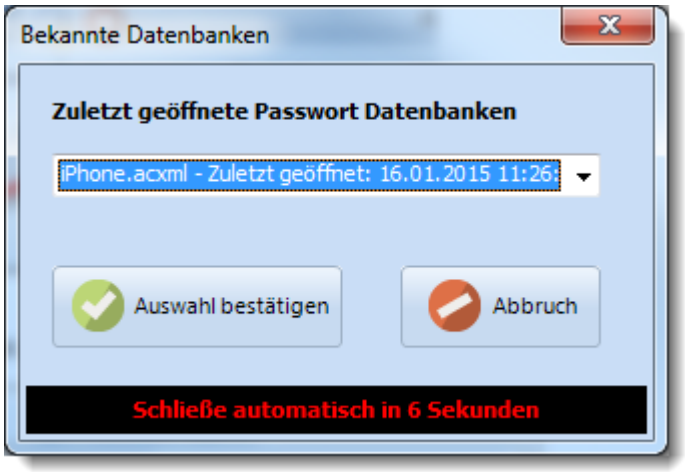
Die bequemste Variante ist, in den Einstellungen Rubrik Allgemeines - Start[87] die beiden Optionen **Mit Windows starten** und **Automatisch letzten Passwort Safe öffnen** zu aktivieren. Wenn Sie gelegentlich zwischen verschiedenen Safes hin- und herschalten, aktivieren Sie unter Einstellungen History[91] die Option **Beim Öffnen History als Auswahl anzeigen**. Sie müssen ArchiCrypt Passwort Safe dann nicht manuell starten und dann den Passwort Safe auswählen.

Alternativ starten Sie den Passwort Safe manuell und klicken dann in der Menüleiste auf das Passwort Safe öffnen[48] Symbol.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Wählen Sie die Passwort Safe Datei aus und klicken Sie auf **Auswahl bestätigen**. Wenn dem Passwort Safe **mehrere Safes** bekannt sind, können Sie bei (2) die **History** aufrufen.



Im **History Auswahlfeld** sehen Sie die letzten Datenbanken mit Datum. Die zuletzt genutzte Datenbank ist vorausgewählt. Der Dialog schließt selbstständig nach 10 Sekunden mit dieser Vorauswahl, falls Sie keine Angaben machen.
Wenn Sie die Maus über das Auswahlfeld bewegen, sehen Sie als Kontexthilfe zusätzlichen den kompletten Pfad der Passwortdatenbank.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Sie werden jetzt nach dem Passwort für den Safe[28] gefragt.

So laden Sie Ihren Passwort Safe aus dem Internet

Wenn Sie **keine eigene WEB-Seite** besitzen, dann nutzen Sie doch einfach unseren ArchiCrypt Passwort Safe - Online[128] Dienst unter www.Passwort-Zentrale.de.

Sicherheit der Daten

Wenn Sie Ihren Passwort Safe im Internet ablegen und von dort laden, brauchen Sie keine Angst um die Daten zu haben. Diese werden grundsätzlich in verschlüsselter Form übertragen und **nicht im Klartext**. Ihr Passwort für den Passwort Safe verlässt dabei Ihren Rechner nicht. Dies gilt unabhängig von den nachfolgend aufgeführten zusätzlichen Sicherheitsmaßnahmen! Das angesprochene HTTPS Protokoll (*die Adresse der Seite beginnt mit https*) verschlüsselt die Daten nochmals auf dem Weg zwischen Ihrem Rechner und dem Server. Dieses Verfahren kennen Sie sicher bereits aus dem sicheren Online-Banking und vom Einkauf in Online-Shops.

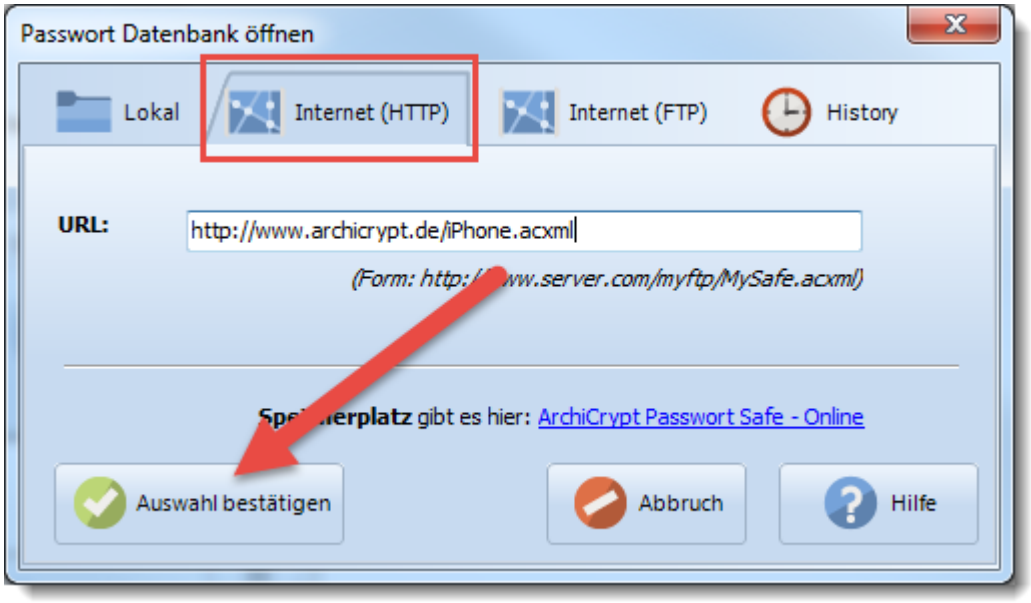
siehe auch: Sicherheit[42]

Mit eigener WEB-Seite geht Folgendes:

Zugriff über http oder https

Wichtig: Einen Passwort Safe, den Sie in ArchiCrypt Passwort Safe via HTTP/HTTPS laden, können Sie nicht ändern. Also keine Daten editieren, löschen oder hinzufügen. Diese Variante ist jedoch, sofern Sie den Zugriff mit https (SSL/TLS) steuern, extrem sicher.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Sofern Sie kein eigenes Zertifikat besitzen, prüfen Sie doch bitte einmal, ob Ihr Anbieter keine spezielle Möglichkeit anbietet, um via HTTPS auf Ihre Internetseite zuzugreifen. Unser ArchiCrypt Passwort Safe - Online[128] Dienst bietet natürlich den zusätzlichen Schutz. Hier greifen Sie per HTTPS auf Ihre Daten zu.

Beispiele:

Angenommen, Ihre Internetseite ist über www.UlrichsSchuhmode.de erreichbar. Sie haben Ihren Passwort Safe in ein Unterverzeichnis Geheim als MeinSafe.acxml auf Ihren Server geladen.
Dann ist folgender Eintrag als URL korrekt
http://www.UlrichsSchuhmode.de/Geheim/MeinSafe.acxml

Jetzt haben Sie ein Zertifikat für Ihre Internetseite erworben und können auch mittels https auf die Seite zugreifen. Folgende URL wäre korrekt:

https://www.UlrichsSchuhmode.de/Geheim/MeinSafe.acxml

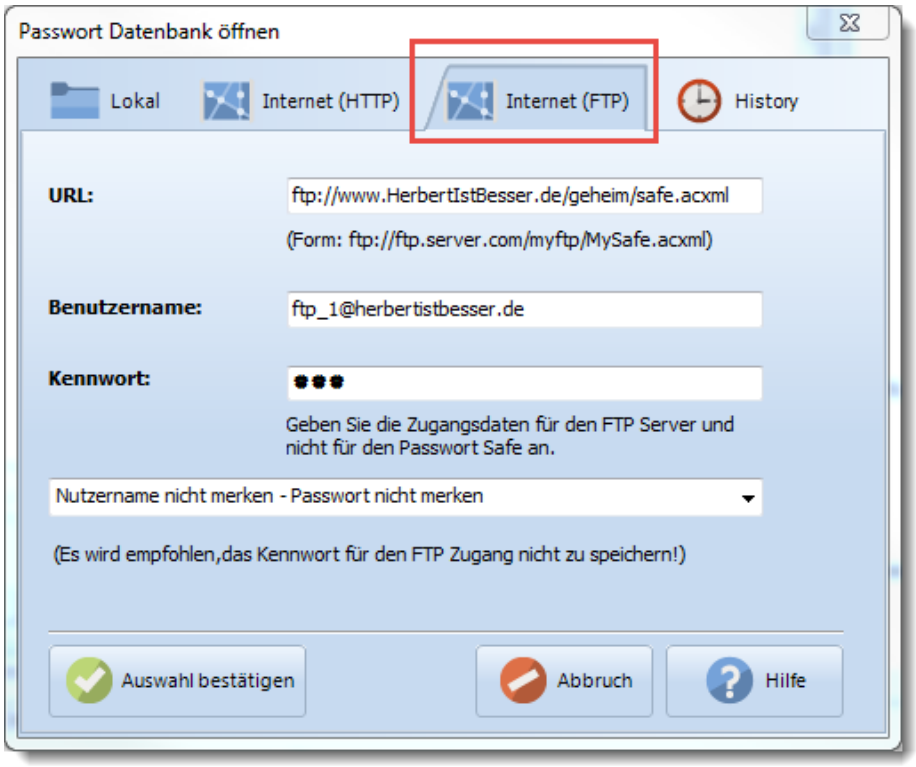
Unser ArchiCrypt Passwort Safe - Online[128] Dienst bietet natürlich den zusätzlichen Schutz. Hier greifen Sie per **SSL** auf Ihre Daten zu.

siehe auch: ArchiCrypt Passwort Safe - Online[128]

Zugriff via FTP

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Der Vorteil gegenüber dem Zugriff via HTTP/HTTPS besteht darin, Daten im Passwort Safe auch ändern zu können. Sie können Daten also editieren, löschen und hinzufügen. Sie sollten hier aber immer Ihre Anbindung ans Internet und die Größe Ihres Passwort Safes im Auge haben. Der Passwort Safe muss hier nicht nur einmalig eingelesen werden, sondern es werden (*sofern in den Einstellungen*[86] *aktiviert, empfohlen*), auch Sicherungskopien auf dem FTP Server erstellt und natürlich auch die Änderungen übertragen. Vermeiden Sie daher das Speichern großer Dateien (*Bilder und Dateien*) in Ihrem Passwort Safe, halten Sie den Safe schlank!



Richten Sie den FTP Server ggf. zunächst ein und speichern Sie dann Ihre Safe Datei **mit einem FTP Programm** auf dem Server. Gehen Sie jetzt zu ArchiCrypt Passwort Safe und rufen Sie die Funktion Safe öffnen auf. Im Dialog wählen Sie die Registerkarte **Internet (FTP)**.

Tragen Sie die URL ein und achten Sie darauf, dass Sie der URL unbedingt **ftp://** voranstellen müssen.

Fügen Sie jetzt die **FTP Login** Daten ein. Also Benutzername und FTP Passwort (**NICHT das "Passwort Safe" Passwort -**

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

die Passwörter für FTP und den Safe sollten sich unbedingt unterscheiden)

Abschließend legen Sie bitte fest, was sich ArchiCrypt Passwort Safe neben der URL merken soll. Es wird **empfohlen**, nur den Nutzernamen (*Benutzername*) zu speichern. Wenn Sie ausschließen können, dass andere Zugang zu Ihrem Rechner haben, können Sie auch das FTP Passwort von ArchiCrypt Passwort Safe sichern lassen.

Wenn Sie die Auswahl bestätigen und die Angaben korrekt sind, wird der Safe geladen. Falls Probleme auftreten, sehen Sie sich bitte das Log Buch[119] an. Hier werden ggf. Fehlermeldungen des FTP Servers aufgeführt.

Was tun, wenn Sie einen Passwort Safe via FTP geöffnet haben und die Verbindung zum Internet abbricht?

Sofern Sie keine Änderungen vorgenommen haben, ist der Abbruch nicht tragisch. Um zu verhindern, dass der Passwort Safe von mehreren Rechnern gleichzeitig mit Schreibrechten (*Daten dürfen geändert werden*) geöffnet werden kann, wird auf dem FTP Server eine Sperre auf die Safe Datei erzeugt. Diese Sperre können Sie wieder entfernen, indem Sie die Datei "Name der Passwort Safe Datei + .lck" (*im Beispiel* **MeinSafe.acxml.lck**) löschen. Aber NIEMALS die Datei einfach so löschen. Wenn dadurch der Safe von mehreren gleichzeitig schreibend geöffnet wird, überschreiben sich die verschiedenen Safes gegenseitig.

Falls Sie Änderungen durchgeführt haben, die jetzt wegen fehlender **Internetverbindung** nicht mehr auf dem Server gespeichert werden können. Speichern Sie die Daten lokal über die Funktion "Safe kopieren nach ...[46]". Laden Sie diese Datei anschließend bei Bedarf wieder auf den FTP Server um die neuste Version des Safes mobil verfügbar zu haben.

So sicher sind Ihre Daten im Safe

Der Safe verschlüsselt alle Daten mit dem **Advanced Encryption Standard (AES)** in der besonders sicheren 256 BIT Variante. Im Gegensatz zu vielen anderen Passwort Safes werden **alle**

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Inhalte verschlüsselt. Also auch Ihr Benutzername, die Einträge im Freitextfeld, eine gegebenenfalls vorhandene Grafik, eine Datei etc.

Detaillierte Informationen über die Vorgänge beim Verschlüsseln und Entschlüsseln sowie weitere Informationen über eingesetzte Verfahren finden Sie im Kapitel Umgang mit der Software - Sicherheit 42

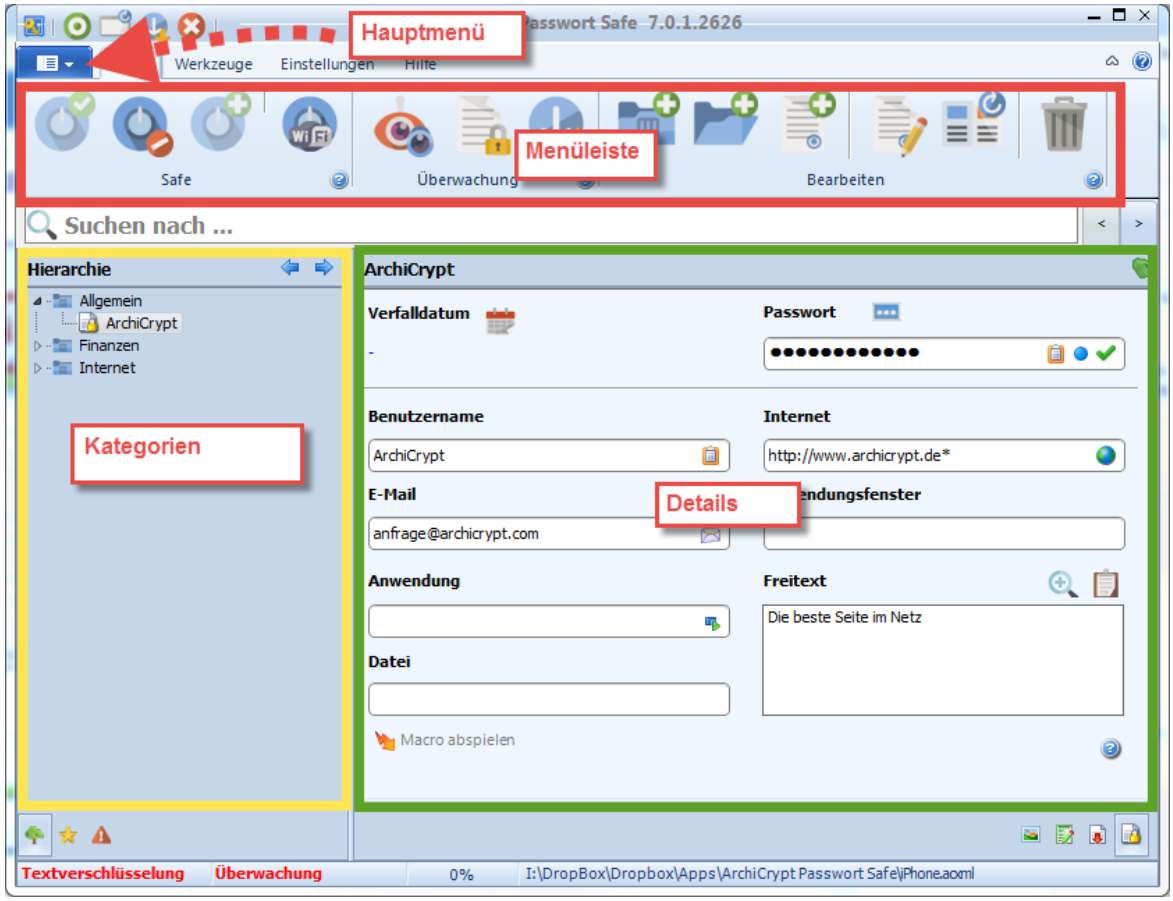
Folgende Themen könnten Sie ebenfalls interessieren:

Idee für ein Passwort 27
ArchiCrypt Passwort Safe - Online 128
Einen Safeeintrag erstellen 8
Menüleiste Safe 48
Video Ersteinrichtung von ArchiCrypt Passwort Safe
Dialog für die Passworteingabe 30

8.5 Die Bedienoberfläche

Die Oberfläche von ArchiCrypt Passwort Safe ist in die 5 Bereiche **Hauptmenü** 40, **Menüleisten** 41, **Kategorien** 41, **Passwortdetails** 42 **und die Suche** 43 aufgeteilt.

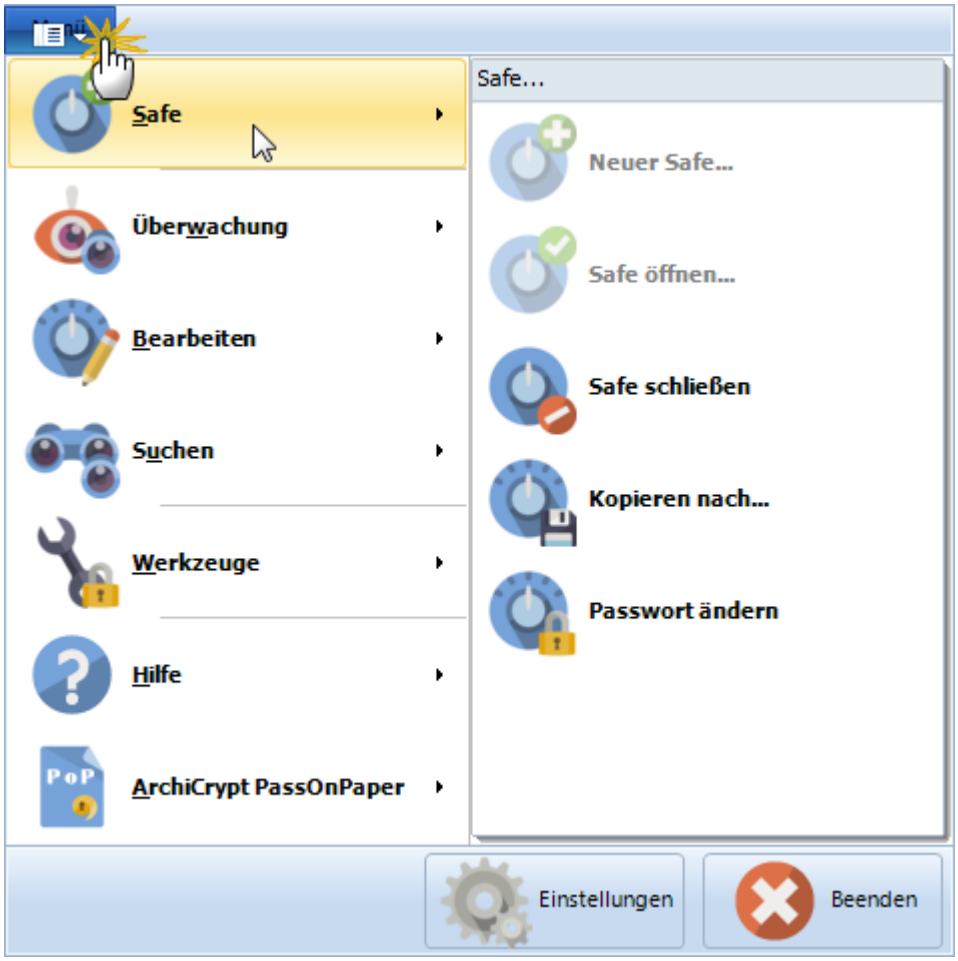
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Hauptmenü

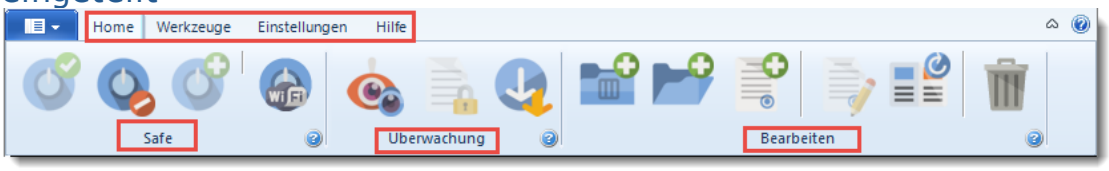
Über das Symbol in der linken oberen Ecke erreichen Sie das **Hauptmenü**.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Menüleisten

Hier finden Sie die wichtigsten Funktionen in verschiedene Gruppen eingeteilt



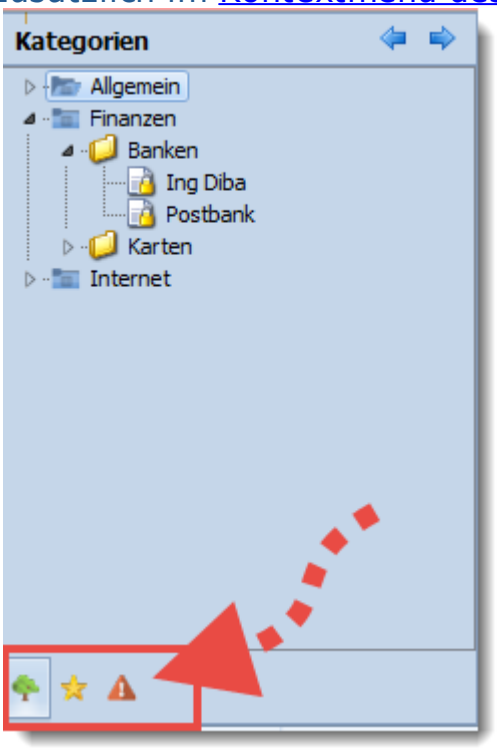
Hier erfahren Sie mehr über die Menüleisten 45

Kategorien

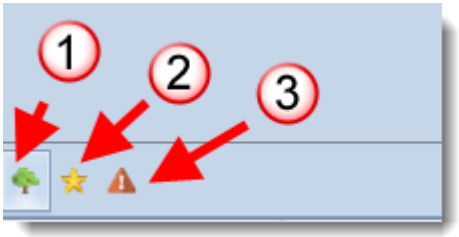
Hier werden die **Kategorien** und **Ordner** angezeigt in denen Sie die eigentlichen Safe Einträge organisieren. Sie können Kategorien und Ordner nach Belieben erstellen und anordnen. Funktionen zum Bearbeiten von Einträgen finden Sie bei den Hauptfunktionen 47.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

In der **Kategorie-Ansicht** können Sie auch bequem Einträge und ganze Ordner per **Drag&Drop** verschieben. Häufig benötigte Einträge können Sie als **Favorit** übernehmen (*rechte Maustaste und Kontextmenü-Eintrag Favorit*[52] *wählen*). Die Favoriten werden zusätzlich im Kontextmenü des Tray-Symbols[89] angezeigt.



Mit den drei Symbolen am unteren Rand könne Sie schnell zwischen Kategorie (**1**)- und Favoriten(**2**)-Ansicht wechseln und sich ansehen, ob es Passworteinträge gibt, deren (**3**) Verfalldatum überschritten ist bzw. ob eine **Passwortdiebstahl-Warnung** existiert.



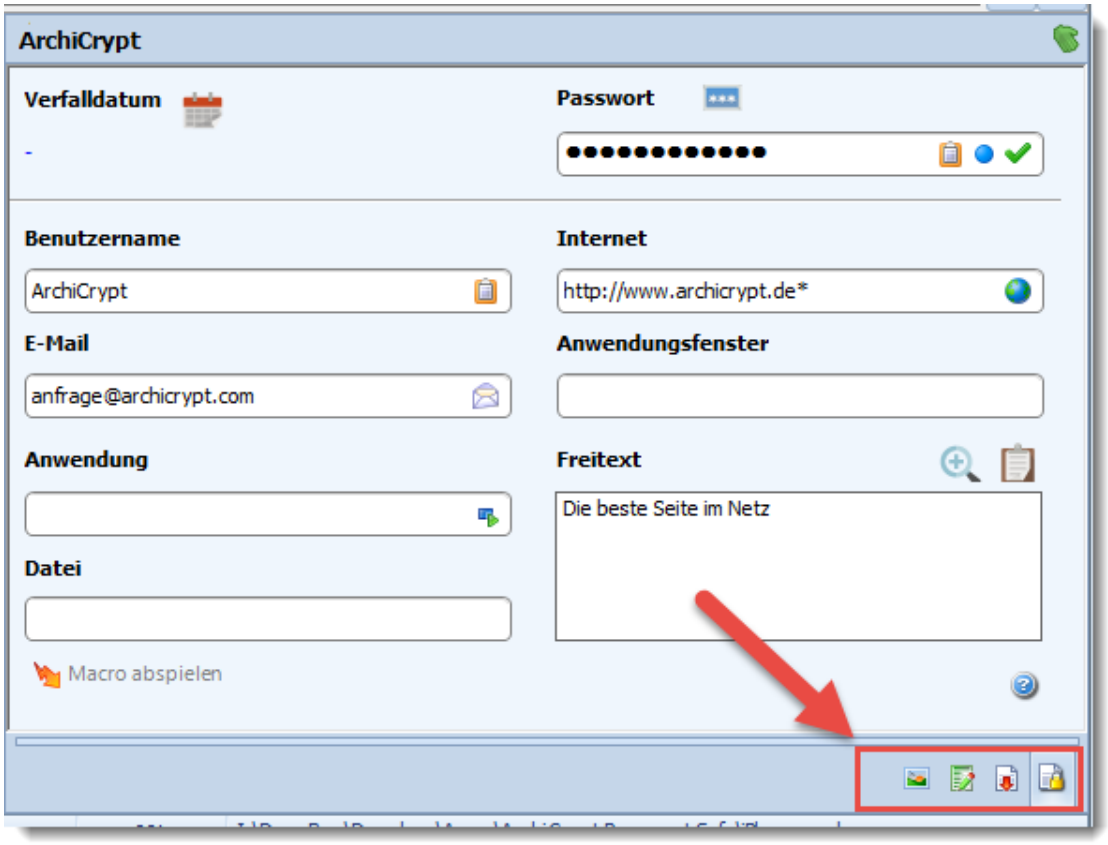
siehe auch Einstellungen[88]

Passworteintrag

Hier werden die Informationen angezeigt, die zu dem ausgewählten Passworteintrag[67] bereitstehen. Am unteren Rand

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

(*siehe Pfeil*) können Sie zwischen verschiedenen Ansichten wechseln.



Hier erfahren Sie mehr über die Detailansicht 70

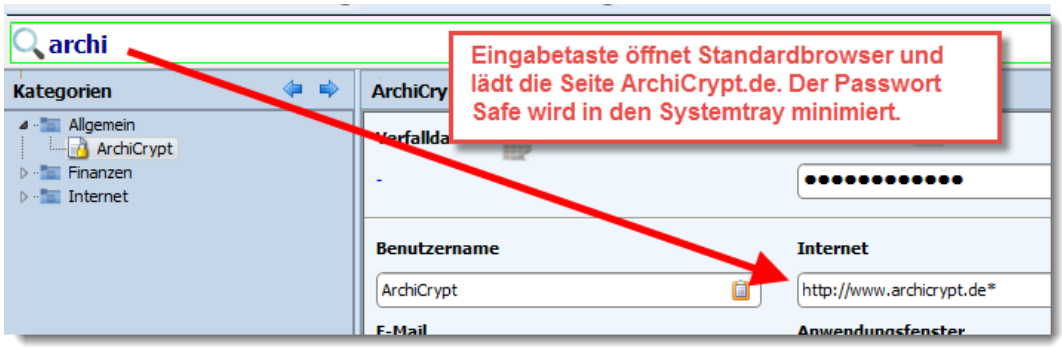
Suche

Wer den Passwort Safe länger verwendet, wird ihn schätzen lernen und immer mehr Daten darin ablegen. Schnell hat man ein paar hundert Einträge. Das wird trotz der Organisation in Kategorien und Ordner rasch unübersichtlich. Die Suche spielt in der neuen Version eine zentrale Rolle. Startet man den Passwort Safe oder holt ihn aus dem Systemtray in den Vordergrund (*Doppelklick auf das Tray Symbol*), wird der Eingabecursor automatisch in das Suchfeld gesetzt. Sie können also direkt einen Suchbegriff eingeben.

Mit den Pfeilen rechts neben dem Suchfeld navigieren Sie zur vorherigen oder nächsten Fundstelle. Auf der Tastatur können Sie die **Pfeil hoch** und **Pfeil nach unten** Taste verwenden.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Falls der Passworteintrag einen Verweis auf eine Internetseite enthält, können Sie durch Betätigen der **Eingabetaste** (*Enter*) den Passwort Safe in den **Systemtray minimieren**[49] und zur Internetseite springen.



Video Workshop ArchiCrypt Passwort Safe[23]

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

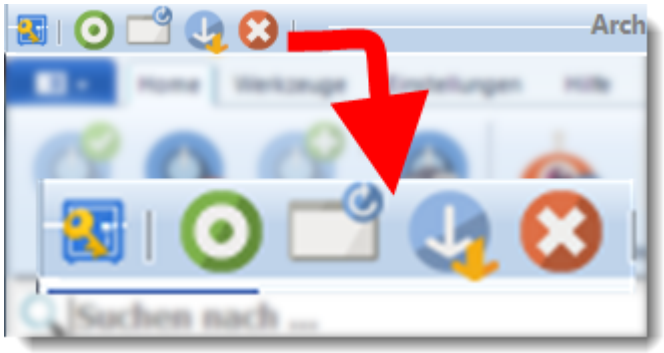
Folgende Themen könnten Sie ebenfalls interessieren:

Menüleisten[45]
Erster Start - So richten Sie ArchiCrypt Passwort Safe ein[27]
Einstellungen - So legen Sie Hotkeys fest[101]
So übertragen Sie Passwort&Co an den Browser[102]
So legen Sie fest, welcher Browser unterstützt werden soll[93]

8.6 Übersicht über Menüs

Die Funktionen des Safes sind in die Bereiche **Minileiste**[45], **Hauptmenü**[46], **Hauptfunktionen**[47], **Werkzeuge**[54] und **Hilfe**[65] unterteilt.

Minileiste



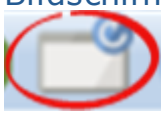
Die Minileiste befindet sich in der linken oberen Ecke des ArchiCrypt Passwort Safe Fensters.

Hier können Sie

den **Vordergrund-Modus** aktivieren

Der Vordergrund-Modus sorgt dafür, dass das Fenster des Passwort Safes vor allen anderen Fenstern gehalten wird. Sie können so zum Beispiel Daten eines Safeeintrags per Drag&Drop in eine andere Anwendung verschieben oder bei der Drag&Drop Verschlüsselung[83] Dateien einfach auf das Detailfenster ziehen.

das Safe Fenster auf die Standardmaße zurücksetzen und auf dem Bildschirm zentrieren



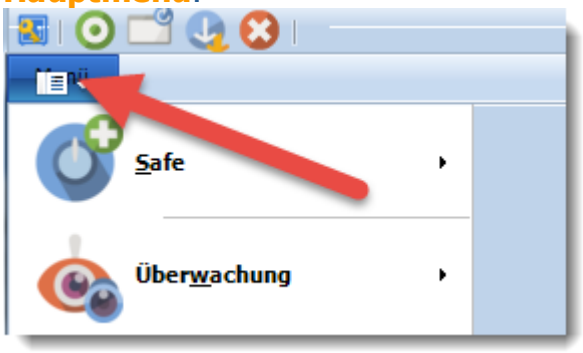
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

den Safe in den Standby-Modus[49] (*in den Systemtray*) versetzen

den Passwort Safe beenden

Hauptmenü

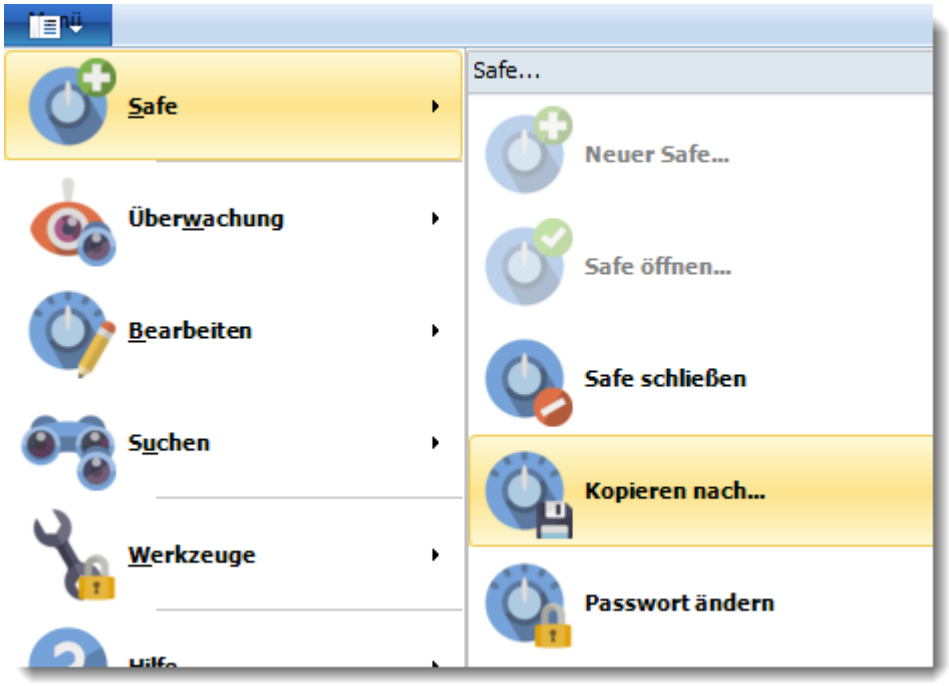
Über das Symbol in der linken oberen Ecke erreichen Sie das **Hauptmenü**.



So erstellen Sie eine Kopie Ihres Safes

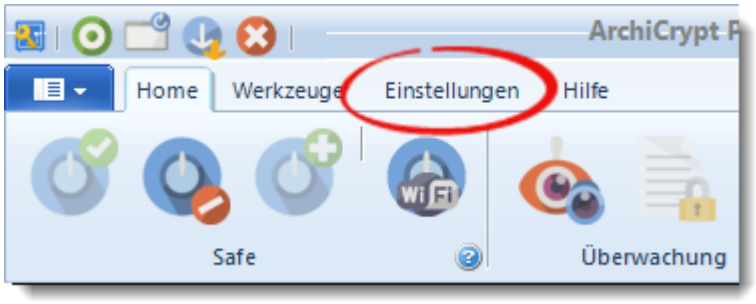
Laden Sie den Safe, von dem Sie eine Kopie erstellen möchten. Rufen Sie dann im **Hauptmenü** die Kategorie **Safe** und dort die Funktion **Kopieren nach...** auf. Wählen Sie das Zielverzeichnis aus und geben Sie einen Namen für den neuen Safe ein. Klicken Sie jetzt auf Speichern. Die Kopie wird sofort erstellt. ArchiCrypt Passwort Safe erstellt eine exakte Kopie. Kopien eines bestimmten Safes können **synchronisiert** werden.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



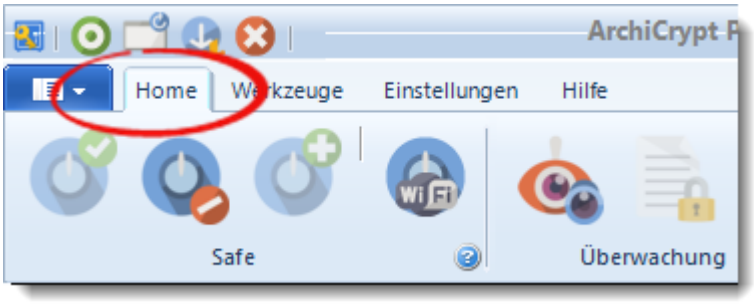
So ändern Sie Einstellungen

Betätigen Sie das Tastaturkürzel F10, rufen Sie im Hauptmenü[40] die Funktion **Einstellungen...** auf oder klicken Sie auf die Leiste **Einstellungen**. Sie können die Änderung von Einstellungen auch durch das Betätigen der Esc-Taste abbrechen.



Hauptfunktionen - Home

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Die Hauptfunktionen fassen dabei Befehle zusammen, die Sie bei der täglichen Arbeit mit dem Safe am häufigsten benötigen.

Menüleiste Safe

Erläuterung von links nach rechts

Öffne Passwort Safe

Wählen Sie einen Safe aus. Und geben Sie nach Aufforderung das Passwort für den Safe ein.
siehe auch Automatisch letzten Passwort Safe öffnen 88

(Strg+Alt+O)

Schließe Passwort Safe

Schließt den Passwort Safe. Im Safe Portable (USB) und in der U3 Version schließt diese Funktion die Anwendung komplett.

(Strg+Alt+S)

Neuer Passwort Safe

Erstellen Sie einen neuen Passwort Safe 30

Diese Funktion ist in der Safe Portable (USB) und der U3 Version nicht verfügbar.

(Strg+Alt+N)

Datenbank senden

Sie können das externe **SafeXChange Tool** starten und den aktuell geöffneten Passwort Safe dort zur Übertragung anmelden. Sie können Datenbanken via LAN/WLAN (WiFi)

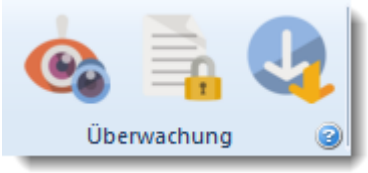
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

zwischen verschiedenen Plattformen (*Windows, iOS und Android*) austauschen.

Siehe Austausch von Passwort Datenbanken[120] .

Anm.: Die Funktionen sind teilweise nicht verfügbar, sofern Sie einen Safe Portable nutzen.

Menüleiste Überwachung



Bei diesen Funktionen wird der Safe in den **Infobereich** (*Systemtray*) minimiert, von wo aus Sie ihn über sein Kontextmenü[89] oder per Doppelklick auf das Symbol wieder in den Vordergrund holen können. Sie können den Funktionen Hotkeys[101] zuordnen um schnell Zugriff auf sie zu haben.

Erläuterung von links nach rechts

Überwachung starten

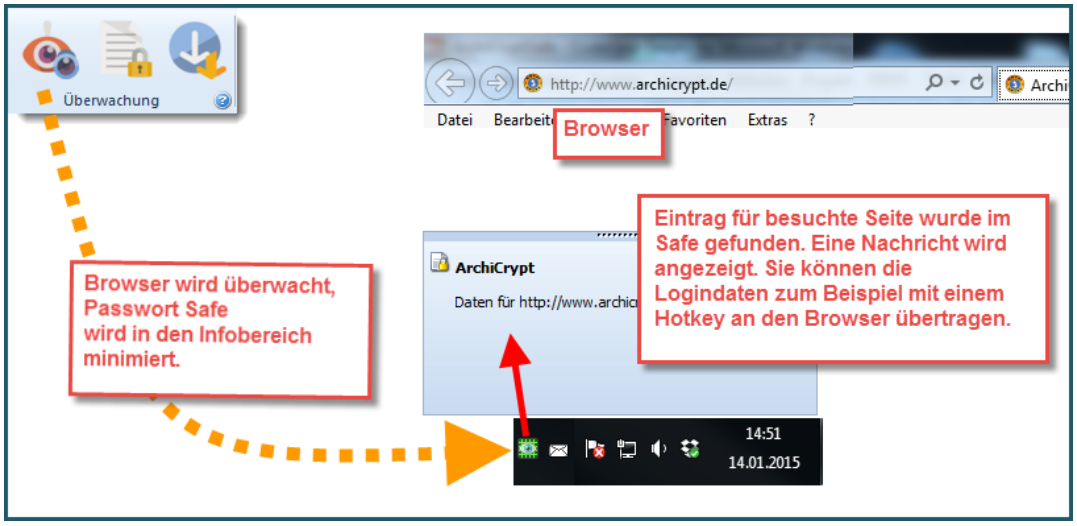
ArchiCrypt Passwort Safe überwacht jetzt, welche Internetseiten Sie in Ihrem Browser besuchen und welche Anwendungsfenster im System erscheinen. Falls ein passender Eintrag vorhanden ist, wird dieser bereitgestellt. Ein akustisches Signal und ein Nachrichtenfenster informieren. Sie können dann z.B. Daten aus dem Passwort Safe mit Hilfe der Hotkeys[101] in die Internetseite übertragen.

siehe auch Überwachung[79]

Das **Symbol im Infobereich** ist bei aktiver Überwachung grün, ansonsten rot. Der Safe reagiert auf Hotkeys[101] und bietet sein Kontextmenü[89] (*Klick auf Symbol mit rechter Maustaste*) an.

(Strg+I)

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Text verschlüsseln

Wenn Sie diese Funktion aufrufen, schaltet der Safe automatisch in den Modus **Textverschlüsselung**. Er wird minimiert und erscheint als Symbol im Infobereich. Text den Sie jetzt in die **Zwischenablage** kopieren, wird automatisch verschlüsselt, kopieren Sie bereits verschlüsselten Text in die Zwischenablage, wird der Text entschlüsselt. Für die Ver- und Entschlüsselung wird das Passwort genutzt, welches gerade im Passwort Safe aktiv ist.

siehe dazu Textverschlüsselung[81]

(Strg+W)

Standby

Der Safe wird in den Infobereich minimiert. Das Symbol ist rot, es findet keine Browserüberwachung statt. Der Safe reagiert auf Hotkeys[101] und bietet sein Kontextmenü[89] (*Klick auf Symbol mit rechter Maustaste*) an.

(Strg+R)

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Menüleiste Bearbeiten

Mit den Funktionen dieser Menüleiste bauen Sie Ihren Passwort Safe auf.

Erläuterung von links nach rechts

Neue Kategorie erstellen

Sie benötigen in jedem Passwort Safe mindestens eine Kategorie. Kategorien haben nur den Zweck, Ordnung in Ihren Safe zu bringen. Kategorien könnten zum Beispiel sein: Banken, Wissen, Erholung, Ferien, etc. In Kategorien können Sie Ordner und Safeeinträge erstellen.

(Strg+K)

Neuer Ordner

Ordner müssen Sie nicht zwingend anlegen, es empfiehlt sich jedoch, da Sie die Einträge in Ihrem Safe so besser ordnen können. Ordner können Sie innerhalb einer Kategorie erstellen oder innerhalb eines anderen Ordners. Ordner können Sie per Drag&Drop in Kategorien oder andere Ordner verschieben. Beispiele für Ordner unterhalb einer Kategorie Wissen könnten z.B. sein: Computer, Politik, Zeitgeschehen, etc.

(Strg+O)

Neuer Safeeintrag

Ein Safeeintrag nimmt die eigentlichen Informationen auf. Falls Sie einen neuen Eintrag erstellen, wird ein spezieller Dialog[8] angezeigt.

siehe auch Safeeintrag erstellen[8]

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

siehe auch Einstellungen[110]

(Strg+E)

Safeeintrag bearbeiten

Der Dialog für die Eingabe eines Safeeintrags wird angezeigt. Sie können dort Werte ändern. Sie können den Safeeintrag alternativ in der Kategorienansicht links markieren und die F2 Taste betätigen oder auf den Eintrag links-doppelklicken.

siehe auch Safeeintrag erstellen[8]

(F2)

Safeeintrag klonen/kopieren

Erstellt eine exakte Kopie der Kategorie, des Ordners oder des Safeeintrags. Die Kopie enthält als Namenszusatz eine Kombination aus aktuellem Datum und der Zeit.

Auswahl löschen

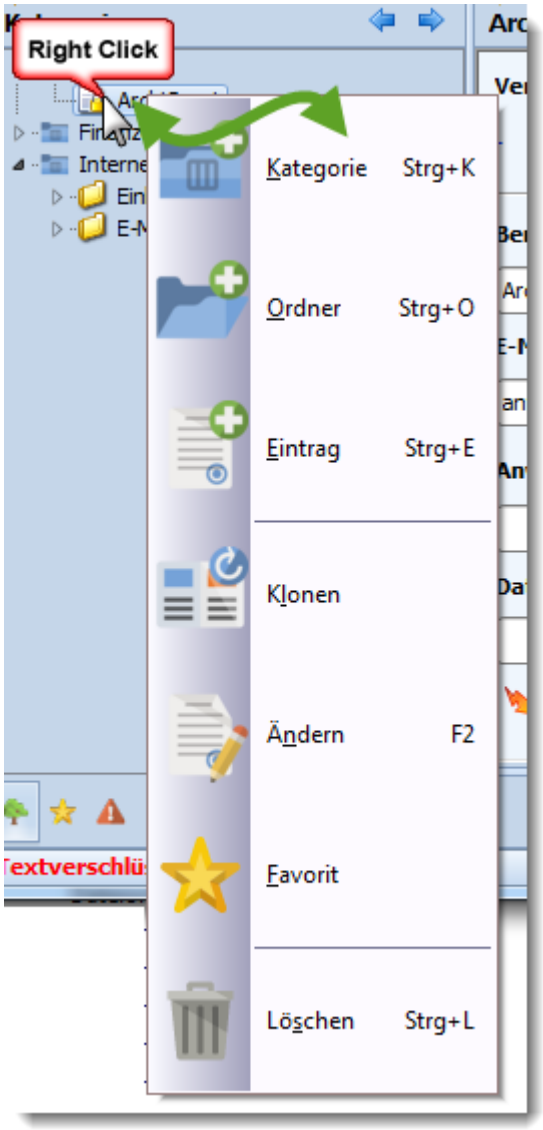
Safeeintrag, Ordner oder Kategorie wird gelöscht. Wenn Sie eine Kategorie oder einen Ordner löschen, werden alle darin enthaltenen Einträge gelöscht. Sie können auch die Entfernen-Taste betätigen.

(Strg+L)

HINWEISE

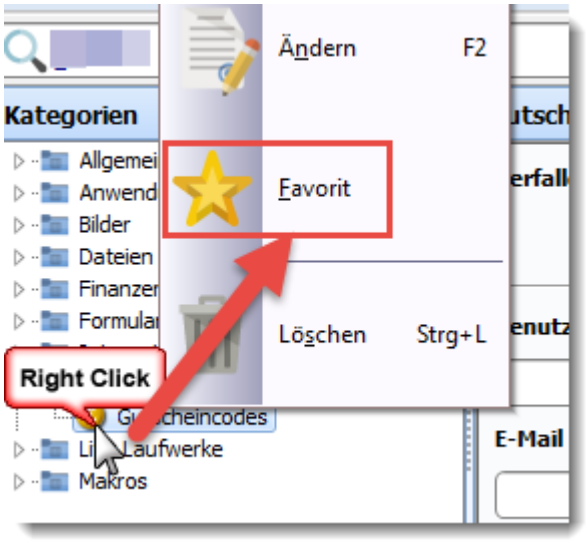
Diese Funktionen stehen Ihnen auch im **Kategorie-Kontextmenü** zur Verfügung. Einfach rechte Maustaste betätigen.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Favorit
Im **Kategorie-Kontextmenü** haben Sie auch die Möglichkeit, einen **Eintrag als Favorit** zu markieren. Dieser Eintrag wird jetzt auf der Seite Favoriten[42] gelistet und steht im Kontextmenü-Systemtray[89] zur Verfügung.

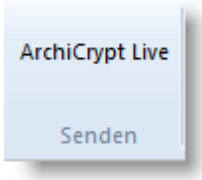
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Werkzeuge

Die Werkzeuge beinhalten Funktionen für die Übertragung von Schlüsseln an **ArchiCrypt Live**, Funktionen für die **Suche**, für den **Import, Export, Synchronisation** von Einträgen, für das **Erstellen von Safe Portable**, das Aufräumen der Datenbank, das Ver- und Entschlüsseln von Dateien und anderes.

Menüleiste Senden

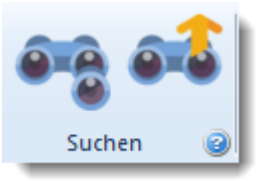


Die Schaltfläche ist nur dann verfügbar, wenn ArchiCrypt Live aktiv ist. Sie können bei ausgewähltem Safeeintrag das aktuelle Passwort an Archicrypt Live senden und dort verwenden.

siehe Beispiel mit ArchiCrypt Live 72

Menüleiste Suchen

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

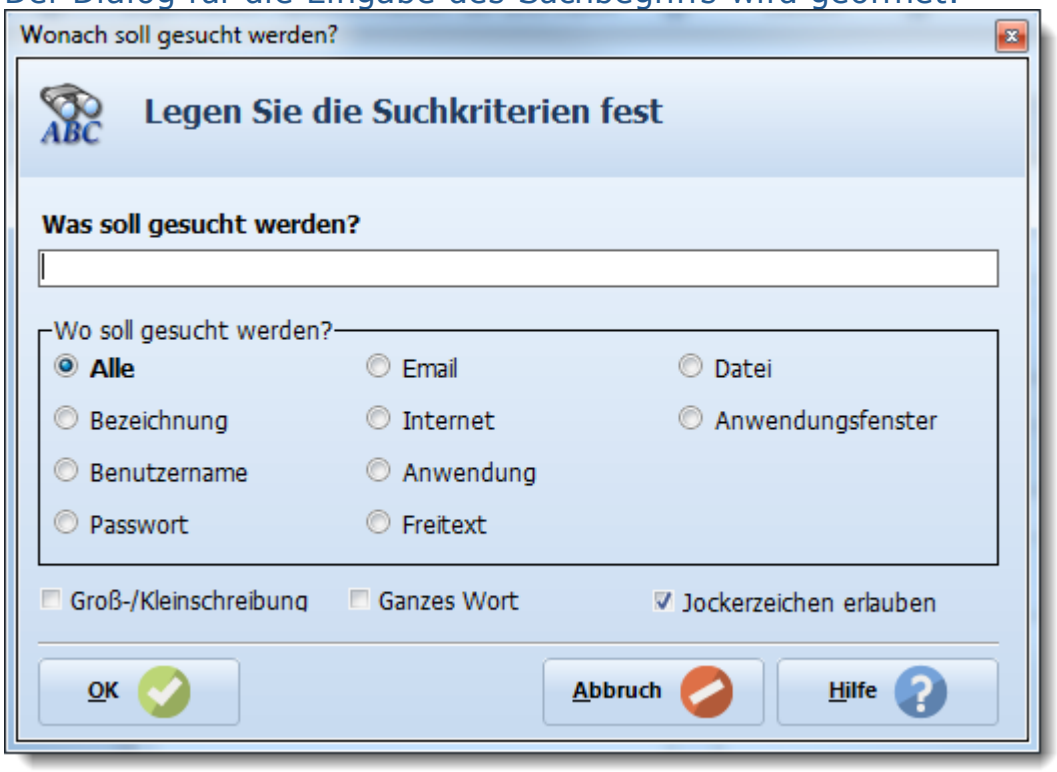


So finden Sie rasch einen bestimmten Safeeintrag

In der **HOME-Ansicht**[47] finden Sie direkt ein Suchfeld[43], in welches Sie den gesuchten Begriff oder Teile davon eingeben können.

Wenn Sie gezielt in einem bestimmten Feld (*E-Mail, Passwort, etc.*) suchen möchten, betätigen Sie bei aktivem Passwortsafe die Tastenkombination Strg+F oder klicken Sie bei den Werkzeugen auf das **Suchen** Symbol.

Der Dialog für die Eingabe des Suchbegriffs wird geöffnet.



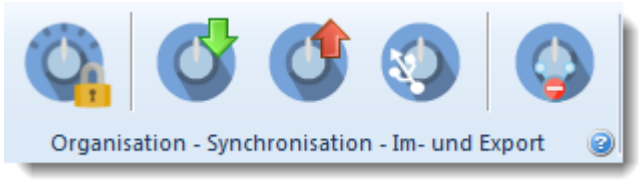
Geben Sie im Dialog den gesuchten Begriff ein, legen Sie ggf. weitere Suchkriterien fest und klicken Sie auf OK. Falls ein Eintrag vorhanden ist, der den Suchkriterien entspricht, wird er ausgewählt. Sie können weiter suchen, indem Sie die F3 Taste

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

betätigen oder das **Weiter suchen** Symbol (*Fernglas mit Pfeil*) anklicken.

Siehe auch Dialog zur Suche[26]

Menüleiste Organisation - Synchronisation - Im- und Export



Safe Passwort ändern

So ändern Sie das Passwort für Ihren Passwort Safe

Rufen Sie die Funktion für die Änderung des Passworts auf, indem Sie auch die Schaltfläche in der Menüleiste klicken oder die Tastenkombination Strg+Alt+P betätigen. Der zugehörige Safe muss geöffnet sein. Wenn Sie aufgefordert werden, geben Sie bitte das neue Passwort ein.
siehe auch Passworteingabe[28]

(Strg+Alt+P)

Daten importieren

Gut zu wissen!

Wenn Sie einen neuen Passwort Safe erzeugen, wird dabei eine eindeutige Kennung erzeugt und in der Safe Datei gespeichert. Wenn Sie die Safe Datei kopieren (entweder im Windows Explorer oder via "Kopieren nach ...") bzw. einen

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

mobilen Safe erzeugen, bleibt diese Kennung erhalten. Anhand dieser Kennung ist es ArchiCrypt Passwort Safe möglich, verschiedene Versionen eines Safes zu synchronisieren. Solche Passwort Safe Dateien sind quasi Verwandte.

So importieren Sie Passwort-Daten

Sie können die Inhalte eines Passwort Safes in den aktuellen Safe **importieren**. Importieren Sie Daten aus einer ArchiCrypt Passwort Safe Datei, hängt die Art des Imports davon ab, ob es sich bei den beiden Safedateien um **Verwandte**[56] handelt! Bei Verwandten findet eine Synchronisation statt. D.h. geänderte Einträge werden geändert übernommen, neue Einträge an der richtigen Position eingefügt.
Handelt es sich hingegen um Passwort Safe Dateien, die jeweils unabhängig voneinander erstellt wurden, werden die Daten des einen Safes in den gerade geöffneten Passwort Safe übernommen und in einem Ordner Import (*Zeitstempel*) abgelegt.

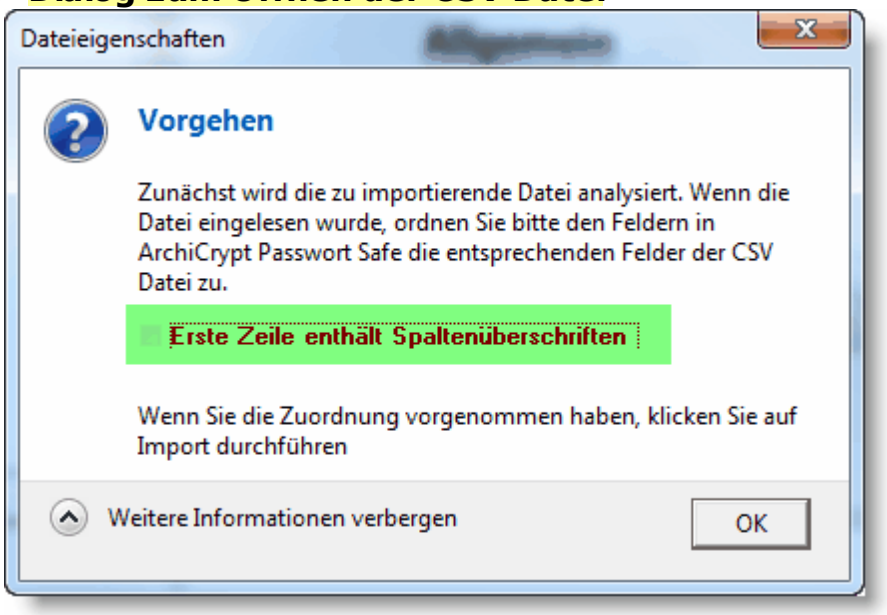
➡**WICHTIG: Sofern Sie Daten aus einem anderen Passwort Safe importieren möchten, achten Sie darauf, dass der zu importierende Safe im aktuellen Format vorliegt. Wenn Sie sich nicht sicher sind, ob dies der Fall ist, öffnen Sie zunächst den zu importierenden Passwort Safe. Falls eine Konvertierung (*Umwandlung in ein neues Format*) nötig ist, werden Sie beim Öffnen darauf hingewiesen.**

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Um Daten aus einer **CSV Datei** (*einzelne Felder und Einträge sind durch Komma getrennt. Jeder Eintrag steht in einer eigenen Zeile*) zu importieren klicken Sie auf **CSV**, um Daten aus einem anderen Passwort Safe zu importieren klicken Sie auf **Safe**, um den Import abzubrechen, klicken Sie auf ABBRUCH.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

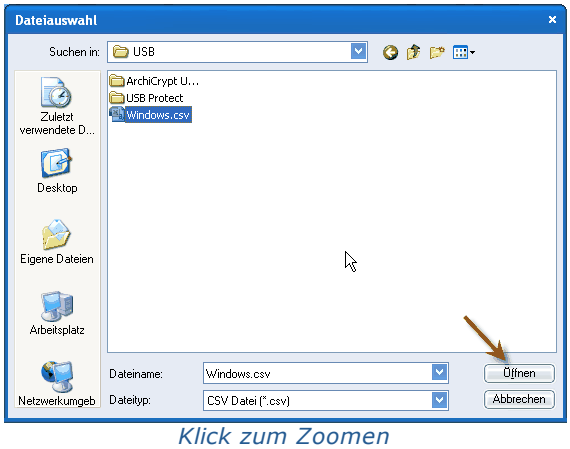
1 Dialog zum Öffnen der CSV Datei



Sie werden zunächst gefragt, ob die Datei in der ersten Zeile Spaltenüberschriften enthält. ArchiCrypt Passwort Safe ignoriert diese Zeile dann beim Import.

TIPP: CSV Dateien sind normale Textdateien, die Sie zum Beispiel mit Notepad öffnen können. Sie können so prüfen, ob die erste Zeile eine Überschrift ist.

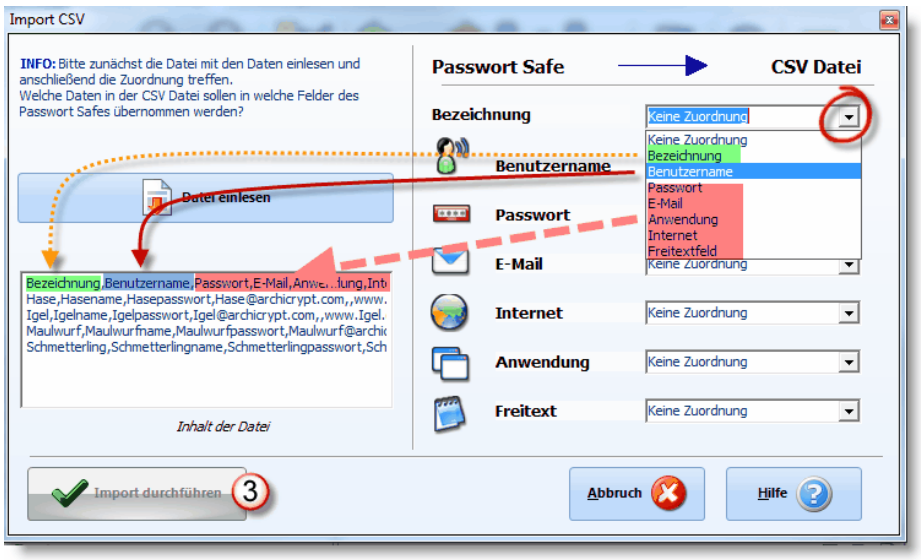
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Klick zum Zoomen

Im Dialog zur Übernahme wird Ihnen zur Kontrolle der Inhalt der CSV Datei angezeigt.

2 Ordnen Sie jetzt den Feldern im Passwort Safe die Daten der CSV Datei zu

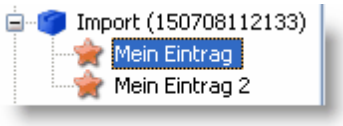


Sie müssen nicht jedem Eintrag im Passwort Safe einen Eintrag aus der CSV Datei zuordnen!
Das Beispiel zeigt die Verhältnisse, bei einer Datei mit Spaltenüberschriften in der ersten Zeile. Ist dies nicht der Fall, werden beispielhaft die Daten
aus der ersten Zeile zur Auswahl angeboten.

3 Betätigen Sie jetzt die Import durchführen Schaltfläche

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

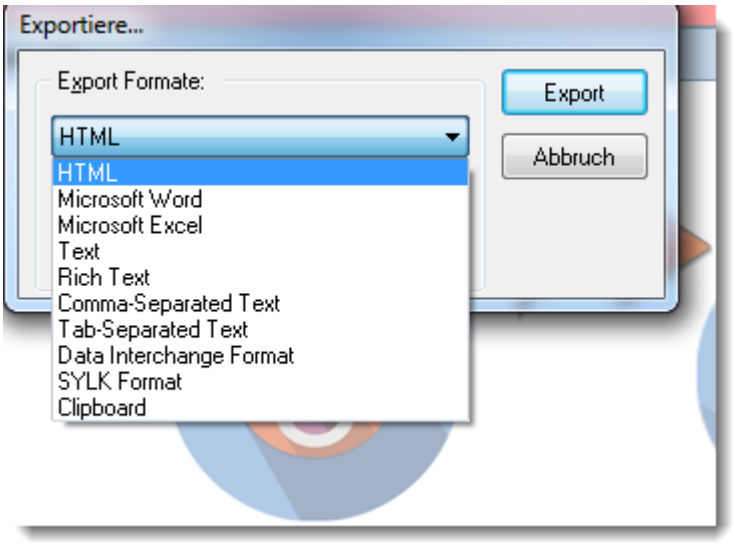
Alle Einträge werden jetzt in den Passwort Safe importiert und stehen in der Kategorie "Import (Datum/Uhrzeit)" zur Verfügung. Sie können die Kategorie natürlich umbenennen und die Passworteinträge bearbeiten.



Tastaturkürzel
(Strg+Alt+Z)

Export der Safedaten

ArchiCrypt Passwort Safe ermöglicht den Export des Safeinhalts in viele verschiedene Formate.



Beispiel: Safe als HTML Datei exportiert

Bitte beachten Sie, dass Passwörter mit bestimmten Sonderzeichen und **Schlüsseldateien** im Allgemeinen nicht korrekt exportiert werden können. Die Zeichen sind in vielen Formaten unleserlich und unbrauchbar. Wenn Sie auf die Exportfunktion angewiesen sind, nutzen Sie keine Schlüsseldateien im Safe (*Sie können den Safe selbst natürlich*

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

mit einer Schlüsseldatei schützen) und verwenden Sie möglichst die Zeichen, wie sie im Passwortgenerator bei Zeichensatz vorschlagen (internetsicher) vorgeschlagen werden.

siehe auch Einstellungen Passwortgenerator 114

Sie haben grundsätzlich die Möglichkeit, den kompletten Passwort Safe zu exportieren oder Einträge einer ausgewählte Kategorie bzw. eines markierten Verzeichnisses.

➡**HINWEIS: Bitte beachten Sie, dass auch dann, wenn Sie beim Export die Option Nur ansehen auswählen, Klartextdaten auf dem Rechner landen können.**

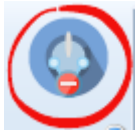
(Strg+Alt+X)

Safe Portable erstellen

Erstellen Sie einen Safe Portable (USB)
Um einen Safe Portable erstellen zu können, müssen Sie einen Passwort Safe geladen haben. Der Passwort Safe wird als Testversion starten. Sie können die USB Version mit den selben Registrierungsdaten registrieren, die Sie zur Aktivierung der PC Version 3 verwendet haben.

siehe **Safe Portable** 38

Passwort Safe aufräumen



Um die Synchronisation verwandter Safe Dateien zu ermöglichen, werden Einträge im Passwort Safe zunächst nicht wirklich gelöscht, sondern nur entsprechend markiert. Erst wenn Sie die Safe Datei aufräumen, werden die Inhalte wirklich aus der Datenbank entfernt.

Menüleiste Dateien

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Erst, wenn Sie einen Eintrag im Passwort Safe ausgewählt haben, der ein Passwort enthält, können wir Dateien verschlüsseln.
Diese Funktion ist nur dazu gedacht, Dateien zu entschlüsseln, die Sie mit einer **ALT - Version** des ArchiCrypt Passwort Safes verschlüsselt haben.

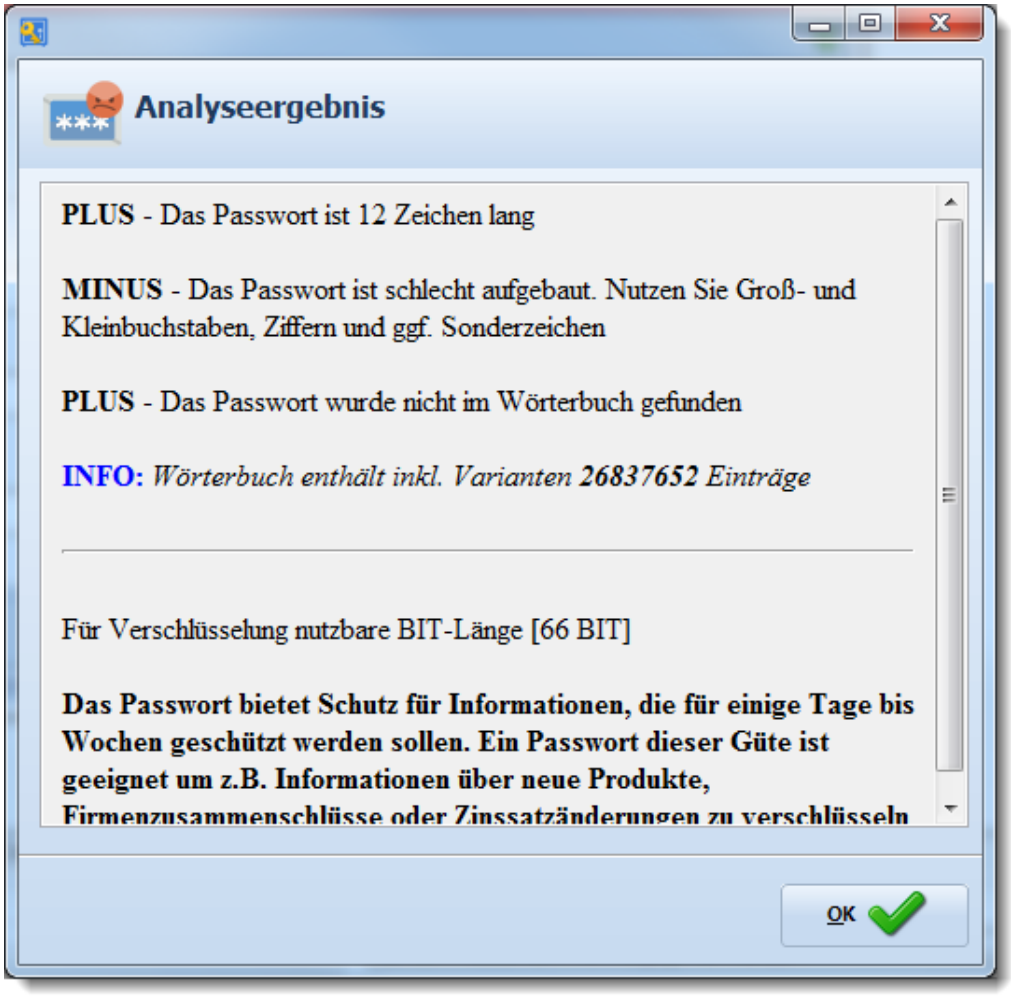
Nutzen Sie statt dessen die Drag-Drop Verschlüsselung[83]

Passwörter bewerten, ArchiCrypt PassOnPaper und QR Passcode

Passwörter bewerten

Sie können sich hier rasch einen Überblick über die grundsätzliche Güte eines Passwortes verschaffen.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



PassOnPaper

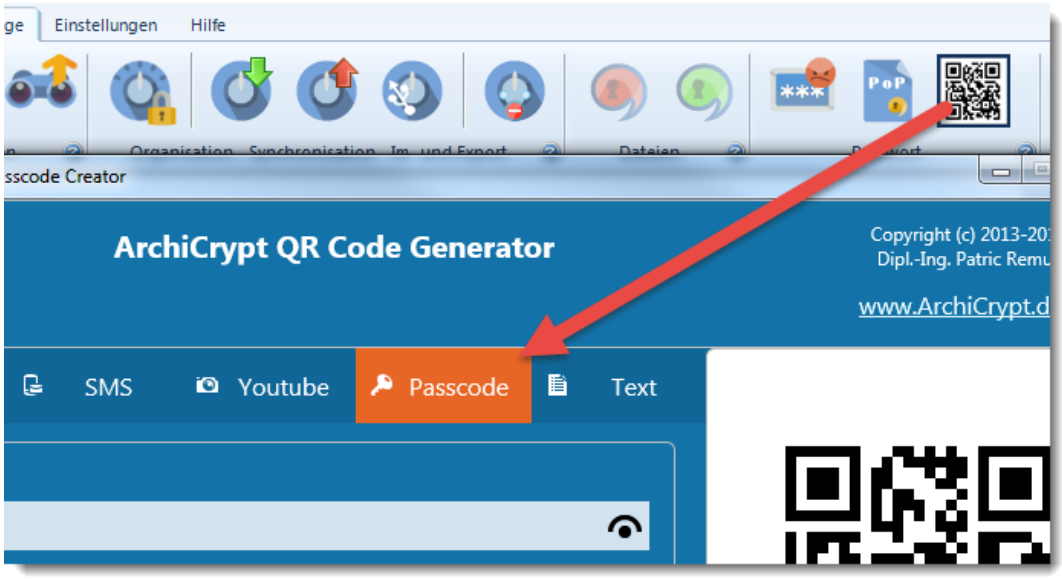
PassOnPaper ist eine eigenständige Anwendung, mit der Sie sich einen Passwort Safe auf Papier erstellen können.

siehe **PassOnPaper**[1]

QR Passcode Generator

Steht nur in der PC Version zur Verfügung. Die externe Anwendung ermöglicht es Ihnen einen speziellen **QR Code** (*QR Passcode*) zu erzeugen, mit dem Sie sich auf iPhone und iPad die Eingabe des Passwortes sparen können. Genaue Hinweise finden Sie im Handbuch für die mobile Passwort Safe Version.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

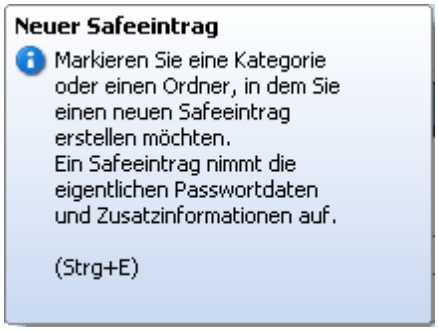


Hilfe

So rufen Sie die Hilfe zu einer Funktion auf

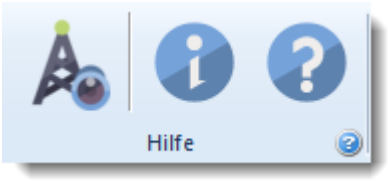
Bewegen Sie die Maus über eine der Schaltflächen um sich eine **Kurzhilfe** anzeigen zu lassen. Gleichzeitig wird, sofern verfügbar, die Tastenkombination für den direkten Aufruf der Funktion angezeigt.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Hilfe zur Schaltfläche Neuer Safeeintrag mit Tastaturkürzel Strg+E

Menüleiste Hilfe



Neue Version vorhanden?

Prüft, ob eine neuere Version verfügbar ist und führt ggf. ein Update aus.
Nicht verfügbar bei Safe Portable Variante.

Über...

Information über ArchiCrypt Passwort Safe. Internet Adressen - Versionsnummer etc.

Hilfe

Ruft die Online-Hilfe auf, die Sie an jeder Stelle in der Anwendung mit der F1 Taste aufrufen können. Dabei wird in das jeweilige Kapitel der Hilfe gesprungen.

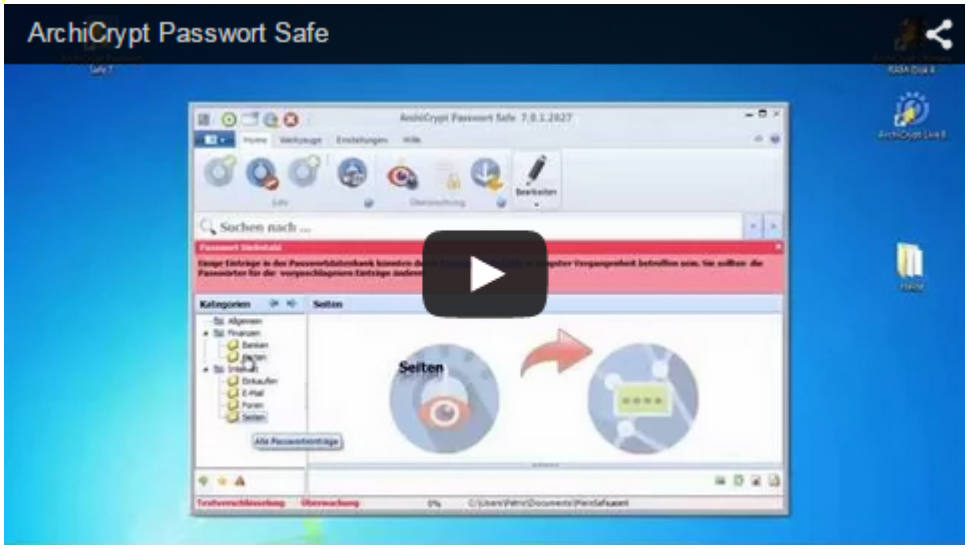
(F1)

Menüleiste ArchiCrypt im Internet

Besuchen Sie die ArchiCrypt Homepage oder senden Sie uns Ihre konstruktive Kritik und Ihre Anregungen.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Video Workshop ArchiCrypt Passwort Safe[23]



Folgende Themen könnten Sie ebenfalls interessieren:

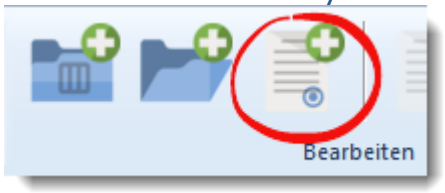
- Die Bedienoberfläche[39]
- Einstellungen - So legen Sie Hotkeys fest[101]
- Tastaturkürzel[37]
- Erster Start - So richten Sie ArchiCrypt Passwort Safe ein[27]

8.7 Passworteintrag

Ein Safeeintrag in ArchiCrypt Safe umfasst nicht alleine das Passwort, sondern zahlreiche sehr flexibel nutzbare Informationen.

Einen Safeeintrag können Sie auf verschiedene Weise erzeugen:

1. Klick auf das Symbol in der Menüleiste

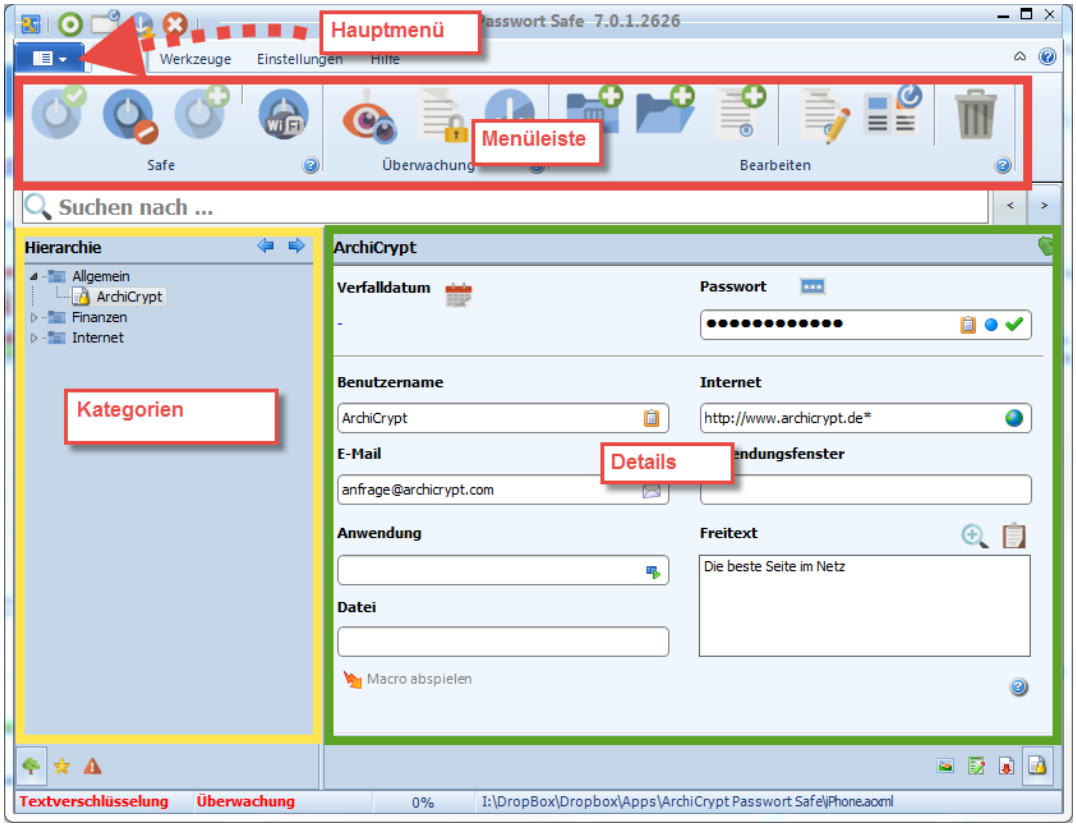


2. Tastaturkürzel Strg+E **sofern der Passwort Safe angezeigt wird**

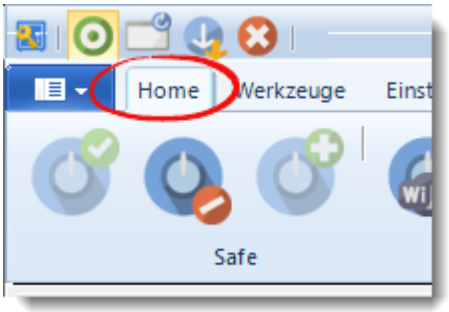
3. Beim Surfen, wenn Sie den Hotkey für Erstelle neuen Safe Eintrag[110] festgelegt haben.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

(siehe dazu einen Safeeintrag erstellen[8])



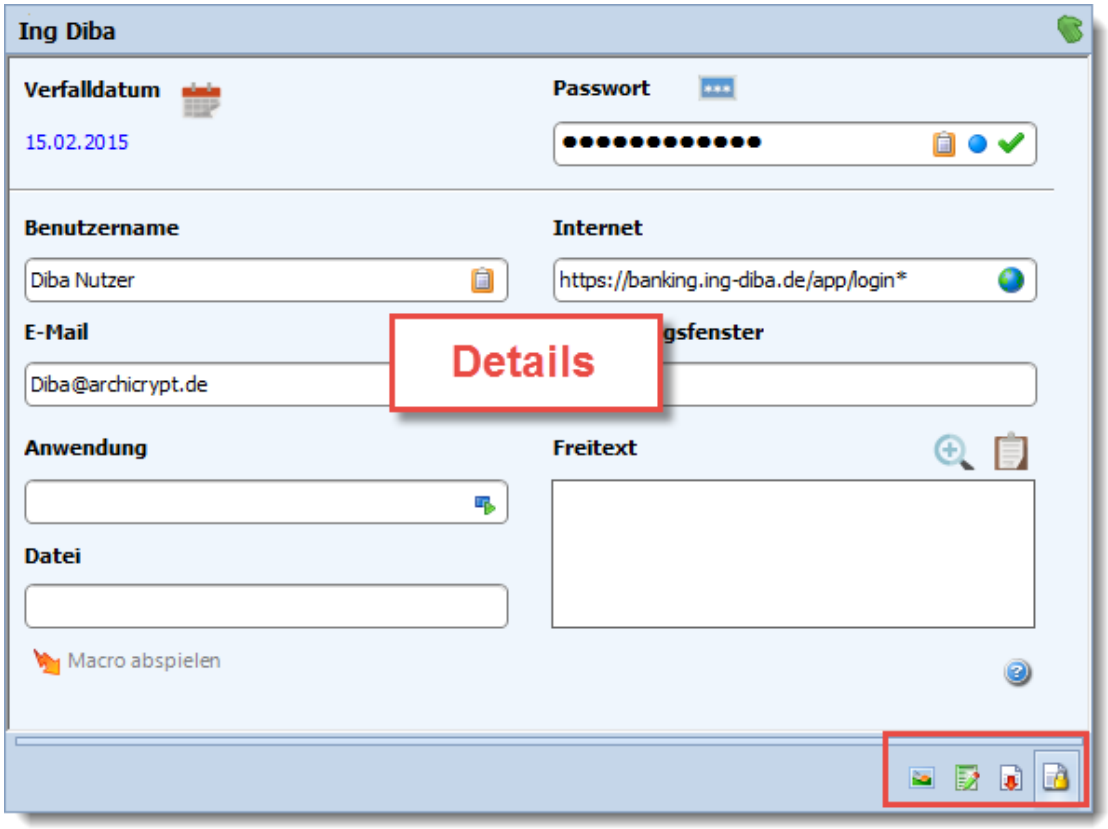
In der **Home-Ansicht** des Safes (**Home Register**)



sehen Sie links die Kategorien. Um die Details zu einem Passwort anzuzeigen, klicken Sie auf einen Eintrag.

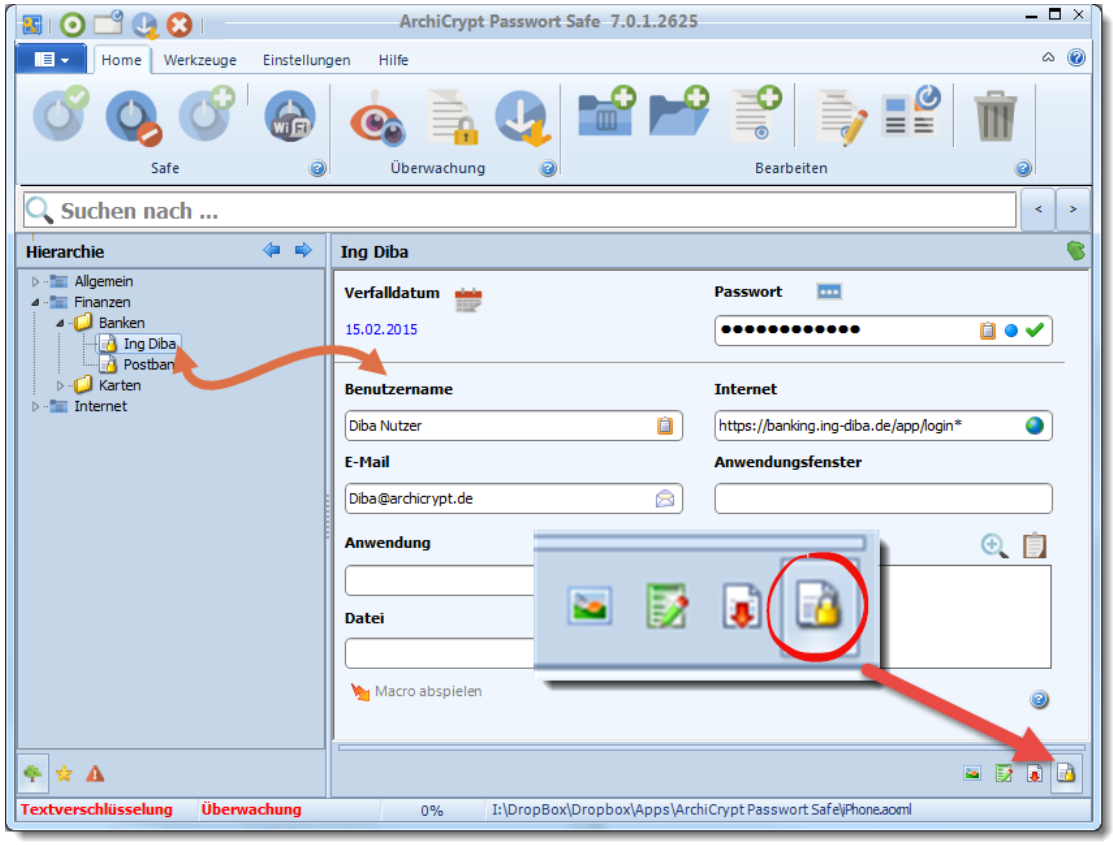
Sie sehen jetzt rechts in der Detailansicht[70] die zum Eintrag gehörenden Informationen. Am unteren Rand können Sie sich eventuell festgelegte Listen[76], Formularwerte[77] oder eine zugeordnete Grafik[77] ansehen.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



So sehen Sie sich die Informationen zu einem Passworteintrag an

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Passwortdetails

Benutzername

Dieses Feld kann neben einem Namen selbstverständlich eine beliebige Zeichenkombination aufnehmen. Wenn man die

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Browserüberwachung nutzt und Online-Banking durchführt, kann man hier zum Beispiel seine Kontonummer eingeben, die für das Login auf einer Seite erforderliche E-Mail Adresse etc.

Mit der Schaltfläche können Sie den Inhalt in die Zwischenablage kopieren. In nahezu jeder Anwendung können Sie den Inhalt dann in ein Eingabefeld einfügen (*entweder über ein Kontextmenü via rechter Maustaste oder durch Betätigen der Tastenkombination* Strg + V).

Selbstverständlich können Sie den Inhalt auch per **Drag&Drop** in das Eingabefeld ziehen, oder, die beste und schnellste Möglichkeit, mit Hotkeys[101] (*siehe auch Einstellungen*[86]) übertragen.

Passwort

Hier ist Ihr Passwort, Kennwort, eine PIN, der Inhalt einer Schlüsseldatei oder eine sonstige Information abgelegt. Sie können anhand des Symbols erkennen, ob es sich um ein Passwort (*Text*) oder um eine Schlüsseldatei handelt.

Wenn Sie die Schlüsseldatei auf einem externen Datenträger speichern möchten, Klicken Sie einfach mit der Maus auf die Schaltfläche **Export...** , die nur dann sichtbar ist, wenn eine Schlüsseldatei verfügbar ist.

Mit der Schaltfläche können Sie den Inhalt in die Zwischenablage kopieren. In nahezu jeder Anwendung können Sie den Inhalt dann in ein Eingabefeld einfügen (*entweder über ein Kontextmenü via rechter Maustaste oder durch Betätigen der Tastenkombination* Strg + V). Selbstverständlich können Sie den Inhalt auch per **Drag&Drop** in das Eingabefeld ziehen, oder, die beste und schnellste Möglichkeit, mit **Hotkeys**[101] (*siehe auch* Einstellungen[86]) übertragen.

Mit der Schaltfläche können Sie sich das Passwort im Klartext anzeigen lassen oder vom Klartext in die verdeckte Anzeige zurück wechseln. Sofern Sie keine Angst haben müssen, dass Sie jemand beobachtet, spricht nichts gegen die

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Klartextansicht. Nach einigen Sekunden schaltet die Ansicht automatisch wieder in die verdeckte Ansicht.

Mit der Schaltfläche ✔ können Sie das aktuelle Passwort bewerten[63] lassen.

E-Mail

Hier können Sie eine E-Mail Adresse ablegen und, falls Sie einen **MAPI** fähigen E-Mail Client besitzen (*z.B. MS-Outlook oder Thunderbird*), durch Betätigen der Schaltfläche **Senden** eine E-Mail erstellen lassen.

Der Safe schaltet automatisch in den **Modus Textverschlüsselung**.

siehe dazu Textverschlüsselung[81]

Anwendung

Hier kann eine Datei oder eine Anwendung eingetragen sein. Betätigen Sie die Schaltfläche **Starten...** und die Datei wird mit der auf Ihrem System verknüpften Anwendung geöffnet oder die Anwendung wird gestartet.

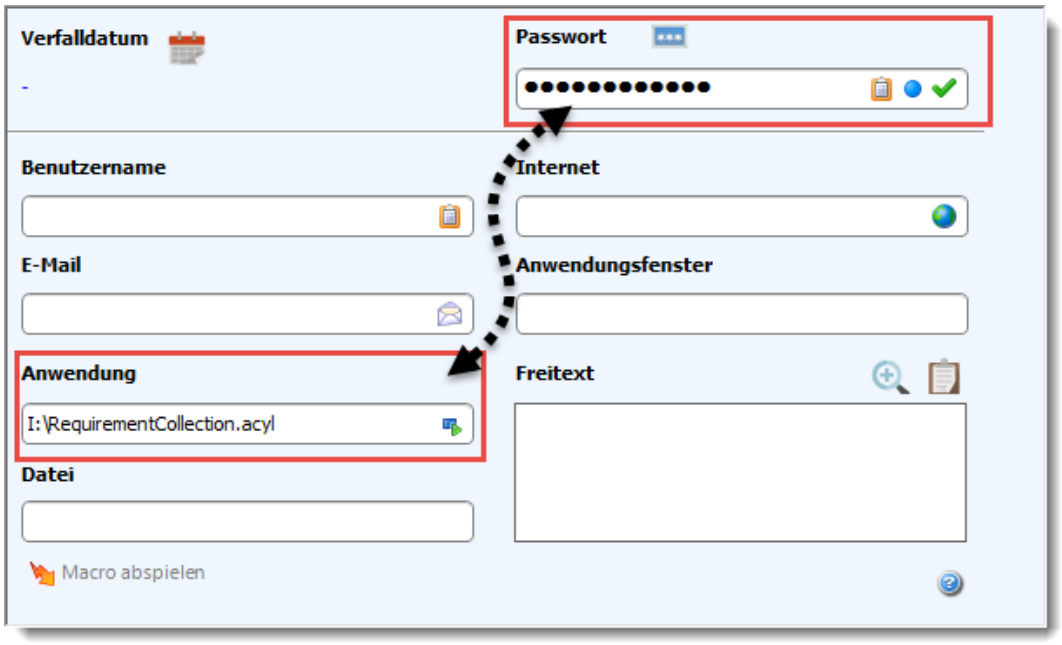
Sie können der Anwendung auch über Parameter die Inhalte von Safe Einträgen übergeben[13] . Damit ist es zum Beispiel möglich, einem Eintrag einen ganz bestimmten Browser zuzuordnen.

Falls Sie **ArchiCrypt Live** besitzen, können Sie hier eine ArchiCrypt Live Laufwerksdatei angeben. Die Datei muss zwingend die Endung **acl** bzw. **acyl** tragen.

So nutzen Sie den Passwort Safe um ein ArchiCrypt Live Laufwerk zu laden

Wählen Sie im Passwort Safe den Eintrag aus. Der Eintrag muss ein Passwort bzw. Schlüsseldatei und den Pfad und Namen der Laufwerksdatei im Feld Anwendung enthalten.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Datei

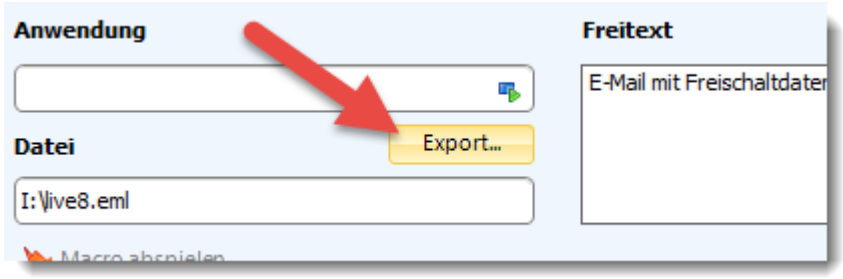
Hier können Sie kleinere Dateien in Ihrem Passwort Safe ablegen. Die Dateien werden dabei verschlüsselt abgelegt. Bitte nutzen Sie diese Funktion nur für **kleine Dateien**, wie Sie zum Beispiel bei machen Softwareherstellern zum Registrieren von Anwendungen verschickt werden.

Dateien können bis **maximal 200 KByte** in die Datenbank übernommen werden. Insgesamt sollten Sie nicht zu viele dieser Dateien im Safe ablegen, da der Safe so sehr langsam wird. Bereits ab einer Dateigröße von **10 KByte** warnt der Passwort Safe.

So speichern Sie die Datei unverschlüsselt auf Ihrem Rechner

Sofern dem Passwort Eintrag eine Datei zugeordnet ist, wird der Dateiname angezeigt und es erscheint eine Schaltfläche **Export...**

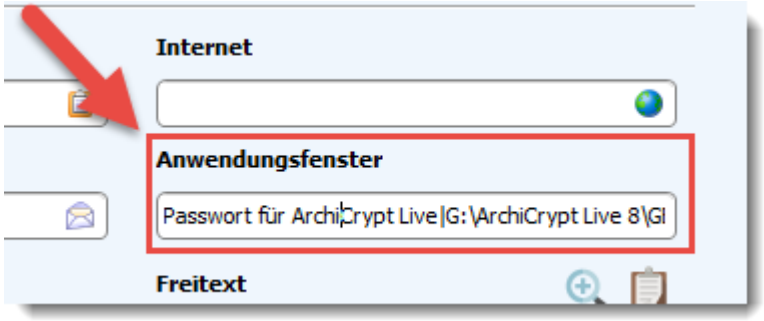
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Klicken Sie auf die Schaltfläche **Export** und legen Sie den Speicherort für die Datei fest.

Anwendungsfenster

Hier kann das Fenster einer bestimmten Anwendung angegeben sein, bei dem der Passwort Safe den zugehörigen Eintrag bereitstellen soll. Ähnlich wie beim Besuch einer bestimmten WEB-Seite reagiert ArchiCrypt Passwort Safe auf das **Erscheinen des Fensters** mit der Bereitstellung dieses Passworteintrags.

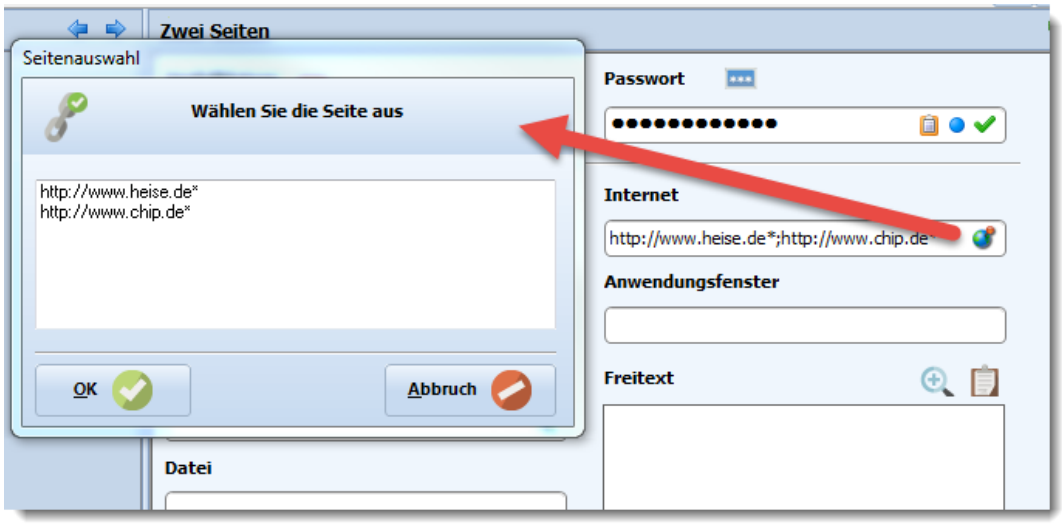


siehe Anwendungsfenster bei Safeeintrag erstellen 18

Internet

Hier können eine oder mehrere Internetseiten eingetragen sein. Wenn Sie eine der aufgeführten Internetseiten besuchen möchten, betätigen Sie die Schaltfläche **Besuchen...** Falls mehr als eine Internetseite angegeben ist, erscheint ein **Auswahldialog**, in dem Sie eine Seite auswählen können.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



siehe auch Einstellungen[89] Besuchen aktiviert Überwachung

siehe auch So stellen Sie sicher, dass der Passwort Safe die Internetseite erkennt[17]

Freitextfeld

In diesem Feld können Sie beliebige Textinformationen ablegen.

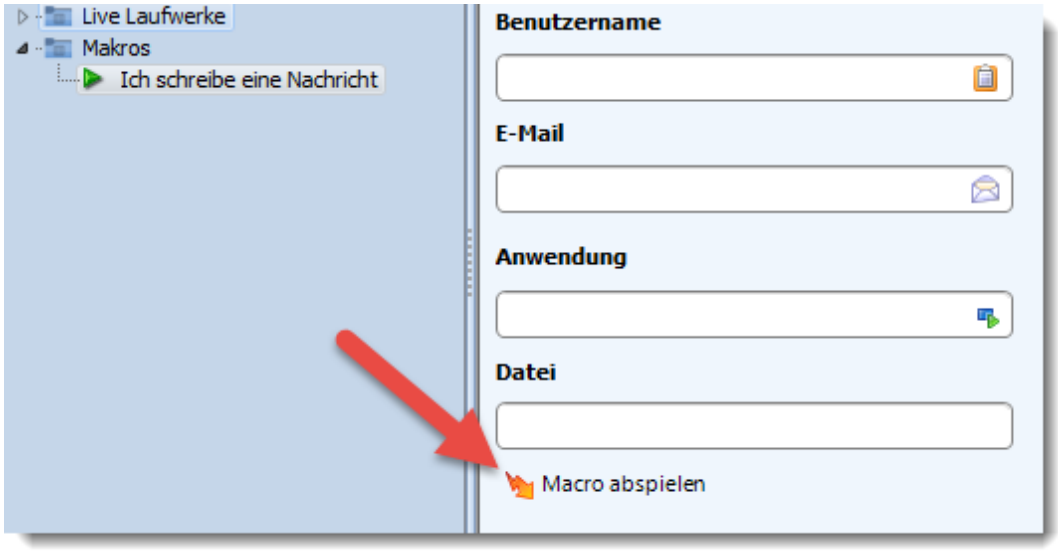
Mit der Schaltfläche können Sie den Inhalt in die Zwischenablage kopieren. In nahezu jeder Anwendung können Sie den Inhalt dann in ein Eingabefeld einfügen (*entweder über ein Kontextmenü via rechter Maustaste oder durch Betätigen der Tastenkombination Strg + V*). Selbstverständlich können Sie den Inhalt auch per **Drag&Drop** in das Eingabefeld ziehen, oder, die beste und schnellste Möglichkeit, mit **Hotkeys**[101] (siehe auch Einstellungen[86]) übertragen.

Wenn Sie viel Text in das Feld eingetragen haben, können Sie den Text in einem eigenen Fenster anzeigen lassen, indem Sie die Schaltfläche betätigen.

Makro ausführen

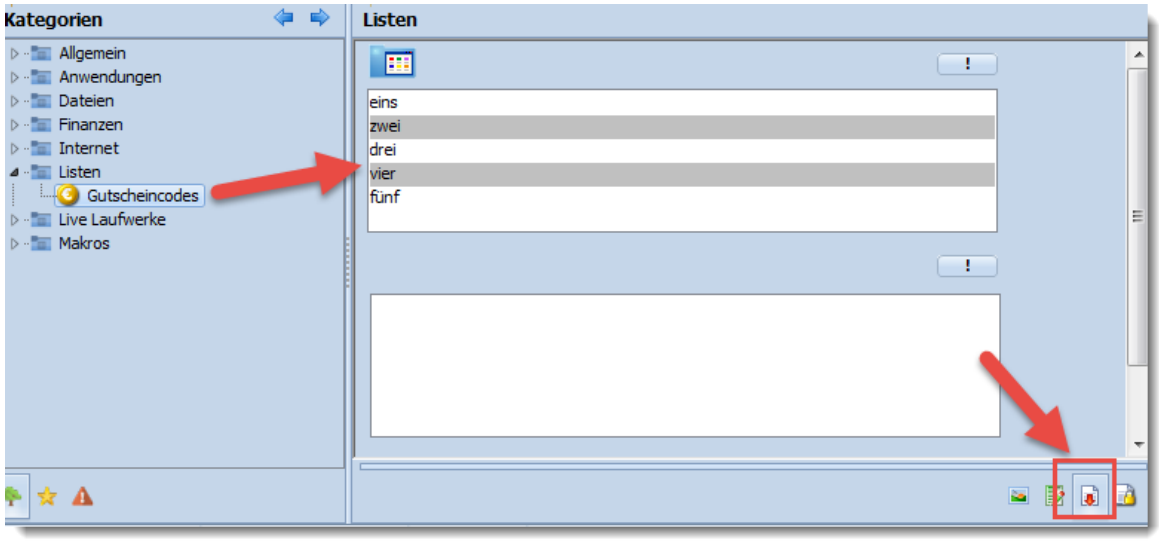
Sofern mit dem Passworteintrag ein Makro verknüpft ist, erscheint die Schaltfläche unterhalb des Feldes für Datei. Klicken Sie auf die Schaltfläche, um das Makro abzuspielen. Sie können in den Einstellungen auch einen **Hotkey**[101] (*siehe auch Einstellungen*[86]) festlegen.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



TOP 67

Listen



In den **Listen** können Sie beliebige Textinformationen speichern. So können Sie zum Beispiel eine Liste mit Gutschein-Codes in die obere Liste eingeben und verbrauchte Einträge in die untere Liste verschieben. Sie können diesen Vorgang mit Hilfe von Hotkeys 101 automatisieren.

Mit der Schaltfläche ! können Sie den Inhalt in die Zwischenablage kopieren. In jeder nahezu jeder Anwendung können Sie den Inhalt dann in ein Eingabefeld einfügen (*entweder über ein Kontextmenü via rechter Maustaste oder durch Betätigen*

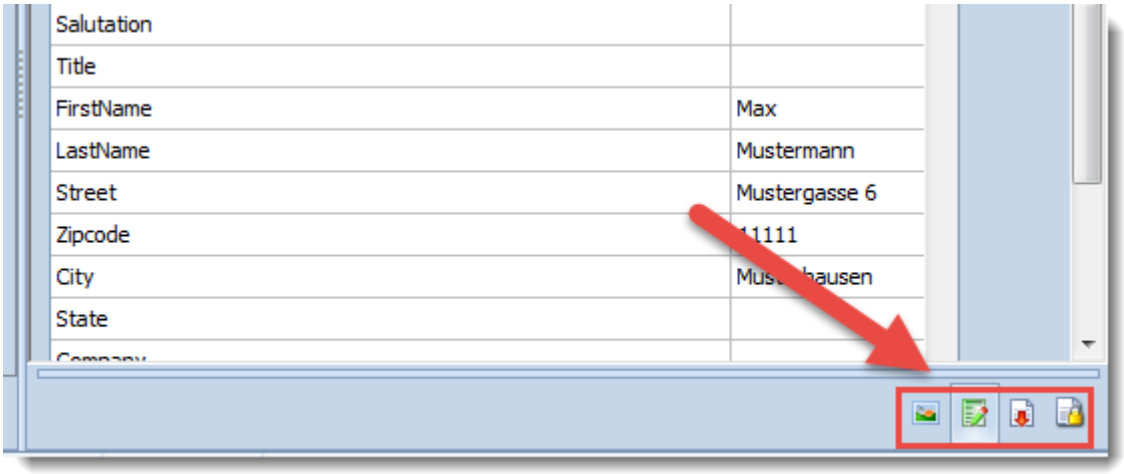
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

der Tastenkombination Strg + V). Selbstverständlich können Sie den Inhalt auch per Hotkey[101] (siehe auch Einstellungen[86]) übertragen.

Falls Sie in den Einstellungen (Hotkeys[101]) die Auswahl **Listeneintrag verschieben** ausgewählt haben, wird dieser Wert anschließend von der oberen Liste in die untere verschoben (*nicht gelöscht*). Wenn Sie jetzt erneut die Tastenkombination betätigen, steht Ihnen der nächste Eintrag aus der oberen Liste zur Verfügung. Dies können Sie so lange fortführen, bis die obere Liste keine Einträge mehr enthält.

TOP[67]

Formular



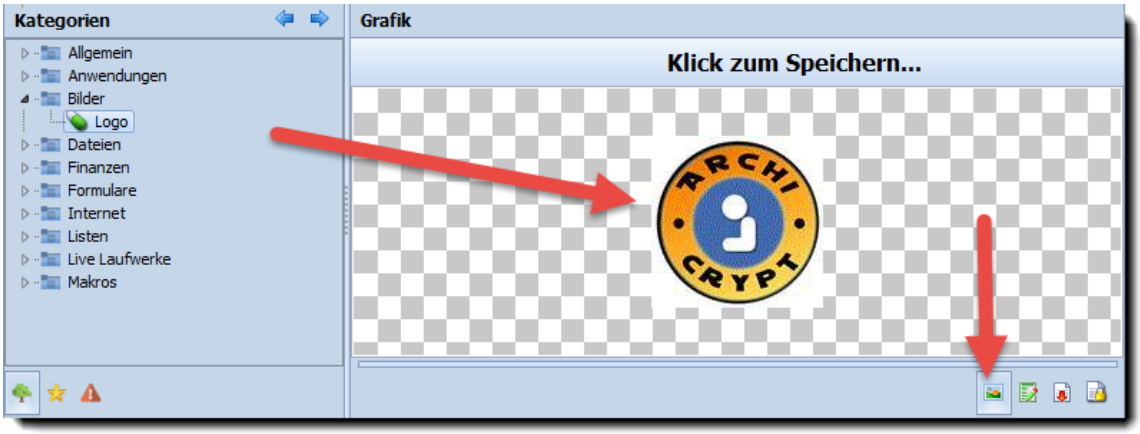
Sofern Sie mit dem Eintrag ein Formular automatisch ausfüllen, sehen Sie hier die Zuordnung von Elementen des Formulars zu Werten im Passwort Eintrag. Wenn Sie einem Eintrag ein Formular zugeordnet haben, können Sie die Inhalte per Hotkey[101] in den **Internet Explorer** übertragen. Andere Browser unterstützen das Verfahren nicht direkt.

siehe Formular bei Safeeintrag erstellen[21]

TOP[67]

Bild

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Wenn Sie dem Eintrag eine Grafik zugeordnet haben, können Sie sich hier die Grafik ansehen. Die Grafik können Sie sich zudem mit Hilfe eines Hotkeys[109] beim Surfen anzeigen lassen.

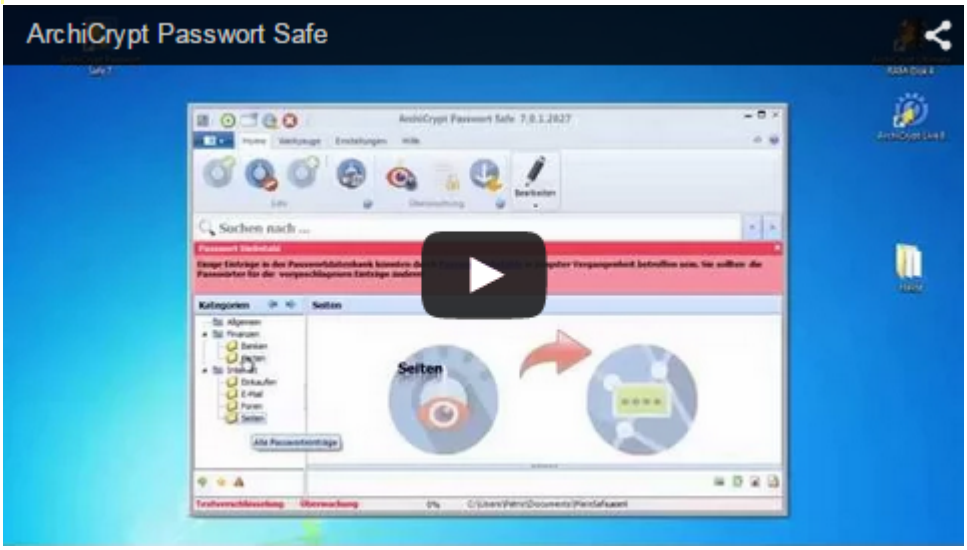
Lupe: **Linksklick** auf das Bild vergrößert, ein **Rechtsklick** verkleinert.

So können Sie die Grafik wieder unverschlüsselt speichern

Die Daten des Bildes sind verschlüsselt in Ihrem Safe. Wenn Sie die Daten unverschlüsselt speichern möchten, klicken Sie auf die Schaltfläche Klick zum **Speichern** oberhalb der Grafik.

TOP[67]

Video Workshop ArchiCrypt Passwort Safe[23]



© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

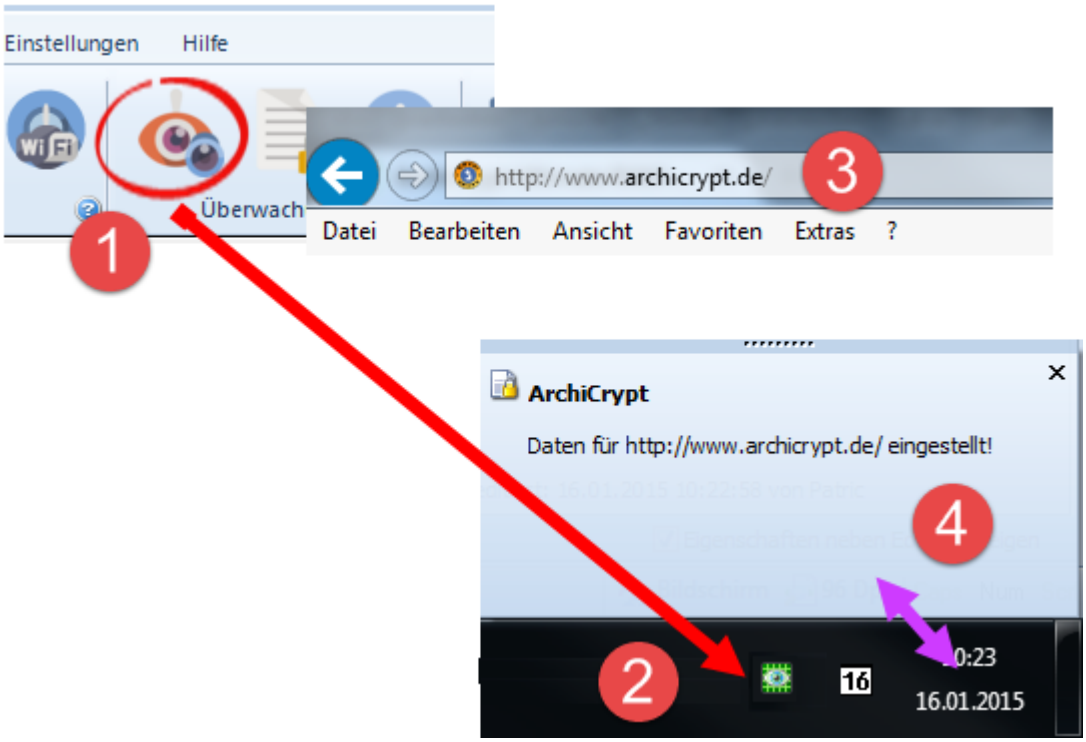
Folgende Themen könnten Sie ebenfalls interessieren:

Einen Safeeintrag erstellen[8]
So erzeugen Sie beim Surfen einen neuen Safe Eintrag[110]
So stellen Sie sicher, dass der Passwort Safe die Internetseite erkennt[17]
So starten Sie die Browserüberwachung automatisch[87]
So übertragen Sie Passwort&Co an den Browser[102]
So legen Sie fest, welcher Browser unterstützt werden soll[93]
So können Sie sich beim Online-Banking Ihre TAN Liste anzeigen lassen[109]
Die Bedienoberfläche[39]
Dialog für die Passworteingabe[30]
Erster Start - So richten Sie ArchiCrypt Passwort Safe ein[27]
Einstellungen - So legen Sie Hotkeys fest[101]

8.8 Überwachung

Die Überwachung

Wenn Sie die **Überwachung** (1) starten wird der Passwort Safe in den Infobereich (2) minimiert.



ArchiCrypt Passwort Safe überwacht jetzt, welche Internetseiten Sie in Ihrem Browser (3) besuchen und welche Anwendungsfenster im

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

System erscheinen. Falls in der Datenbank ein passender Eintrag existiert, erscheint ein **Nachrichtenfenster** (4).

➡**HINWEIS: Es wird nur der Browser überwacht, den Sie in den Einstellungen des Passwort Safes**[93] **ausgewählt haben!**

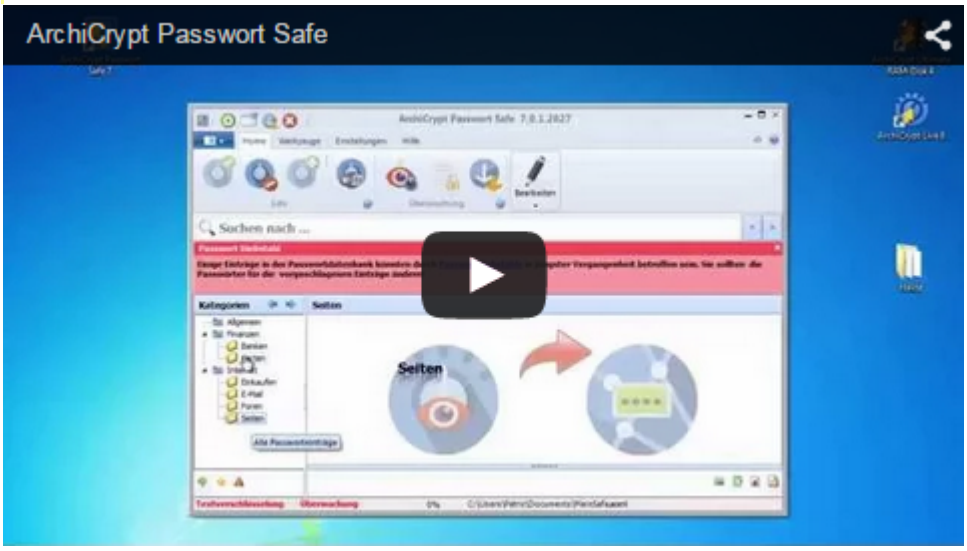
Sie können dann z.B. Daten aus dem Passwort Safe mit Hilfe der Hotkeys[101] in die Internetseite übertragen.

Das **Symbol im Infobereich** (2) ist bei aktiver Überwachung **grün**, ansonsten **rot**. Der Safe reagiert auf Hotkeys[101] und bietet sein Kontextmenü[89] (*Klick auf Symbol mit rechter Maustaste*) an.

siehe auch: Formularfüller[93]

Alternativ können Sie die Überwachung mit dem Hotkey[101] Strg+I starten.

Video Workshop ArchiCrypt Passwort Safe[23]



Folgende Themen könnten Sie ebenfalls interessieren:

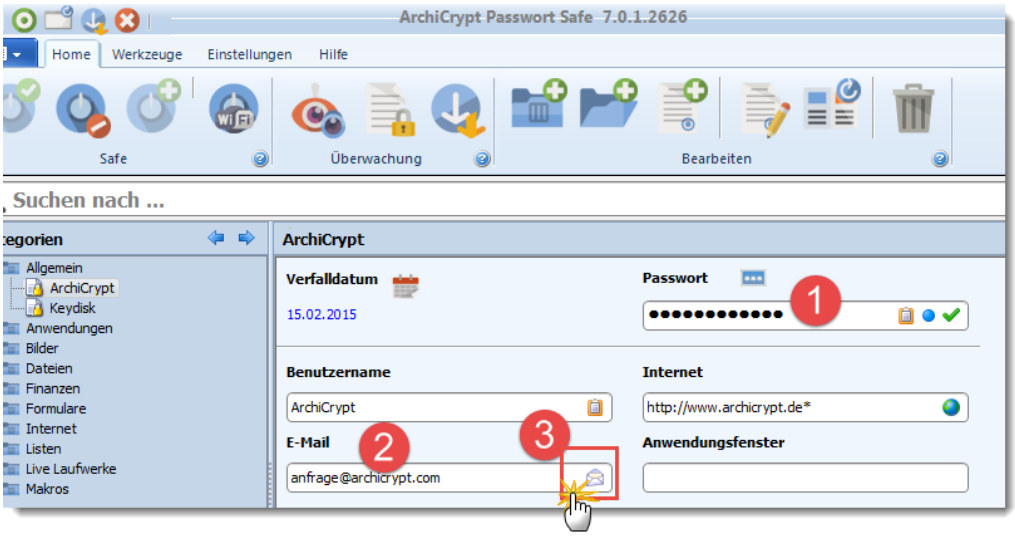
So stellen Sie sicher, dass der Passwort Safe die Internetseite erkennt[17]
Menüleiste Überwachung[49]
Erster Start - So richten Sie ArchiCrypt Passwort Safe ein[27]
Einstellungen - So legen Sie Hotkeys fest[101]
So starten Sie die Browserüberwachung automatisch[87]
So erzeugen Sie beim Surfen einen neuen Safe Eintrag[110]

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

So übertragen Sie Passwort&Co an den Browser[102]
So legen Sie fest, welcher Browser unterstützt werden soll[93]
So können Sie sich beim Online-Banking Ihre TAN Liste anzeigen lassen[109]

8.9 Textverschlüsselung

Die Textverschlüsselung



So tauschen Sie sicher Textnachrichten per E-Mail aus

Vereinbaren Sie mit Ihrem Kommunikationspartner auf sicherem Wege ein Passwort. Z.B. bei einem persönlichen Treffen, notfalls per FAX oder Telefon. Erstellen Sie einen Safeeintrag und geben Sie die **E-Mail Adresse** (2) Ihres Partners und das vereinbarte **Passwort** (1) ein.

Wenn Sie jetzt eine vertrauliche Nachricht versenden möchten, wählen Sie im Safe den Eintrag aus und betätigen Sie die Schaltfläche **Senden (3)**. Der Safe wird jetzt minimiert, die Textverschlüsselung wird automatisch aktiviert und Ihr E-Mail Programm wird gestartet.

Geben Sie jetzt den Text ganz normal in Ihrem Mail - Programm ein. Sobald Sie fertig sind, markieren Sie den kompletten Text in die Zwischenablage. ArchiCrypt Passwort Safe hat den Text jetzt bereits verschlüsselt, Sie können den verschlüsselten Text jetzt über die Zwischenablage einfügen und versenden.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

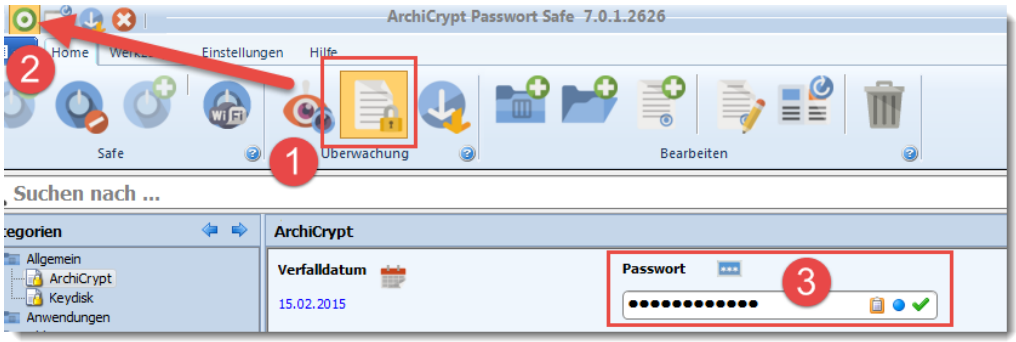
TIPP:

Nahezu jede Anwendung, in der Sie mit Text arbeiten nutzt folgende Tastaturkürzel, mit denen Sie sehr schnell zum Ziel kommen.
Gesamten Text markieren **Strg + A**
Markierten Text in die Zwischenablage kopieren **Strg + C**
Text aus der Zwischenablage einfügen **Strg + V**
Lassen Sie den Text markiert, wenn Sie den verschlüsselten Text aus der Zwischenablage einfügen. So wird der Klartext sofort überschrieben.
Oder noch kürzer: **Strg+X** zum Ausschneiden und anschließend **Strg+V**.

Sie können überprüfen, ob die Ver-/Entschlüsselung korrekt arbeitet, indem Sie den jetzt verschlüsselten Text nochmals in die Zwischenablage kopieren und das Ergebnis einfügen. Der Text sollte jetzt wieder im Klartext erscheinen.

➡**WARNUNG: Ändern Sie bitte kein einziges Zeichen der Verschlüsselten Nachricht. Die Nachricht kann ansonsten nicht entschlüsselt werden.**

So können Sie eine verschlüsselte Textnachricht entschlüsseln



Markieren Sie im Passwort Safe den Eintrag der das Passwort (3) enthält, das mit dem Absender vereinbart wurde. Betätigen Sie die Schaltfläche Text ver-/entschlüsseln (1). Markieren Sie den kompletten verschlüsselten Text und kopieren sie ihn in die Zwischenablage. ArchiCrypt Passwort Safe entschlüsselt die Nachricht und zeigt dies durch eine Nachricht an. Sie können den unverschlüsselten Text jetzt über die Zwischenablage in ein anderes Programm einfügen.

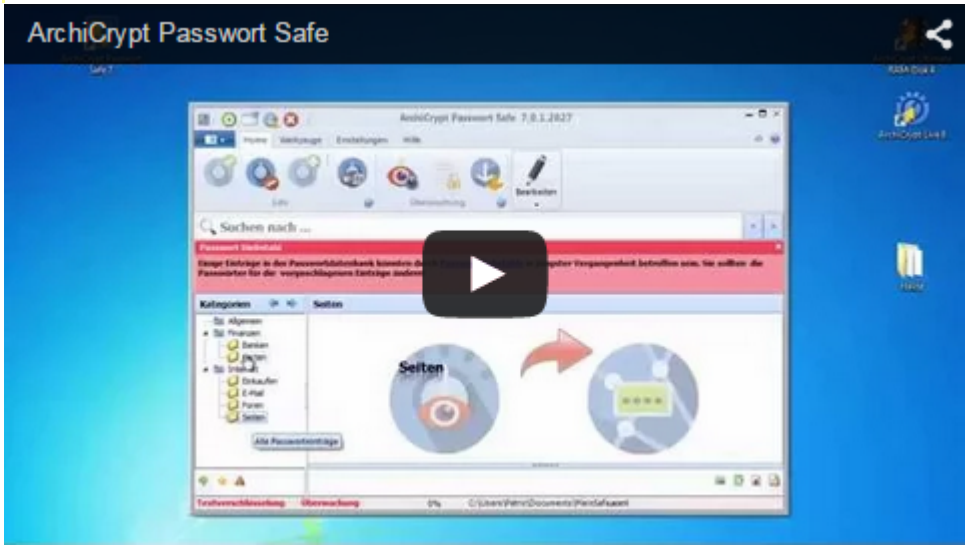
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Was tun, wenn der Empfänger keinen ArchiCrypt Passwort Safe besitzt?

Nicht jeder besitzt ArchiCrypt Passwort Safe und nicht jeder möchte das Programm sofort käuflich erwerben. Dennoch möchten Sie unter Umständen auch mit diesem Personenkreis vertrauliche Nachrichten austauschen. Zu diesem Zweck stellen wir ein kostenloses Programm - **ArchiCrypt Easy Encryption -** zur Verfügung, mit dem man auch ohne den Passwort Safe Text ver- und entschlüsseln kann. In der verschlüsselten Nachricht ist der Downloadlink für dieses kleine Programm enthalten. Der Passwort Safe kann selbstverständlich Nachrichten entschlüsseln, die mit Easy Encryption erstellt wurden.

siehe: ArchiCrypt Zero Tools...

Video Workshop ArchiCrypt Passwort Safe 23



Folgende Themen könnten Sie ebenfalls interessieren:

Menüleiste Überwachung 49
Einstellungen - So legen Sie Hotkeys fest 101
So ver- und entschlüsseln Sie eine Datei 62
Drag Drop Verschlüsselung 83

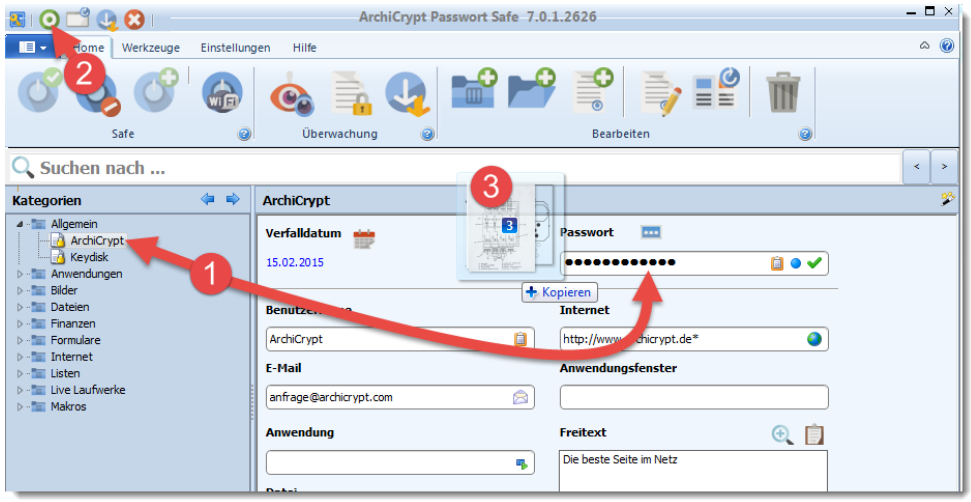
8.10 Drag-Drop Verschlüsselung

Drag & Drop Verschlüsselung

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Drag & Drop kennen Sie sicher aus anderen Anwendungen. Man bezeichnet damit das **Ziehen und Ablegen** von Dateien. Man zieht die Dateien aus dem Dateimanager auf eine Anwendung, die dann eine Aktion mit den Dateien oder Verzeichnissen ausführt. Und genau so funktioniert das auch mit ArchiCrypt Passwort Safe.

So verschlüsseln Sie Dateien mit ArchiCrypt Passwort Safe



1 Wählen Sie den gewünschten Eintrag (1) im Passwort Safe aus, der das **Passwort** enthält, **mit dem die Dateien verschlüsselt** werden sollen.

2 Aktivieren Sie ggf. den Vordergrund-Modus[45] (2) von ArchiCrypt Passwort Safe.

3 Ziehen Sie jetzt die zu verschlüsselnden Daten aus dem Windows Dateimanager oder dem Desktop auf **die Detailansicht** (*Nähe des Passwortes*) und legen Sie die Dateien dort ab.

Gut zu wissen

1. Dateiendung - ArchiCrypt Passwort Safe packt mehrere Dateien in eine einzige Datei, die dann in verschlüsselter Form die **Dateiendung aef** trägt.
2. Die Dateien werden vor dem Verschlüsseln noch komprimiert. Daher wird das Paket wahrscheinlich deutlich weniger Platz belegen, als die einzelnen Dateien. Dies

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

hängt jedoch vom Dateityp ab, da nicht jede Datei gleich gut komprimierbar ist.

4 Legen Sie jetzt den Speicherort für das verschlüsselte Paket fest.

So versenden Sie verschlüsselte Daten per E-Mail

Wenn Sie einem Freund, Bekannten oder Geschäftspartner vertrauliche Daten zusenden möchten, bietet ArchiCrypt Passwort Safe eine passende Funktion! Legen Sie einen Passworteintrag an, in dem Sie das vereinbarte Passwort ablegen und die E-Mail Adresse des Empfängers eintragen. Gehen Sie jetzt so vor, wie oben beschrieben.

UNTERSCHIED: Halten Sie die **STRG-Taste** fest, wenn Sie die Dateien auf das **Passwortfeld** ziehen und dort ablegen. Auch hier wird nach dem Speicherort gefragt. Nachdem das verschlüsselte Paket erzeugt wurde, wird Ihr **Mail Programm gestartet** und das verschlüsselte Paket befindet sich bereits als Anhang in der E-Mail. Wenn Sie auch noch eine vertrauliche Textnachricht übermitteln möchten, nutzen Sie die Textverschlüsselung[81].

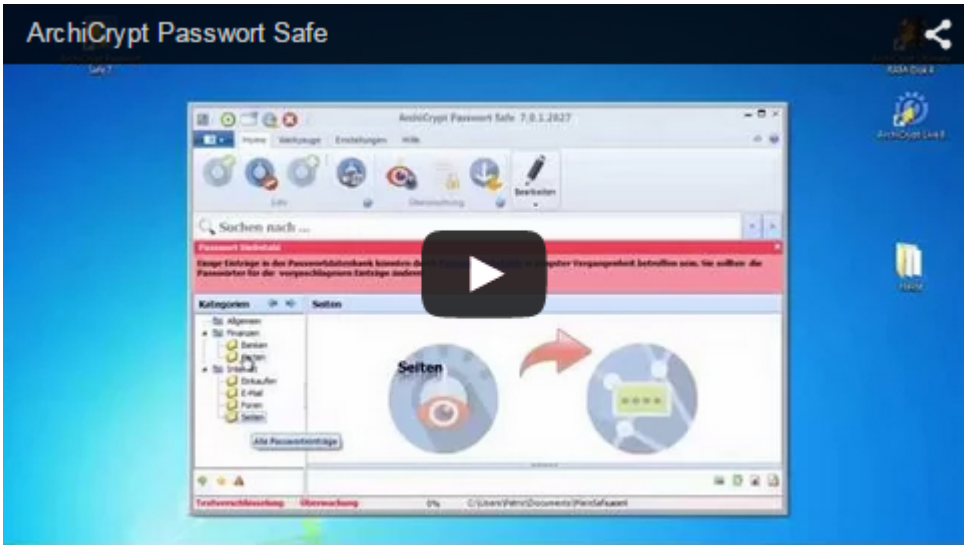
So entschlüsseln Sie Dateien mit ArchiCrypt Passwort Safe

Stellen Sie das zur Verschlüsselung verwendete Passwort ein und ziehen Sie die verschlüsselte Datei auf das **Passwortfeld**. Nachdem Sie das Zielverzeichnis angegeben haben, werden die Daten dorthin entschlüsselt.

➡**HINWEIS: Falls Sie die Datei mit dem gerade offenen Passwort Safe verschlüsselt haben, gibt es eine noch einfachere Methode, die Daten zu entschlüsseln. Sie müssen sich nicht daran erinnern, welchen Eintrag Sie im Safe genutzt haben, um das verschlüsselte Paket zu erzeugen. Einfach einen beliebigen Eintrag auswählen und die verschlüsselte Datei auf das Passwortfeld ziehen. ArchiCrypt Passwort Safe findet den passenden Eintrag.**

Video Workshop ArchiCrypt Passwort Safe[23]

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Folgende Themen könnten Sie ebenfalls interessieren:

So ver- und entschlüsseln Sie eine Datei 62
Textverschlüsselung 81

8.11 Einstellungen

Einstellungen

Sie ändern Sie Einstellungen

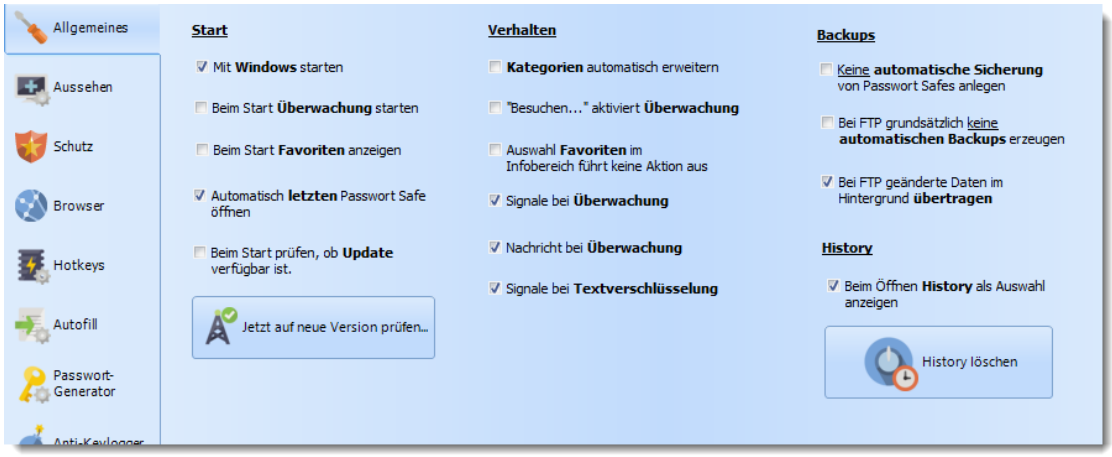
Stellen Sie sicher, dass ein Passwort Safe geladen ist. Betätigen Sie das Tastaturkürzel F10, rufen Sie im Hauptmenü 40 die Funktion **Einstellungen...** auf oder Klick auf **Registerseite Einstellungen**.

Unter Einstellungen können Sie das Verhalten von ArchiCrypt Safe festlegen. Die Einstellungen sind unterteilt in die **Gruppen**

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Allgemeines 87
Aussehen 92
Schutz 93
Browser 93
Hotkeys 101
Autofill 113
Passwort-Generator 114
Anti-Keylogger 117
LogBuch 119

Allgemeines



START

Mit Windows starten

Der Passwort Safe wird beim Start von Windows automatisch geladen.

TIPP: Nutzen Sie diese Option zusammen mit **Beim Start Überwachung starten** und **Automatisch letzten Passwort Safe öffnen** um bereits beim Start von Windows den Safe zu aktivieren.

Beim Start Überwachung starten

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Sobald Sie einen Passwort Safe öffnen, wird sofort die Überwachung des Browsers und von Anwendungsfenstern aktiviert (siehe auch Überwachung[79])

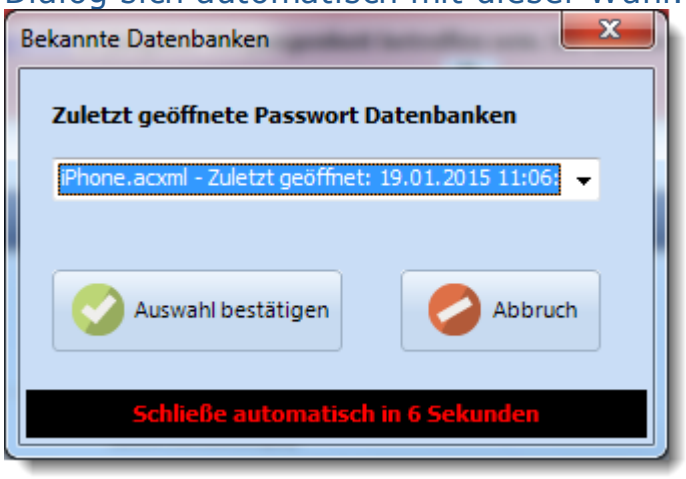
➡**Hinweis: Setzt voraus, dass ebenfalls die Funktion Automatisch letzten Passwort Safe öffnen aktiv ist.**

Beim Start Favoriten anzeigen

Die Registerseite mit den Favoriten wird direkt angezeigt.

Automatisch letzten Passwort Safe öffnen

Beim Start des Passwort Safes wird automatisch nach dem Passwort des zuletzt geöffneten Safes gefragt. Möchten Sie diesen nicht laden, klicken Sie im Passwort Dialog einfach auf Abbrechen. Wenn Sie im Abschnitt History[91] die Option **Beim Öffnen History als Auswahl anzeigen** aktiviert haben, wird eine Liste mit den zuletzt verwendeten Datenbanken angezeigt. Vorausgewählt ist die letzte Datenbank. Wenn Sie innerhalb von 10 Sekunden keine abweichende Wahl treffen, schließt der Dialog sich automatisch mit dieser Wahl.



Beim Start prüfen, ob neue Version verfügbar ist

Falls beim Start eine Internet Verbindung besteht, prüft ArchiCrypt Passwort Safe, ob eine neuere Version verfügbar ist. Sie erhalten dann eine Meldung und können wählen, ob Sie die neue Version einspielen möchten.

Jetzt auf neue Version prüfen

Sie können mit dieser Funktion jederzeit prüfen, ob eine neuere Version des Passwort Safes verfügbar ist. Der Passwort Safe darf nicht von einem Firewall behindert werden und es muss eine Online Verbindung bestehen.

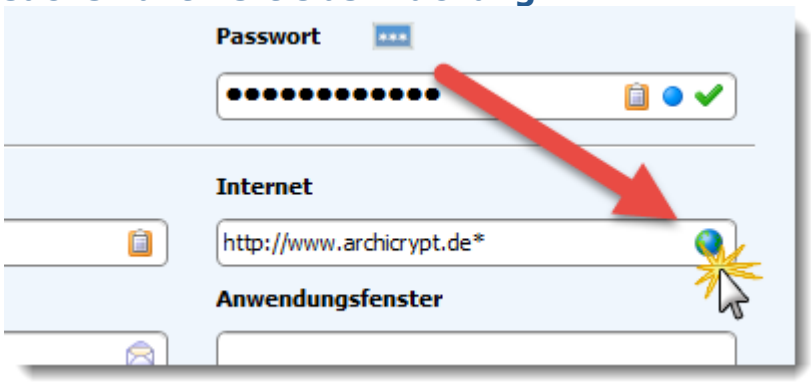
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

VERHALTEN

Kategorien automatisch erweitern

Möchten Sie, dass alle Einträge des Safes nach dem Laden sofort sichtbar sind (*alles aufklappen*), schalten Sie diese Funktion ein. Möchten Sie, dass nur die Kategorien sichtbar sind, schalten Sie die Funktion ab.

Besuchen aktiviert Überwachung



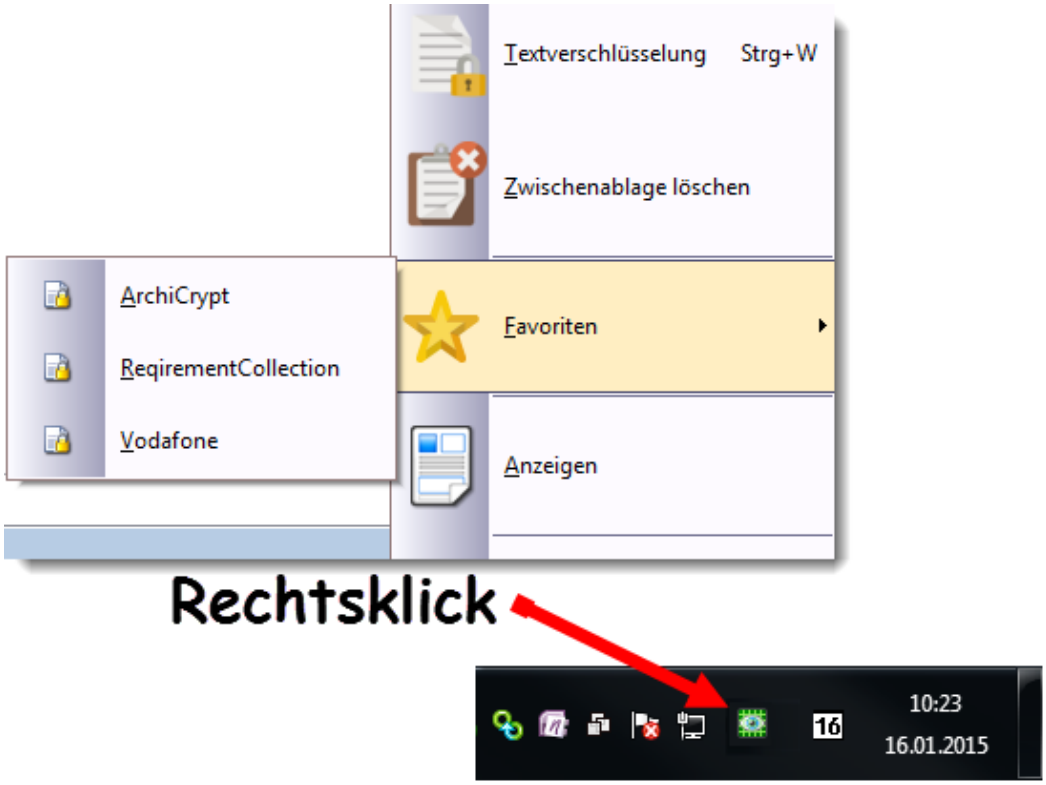
Wenn Sie im Safe die Schaltfläche **Besuchen...** anklicken, minimiert sich der Safe automatisch in den Infobereich und aktiviert die Überwachung[79] .

Auswahl Favoriten im Infobereich führt keine Aktion aus

Beim Klick auf den Favoriten wird der Eintrag im Safe ausgewählt. Gleichzeitig wird, falls angegeben die Internetseite besucht. Ist kein Eintrag zu Internetseite vorhanden, wird geprüft, ob eine E-Mail Adresse angegeben ist. Falls ja, wird eine leere Mail erstellt und die Textverschlüsselung aktiviert. Ist auch hier kein Eintrag vorhanden, wird eine eventuell angegebene Anwendung gestartet. Um dieses Verhalten zu unterbinden und nur den Eintrag im Safe auszuwählen, aktivieren Sie diese Option.

Kontextmenü-Systemtray

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Signal bei Überwachung

Wird zu der aktuellen Internetseite oder einem Anwendungsfenster ein Eintrag im Safe gefunden, wird eine Signal ausgegeben.
(siehe auch Überwachung[79])

Nachricht bei Überwachung

Wird zu der aktuellen Internetseite oder einem Anwendungsfenster ein Eintrag im Safe gefunden, wird eine kurze Nachricht angezeigt.
(siehe auch Überwachung[79])

Signale bei Textverschlüsselung

Falls Sie die Textverschlüsselung aktiviert haben, ertönt bei der Ver- und Entschlüsselung ein akustisches Signal.
(siehe auch Textverschlüsselung[81])

BACKUPS

Keine automatische Sicherung von Passwort Safes anlegen

Bei jedem erfolgreichen Öffnen wird eine Sicherungskopie Ihres Safes erstellt, auf den Sie im Falle einer Katastrophe zurückgreifen können. Die Sicherungen tragen die Dateiendung bacxml und liegen im gleichen Verzeichnis wie die Safedatei. Wird eine Safe Datei beschädigt, gehen Sie bitte in das

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Verzeichnis der Safe Datei. Suchen Sie dort die letzte Sicherung und ändern Sie die Dateiendung in acxml. Jetzt können Sie diese Datei mit Ihrem Passwort öffnen. Wenn Sie hier die Option deaktivieren, werden **KEINE automatischen Sicherungen** mehr erzeugt.

➡**WICHTIG: Die Funktion der automatischen Sicherung entbindet Sie nicht von der Pflicht, sich regelmäßig Sicherungen Ihrer wichtigen Daten, wozu sicher auch der Passwort Safe gehört, anzufertigen!**

Bei FTP grundsätzlich keine automatischen Backups erzeugen

Wenn Sie diese Funktion aktiviert haben, werden auf dem FTP Server keine automatischen Sicherungen angelegt. Vom Aktivieren dieser Option wird abgeraten, außer eine sehr geringe Bandbreite rechtfertigt dies. Sichern Sie sich unbedingt regelmäßig die Daten vom FTP Server lokal.

➡**WICHTIG: Die Funktion der automatischen Sicherung entbindet Sie nicht von der Pflicht, sich regelmäßig Sicherungen Ihrer wichtigen Daten, wozu sicher auch der Passwort Safe gehört, anzufertigen!**

Bei FTP geänderte Daten im Hintergrund übertragen

Ist diese Option aktiviert (*empfohlen*), nutzt ArchiCrypt Passwort Safe Phasen, in denen die Anwendung keine Aufgabe hat, zum Übertragen ggf. geänderter Daten. Ansonsten werden die Daten erst beim Schließen eines Passwort Safes oder beim Beenden von ArchiCrypt Passwort Safe übertragen.

➡**WICHTIG: Wenn Sie den Rechner herunterfahren und dabei der Passwort Safe beendet wird, kann es, wegen Überschreiten von Betriebssystem-eigenen Zeitlimits zu Problemen und Datenverlust kommen, sofern noch geänderte Safe Daten zu übertragen sind!!!!**

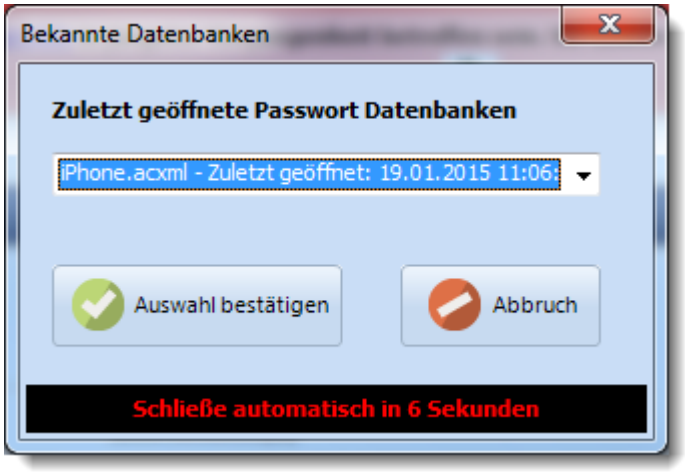
History

Beim Öffnen History als Auswahl anzeigen

Wenn Sie die Auswahl **Automatisch letzten Passwort Safe öffnen**[88] aktiviert haben, wird beim Start ein Auswahlfenster mit den zuletzt verwendeten Passwortdatenbanken angezeigt.

Vorausgewählt ist die letzte Datenbank. Wenn Sie innerhalb von 10 Sekunden keine abweichende Wahl treffen, schließt der Dialog sich automatisch mit dieser Wahl.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Es müssen mindestens zwei Datenbanken bekannt sein!

Mit **History löschen** können Sie die Liste gemerkter Passwortdatenbanken zurücksetzen.

TOP 86

Aussehen

Optik

Sie haben verschiedene Ansichten zur Auswahl. Gelegentlich müssen Sie die gewünschte Optik zwei Mal auswählen, damit die Ansicht aktualisiert wird.

Erweiterte Kurzhilfe anzeigen

Sofern Sie die Maus über eine der Schaltflächen in den Menüleisten bewegen, wird Ihnen eine etwas längere Information über die Funktion der Schaltfläche angezeigt. Sollten Sie keine Hilfe sehen, deaktivieren Sie bitte diese Option. Sie erhalten dann die Windows Standardhilfe.

Neustart des Passwort Safes nötig!

Anzeige der Kurzhilfe in Sekunden

Wenn Sie den Mauszeiger über eine Schaltfläche auf einer Menüleiste bewegen, wird Ihnen eine Kurzhilfe angezeigt. Hier können Sie festlegen, wie lange die Kurzhilfe angezeigt werden soll.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

TOP 86

Schutz

So stellen Sie sicher, dass sich der Safe schließt, wenn Sie Ihren Rechner verlassen

ArchiCrypt Passwort Safe bei Inaktivität schließen nach

Legen Sie fest, ob und nach wie vielen Minuten der Safe bei Nichtbenutzung automatisch geschlossen werden soll. Die Funktion ist sehr nützlich, wenn Sie Ihren Rechner verlassen und vergessen, Ihren Safe zu schließen.

So stellen Sie sicher, dass immer in folgendem Verzeichnis nach einer Schlüsseldatei gesucht wird

Schlüsseldatei immer suchen unter

Legen Sie hier den Pfad zur Schlüsseldatei fest. Es kann sich auch um einen Laufwerksbuchstaben für einen USB Stick handeln.

Wo möglich, Virtuelle Tastatur zur Eingabe von Passwörtern nutzen

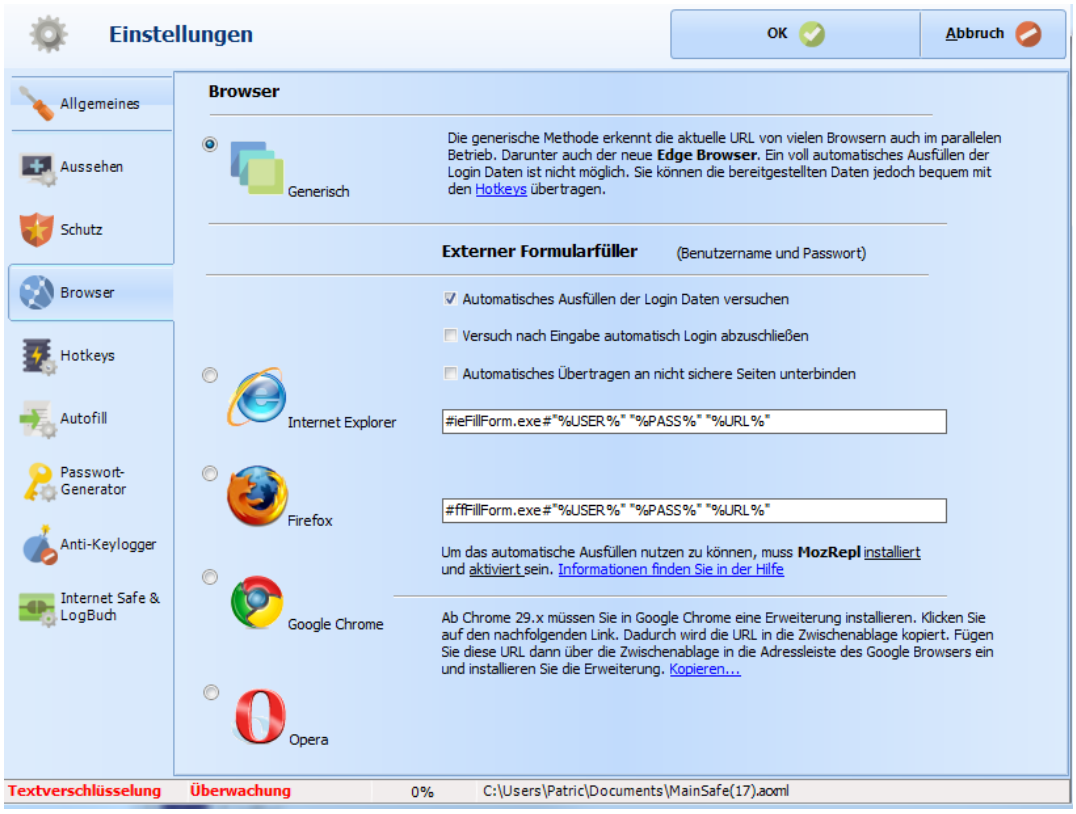
Ist ein Passwort einzugeben, wird, sofern möglich, die virtuelle Tastatur angezeigt.

TOP 86

Browser

ArchiCrypt Passwort Safe unterstützt den Internet Explorer, Firefox, Google Chrome. Aktivieren Sie den Browser, mit dem Sie arbeiten möchten.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



➡**HINWEIS: Was funktioniert mit welchem Browser?**

Der **generische Modus** erkennt bei vielen Browsern die besuchte Adresse und stellt dann die passenden Daten im Safe bereit. Hierbei wird auch der **Edge Browser** unterstützt. Im generischen Modus werden die Passwortdaten nicht automatisch in die WEB-Seite übertragen. Stattdessen wird der passende Eintrag bereitgestellt, Sie werden in einem kleinen Infofenster darüber benachrichtigt und können dann per Hotkey die Daten halbautomatisch in die Eingabefeder übertragen. Ein weiterer Vorteil der generischen Methode ist, dass Sie mit mehreren Browsern parallel arbeiten können.

➡**WICHTIG: Unter Windows XP und Vista müssen Sie unbedingt das Update KB971513 einspielen. Das Update finden Sie auf den Microsoft Seiten.**

Anm.: Auch der Safari Browser wird unterstützt. Hier muss sich aber der Eingabecursor bzw. Eingabefocus in der Adressleiste des Browsers befinden. Ansonten wird die Internetadresse nicht erkannt.

Featurematrix Browser

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Browser / Feature	Automatisches Erkennen der Internetseite	Übertragen von Daten per Hotkey	Automatisches Übertragen von Login Daten	Ausfüllen von Formularen
Internet Explorer	**X**	**X**	**X**	**X**
Firefox	**X**	**X**	**(X) vorausgesetzt, MozRepl Installation**	**0**
Google Chrome	**(X)** ab Chrome 29.X muss die Erweiterung URL in Title installiert sein.	**X**	**0**	**0**
Opera	**(X) abhängig von Version**	**X**	**0**	**0**

Entsprechend bieten nur **Internet Explorer** und **Firefox** einen externen **Formularfüller** für Benutzername und Passwort.

WICHTIG bei Google Chrome
Google Chrome lässt das Erkennen der aktuellen URL durch andere Programme nicht direkt zu. Daher müssen Sie zwingend die Erweiterung **URL in Title** installieren und aktivieren.
Starten Sie Google Chrome und rufen Sie dort die URL
https://chrome.google.com/webstore/detail/url-in-title/ignpacbgnbnkaiooknalneoeladjnfgb
auf. Installieren Sie die Erweiterung. Starten Sie Google Chrome neu.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Damit die Login Daten automatisch an den ausgewählten Browser übertragen werden, aktivieren Sie bitte die Funktion "**Automatisches Ausfüllen der Login Daten versuchen**".
Wenn Sie jetzt eine Internetseite besuchen, die mit einem Eintrag im Passwort Safe verknüpft ist, werden der Benutzername und das Passwort automatisch in die Formularfelder übertragen. Um sich einzuloggen, müssen Sie ggf. noch eine Schaltfläche anklicken oder die Eingabetaste betätigen.

Wenn Sie möchten, dass ArchiCrypt Passwort Safe den Login Vorgang für Sie abschließt, aktivieren Sie zusätzliche die Funktion "**Versuch nach Eingabe automatisch Login abzuschließen**".
Bitte lesen Sie sich unbedingt die Hinweise durch, da es im Zusammenhang mit dieser Funktion zu Problemen kommen kann.

Wenn Sie eine Seite besuchen und die CTRL-Taste gedrückt halten, werden keine Daten automatisch übertragen, wohl aber im Passwort Safe ausgewählt. Sie können die Daten damit immer noch per Hotkey übertragen.

➡**HINWEIS: In weit mehr als 95% aller Fälle arbeitet die Funktion zum automatischen Übertragen der Daten ganz ohne Probleme. Auf einigen Seiten, die den Login Dialog mit speziellen Plugins (*z.B. Flash-Plugin*) realisieren, funktioniert das automatische Übertragen nicht. Das Übertragen mit Hotkey funktioniert hingegen nahezu immer.**

➡**HINWEIS: Bei aktivierter Funktion "Versuch nach Eingabe automatisch Login abzuschließen" kann es zu Problemen kommen, wenn Sie beim Abmelden automatisch wieder auf die Seite zum Anmelden geleitet werden. ArchiCrypt Passwort Safe wird Sie immer wieder automatisch anmelden, da er nicht weiß, ob Sie sich gerade abgemeldet haben, oder neu anmelden wollen. Sie landen also in einer Endlosschleife.**

Sie können diese Endlosschleife unterbrechen, indem Sie beim Ausloggen die CTRL-Taste gedrückt halten.

➡**HINWEIS: Die Übertragung von Daten an eine WEB-Seite erfolgt immer dann, wenn diese zum Eintrag bei Internet in einem Passwort Eintrag passt. Seien Sie daher vorsichtig mit der Verwendung von Platzhaltern. Haben Sie dort zum Beispiel einen Eintrag wie**

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

https://www.postbank.de/* wird allen Seiten, die zu dieser Domain gehören auch die Kombination aus Benutzername und Passwort gesandt. Dies kann dazu führen, dass nicht nur Daten in die Felder der Login Seite, sondern auch in andere Formulare geschrieben werden. Seien Sie also bei der Angabe der WEB-Seiten Adresse so präzise wie möglich! Besser wäre https://banking.postbank.de/rai/login da dann die Daten korrekt ausschließlich an die Login Seite gesendet werden.

Seiten, mit denen man sich an einem Dienst anmeldet (*Online-Shop bei Angabe von persönlichen Daten, Online-Banking, WEB E-Mail,...*) sollten grundsätzlich als Protokoll das sichere https verwenden. Ihre Daten werden dabei abhörsicher verschlüsselt übertragen. ArchiCrypt Passwort Safe verhindert bei aktivierter Funktion **"Automatisches Übertragen an nicht sichere Seiten unterbinden**" dass Login Daten an unsichere Seiten übertragen werden.

MozRepl Installation für Firefox

MozRepl ist ein Add On für Firefox welches anderen Anwendungen ermöglicht, auf die Inhalte von Internetseiten zuzugreifen, die in Firefox angezeigt werden. ArchiCrypt Passwort Safe nutzt diese Möglichkeit, um Login Daten beim Besuch automatisch in die Seite zu schreiben, sofern Sie die Option aktiviert haben.

➡Anm.: Die Frequenz mit der das Firefox Entwicklerteam neue Hauptversionen veröffentlicht, macht es den Anbietern von Erweiterungen extrem schwer. Alle 6 Wochen müssen mehr oder weniger große Anpassungen erfolgen, damit die Erweiterung im aktuellen Firefox funktioniert. Zum Zeitpunkt der Veröffentlichung von ArchiCrypt Passwort Safe wurde Firefox 35 veröffentlicht.

Bitte **prüfen** Sie zunächst auf der offiziellen Seite, ob es eine für Ihre **Firefox Version** geeignete Version gibt.

https://addons.mozilla.org/en-US/firefox/addon/mozrepl/

Klicken Sie auf dieser Seite den Button Add to Firefox und folgen Sie den Anweisungen um MozRepl zu installieren. Bitte beachten Sie Punkt 6 der

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

nachfolgenden Anweisungen zur Installation unserer Version, da die Einstellung generell nötig ist.

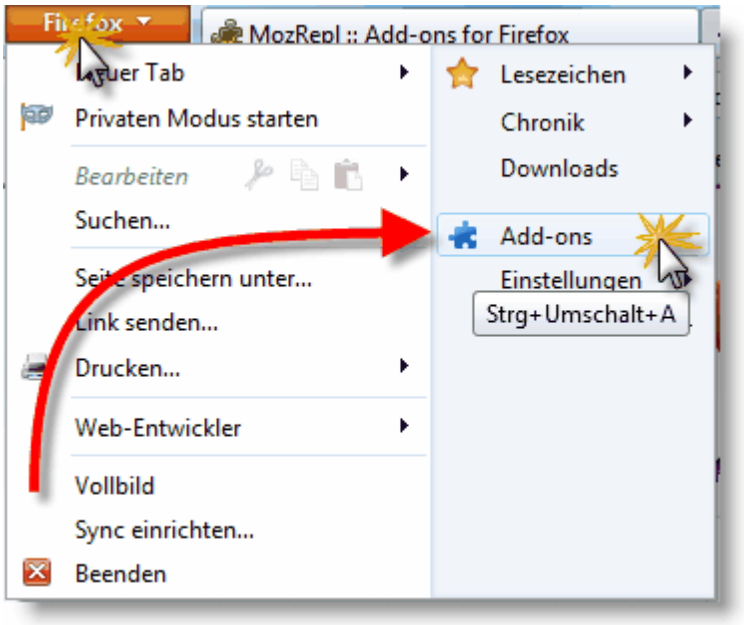
Den Quellcode und Entwicklerinformationen finden Sie hier:

https://github.com/bard/mozrepl/wiki

Falls es KEINE offizielle Version für Ihre Firefox Version gibt und NUR dann, laden Sie die Version von unserer Internetseite:

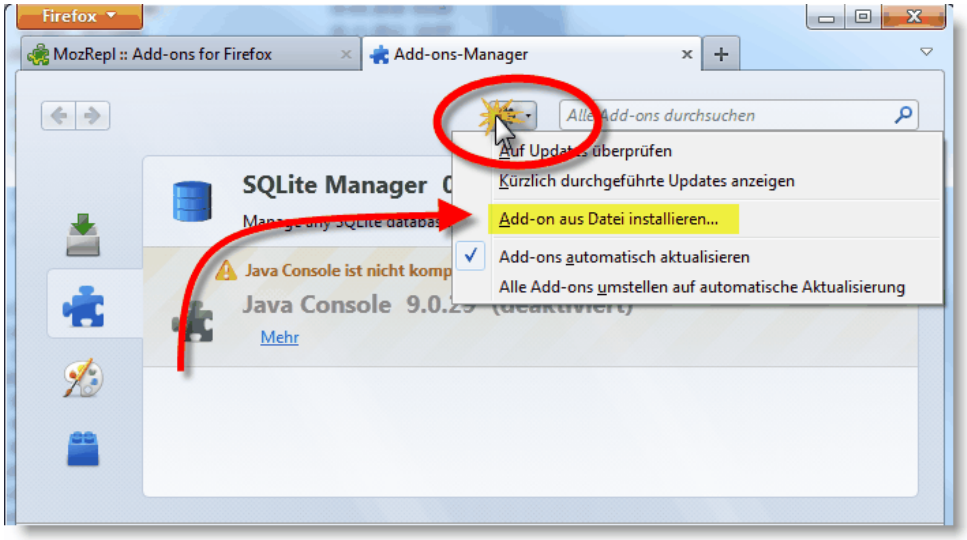
http://load.archicrypt.de/mozRepl_FF8.xpi

1 So installieren Sie unsere Version für Firefox 8+. Starten Sie Firefox 8 + und rufen Sie den Punkt **Add-ons** auf

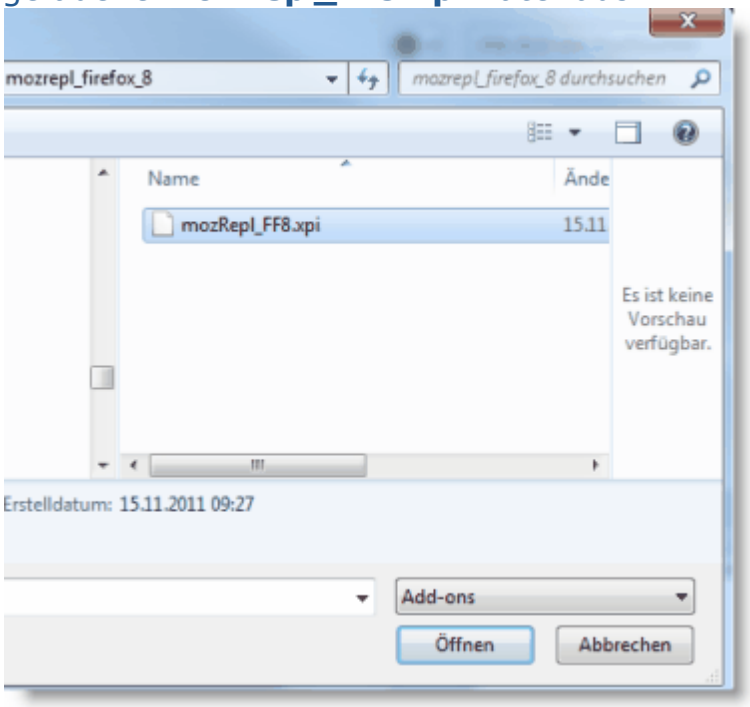


2 Rufen Sie im **Add-ons Manager** den Punkt **Add-ons aus Datei installieren** aus.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

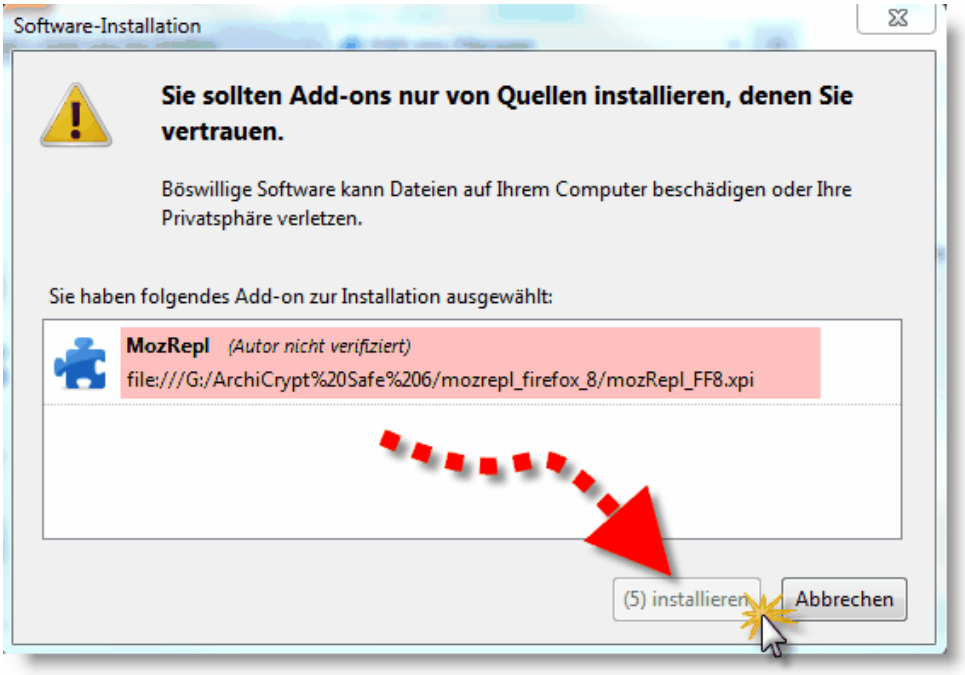


3 Wählen Sie im Windows Dialog die soeben von unserer Seite geladene **mozRepl_FF8.xpi** Datei aus.

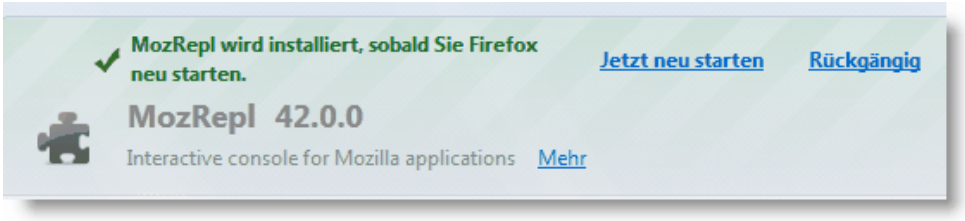


4 Klicken Sie im Dialog von Firefox auf **installieren**.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

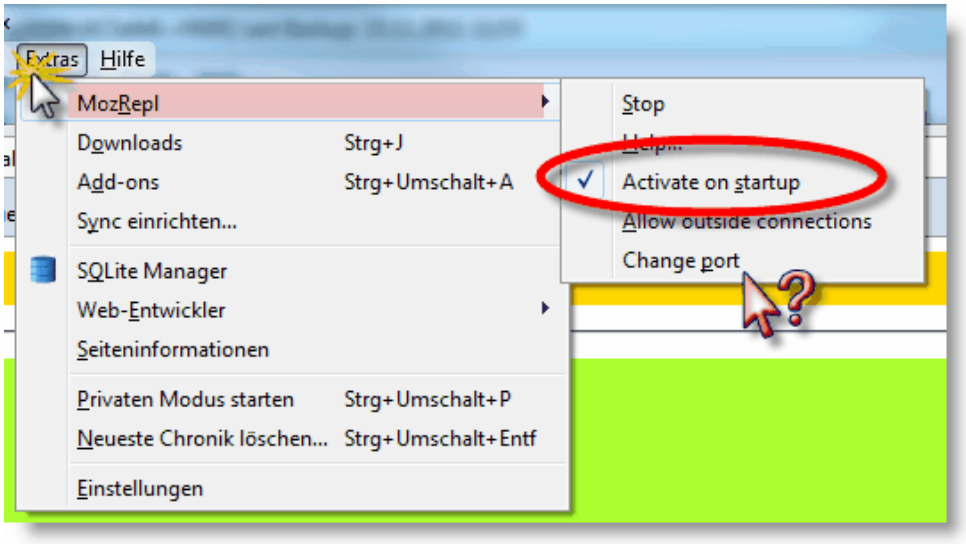


5 **Starten Sie Firefox** neu, um die Installation abzuschließen.



6 Wenn Sie Firefox neu gestartet haben, dann stellen Sie bitte sicher, dass MozRepl so eingerichtet ist, dass es beim Start von Firefox aktiviert wird.
Dazu im Menü von Firefox auf **Extras - MozRepl** und dort **Activate on startup** aktivieren. Bitte prüfen, ob bei **Change port** der Wert **4242** eingestellt ist.
Nur dann kann sich ArchiCrypt Passwort Safe lokal mit Firefox verbinden.

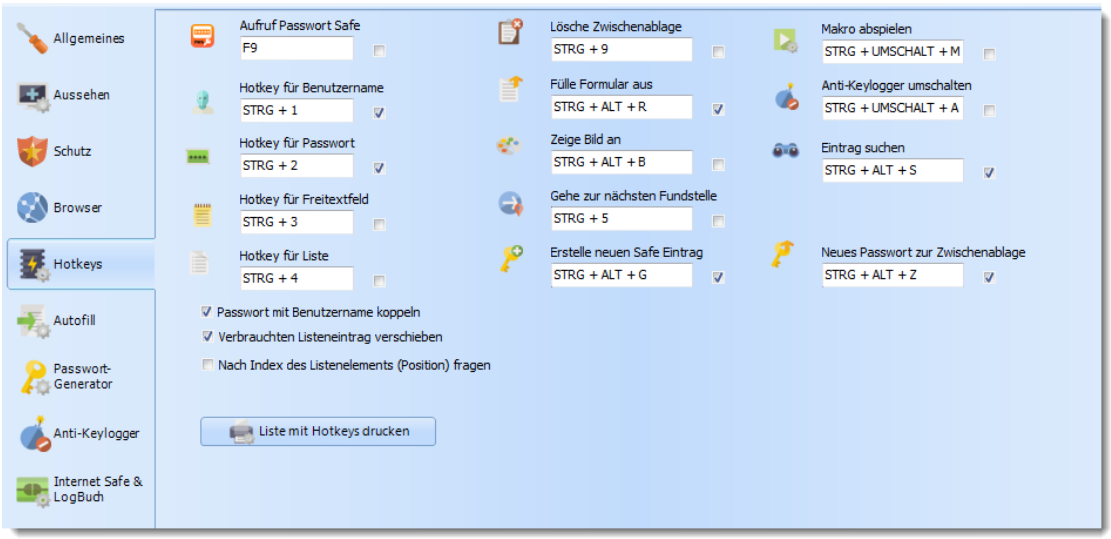
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



TOP 86

Hotkeys - Tastaturkürzel

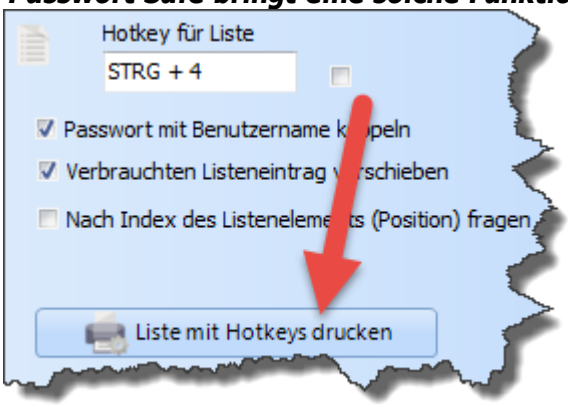
Hier legen Sie Tastaturkürzel fest, mit denen Sie einfach aus jeder beliebigen Anwendung heraus Funktionen oder Inhalte aus Ihrem Safe abrufen können.



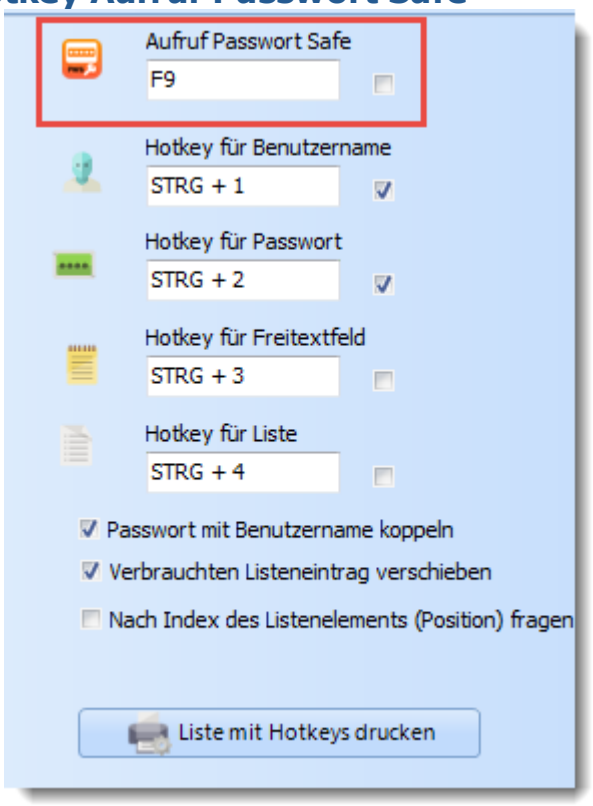
In den Beispielen werden die Tastaturkürzel verwendet, die ArchiCrypt Passwort Safe vorgibt. Falls Sie diese Werte geändert haben, nutzen Sie entsprechend Ihre Hotkeys.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

TIPP: ***Drucken Sie sich die Liste der Hotkeys einfach aus! Der Passwort Safe bringt eine solche Funktion mit.***



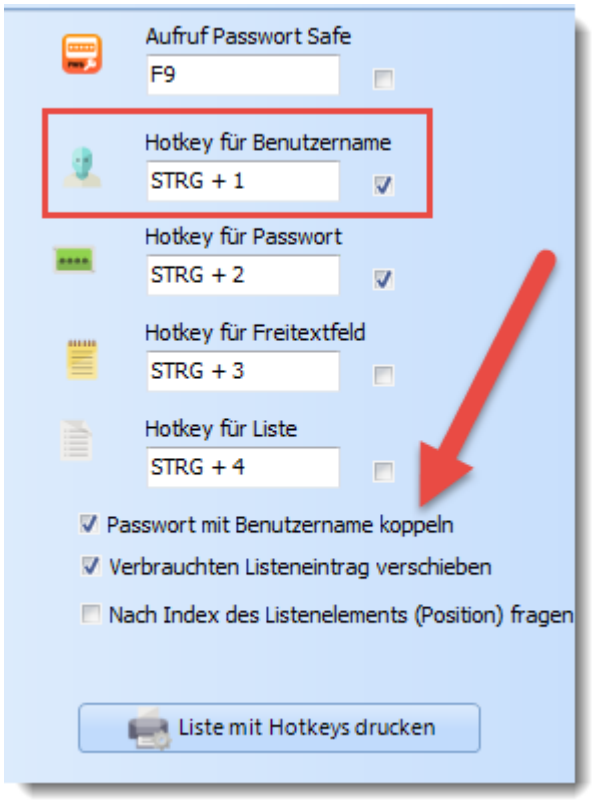
Hotkey Aufruf Passwort Safe



Hier können Sie eine Taste / Tastenkombination festlegen, mit der Sie den Safe schnell aktivieren oder deaktivieren können. Im obigen Beispiel ist die Taste F9 vorgesehen.

Hotkey für Benutzername

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



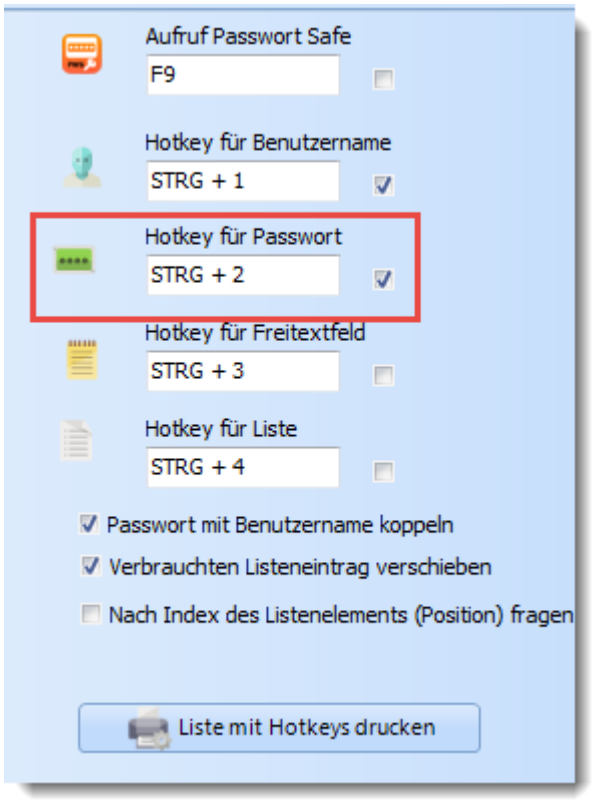
Bei Betätigen der Tastenkombination wird der Text aus dem Feld Benutzername in das aktuelle Eingabefeld eingetragen. Lösen Sie sich unbedingt von den Bezeichnungen der Felder. Sie sind nur Beispielhaft. Dem Passwort Safe ist es völlig gleichgültig, ob in dem Feld eine Kontonummer, eine Bankleitzahl, ein Name oder etwa eine Mail Adresse abgelegt ist. In diesem Zusammenhang ist die Option "**Passwort mit Benutzername koppeln**[107] " sehr nützlich. Sie sorgt dafür, dass nach dem Übertragen des Benutzernamens automatisch in das nächste Eingabefeld das Passwort übertragen wird.

So übertragen Sie die Daten per Tastenkombination in Ihren Browser

Schalten Sie die Überwachung[79] ein und besuchen Sie die gewünschte Internetseite. ArchiCrypt Passwort Safe meldet jetzt, dass er die Daten für eine bestimmte Internetseite bereit gestellt hat. Setzen Sie jetzt den Cursor in das erste Feld im Browser und betätigen Sie dann das Tastenkürzel (**z.B. Strg + 1**). Der Safe überträgt daraufhin den Wert, den Sie in das Feld Benutzername eingetragen haben.

Hotkey für Passwort / Schlüssel

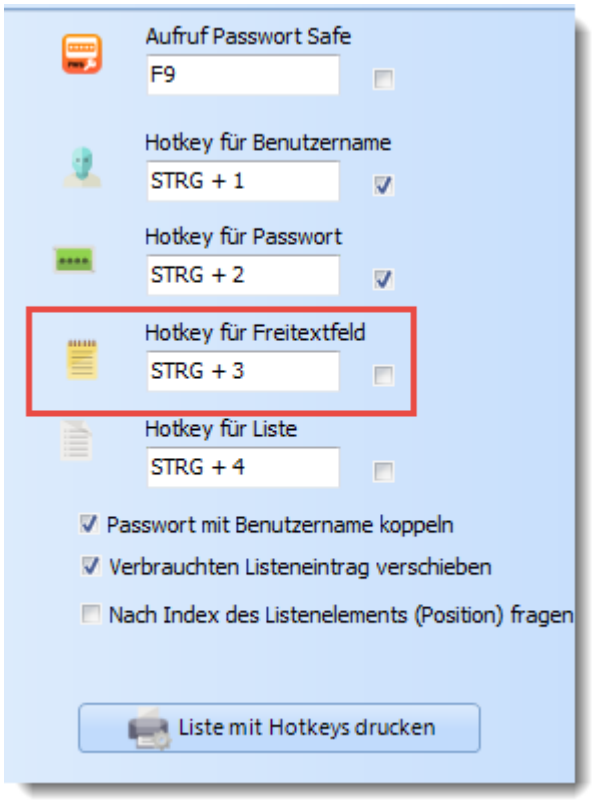
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Bei Betätigen der Tastenkombination wird das Passwort in das aktuelle Eingabefeld eingetragen.

Hotkey für Freitextfeld

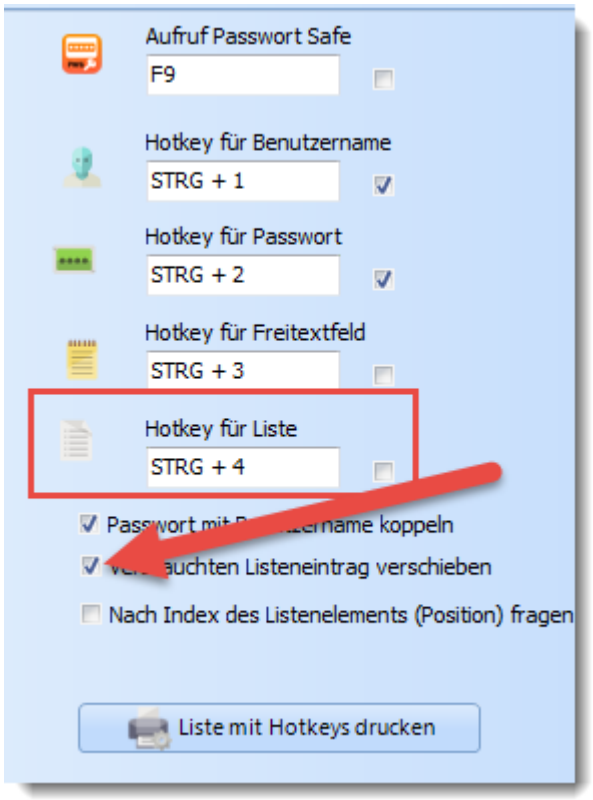
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Bei Betätigen der Tastenkombination wird der Text aus dem Freitextfeld in das aktuelle Eingabefeld eingetragen.

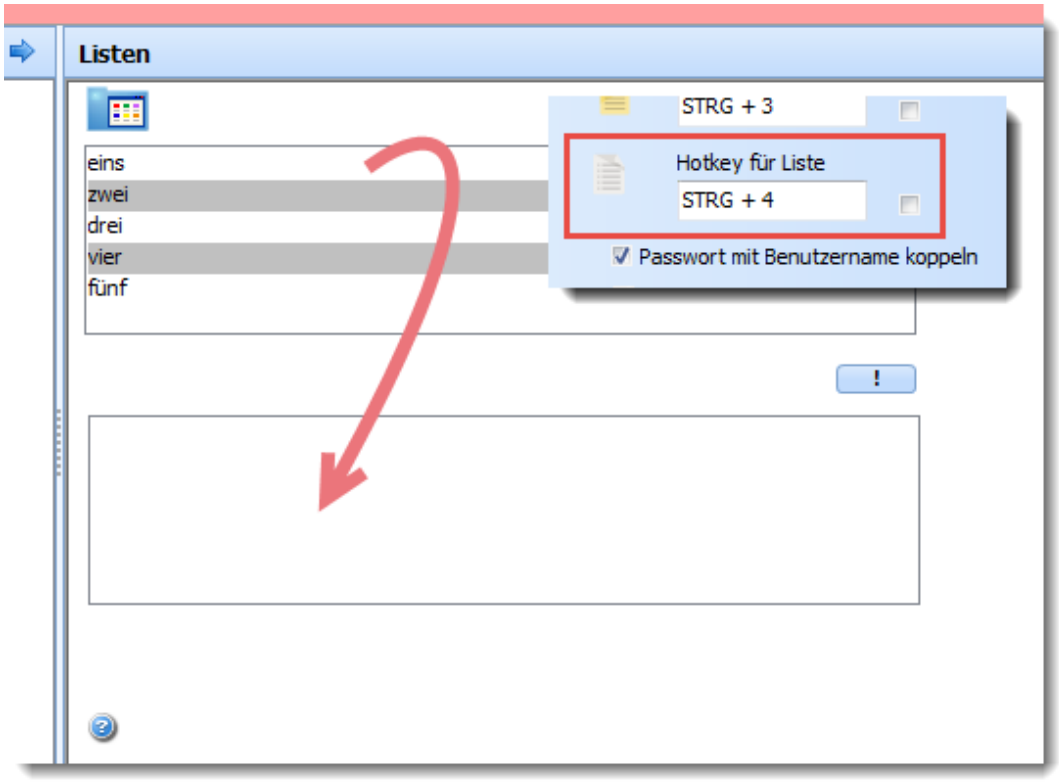
Hotkey für Liste

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

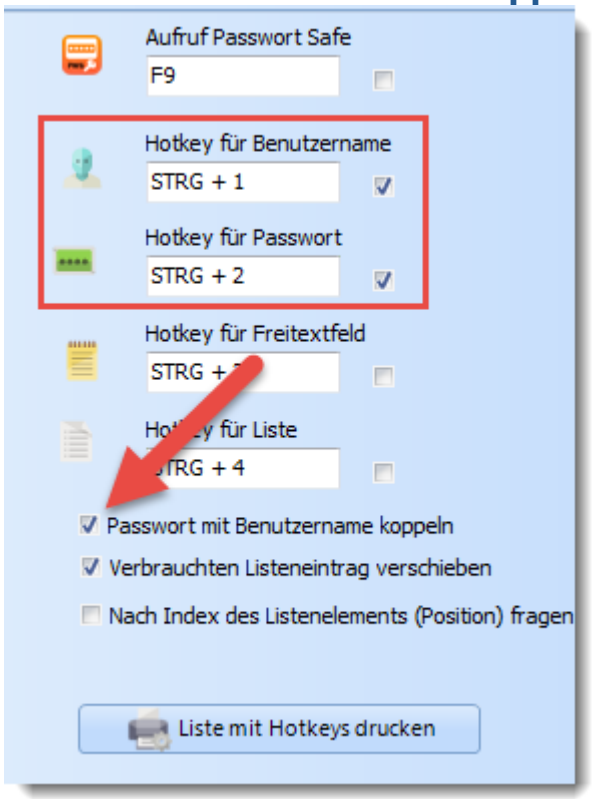


Bei Betätigen der Tastenkombination wird der erste Listeneintrag der oberen Liste in das aktuelle Eingabefeld eingetragen.
Falls Sie die Auswahl **Verbrauchten Listeneintrag verschieben** ausgewählt haben, wird dieser Wert anschließend von der oberen Liste in die untere verschoben (nicht gelöscht). Wenn Sie jetzt erneut die Tastenkombination betätigen, steht Ihnen der nächste Eintrag aus der oberen Liste zur Verfügung. Dies können Sie so lange fortführen, bis die obere Liste keine Einträge mehr enthält. Voraussetzung ist, dass die Option **Nach Index des Listenelements (Position) fragen** nicht aktiv ist.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



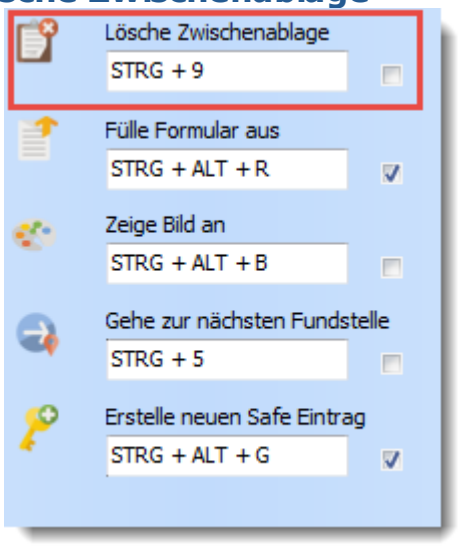
Passwort mit Benutzername koppeln



© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

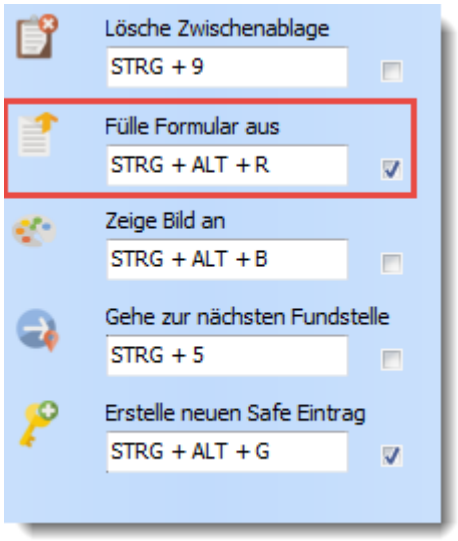
Bei aktivierter Option wird beim Betätigen des Hotkeys für den Benutzernamen automatisch mit der Tabulatortaste in das nächste Eingabefeld gesprungen. In dieses Feld wird dann das Passwort eingetragen.

Lösche Zwischenablage



Text der sich in der Zwischenablage befindet, wird gelöscht.

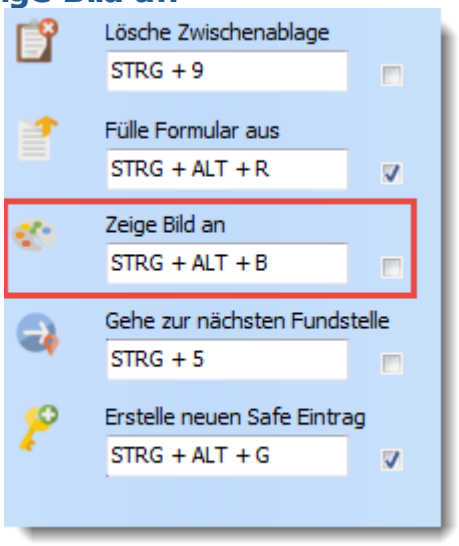
Fülle Formular aus



Dieser Hotkey ist nur im Zusammenhang mit der Überwachung[79] sinnvoll einsetzbar und funktioniert nur dann, wenn Sie den **Internet Explorer** besitzen. Wenn Sie ein Formular einer bestimmten Seite beim Erstellen eines Passworteintrags aufgenommen haben, können Sie mit diesem Hotkey die Textfelder automatisch ausfüllen lassen. (siehe auch Überwachung[79] und Featurematrix Browser[93]).

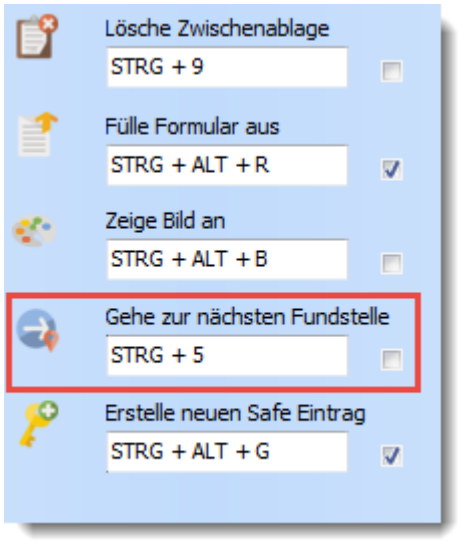
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Zeige Bild an



Falls Sie einem Safe Eintrag eine Grafik zugeordnet haben, können Sie sich diese Grafik mit Hilfe dieser Tastenkombination anzeigen lassen.

Gehe zur nächsten Fundstelle



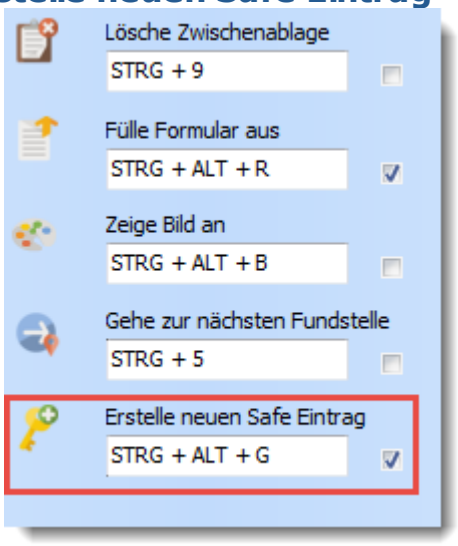
Dieser Hotkey ist nur im Zusammenhang mit der Überwachung[79] sinnvoll einsetzbar. Es ist durchaus möglich, dass einer bestimmten Internetseite mehrere Safe Einträge zugeordnet sind. Zum Beispiel dann, wenn Sie mehrere Accounts besitzen oder, wenn Sie bei einer Bank mehrere Konten haben. Die Überwachung sucht immer den ersten passenden Eintrag aus der Passwortdatenbank. Um den nächsten Eintrag aus dem Safe auszuwählen, betätigen Sie bitte die Tastenkombination. ArchiCrypt Safe wechselt dann zur nächsten Fundstelle. (siehe auch Überwachung[79])

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

➡ACHTUNG: Wenn Sie die Funktionen zur automatischen Übertragung der Login Daten aktiviert haben, wird IMMER der erste passende Eintrag in der Datenbank genutzt.

So erstellen Sie sich ein sicheres Passwort für eine Internetseite

Erstelle neuen Safe Eintrag

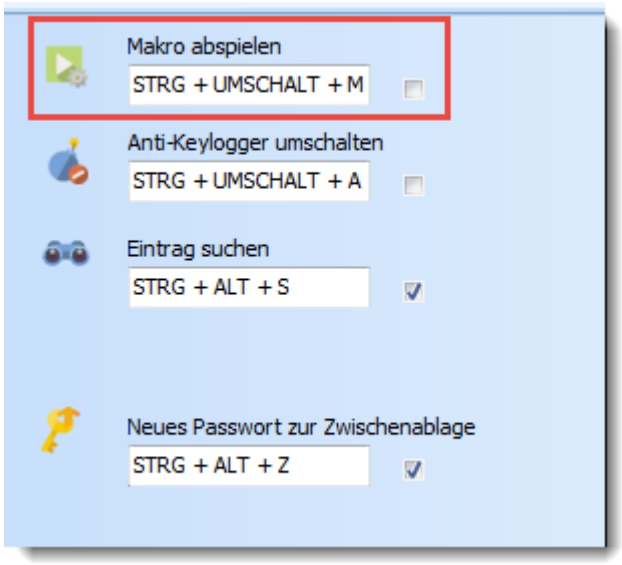


Oft surft man im Internet und muss sich plötzlich registrieren. Die üblichen Informationen müssen festgelegt werden, darunter zumeist ein Passwort. Der Passwort Safe hat einen integrierten Passwortgenerator[114], den Sie an Ihre Bedürfnisse anpassen können. Zudem möchten Sie den Zugang zu der Seite sicher sofort in den Passwort Safe übertragen.

Rufen Sie den Passwort Safe mit dem Tastaturkürzel (**Voreinstellung** STRG+G) auf geben Sie gewünschte Werte ein, lassen Sie sich ein Passwort generieren und übernehmen Sie die Adresse der Internetseite.

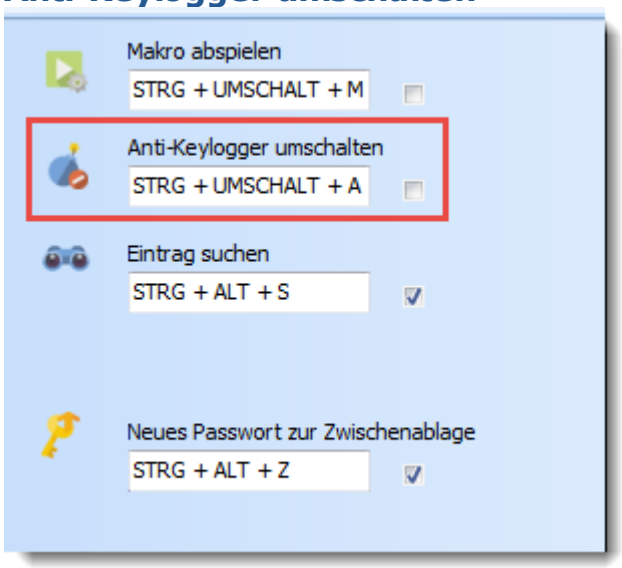
Makro abspielen

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Sie können einem Passworteintrag ein Makro zuordnen[23], welches Sie mit dem integrierten Makrorekorder aufgezeichnet haben. Sobald Sie den Hotkey betätigen, wird das Makro abgespielt.

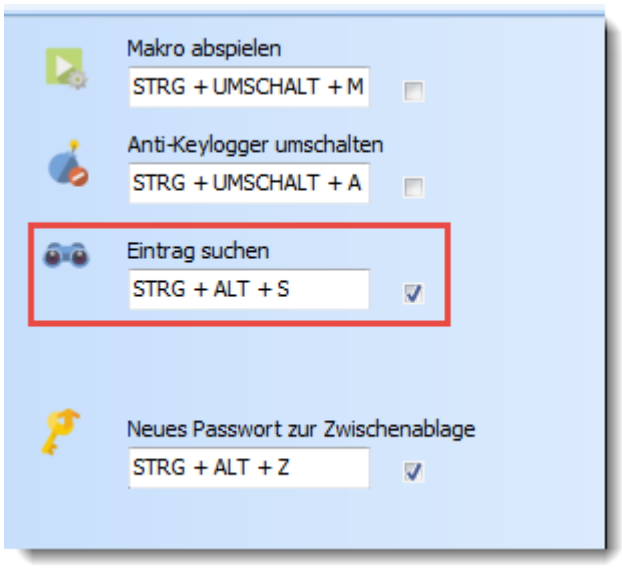
Anti-Keylogger umschalten



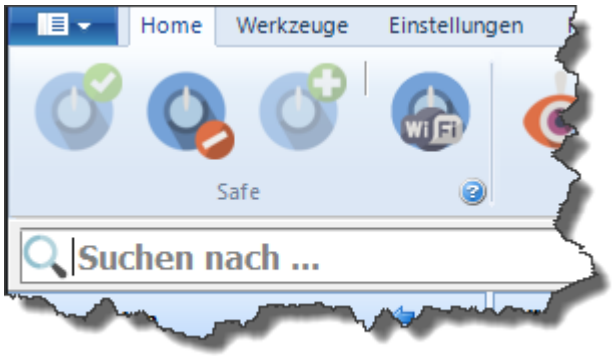
Schalten Sie mit diesem Hotkey die Anti-Keylogger Funktion an oder aus.

Eintrag suchen

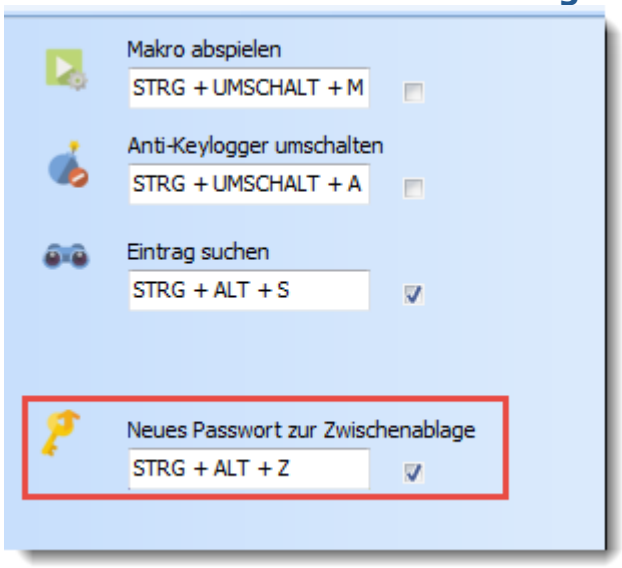
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Wenn der Passwort Safe in den Infobereich minimiert ist, können Sie ihn in den Vordergrund holen und direkt im Suchen Feld nach einem bestimmten Eintrag suchen.



Neues Passwort zur Zwischenablage



© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Sie können sich ein Passwort erzeugen und in die Zwischenablage kopieren lassen. Nach dem Betätigen des Hotkeys können Sie dann das so erzeugte Passwort über die Zwischenablage (*zum Beispiel über* **Strg+V**) einfügen.

➡HINWEIS: Das Passwort wird nicht im Passwort Safe gespeichert. Sie müssen es also manuell sichern!

Siehe auch **Erstelle neuen Safe Eintrag**[110]

TOP[86]

Autofill

Wenn Sie beim Surfen auf eine Seite gelangen, auf der Sie bestimmte Angaben machen müssen, können Sie versuchen, die Werte mit der Autofill Funktion automatisch in das Formular zu übertragen. Die Funktion macht es sich zu Nutze, dass sehr häufig die gleichen Angaben gefordert werden und die Benennung der Eingabefelder auf vielen Seiten identisch sind.

Diese Werte werden **UNVERSCHLÜSSELT** in einer kleinen TEXTDATEI gespeichert und sind **NICHT abgesichert**. Auf die hier gemachten Angaben können Sie sich in jedem Passworteintrag beziehen. Änderungen an dieser Stelle wirken sich dann auf alle Passworteinträge aus, die diese Werte referenzieren. (siehe auch Safeeintrag erstellen[8])

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Anm.: UID = Umsatzsteuer ID

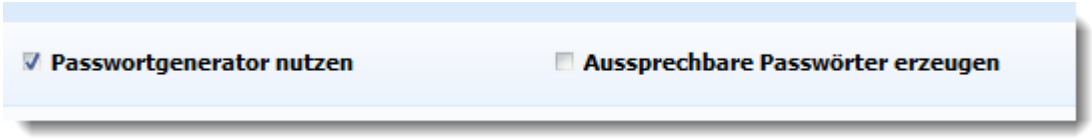
Wenn Sie auf eine Seite gelangen, auf der sich ein Formular befindet, betätigen Sie den Hotkey zu **Fülle Formular aus (Voreingestellt STRG + R).** Gibt es einen Eintrag im Passwort Safe, der individuelle Daten für dieses Formular gespeichert hat, werden diese Daten genutzt, wird nichts gefunden, greift ArchiCrypt Passwort Safe auf die bei **Autofill** abgelegten Daten zurück.

TOP 86

Passwortgenerator

ArchiCrypt Passwort Safe sammelt vom Start ab **Zufallsdaten**, die bei der Erzeugung von Passwörtern genutzt werden. Den Passwortgenerator sollten Sie nur im Ausnahmefall bei Problemen deaktivieren. Nutzen Sie den Passwortgenerator um sichere Passwörter zu erzeugen.

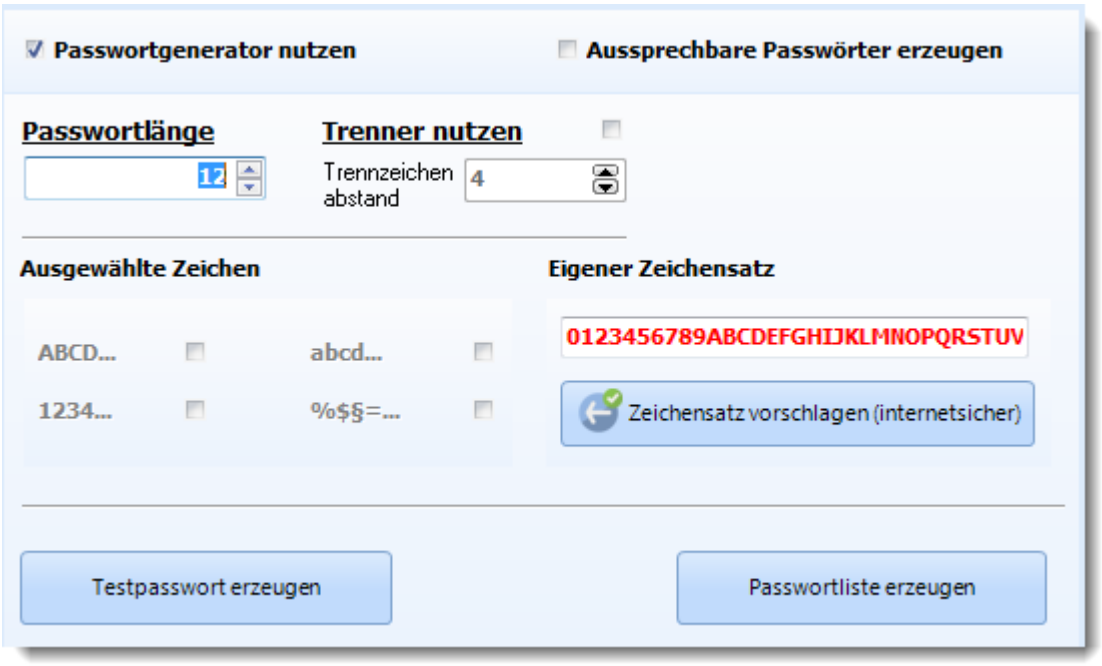
Sie haben zwei verschiedene Varianten zur Auswahl.



Den klassischen Passwortgenerator 114 (*Passwortgenerator nutzen*), der aus vorgegebenem Zeichenvorrat völlig zufällige und beliebige Passwörter erzeugt und den neuen Passwortgenerator (*aussprechbare Passwörter erzeugen*).

Der klassische Passwortgenerator

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Unter Ausgewählte Zeichen legen Sie fest, welche Zeichen beim Aufbau eines Passwortes zum Einsatz kommen sollen. Grundsätzlich können Sie alle Zeichen aktivieren. Aber Vorsicht! Häufig werden Passwörter mit bestimmten Sonderzeichen nicht anerkannt oder führen zu Fehlern in der Anwendung. Auch kann die Lesbarkeit eines Passwortes stark leiden, wenn Sie alle Zeichen zulassen. Falls Sie die Anzahl an Zeichen einschränken und zum Beispiel einen **eigenen Zeichensatz** verwenden, sollten Sie die Länge des Passwortes erhöhen. Es spricht nichts gegen eine Länge von **16 Zeichen oder mehr**, Sie müssen sich das Passwort ja nicht mehr selbst merken.

Passwortlänge
Wie lange soll das generierte Passwort sein?

Trenner nutzen
Zur übersichtlicheren Aufbereitung eines Passwortes, kann man ein Trennzeichen - einfügen.
Trennzeichen zählen nicht zur Passwortlänge!!

Testpasswort erzeugen
Ein Beispielpasswort gemäß Ihren Vorgaben wird generiert

Passwortliste erzeugen
Sie können sich hier eine Liste mit Passwörtern gemäß Ihren Vorgaben erzeugen lassen. Dabei werden nur solche Passwörter in die Liste übernommen, die gegen Wörterbuchattacken immun sind. Nach Betätigen der Schaltfläche werden Sie zunächst nach der

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

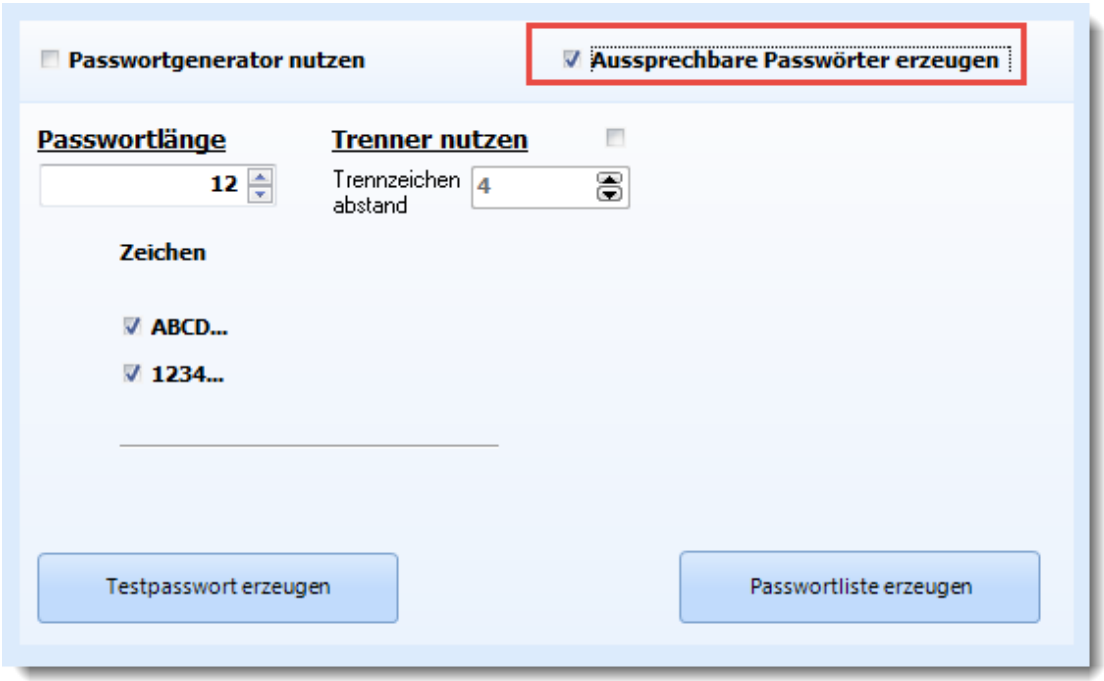
Anzahl zu erzeugender Passwörter gefragt. Nachdem die Liste erstellt wurde, werden Sie nach einem Speicherort gefragt. Die Liste wird als Textdatei gespeichert, die Sie weiter verarbeiten können.

Eigener Zeichensatz
Sobald Sie hier Zeichen eingeben, werden diese genutzt um Passwörter zu erzeugen. Andere Auswahlmöglichkeiten werden jetzt ausgegraut. Sollen wieder Passwörter erzeugt werden, die aus den von Ihnen aktivierten Zeichen gebildet werden, leeren Sie das Eingabefeld "Eigener Zeichensatz" wieder.

Zeichensatz vorschlagen (internetsicher)
Bestimmte Zeichen, die maximale Kompatibilität (*es treten keine Probleme auf*) mit den Anforderungen an Passwörter im Internet bieten.

Erzeugen aussprechbarer Passwörter

Die Idee für diesen Passwortgenerator lieferte (*FIPS PUB 181; Federal Information Processing Standards Publication 181*). In diesem Dokument wird ein Verfahren beschrieben, mit dem man zufällige Passwörter aus Silben erzeugen kann. Passwörter, die man auf diese Art erzeugt, haben den Vorteil, dass sie aussprechbar sind und man sie sich recht einfach merken kann.



Passwortlänge
Wie lange soll das generierte Passwort sein?

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Trenner nutzen
Zur übersichtlicheren Aufbereitung eines Passwortes, kann man ein Trennzeichen - einfügen.
Trennzeichen zählen nicht zur Passwortlänge!!

Testpasswort erzeugen
Ein Beispielpasswort gemäß Ihren Vorgaben wird generiert

Passwortliste erzeugen
Sie können sich hier ein Liste mit Passwörtern gemäß Ihren Vorgaben erzeugen lassen. Dabei werden nur solche Passwörter in die Liste übernommen, die gegen Wörterbuchattacken immun sind. Nach betätigen der Schaltfläche werden Sie zunächst nach der Anzahl zu erzeugender Passwörter gefragt. Nachdem die Liste erstellt wurde werden Sie nach einem Speicherort gefragt. Die Liste wird als Textdatei gespeichert.

Zeichen
Wenn Sie ABCD... aktivieren, wird das erzeugte Passwort auch Großbuchstaben enthalten. Sofern Sie 1234... aktivieren, werden an den Anfang bzw. an das Ende des Passwortes zufällige Ziffern gesetzt.

TIPP: Setzen Sie die Passwortlänge um 2 höher als im klassischen Passwortgenerator (empfohlen 16+) und verzichten Sie ggf. auf Ziffern (Länge um 4 höher). Die Sicherheit des Passwortes ist dadurch annähernd gleich, die Merkbarkeit steigt jedoch.

TOP 86

Anti-Keylogger

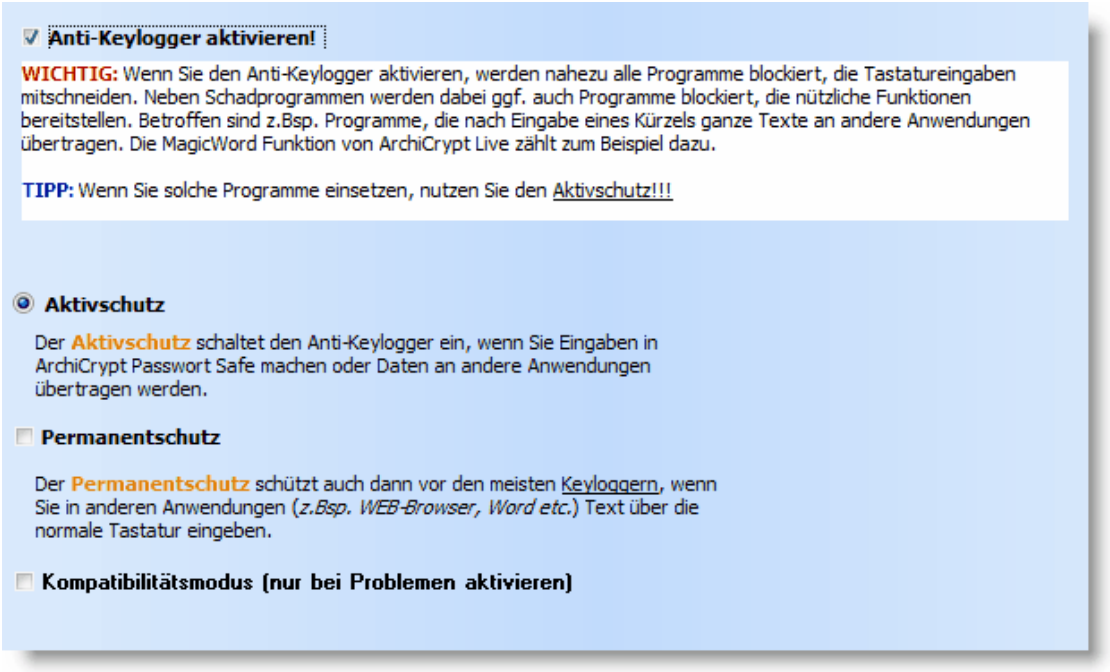
➡WICHTIG: Diese Funktion ist unter Windows 10 nicht verfügbar.

Die Anti-Keylogger Funktion schützt Sie vor Programmen, die Ihre Tastatur- und Mauseingaben aufzeichnen und anschließend versenden. Man unterscheidet hierbei im Wesentlichen 2 Kategorien.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Hinweise zur Sicherheit:
Es gibt Key-Logger, die sich in den Tiefen des Systems verstecken und mit Hilfe eines s.g. Kerneltreibers Ihre Eingaben mitschneiden. Diese Schadprogramme sind kompliziert zu erstellen, oft ungenau im Mitschnitt und sie benötigen zwingend Administratorrechte um Schaden anzurichten. Diese Art von Keyloggern ist weniger verbreitet. Gegen sie hilft die Anti-Keylogger Funktion von ArchiCrypt Passwort Safe NICHT. Sie können Ihre Eingaben jedoch über die virtuelle Tastatur[31] eingeben und so Keylogger generell unterlaufen.

Daneben gibt es Key-Logger, die man sich auch beim "normalen" Besuch von Internetseiten "einfangen" kann. Es handelt sich um geschickt programmierte Anwendungen, die keine besonderen Rechte benötigen, um Sie auszuspionieren. Gegen diese weit verbreitete Art von Schädlingen schützt die Anti-Keylogger Funktion.



Der **Aktivschutz** verhindert das Ausspionieren während Sie Daten in den Passwort Safe einfügen. **Andere Anwendungen** werden also **nicht mit geschützt**.

Der **Permanentschutz** schützt auch dann, wenn Sie Daten in einer anderen Anwendung eingeben. Bitte beachten Sie jedoch, dass einige Programme mit aktivem Permanentschutz nicht mehr korrekt arbeiten. Zum Beispiel wird die MagicWord Funktion von ArchiCrypt Live nicht mehr funktionieren.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Treten generell Probleme auf, versuchen Sie den **Kompatibilitätsmodus**. Dieser setzt eine etwas abgeschwächte Form des Schutzes ein, die dennoch sehr wirksam ist.

➡**WICHTIG: Es ist durchaus möglich, dass Antiviren- oder Anti Spyware-Programme Alarm schlagen, sobald Sie die Anti-Keylogger Funktion aktivieren. Es handelt sich jedoch um einen Fehlalarm, der ausgelöst wird, weil ArchiCrypt Passwort Safe Keylogger mit den eigenen Mitteln schlägt. Nehmen Sie ArchiCrypt Passwort Safe im Falle eines Alarms in die Ausnahmeliste Ihres AV- oder AntiSpyware Programms auf. Hinweise dazu finden Sie in der jeweiligen Hilfe oder auf den Supportseiten der Hersteller.**

Sofern Sie den Permanentschutz aktiviert haben, können Sie den Schutz über einen Hotkey[37] beliebig aktivieren und deaktivieren.

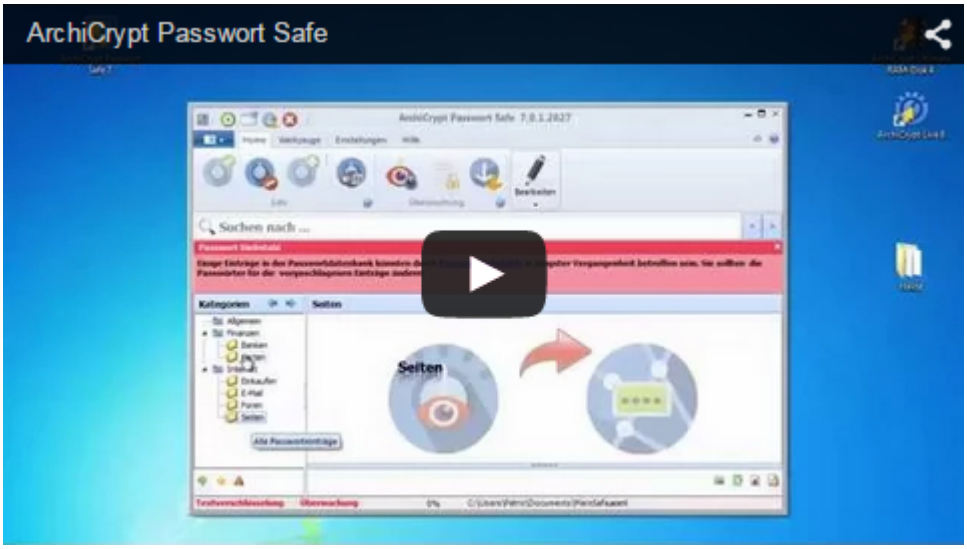
LogBuch

Im LogBuch werden wichtige Informationen abgelegt. Die Daten im Logbuch werden nicht gespeichert, sondern nach dem Beenden von ArchiCrypt Passwort Safe wieder gelöscht. Vor allem im Zusammenhang mit Netzwerk und Internetfunktionen[35] (*Passwort Safe im Internet auf FTP Server*) kann das LogBuch wertvolle Hilfe leisten. Fehler, die der Server im Internet zurück gibt, werden hier aufgelistet und können dann meist schnell beseitigt werden. Dazu sollten Sie die Funktion "**Netzwerk-Kommunikation anzeigen (hilfreich bei Fehlersuche)**" aktivieren.

TOP[86]

Video Workshop ArchiCrypt Passwort Safe[23]

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

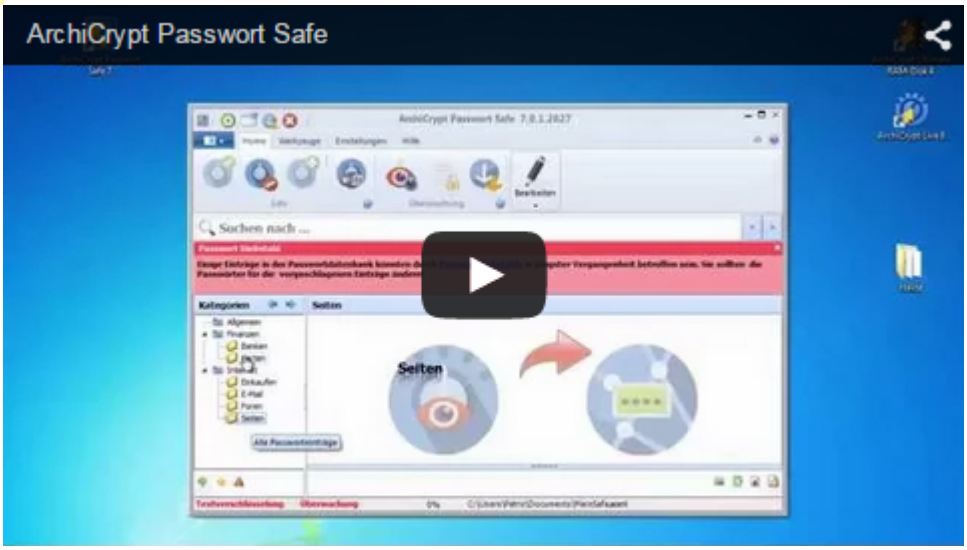


Folgende Themen könnten Sie ebenfalls interessieren:

Menüleisten[49]
Erster Start - So richten Sie ArchiCrypt Passwort Safe ein[27]

8.12 Austausch von Passwort Datenbanken

Video Workshop ArchiCrypt Passwort Safe[23]



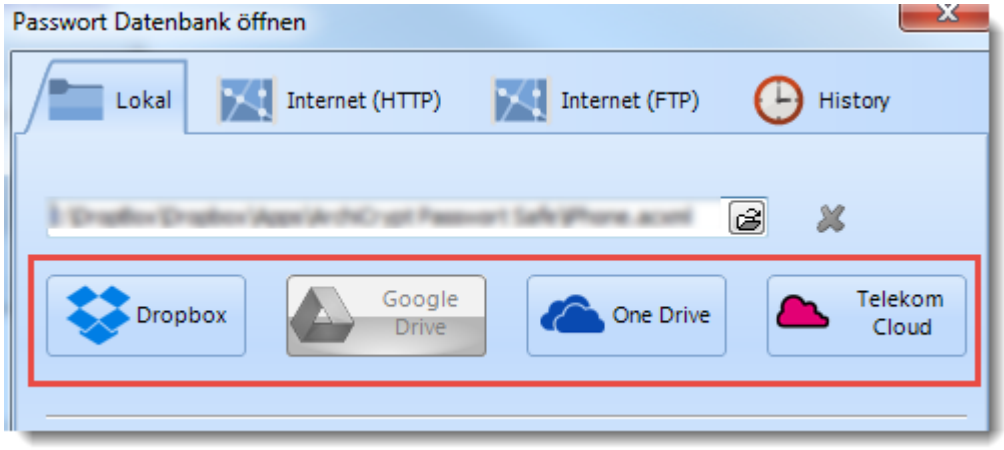
Austausch über Drittanbieter

Cloud Dienste

Cloud-Dienste sind nicht mehr wegzudenken. Von Sicherheit, kann in den meisten Fällen keine Rede sein. Das spielt für die Daten eines Passwort Safes keine wichtige Rolle. Die Sicherheit[42] steckt

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

hier in ArchiCrypt Passwort Safe. Beim Anlegen eines neuen Passwort Safes oder beim Öffnen, haben Sie die Möglichkeit als Speicherort einen Ordner zu wählen, der von einem bestimmten Dienst dann über Systemgrenzen hinweg synchronisiert wird. In der Cloud landen niemals Klartextversionen der Passwortdatenbank.



Wenn Sie auf Windows Rechner A einen Safe in One Drive speichern, können Sie auf Rechner B auf diesen Safe zugreifen. Die Synchronisation übernimmt der Cloud Dienst. In der Cloud liegt immer die Verschlüsselte Datenbank. Das Passwort für den Passwort Safe ist dem Cloud Dienst nicht bekannt! siehe Sicherheit[42]

➡**WICHTIG: Wenn Sie einen Cloud Dienst verwenden möchten, um eine Passwort-Datenbank mit mobilen Endgeräten auszutauschen, nutzen Sie Dropbox oder GDrive (Google Drive). In die Android und iOS Versionen sind spezielle Funktionen integriert, die auf Dropbox und Google Drive zugreifen können.**

Wenn Sie Daten über Google Drive austauschen möchten, dann müssen die entsprechenden Passwort Safe im Verzeichnis "ArchiCrypt Passwort Safe" abgelegt werden. Das entsprechende Verzeichnis ist gegebenenfalls anzulegen!

ArchiCrypt Passwort Zentrale

Eine von uns betriebene Upload-Plattform[128], auf die Sie eine Passwort Safe Datei laden können. Auf diese Passwort-Datenbank können Sie dann aus den mobilen Versionen und dem Windows Rechner lesend zugreifen. Die verschlüsselt Passwort Datenbank wird beim Übertragen über das Internet ZUSÄTZLICH mit sicherer SSL Verschlüsselung übertragen.

siehe ArchiCrypt Passwort Safe Online[128]

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

zur Passwort Zentrale

Austausch ohne Drittanbieter

Wer Drittanbietern nicht vertraut oder aus anderen Gründen beim Austausch von Passwort Datenbanken nicht auf Dritte zurückgreifen möchte, der hat die Möglichkeit, **im eigenen Netzwerk** auf das Passwort Safe LAN/WLAN WiFi Modul zurückzugreifen.

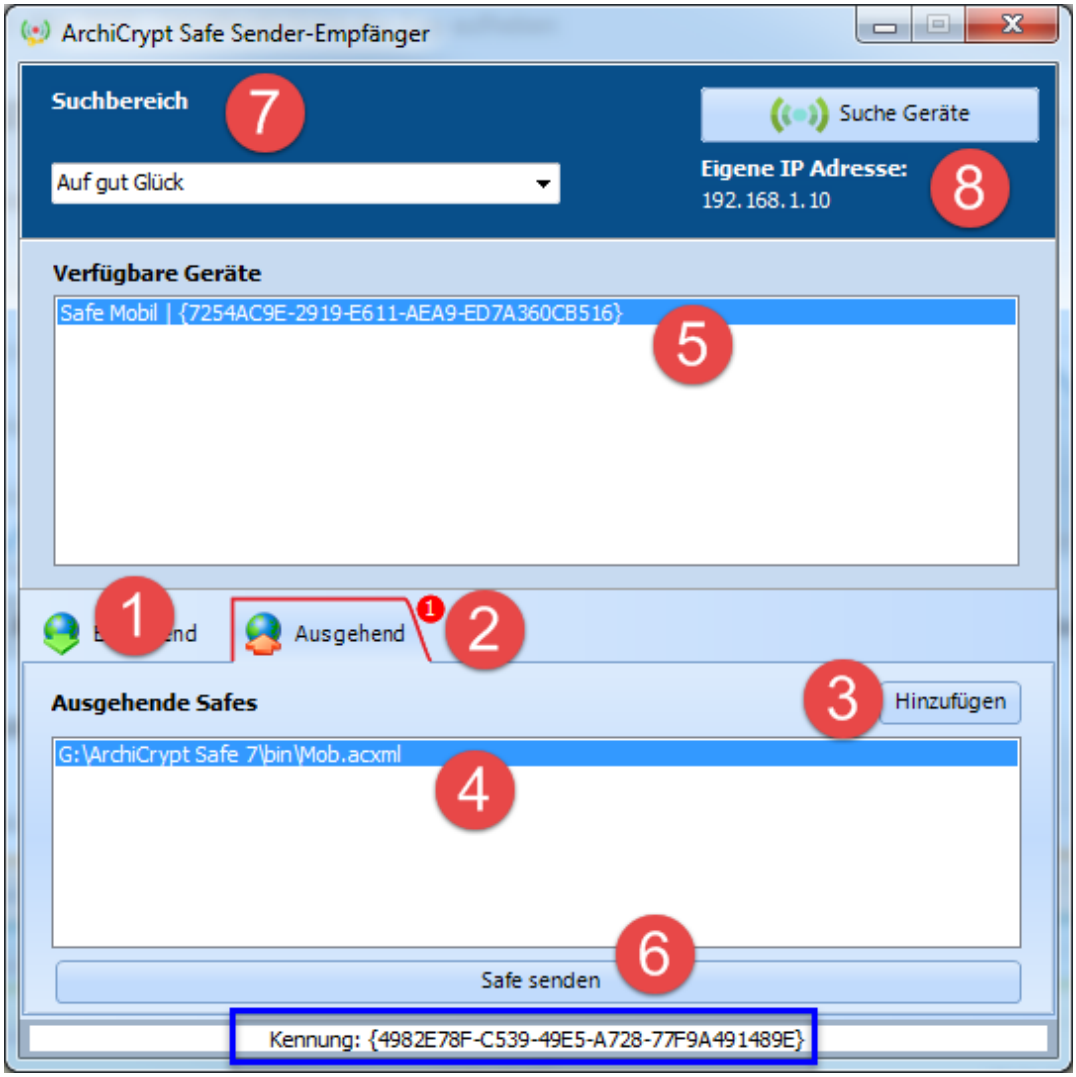
Eine Safe-Datenbank versenden

Starten Sie das **WiFi Modul**. Sofern im Passwort Safe eine Datenbank geöffnet ist, wird dieser Safe bei (4) **Ausgehende Safes**.

Starten Sie auf den anderen Rechnern ebenfalls das **WiFi Modul**. Diese werden dann mit ihrer Kennung bei (5) **Verfügbare Empfänger** gelistet.

Sie können auch einen Passwort Safe manuell in die Liste **Ausgehende Safes** einfügen. Dazu klicken Sie auf (3) **Hinzufügen** und wählen die entsprechende Datei auswählen.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

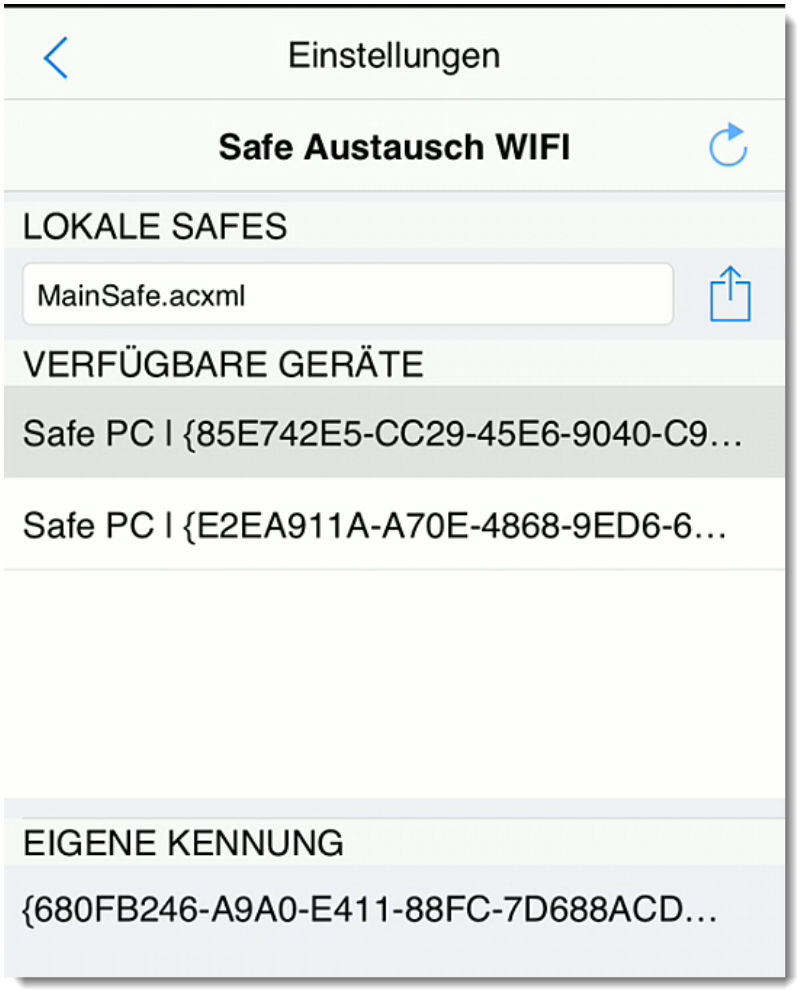


Um eine bestimmte Datei an einen Empfänger zu senden, markieren Sie die Datei bei **Ausgehende Safes** (4). Anschließend wählen Sie den Empfänger (5) aus und klicken auf **Safe senden** (6).

➡**TIPP: Betätigen Sie auf beiden Seiten die Schaltfläche Aktualisieren, wenn sich die WiFi Module nicht finden. Unter (7) können Sie in der Auswahlbo die Voreinstellung Auf gut Glück ändern. Diese Einstellung verwendet Parameter, die in den meisten Heimnetzwerken korrekt arbeiten. Bei (8) sehen Sie Ihre eigene IP Adresse. Wenn nichts gefunden wird, klicken Sie auf den keinen Pfeil im Auswahlfeld bei (7) und wählen Sie "Geben Sie eine IP Adresse an". Geben Sie jetzt eine IP Adresse in der Form 192.168.10.1 an. Die IP Adresse sollte mit der unter eigene IP angezeigten IP Adresse des Empfängers übereinstimmen. Sie können die letzte Ziffer auch auf 0 setzen (also zum Beispiel auf 192.168.10.0). In diesem Fall wird das entsprechende SUB Netz gescannt.**

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

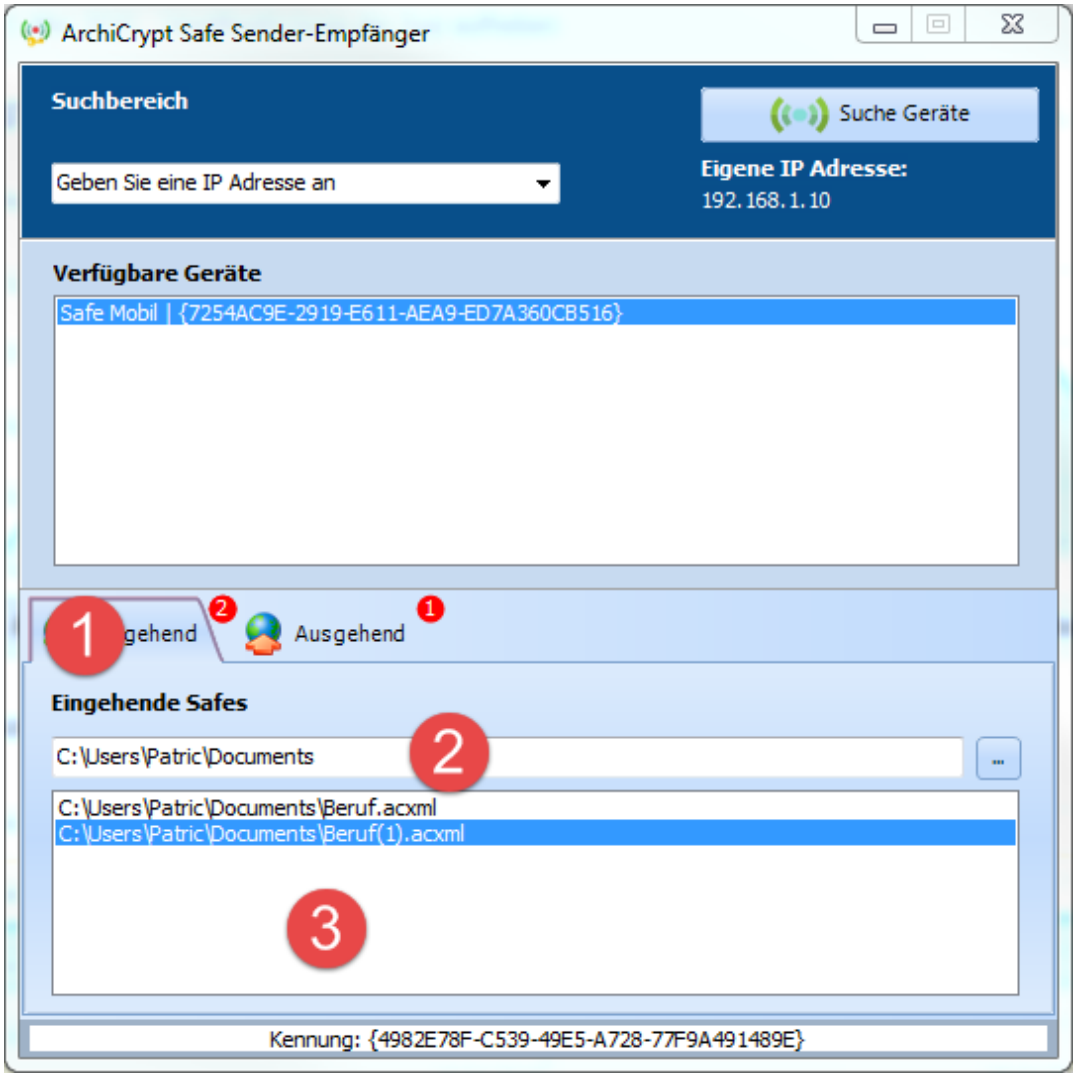
Auf den Mobilgeräten müssen Sie in den Einstellungen zu Synchronisation und dort zu WLAN/WiFi Datenübermittlung. Erst dann wird dort das WiFi Modul aktiv und die Geräte werden untereinander sichtbar.



Eine Safe Datei senden

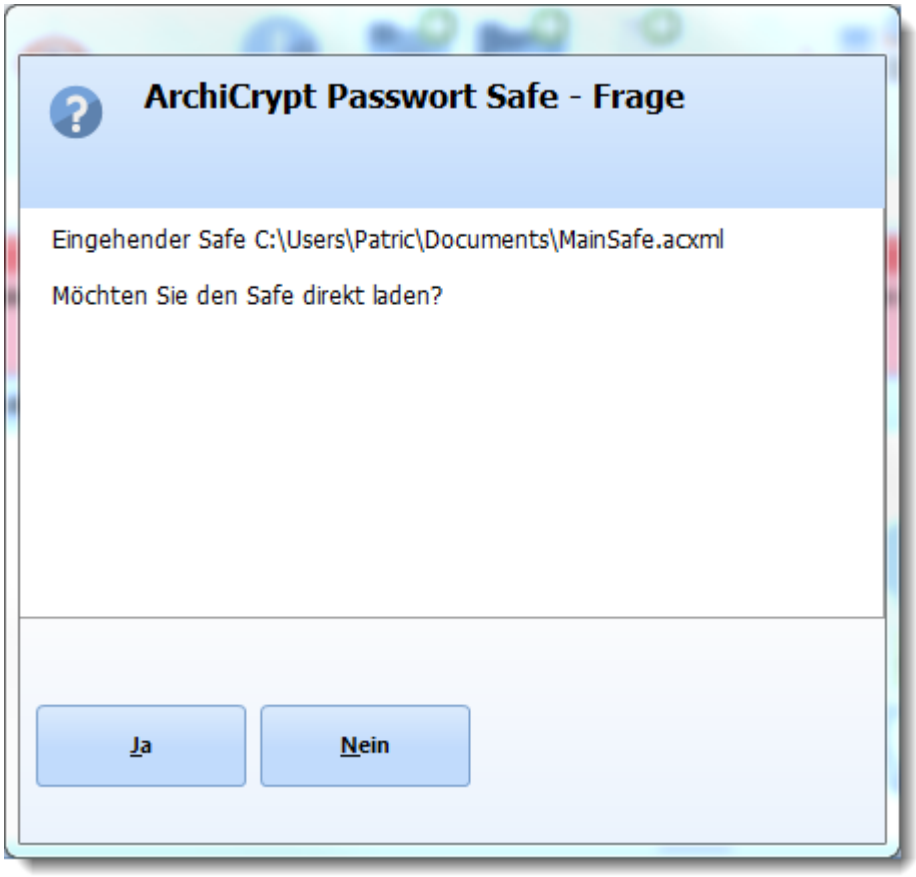
Auf der Empfängerseite wird der übertragene Safe (*PC Version*) auf der Seite **Eingehend** (1) angezeigt.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Der Safe wird im bei (2) festgelegten Verzeichnis abgelegt. Sie können per **Doppelklick** auf den Eintrag bei (3) den Windows Explorer starten. Ist ArchiCrypt Passwort Safe aktiv, wird der Safe an die Anwendung übertragen und kann dort geöffnet werden. Ist der Passwort Safe nicht aktiv, wird die Anwendung gestartet.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Ist ein anderer Passwort Safe geöffnet, wird dieser zunächst geschlossen. Wenn Sie den Safe nicht öffnen, wird der Verweis auf die übertragene Safedatei **in der History gespeichert** und Sie können beim nächsten Öffnen darauf zugreifen.

➡**WICHTIG: Das WiFi Modul auf dem PC prüft beim Eingang eines Passwort Safes, ob es bereits eine Datei mit diesem Namen gibt. Falls ja, wird die eingehende Datei am Ende mit einer Nummer versehen, um ein versehentliches Überschreiben zu verhindern!**

8.13 Was ist ein gutes Passwort?

Ein gutes Passwort

Ihr Passwort **für den Passwort Safe** sollte aus **mindestens 12 Zeichen** aufgebaut sein. Darin sollten sich **Groß-/Kleinbuchstaben**, **Ziffern** und **Sonderzeichen** befinden. **Ideal wären 16 Zeichen.**

TIPP:
Passwörter für Internetseiten.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Viele Sonderzeichen bereiten im Internet Probleme, da diese Zeichen oft eine spezielle Bedeutung haben. Hier empfiehlt es sich, das Passwort rein aus Buchstaben und Ziffern aufzubauen, dafür die Mindestlänge auf 18 Zeichen zu erhöhen. Auch dann wenn Sie die Daten später in lesbarer Form aus dem Passwort Safe exportieren möchten, empfiehlt sich die Verwendung des Internet-sicheren Zeichensatzes[116] .

ArchiCrypt Passwort Safe nutzt verschiedene Verfahren, um Sie vor den schlimmsten Fehlern beim Festlegen eines Passwortes zu schützen. Bitte klammern Sie sich nicht an diese Bewertung und schalten Sie zusätzlich **den gesunden Menschenverstand** ein. Also nicht den Namen des Haustieres mit dem Geburtsdatum der Oma kombinieren!

Der integrierte **Passwort Generator**[114] hilft Ihnen beim Erstellen guter Passwörter. Alternativ finden Sie unter www.Passwort-Zentrale.de bei jedem Besuch für jeden Besucher neu erzeugte Passwörter, die Sie im Original oder gerne auch leicht abgewandelt nutzen können.

Bitte keine Namen, Wörter, Geburtstage, Telefonnummern etc. verwenden, auch keine Teile davon.

Beispiele für schlechte Passwörter:
JohannA021297
BrunnoSommer2000
12BerndMai76Muenchen

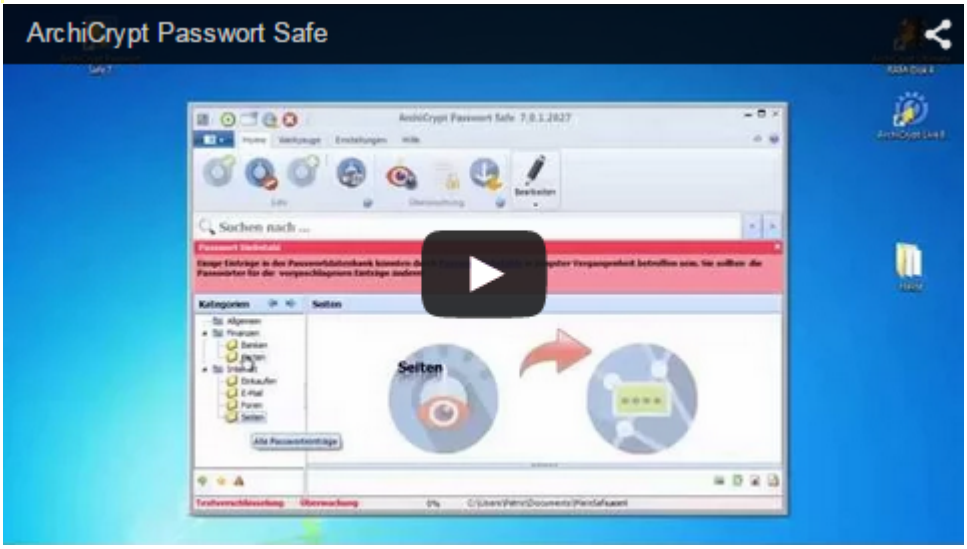
Beispiele für gute Passwörter
TzGa23P=zz5S
K7!-I89=QWar
Z8UUIaaG5=!

Immer wieder erhalten wir E-Mails in denen uns mitgeteilt wird, dass ein sehr langes Passwort als völlig unsicher eingestuft wird. Das ist sehr gut möglich, da es bei dem eingesetzten Verfahren (*Bloom Filtering*) zu s.g. *False-Positives* kommen kann. Die ist jedoch völlig ohne Belang.

> **DAHER GILT:** Nutzen Sie bei der Eingabe eines Passwortes **Ihren gesunden Menschenverstand**. Zusammen mit den mathematischen Verfahren in ArchiCrypt Passwort Safe werden Sie ab sofort keine unsicheren Passwörter mehr erzeugen.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

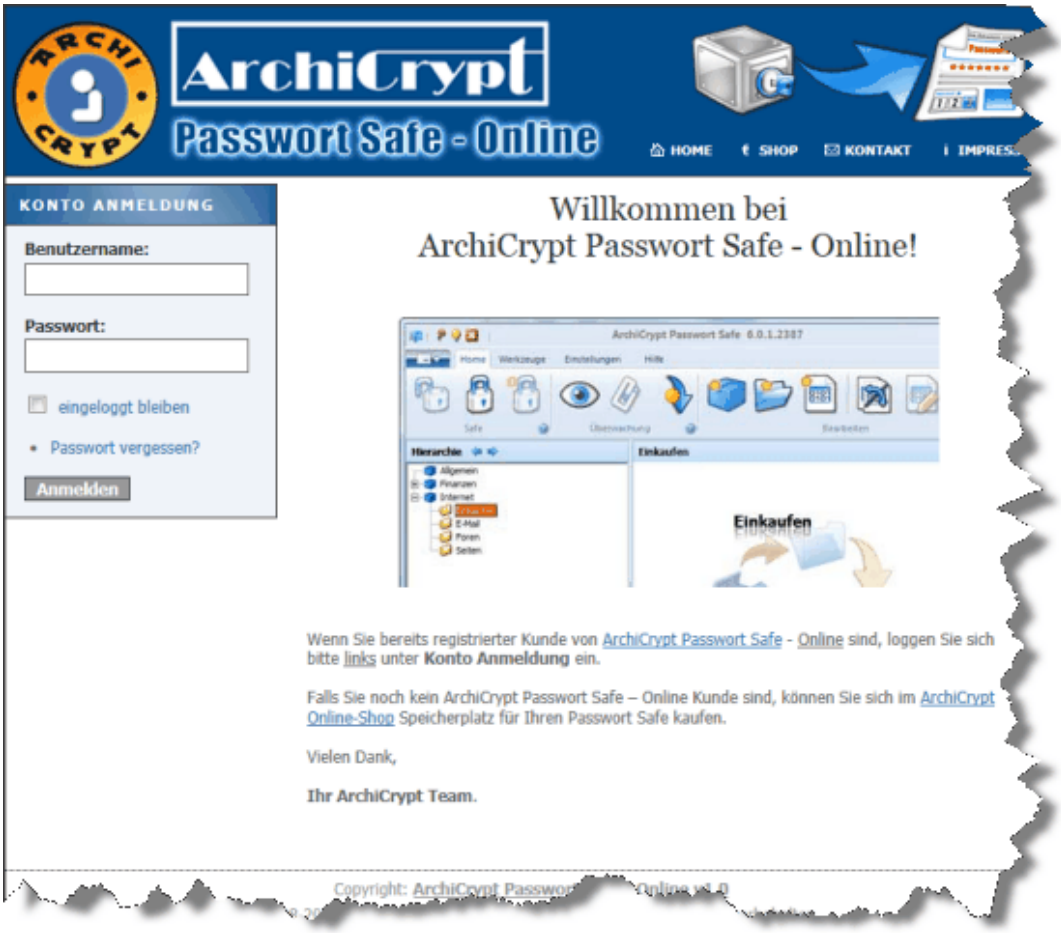
Video Workshop ArchiCrypt Passwort Safe[23]



8.14 ArchiCrypt Passwort Safe-Online

ArchiCrypt Passwort Safe kann den Passwort Safe auch aus dem Internet laden[35]. Das ist praktisch, da man so auf die Daten im Passwort Safe zugreifen kann, ohne die Passwortdatenbank selbst mit sich zu führen. Natürlich können so auch mehrere Anwender gleichzeitig auf einen zentralen Passwort Safe zugreifen.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Nicht jeder verfügt jedoch über eine eigene Internetseite oder ausreichendes Know-how.

Daher haben wir einen Dienst eingerichtet, der genau das bringt, was Sie für sicheren Zugriff via Internet benötigen.

ArchiCrypt Passwort Safe - Online bietet:

1. Sehr **kostengünstiger Dienst**
2. Äußerst **einfache Handhabung**
3. Zusätzliche Sicherheit Dank **SSL Verschlüsselung**

So nutzen Sie ArchiCrypt Passwort Safe - Online

1

Sofern noch nicht geschehen, sollten Sie einen ArchiCrypt

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Passwort Safe **Online Zugang** erwerben. Diesen finden Sie in unserem Online-Shop

2

Sie sollten eine E-Mail mit Betreff ***[ArchiCrypt Passwort Safe - Online] Zugangsdaten*** erhalten haben. Entnehmen Sie dieser E-Mail Ihre Zugangsdaten.

- Benutzername
- Passwort
- E-Mail Adresse

3

Besuchen Sie jetzt die Internetseite www.Passwort-Zentrale.de Die besuchte Internetseite leitet Sie ohne Zutun auf eine sichere SSL Verbindung um - wundern Sie sich daher nicht, wenn die Adresse sich zu https://www.ssl-id.de/passwort-zentale.de/... ändert.

4

Melden Sie sich jetzt mit Ihren Daten an.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

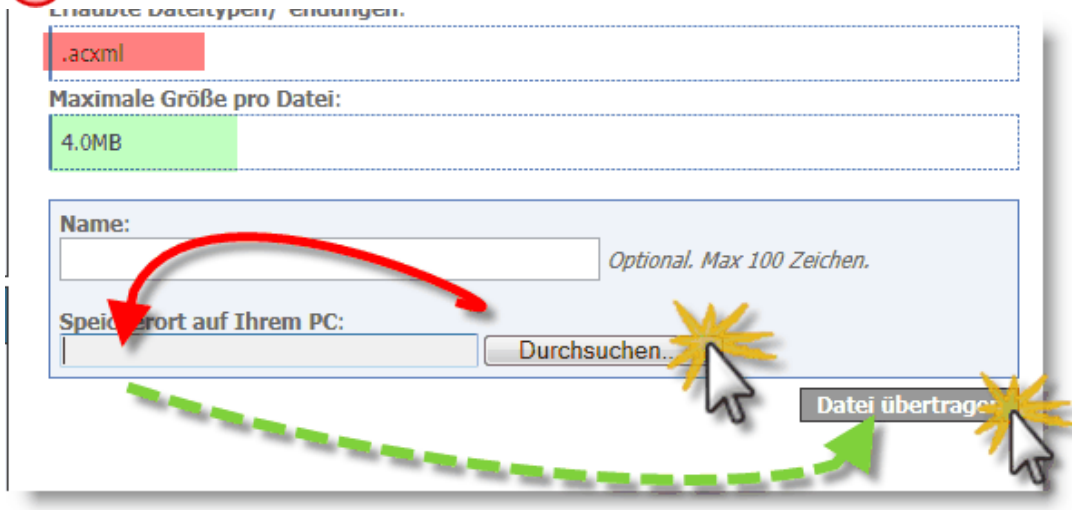
5

Sofern Sie Benutzername und Passwort korrekt angegeben haben, sollten Sie Ihren **Persönlichen Bereich** sehen.

Persönlicher Bereich

Klicken Sie auf **Passwort Safe Upload** und Sie gelangen zur folgenden Seite:

6



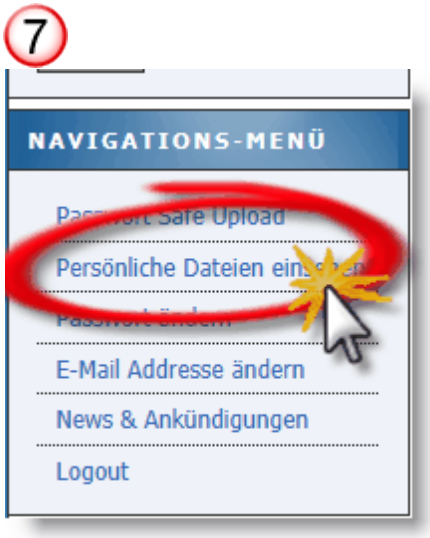
Klicken Sie auf **Durchsuchen...** um im Windows Datei Dialog die Passwort Safe Datei auszuwählen.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

➡**Der Safe MUSS bereits alle Passwortdaten enthalten. Laden via HTTP erlaubt keine Änderungen.** Achten Sie darauf, dass Sie die korrekte Datei wählen (*Dateiendung acxml*) und die Datei die zulässige Größe nicht übersteigt.

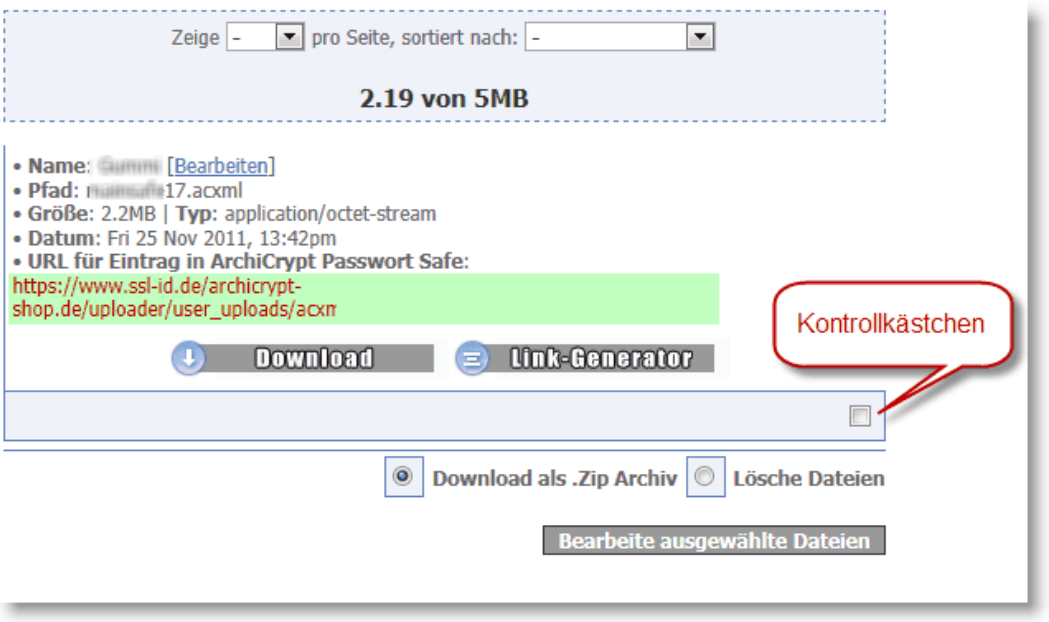
Geben Sie einen Namen für Ihren Safe auf dem Server an (*optional*) und klicken Sie dann auf **Datei übertragen**. Geben Sie dem System etwas Zeit, je nach Anbindung an das Internet kann die Übertragung einige Minuten dauern. Sie erhalten nach Abschluss der Übertragung eine Bestätigungsnachricht und eine E-Mail.

Wechseln Sie jetzt im **Navigations-Menü** zu **Persönliche Dateien einsehen**



Sie sehen jetzt die Informationen zu der übertragenen Datei, die der folgenden Abbildung entsprechen sollte.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Für jede übertragene Datei werden die Informationen angezeigt. Sie können bei jeder Datei das Kontrollkästchen aktivieren und dann durch Klick auf **Bearbeite ausgewählte Dateien** diese entweder als ZIP-Archiv laden (Download als .ZIP Archiv) oder löschen (Lösche Dateien).

Bei jeder Datei finden Sie eine Schaltfläche **Download** mit der Sie die Datei im Original laden können.

Für uns ist jedoch die URL für den Zugriff auf den Safe wichtig. Markieren Sie die rote URL um sie anschließend im Passwort Safe eintragen zu können. Alternativ können Sie auf **Link-Generator** klicken und Sie erhalten die URL per E-Mail zugesandt.

Wie und wo Sie die URL eintragen müssen, sehen Sie hier: ArchiCrypt Passwort Safe - über das Internet laden[35]

TIPP: Wenn Sie den Passwort Safe im Internet aktualisieren möchten, müssen Sie zunächst die vorhandene Safedatei von ArchiCrypt Passwort Safe - Online entfernen (*löschen*). Erst dann können Sie die neue Version ins Internet laden.

Folgende Themen könnten Sie ebenfalls interessieren:

ArchiCrypt Passwort Safe - über das Internet laden[35]

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

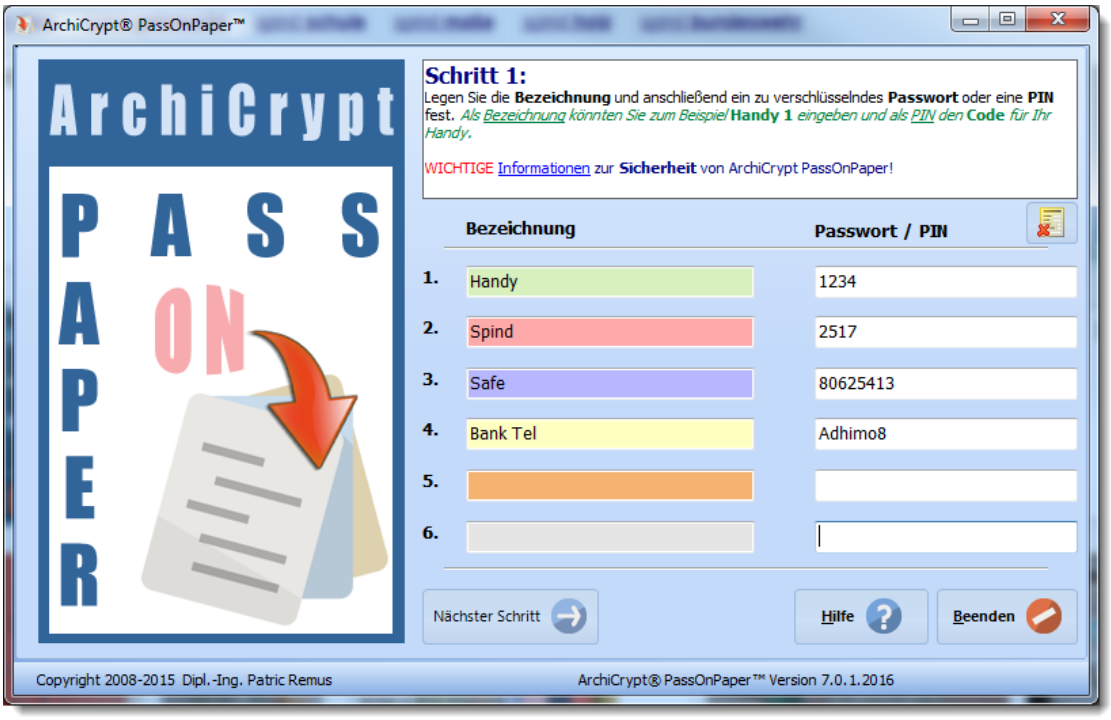
9 PassOnPaper

9.1 Bedienung

Allgemeines

Wäre es nicht hervorragend, wenn Sie Passwortdaten ganz ohne Hilfe von Computer, PDA und Handy transportieren und bei Bedarf nutzen könnten. Gerade unterwegs hat man nicht immer Zugriff auf diese digitalen Helferlein, ist aber oft auf PINs, TANs, Sicherheitscodes, Kombinationen von Zahlenschlössern, Passwörter für Telefonbanking etc. angewiesen.

ArchiCrypt PassOnPaper ist genau das Richtige für diesen Zweck. Es ist hoch sicher, sofern Sie die Anmerkungen im Kapitel Sicherheit 5 berücksichtigen, flexibel in der Anwendung und kinderleicht in der Bedienung!



Eingabe von Bezeichnung und Passwort bzw. PIN

Geben Sie zunächst eine **Bezeichnung** (*maximal 10 Zeichen*) ein. Sie erreichen höhere Sicherheit, wenn Sie nicht im Klartext erläutern, worauf sich das Passwort/die PIN bezieht.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Geben Sie jetzt das zugehörige **Passwort / PIN** (*maximal 12 Zeichen*) ein.

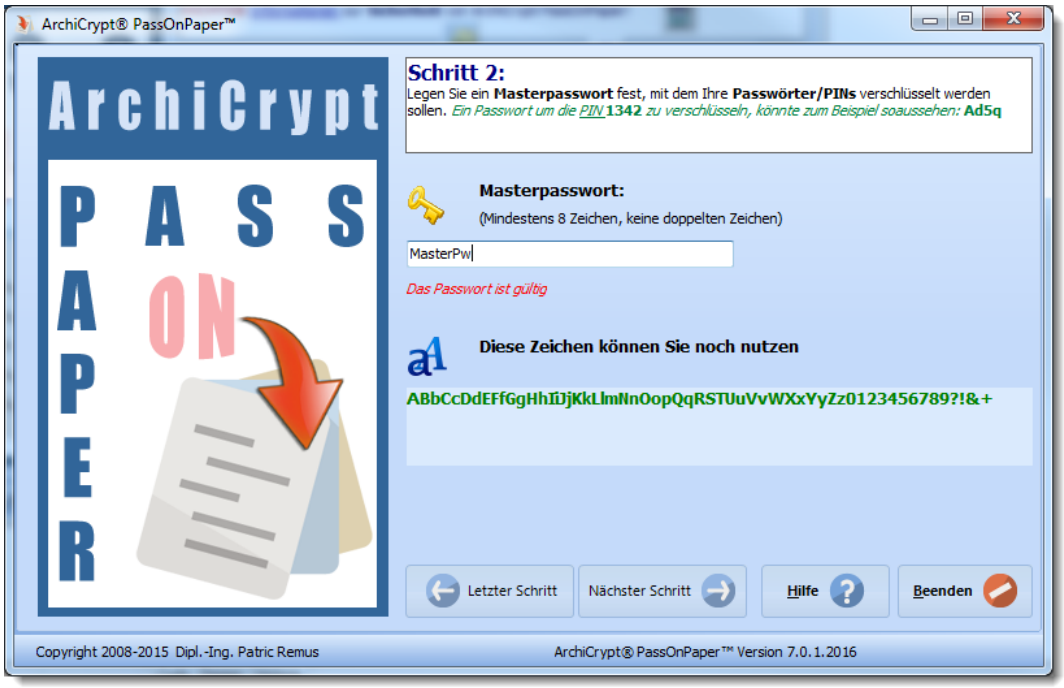
Sie müssen nicht alle Felder ausfüllen. Auf der **PassOnPaper Karte** werden nur solche Kategorien aufgeführt, für die eine Bezeichnung eingegeben wurde!

Sofern Sie alle Angaben gemacht haben, klicken Sie auf **Nächster Schritt**

TIPP: Wenn Sie mehr als 6 Passwörter/PINs etc. verschlüsseln möchten, ist dies kein Problem. Sie können beliebig viele PassOnPaper Karten mit gleichem Masterpasswort erzeugen. Lesen Sie sich jedoch die Sicherheitshinweise durch!

Eingabe des Masterpasswortes

Das **Masterpasswort** wird benötigt, um die Passwörter/ PINs, etc. wieder zu entschlüsseln. Das Masterpasswort müssen Sie sich also **merken**!



Das Masterpasswort muss so lange sein, wie das längste zu verschlüsselnde Passwort / PIN. In unserem Beispiel, ist das

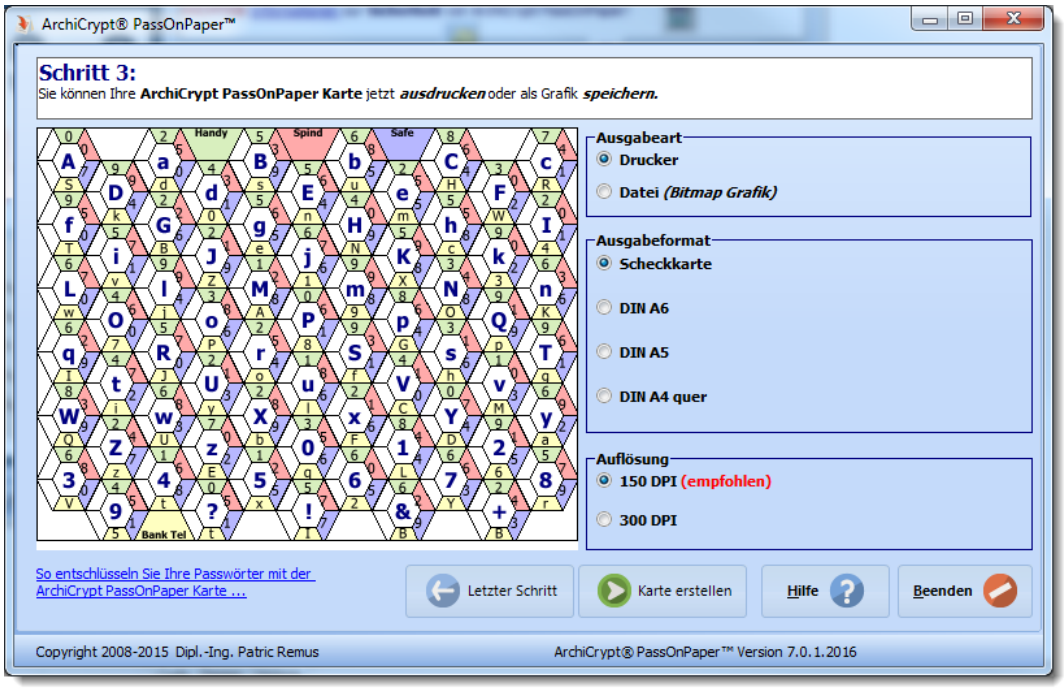
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

längste zu verschlüsselnde Passwort *13Namuki2.* Daher muss das Masterpasswort 9 Zeichen lang sein.

Das Masterpasswort muss aus den aufgeführten Zeichen bestehen, wobei jedes Zeichen genau ein Mal vorkommen darf. Ein Masterpasswort wie AAAbder wäre also nicht möglich. Wenn Sie ein Masterpasswort eingeben, sehen Sie unter "**Diese Zeichen können Sie noch nutzen**" die noch nutzbaren Zeichen.

Wenn das Passwort gültig ist, können Sie mit **Nächster Schritt** fortfahren.

Ausgabe der ArchiCrypt PassOnPaper Karte



In Schritt 3 sehen Sie eine Vorschau der PassOnPaper Karte. Sie können jetzt die **Ausgabeart**, das **Ausgabeformat** und die **Auflösung** festlegen.

Ausgabeart

Sie können die PassOnPaper Karte direkt ausdrucken (*Drucker*) oder aber als Grafik speichern (*Datei Bitmap Grafik*) lassen. Die Grafik lässt sich dann in jedem beliebigen Grafikprogramm weiterverarbeiten.

Ausgabeformat

Sie können verschiedene vordefinierte Formate wählen. Wer gute Augen hat, trifft mit der **Scheckkarte** eine gute Wahl. Ein guter Kompromiss zwischen Lesbarkeit und Größe stellt das **DIN A6** Format dar.

Auflösung
Testen Sie verschiedene Auflösungen mit Ihrem Drucker. Auf den allermeisten Systemen sind die Ergebnisse mit der Auswahl **150 DPI** optimal.

Um die PassOnPaper Karte zu erstellen, müssen Sie die Schaltfläche **Karte erstellen** betätigen.

➡ **WICHTIG: Vernichten Sie Testausdrucke**

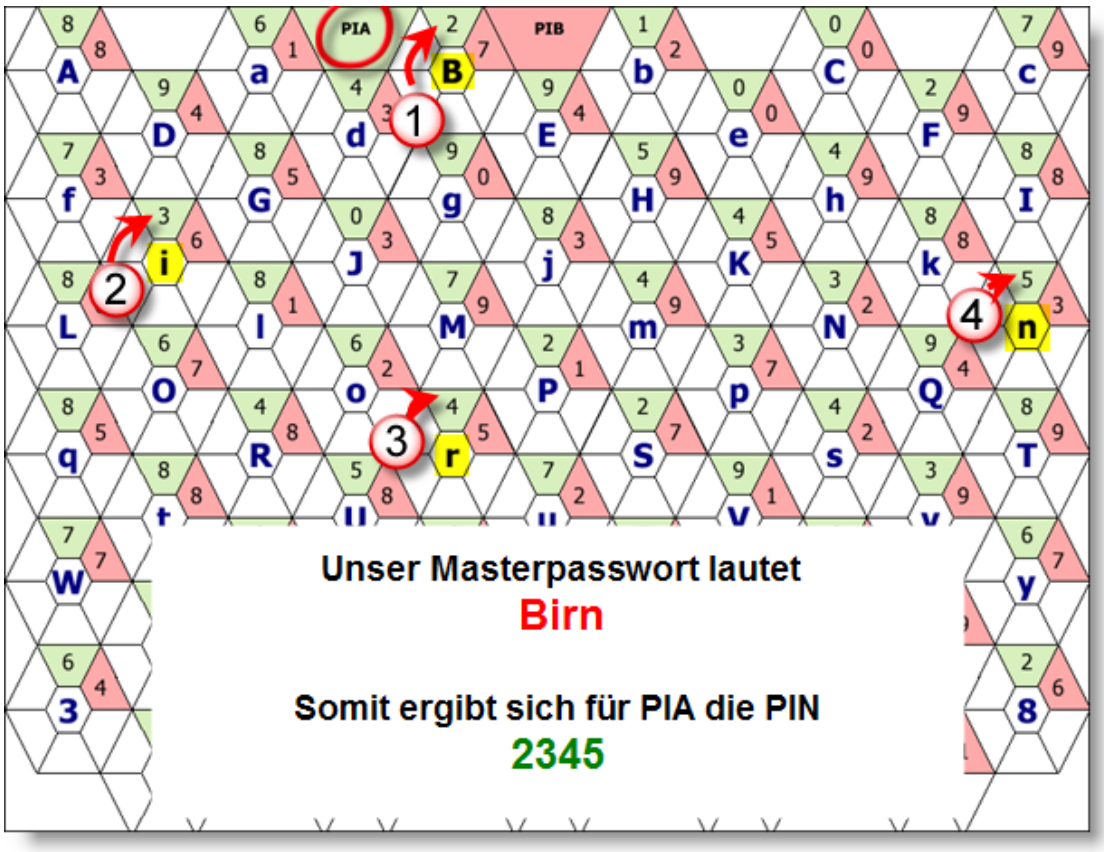
So entschlüsseln Sie Ihre Passwörter mit der ArchiCrypt PassOnPaper Karte

Sie finden die von Ihnen in Schritt 1 angegebenen **Bezeichnungen** am oberen und ggf. am unteren Rand der PassOnPaper Karte. Der Bezeichnung ist ein **Farbcode** zugeordnet. Für das Beispiel **PIA** ist der Farbcode **GRÜN**. In den Wabenmitten finden Sie die Buchstaben unseres Verschlüsslungsalphabets. Also *A,a,B,b* usw. Als Masterpasswort haben wir **Birn** gewählt.

Wir suchen jetzt die Wabe mit **B** (*erster Buchstabe unseres Masterpasswortes*) in der Mitte. Hier finden wir unser erstes Zeichen (die **2**) der gesuchten PIN im grünen (*unser Farbcode*) Teil dieser Wabe. Jetzt suchen wir die Wabe mit **i** (*zweiter Buchstabe unseres Masterpasswortes*) in der Mitte und entnehmen das 2te Zeichen unserer PIN (die **3**). Entsprechend liefert die Wabe mit **r** (*dritter Buchstabe unseres Masterpasswortes*) das Zeichen (die **4**) und Wabe mit **n** (*vierter Buchstabe unseres Masterpasswortes*) das Zeichen (die **5**). Wir haben unsere PIN entschlüsselt.

Hätten wird die PIN zu der Bezeichnung **PIB** gesucht, wäre der Farbcode **rot** gewesen und die gesuchte PIN hätte sich zu **7653** mit der gleichen Vorgehensweise ergeben.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



9.2 Sicherheit von PassOnPaper

Sicherheit von PassOnPaper

Sie können sich vorstellen, dass PassOnPaper nicht die gleiche Sicherheit bieten kann, wie Verschlüsselungsverfahren auf Ihrem Rechner. Das Verfahren ist dennoch so zuverlässig, dass Sie viele Arten von Passwörtern bedenkenlos mit PassOnPaper sichern können. Nachfolgende **Tabelle** gibt Ihnen einen Überblick darüber, inwiefern bestimmte Passwortarten (*Passwörter/PINs oder TANs*) für die Speicherung in **PassOnPaper** geeignet sind.

Allgemeines:

Sicher wissen Sie, dass man keine Passwörter nutzen soll, die in Wörterbüchern zu finden sind. Falls Sie doch solche Passwörter nutzen, speichern Sie diese nicht in PassOnPaper.

Selbstverständlich können Sie mit einem Masterpasswort mehrere PassOnPaper Karten erstellen. Sie dürfen jedoch niemals mehrere PassOnPaper Karten mit gleichem Passwort und gleichen Einträgen erstellen.

Beispiel dazu:

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Es ist erlaubt eine Karten mit Bezeichnung Bank1 und PIN 12345 mit Masterpasswort PhjLf und eine Karte mit Bezeichnung Bank2 und PIN 24314 ebenfalls Masterpasswort PhjLf zu erstellen.

Sichert man mit gleichem Masterpasswort in 2 Karten gleiche Werte, könnte man leicht durch "übereinanderlegen" der beiden PassOnPaper Karten feststellen, welche Werte in beiden Karten identisch sind. Man hätte damit das Masterpasswort herausgefunden.

In der Praxis werden Sie genau dies nicht tun, da Sie verschiedene Passwörter mit einem Masterpasswort sichern möchten.

➡ **WICHTIG: Vernichten Sie Testausdrucke**

Geeignetheit verschiedener Passwortarten für PassOnPaper

Zu schützende Information	Geeignetheit	Anmerkung
EC- und Kreditkarten PIN	**hervorragend**	-
Koffer, Zahlenschloss	**hervorragend**	-
Fahrrad, Zahlenschloss	**hervorragend**	-
Tresor, Kombination	**hervorragend**	-
Handy, PDA PIN	**hervorragend**	-
Telefonbanking Passwort	**hervorragend**	-
TANs für Online-Banking	**hervorragend**	-
Loggin Daten PC/Laptop	**gut**	-
E-Mail Zugang	**hervorragend**, sofern nach mehrmaligem Fehlversuch eine Zeitsperre eintritt. (z. Bsp. erneuter	

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

	Versuch erst nach 24 Stunden) **nicht geeignet**, sofern es eine solche Sperre nicht gibt	
Zugangspasswort Online-Banking	**hervorragend**, sofern nach mehrmaligem Fehlversuch eine Sperre eintritt.	Zur Zeit ist keine deutsche Bank bekannt, die keine Sperre bei mehrmaliger Falscheingabe setzt. Meist wird der Zugang bei 3 maliger Falscheingabe komplett gesperrt. Gibt es eine solche Sperre bei Ihrer Bank nicht, lassen Sie bei dieser Bank generell die Finger vom Online-Banking!!!
ArchiCrypt Card, PIN	**hervorragend**	-
Verschlüsselungssoftware, Passwort zur Entschlüsselung	**ungeeignet**	gilt generell und ist nicht auf ein bestimmtes Programm eines bestimmten Herstellers beschränkt!
FTP Zugang	**ungeeignet**	-
WEB Seite Zugang	**hervorragend**, sofern nach mehrmaligem Fehlversuch eine Zeitsperre eintritt. (z. Bsp. erneuter Versuch erst nach 24 Stunden) **nicht geeignet**, sofern es eine solche Sperre nicht gibt	-

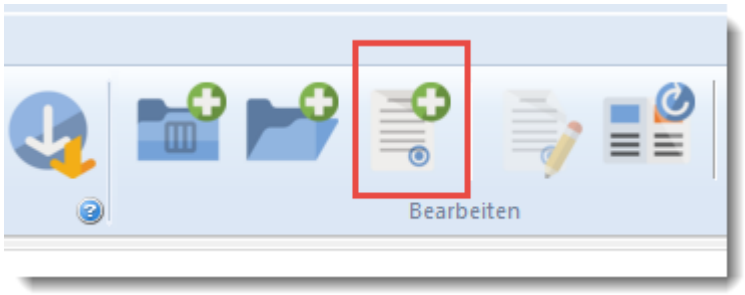
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

10 Dialoge

10.1 Safeeintrag erstellen

Einen Safeeintrag können Sie auf verschiedene Weise erzeugen:

1. Klick auf das Symbol in der Menüleiste

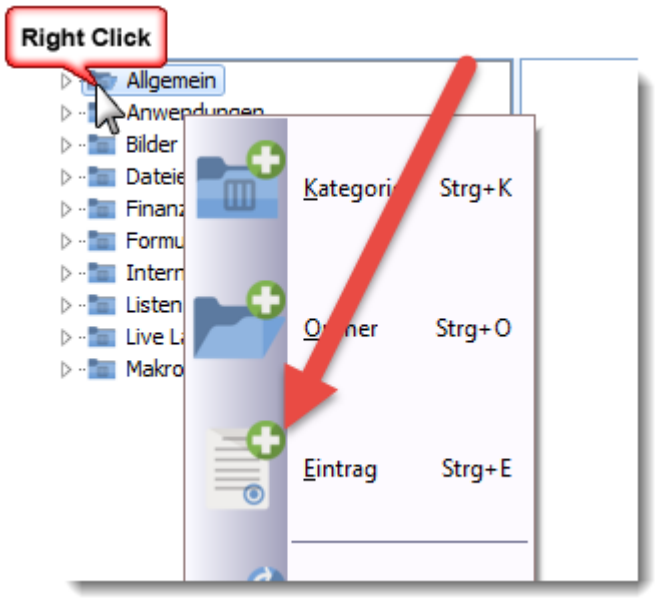


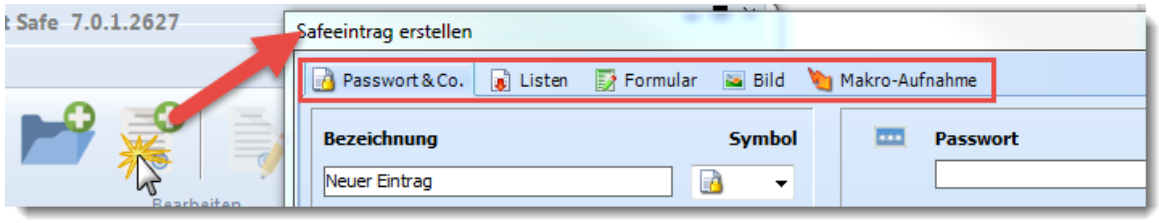
2. Tastaturkürzel Strg+E **sofern der Passwort Safe angezeigt wird**

3. Beim Surfen, wenn Sie den Hotkey für Erstelle neuen Safe Eintrag[110] festgelegt haben.

4. Sie können in der **Kategorieansicht** mit der rechten Maustaste das **Kontextmenü** aufrufen.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt





Sie sehen den Dialog mit den Registerseiten **Passwort&Co.**[10], **Listen**[20], **Formular**[21], **Bild**[22] und **Makro-Aufnahme**[23] am oberen Rand.

In den meisten Fällen erzeugt man Passworteinträge, bei denen man ausschließlich einige Angaben unter **Passwort&Co.** machen muss.

Welche Angaben müssen beim Erstellen eines Passworteintrags gemacht werden?

Keine! Sie können, auch wenn dies kaum Sinn macht, leere Einträge erstellen. Bedenken Sie jedoch, dass es durchaus Sinn macht, Einträge zu erstellen, bei denen Sie einfach nur ein Bild sicher ablegen möchten.

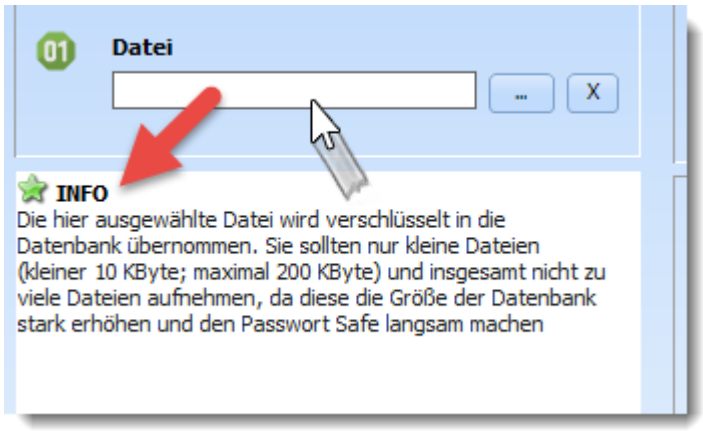
Vorbemerkung

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Lösen Sie sich von den Begriffen. Es gibt keine Vorschrift die verbietet, dass Sie unter Benutzername eine Kontonummer, eine Bankleitzahl oder sonstiges eingeben. Auch das Passwortfeld ist universell nutzbar und kann selbstverständlich alternative eine PIN oder andere Informationstypen aufnehmen.

Direkte Hilfe

Bewegen Sie den Mauszeiger über ein Element im Dialog und Sie erhalten eine Kurzhilfe, die den Blick in die Hilfe oft erspart.



Passwort & Co.

Bezeichnung

Beliebiger Wert, der das Auffinden erleichtert.

Symbol

Beliebige Grafik, die das Auffinden erleichtert. Grafik wird bei Favoriten, im Kontextmenü und bei Nachrichten angezeigt.

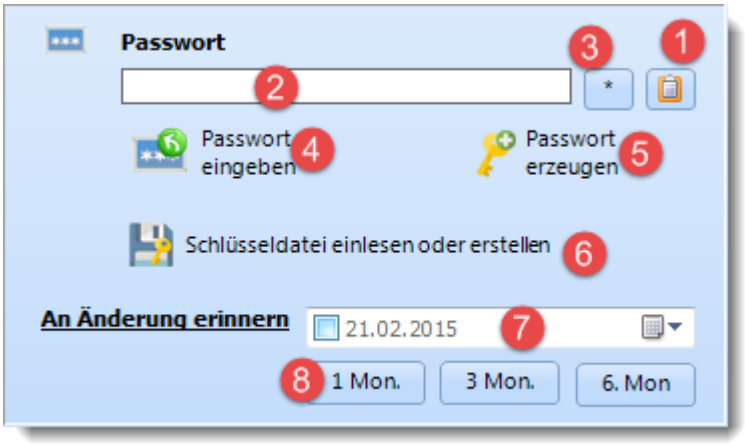
Benutzername

Beliebiger Wert, den Sie später per Drag&Drop oder Hotkey[101] in eine andere Anwendung übertragen können.

siehe auch Informationen eines Passworteintrags Benutzername[70]

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Passwort



Schnelle Variante für ein neues Passwort

Falls Sie ein neues und sicheres Passwort benötigen, klicken Sie einfach auf die Schaltfläche Passwort erzeugen **5**
Der Passwort Safe erzeugt dann mit Hilfe der des Passwortgenerators[114] ein neues Passwort.

Sie möchten selbst ein Passwort eingeben

Falls Sie selbst ein Passwort festlegen möchten, können Sie es direkt in das Eingabefeld eingeben **2** oder mit Prüfung gegen Falscheingabe und Bewertung mit **4**.
siehe auch Idee für ein Passwort[126]

Sie haben ein Passwort in der Windows Zwischenablage

Falls Sie ein Passwort über die Zwischenablage einfügen möchten, klicken Sie auf **1**.

Sie möchten eine Schlüsseldatei erzeugen oder nutzen

Eine Schlüsseldatei erzeugen und einlesen können Sie mit **6**.

Sie möchten sehen, was im Passwortfeld steht

Klicken Sie auf **3**

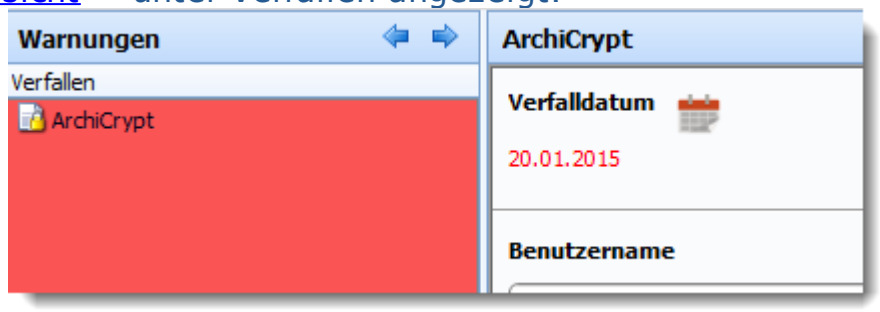
Sie möchten an einem bestimmten Datum erinnert werden

Legen Sie das Datum fest UND setzen Sie das Häkchen

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Durch Betätigen der Schaltflächen 1 Mon. 3 Mon. oder 6 Mon. wird das Erinnerungsdatum auf "heute" + Monatszahl gesetzt.

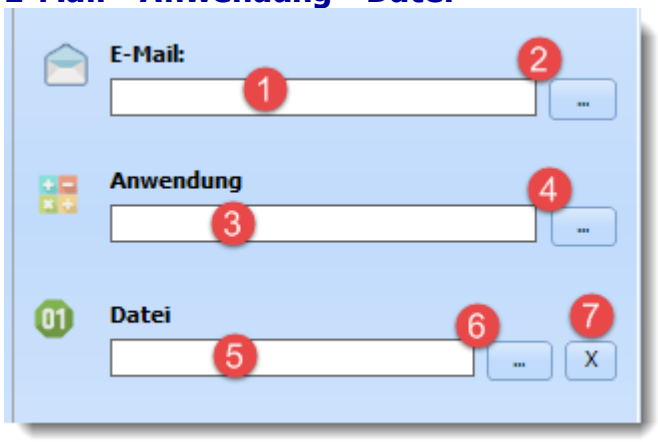
Der Eintrag wird bei Erreichen des Enddatums in der Home-Ansicht[39] unter Verfallen angezeigt.



Doppelklicken Sie auf den Eintrag mit links und Sie können den Eintrag bearbeiten.

TOP[8]

E-Mail - Anwendung - Datei



E-Mail

Wenn Sie hier eine Adresse eingeben, können Sie später per Klick eine E-Mail erstellen und zum Beispiel eine verschlüsselte Nachricht senden oder verschlüsselte Dateien als Anhang einer E-Mail an diesen Empfänger verschicken.

Unter **E-Mail** können Sie mit der Schaltfläche Auswahl **2** das MS-Windows Adressbuch aufrufen und daraus verschiedene Adressen übernehmen. Selbstverständlich können Sie die E-Mail Adressen auch manuell eingeben **1**. Falls Sie MS Outlook

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

oder Outlook Express verwenden, können Sie auch mehrere Empfänger durch Semikolon (;) getrennt eingeben.

➡ **HINWEIS: Auf neueren Systemen ist das klassische Adressbuch nicht mehr vorhanden!**

siehe auch Informationen eines Passworteintrags E-Mail[72]

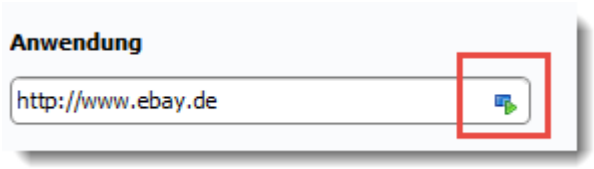
Anwendung

Der Eintrag **Anwendung** nimmt den Pfad zu einer Anwendung oder einer bestimmten Datei auf. Sie können den Pfad zur entsprechenden Datei manuell eingeben, oder aber die Schaltfläche ... **4** betätigen und im Dateidialog die Datei auswählen. Die hier eingetragene Datei wird **NICHT** in den Passwort Safe übernommen, sondern lediglich ein Verweis. Wenn Sie den Passwort Safe an einem anderen Rechner nutzen, hat dieser Eintrag daher unter Umständen keine Bedeutung mehr!

Sinnvoll lässt sich dieses Feld mit Anwendungen nutzen, die ein Passwort erwarten. Starten Sie die Anwendung und übertragen Sie das Passwort mit einem Hotkey[101] .

siehe auch So nutzen Sie den Passwort Safe um ein ArchiCrypt Live Laufwerk zu laden[72]

TRICK: Ab und zu kann es zu Problemen kommen, wenn Sie eine Internetadresse mit Jokerzeichen eintragen und diese Seite direkt über die Besuchen Schaltfläche im Passwort Safe im Browser aufrufen möchten. Wenn Sie keine Anwendung für diesen Safe Eintrag benötigen, können Sie in das Feld auch eine Internetadresse eintragen, die dann bei Klick auf "Anwendung starten" im Standard-Browser geöffnet wird.



Parameter an Anwendungen übergeben

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Sie können einer Anwendung auch mittels s.g. **Platzhalter** die Inhalte von Safeeinträgen als Parameter übergeben.

Feld aus Safeeintrag	Parameter
Benutzername	<usr>
E-Mail	<mail>
Passwort	<pwd>
Freitextfeld	<ftx>
Internet	<www>

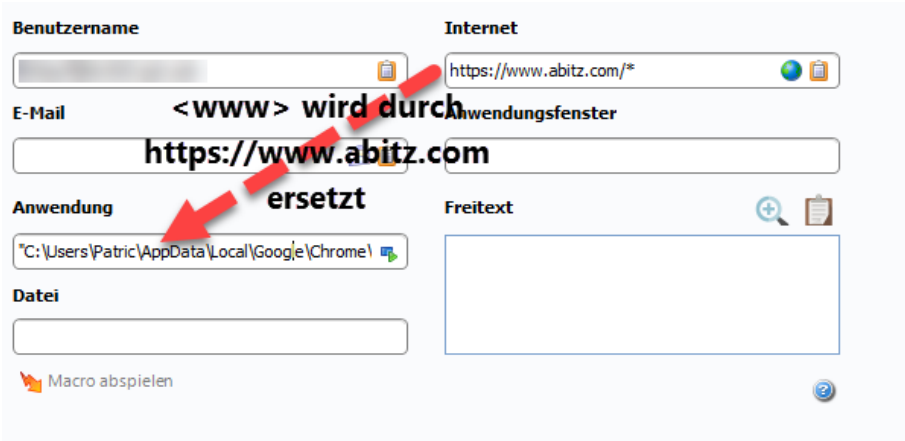
Wir erläutern das Prinzip an einem Beispiel:

Wir möchten eine im Passwort Safe eingetragene Internetseite nicht mittels Schaltfläche besuchen im Standard-Browser öffnen, sondern zum Beispiel in Google Chrome.

Google Chrome ist unter dem Pfad **C:\Users\Anwendername\AppData\Local\Google\Chrome\Application\chrome.exe** zu finden. Der Dokumentation von Chrome können wir entnehmen, dass man eine zu öffnende Seite als URL übergeben kann. Mittels --new-window wird ein neues Browserfenster geöffnet, alternativ mittels --new-tab ein neuer Reiter in Chrome.

Wir tragen im Feld Anwendung also ein:

"C:\Users\Anwendername\AppData\Local\Google\Chrome\Application\chrome.exe" "<www>" --new-window



© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Den Pfad zur Anwendung sollten Sie immer in Hochkommata einschließen. Die Art und Weise, wie man Parameter an die entsprechende Anwendung übergibt, entnehmen Sie bitte der Dokumentation der jeweiligen Anwendung.

Oft hilft eine Google Suche mit dem Anwendungsnamen und dem Stichwort Kommandozeile

Datei

Während bei Anwendung **3** lediglich ein Verweis auf die entsprechende Datei im Passwort abgelegt wird, wird hier die **komplette Datei im Passwort Safe** verschlüsselt abgelegt. Wenn Sie den Passwort Safe also an einem anderen Rechner verwenden, dann können Sie dennoch auf die Inhalte der so abgelegten Dateien zugreifen. Wenn Sie die Datei wieder aus dem Passwort Safe entfernen möchten, klicken Sie auf **X** bei **7**.

➡ **HINWEIS: Das Feld dient primär der Ablage kleiner Dateien wie sie beim Registrieren von Software bei bestimmten Anbietern zum Einsatz kommen. Der Inhalt ist jedoch prinzipiell beliebig. Die in die Datenbank übernommene Datei darf nicht größer als 200 Kilobyte sein. Insgesamt achten Sie bitte darauf, dass die Zahl derartig in den Passwort Safe übernommenen Dateien nicht zu groß wird. Der Passwort Safe braucht ansonsten zu viel Hauptspeicher und wird träge.**

Internet und Anwendungsfenster

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Internet

Der Eintrag **Internet** ist für die **Überwachung** des Browsers von entscheidender Bedeutung. Dieser Eintrag hier legt fest, wann der Passwort Safe bei aktivierter Überwachung[79] die Daten dieses Passworteintrags bereit stellen soll und ggf. automatisch in den Browser zu übertragen hat.

Es gibt mehrere Möglichkeiten, die Adresse der Internetseite hier einzutragen:

A) Sie befinden sich gerade auf der Internetseite, zu der Sie einen Eintrag erstellen möchten
Wenn Sie sich im Browser gerade auf der Seite befinden, zu der Sie einen Eintrag im Passwort Safe erstellen möchten, klicken Sie auf die Schaltfläche **Übernehmen...**
Die Adresse der aktiven Seite wird jetzt übernommen, sofern Sie in den Einstellungen auch den entsprechenden Browser[93] aktiviert haben.
Eventuelle müssen Sie noch etwas Handarbeit leisten.
siehe So stellen Sie sicher, dass der Passwort Safe die Internetseite erkennt[17]

B) Sie möchten die Seite manuell eingeben
Geben Sie die Seite einschließlich Protokoll (also http:// bzw. https://) an. Also nicht nur www.ArchiCryp.com, sondern http://www.ArchiCrypt.com
siehe So stellen Sie sicher, dass der Passwort Safe die Internetseite erkennt[17]

C) Es gibt mehrere Seiten, auf denen Sie die Daten dieses Safeeintrags nutzen
Aus Sicherheitsgründen ist es ratsam, dies zu ändern!
Sollte dies nicht möglich sein, können Sie mehrere Seiten, getrennt durch Semikolon eingeben **3**.
Beispiel: https://signin.ebay.de/ws/eBayISAPI.dll?SignIn*;https://www.heise.de/login/*

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

So stellen Sie sicher, dass der Passwort Safe die Internetseite erkennt

Sicher haben Sie sich ab und zu über die unleserlichen und recht langen Seitenadressen in Ihrem Browser gewundert.
Sehen Sie sich zum Beispiel die Seite von eBay an, in der Sie sich einloggen müssen:

https://signin.ebay.de/ws/eBayISAPI.dll?SignIn&ru=http%3A%2F%2Fwww.ebay.de%2F

Es gibt Internetseiten, die bei jedem Besuch eine andere Adresse haben

Adressen werden aus Sicherheitsgründen oft mit einem bei jedem Besuch der Seite neu erzeugten Code erweitert. Das Problem ist, dass ArchiCrypt Passwort Safe die Seite beim nächsten Besuch so nicht mehr erkennen würde, da der angehängte Code sich geändert hätte. Die zugehörigen Daten würden folglich nicht mehr bereitgestellt.

Hier müssen wir etwas Hand anlegen!

Besuchen Sie die Internetseite bitte zwei Mal und vergleichen

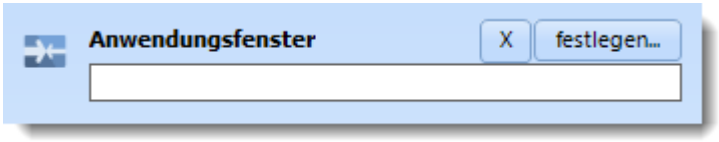
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Sie die zugehörigen Adressen. Die Adresse wird einen Anteil haben, der sich NICHT ändert. Diesen Anteil behalten wir und hängen ein Jokerzeichen (*) an die Adresse an. Jokerzeichen, auch Platzhalter genannt, stehen stellvertretend für eine beliebige Zeichenfolge. Daher können wir dem Passwort Safe die folgende Adresse vorgeben.
https://signin.ebay.de/ws/eBayISAPI.dll?SignIn*

FEHLERFALLE: Wenn wir solche Seitenadressen nutzen, bekommen wir eventuell Probleme, wenn wir unsere Favoriten[88] nutzen, oder im Passwort Safe die Schaltfläche Besuchen[74] betätigen. Unter Umständen wird eine Meldung angezeigt, die sinngemäß "Eine Seite **https://signin.ebay.de/ws/eBayISAPI.dll?SignIn*** kann nicht besucht werden!" lautet.

Mit dem Trick bei Anwendung[13] können Sie jedoch ein anderes Feld im Passwort Safe nutzen, um die Internetseite besuchen zu können.

Anwendungsfenster



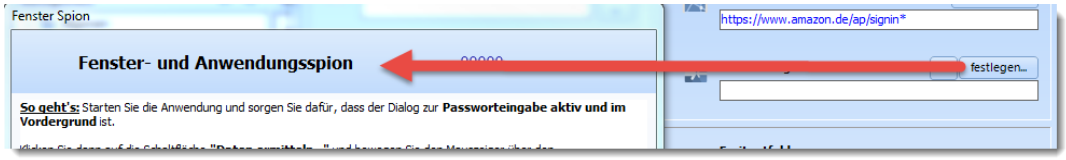
ArchiCrypt Passwort Safe kann Einträge im Passwort Safe auch automatisch aktivieren, wenn bestimmte Anwendungsfenster auftauchen. Um ArchiCrypt Passwort Safe die Angaben machen zu können, die es braucht, um diese Fenster erkennen zu können, haben wir ein Werkzeug integriert.

So bringen Sie ArchiCrypt Passwort Safe bei, beim Erscheinen eines Dialogs ein bestimmtes Passwort bereit zu stellen

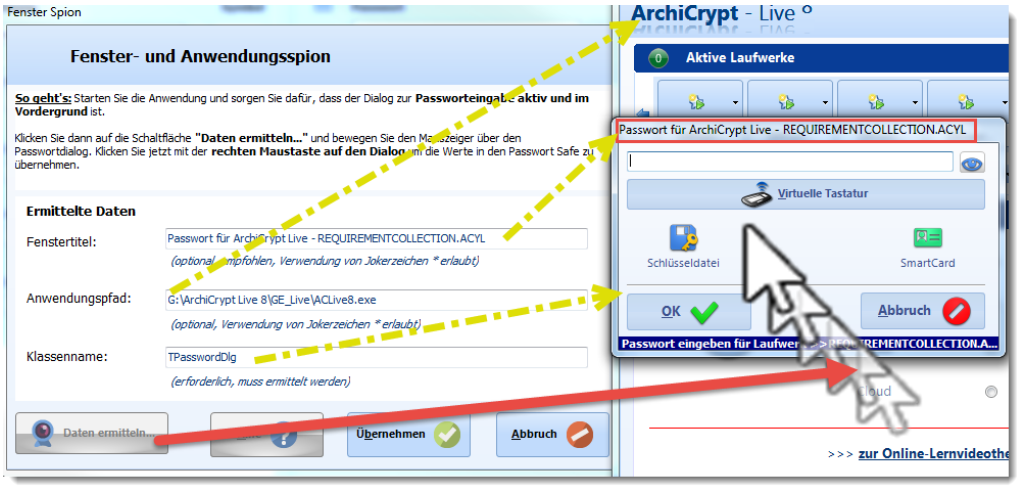
Starten Sie die entsprechende Anwendung und führen Sie alle Schritte durch, damit der entsprechende Dialog erscheint.

Klicken Sie jetzt in ArchiCrypt Passwort Safe bei Anwendungsfenster auf "**festlegen...**". Der **Fenster- und Anwendungsspion** wird angezeigt.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Lesen Sie sich die Anweisungen im Dialog durch und klicken Sie dann auf Daten ermitteln. Bewegen Sie jetzt die Maus über das Fenster, dem der Safe Eintrag zugeordnet werden soll.



Betätigen Sie über diesem Fenster die rechte Maustaste. Es sollten jetzt alle Informationen in die Felder des **Fenster- und Anwendungsspions** übertragen worden sein. Wenn Sie mit den ermittelten Werten zufrieden sind, betätigen Sie die Schaltfläche **Übernehmen**.

Um die Daten in einem Passwort Eintrag aus einem Feld Anwendungsfenster wieder zu entfernen, klicken Sie auf die Schaltfläche **X**. Um den Eintrag zu editieren, klicken Sie erneut auf **festlegen...**

TOP[8]

Freitextfeld

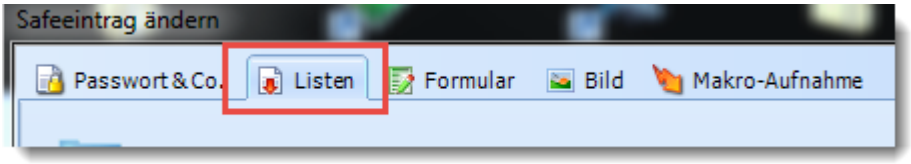
Dieses Feld haben Sie zur freien Verfügung. Es gibt zum Beispiel einige Banken, die eine zweite PIN abfragen. Sie könnten auch einen Merksatz oder eine kurze Notiz einfügen, eine Seriennummer

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

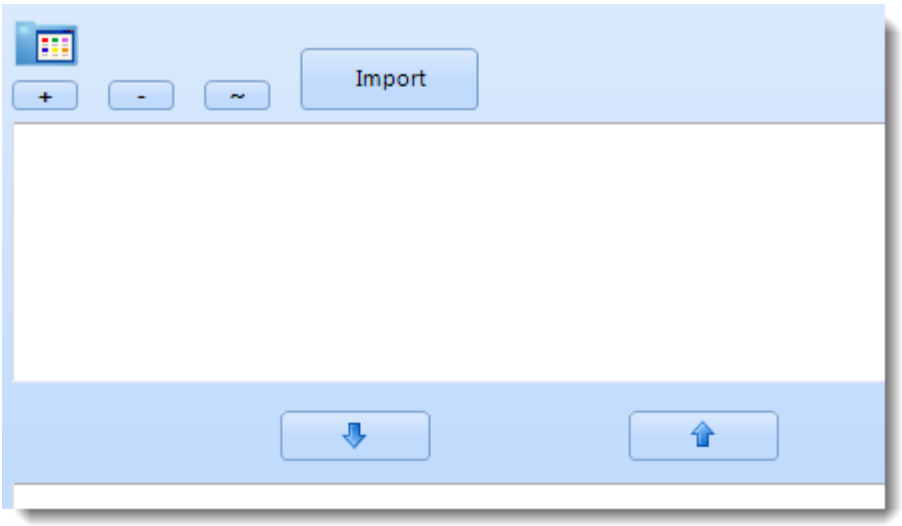
für eine Software und, und, und... Den Inhalt dieses Feldes können Sie ebenfalls per Hotkey[101] übertragen.

TOP[8]

Listen



Generell können Sie in den Listen beliebige Zeichenfolgen ablegen. Ideal geeignet sind die Listen zum Beispiel für Gutscheincodes oder Ähnliches.



Die **Schaltfläche +** öffnet den Dialog zur Eingabe eines neuen Listeneintrags, die **Schaltfläche -** entfernt den ausgewählten Listeneintrag, die **Schaltfläche ~** öffnet den Dialog zur Änderung des ausgewählten Eintrags.

Die **Schaltfläche Pfeil nach oben** verschiebt den ausgewählten Listeneintrag aus der unteren Liste in die obere. Die **Pfeil nach unten Schaltfläche** entsprechend von der oberen in die untere Liste.

siehe auch Listen nutzen[76]
siehe auch Hotkey für Liste[105]
siehe auch Zeige Bild an[109]

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

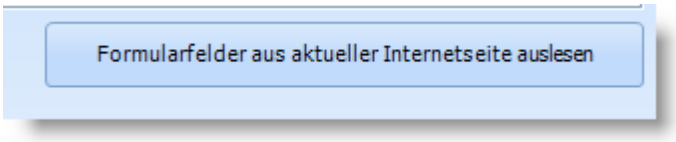
TOP[8]

Formular
Funktion steht nur für den Internet Explorer zur Verfügung

Müssen Sie oft den Inhalt eines Formulars ausfüllen. Dann hilft Ihnen diese Funktion sicher weiter. Zahlreiche Seiten erwarten neben Benutzername und Passwort weitere Daten. Die Nutzung der Formularfunktion erleichtert auch den Zugriff auf die Passwortdaten, da jetzt nur noch ein Tastendruck notwendig ist.

So richten Sie die Formularfunktion ein

Laden Sie die Seite, welche das Formular enthält im Internet Explorer. Füllen Sie das Formular aus und betätigen Sie anschließend die Schaltfläche "**Formularfelder aus aktueller Internetseite auslesen**".

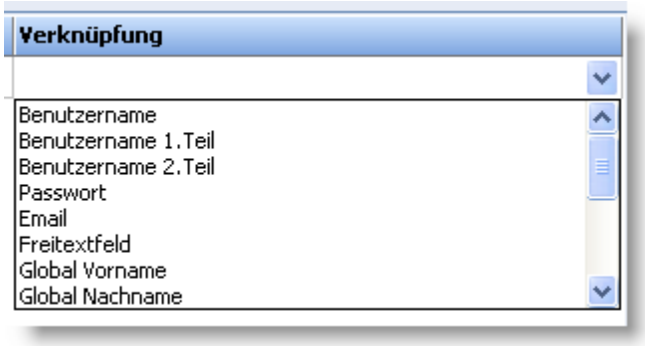


In der Spalte NAME sehen Sie die Namen der Formularfelder (*der Ersteller der Seite hat diese Bezeichnungen festgelegt, sie sind beliebig und ohne große Bedeutung für uns*), in der Spalte VERKNÜPFUNG sehen Sie die Werte, die Sie gerade eingegeben haben. Sie können diese Werte so übernehmen, oder die Formularfelder mit bestimmten Angaben im Passwort Safe verbinden.

So verbinden Sie ein Formularfeld mit einem Wert aus Ihrem Passwort Safe

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Doppelklicken Sie auf den aktuellen Wert in der Spalte **VERKNÜPFUNG** und wählen Sie einen Eintrag aus.



Einträge, die mit der Bezeichnung Global beginnen, beziehen sich auf Ihre Angaben unter Einstellungen - Autofill 113 . Einträge ohne diesen Zusatz beziehen sich auf die gleichnamigen Einträge im aktuellen Passwort Safe Eintrag.

Eine Besonderheit stellen die beiden Werte Benutzername 1. Teil und Benutzername 2. Teil dar.

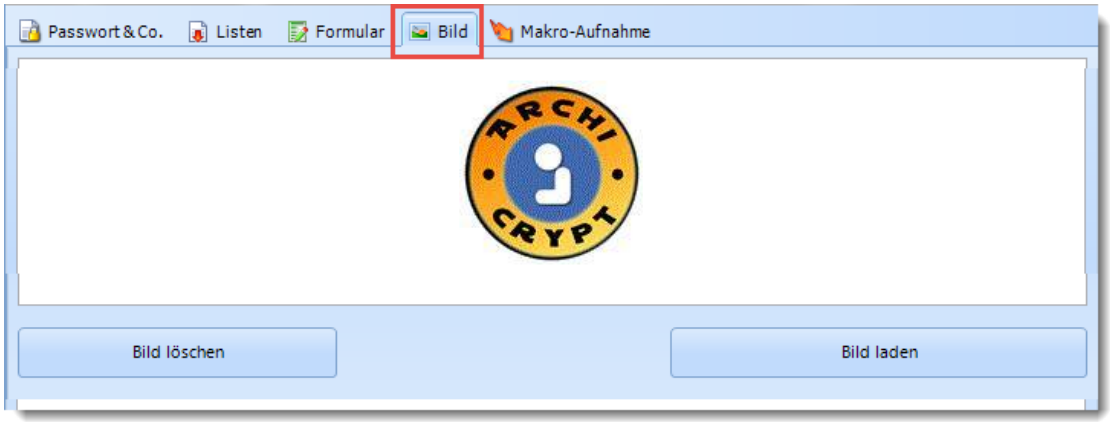
Wenn Sie auf der Seite Passwort&Co. im Feld Benutzername einen Eintrag der Form Vorne##Hinten machen, können Sie hier gezielt auf den vorderen (Vorne) und hinteren Teil (Hinten) des Textes zurückgreifen.

Dies ist zum Beispiel dann sinnvoll, wenn im Formular Vor- und Zuname benötigt werden. In diesem Fall geben Sie Vorname##Zuname ein.

siehe auch Einstellungen - Autofill 113

TOP 8

Bild



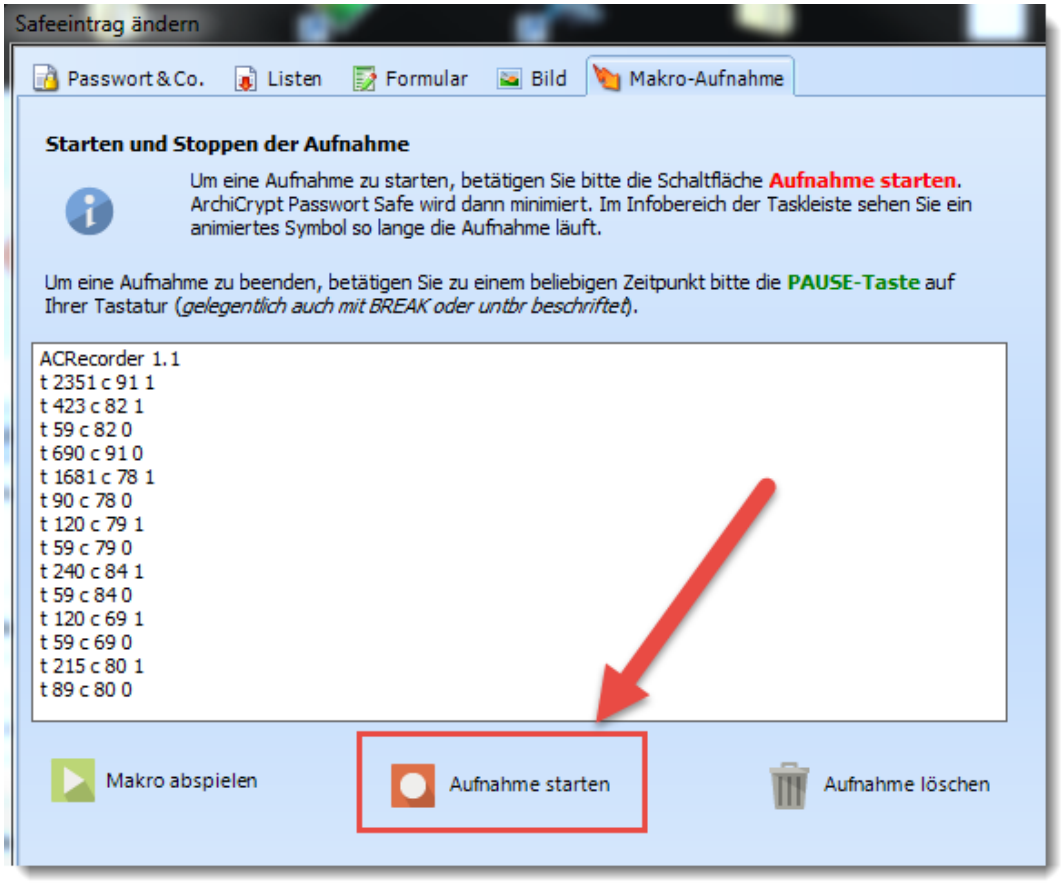
© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Ideal für vertrauliche Dokumente wie Bauzeichnungen, Schaltpläne, Notizzettel, Urkunden etc.

➡**ACHTUNG: Der Passwort Safe ist nicht darauf ausgelegt, große Mengen an Bildern aufzunehmen. Wenn Sie zu viele Bilder übernehmen, sinkt die Geschwindigkeit mit der Daten für eine Internetseite bereitgestellt werden unter Umständen erheblich. Ein paar Bilder sind jedoch kein Problem.**

Makro-Aufnahme

So zeichnen Sie Tastatur- und Mauseingaben auf



Mit dieser sehr nützlichen Funktion können Sie Tastatur- und Mauseingaben aufzeichnen und bei Bedarf wieder abspielen lassen. Die Aufnahme starten Sie, indem Sie die Schaltfläche **Aufnahme starten** betätigen. ArchiCrypt Passwort Safe wird jetzt minimiert, Sie sehen ein animiertes Symbol im Infobereich.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Führen Sie jetzt die Aktionen aus, die Sie aufzeichnen möchten. Wenn Sie die Aufnahme beenden möchten, betätigen Sie auf Ihrer Tastatur die **PAUSE Taste** (*auf manchen Tastaturen wird diese Taste auch mit BREAK oder untbr bezeichnet*).

Tipp zum Aufzeichnen von Makros:

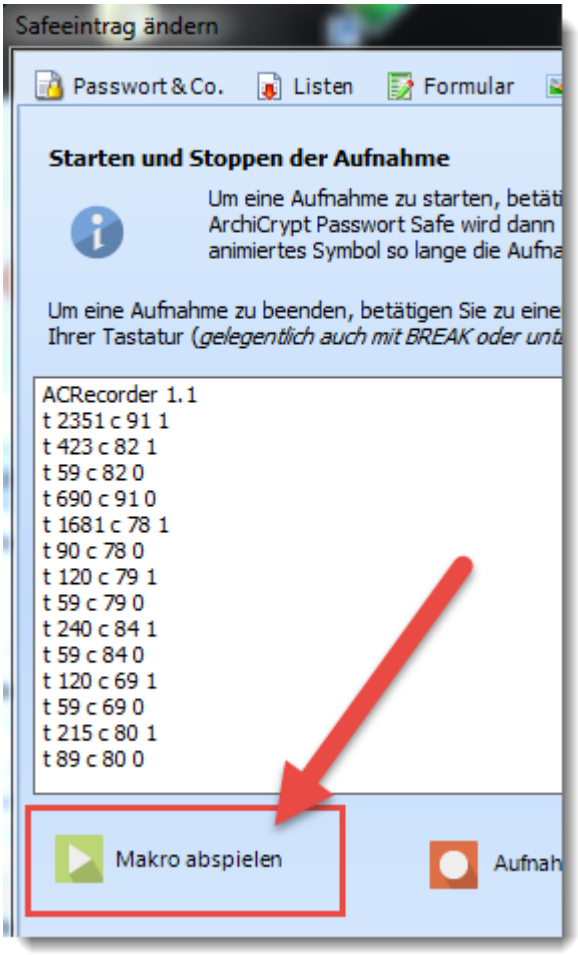
1. Sie sollten sich auf die Aufzeichnung vorbereiten und ggf. eine Art kurzes Drehbuch schreiben.

2. Beenden Sie möglichst alle Anwendungen, die für das Makro keine Rolle spielen.

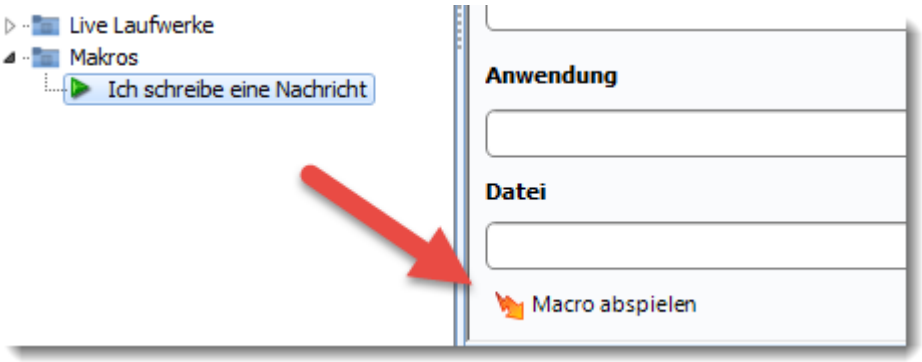
3. Die besten Ergebnisse erzielen Sie, wenn Sie mit Tastaturkürzeln (Hotkeys; Shurtcuts) arbeiten. Sie können Anwendungen meist komplett über solche Kürzel steuern. Sehen Sie ggf. in der Hilfe der jeweiligen Anwendungen nach, welche Hotkeys für die Erzeugung des Makros eine Rolle spielen und notieren Sie sich die Tastaturkürzel.

Sie können das Makro jetzt abspielen, indem Sie die Schaltfläche **Makro abspielen** betätigen.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Achten Sie darauf, dass Anwendungen, die das Makro starten soll, beendet wurden und Eingaben ggf. wieder zurückgesetzt wurden. Wenn Sie die Angaben für den Passworteintrag abgeschlossen haben, wird das Makro diesem Passworteintrag zugeordnet. Sie können das Makro künftig abspielen, wenn dieser Passworteintrag aktiv ist.

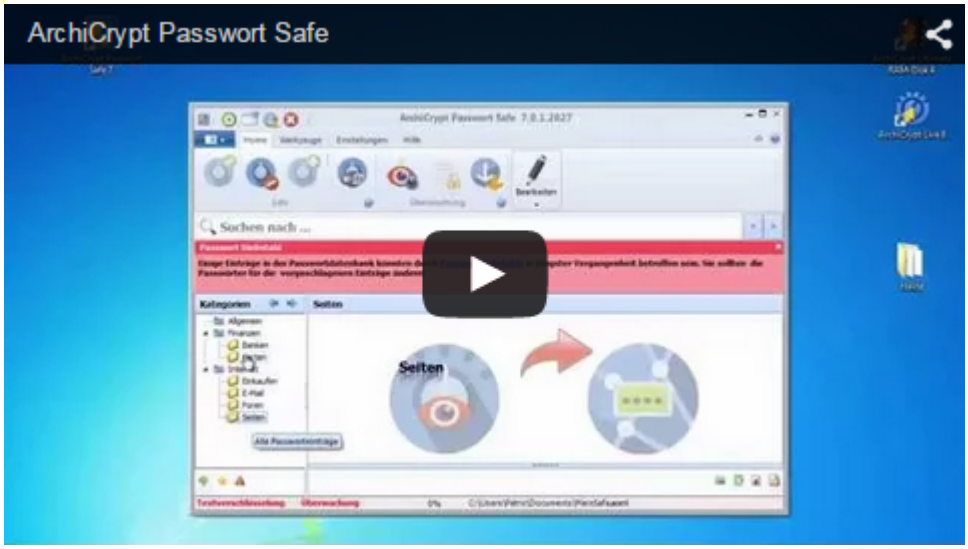


Wählen Sie dazu den Passworteintrag aus, oder richten Sie den Eintrag so ein, dass er beim Besuch einer WEB-Seite

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

automatisch aktiviert wird. Gestartet wird das Makro dann durch Klick auf die **Blitz-Schaltfläche**[75] oder mit Hilfe eines Tastaturkürzels, welches Sie in den Einstellungen[101] (*siehe auch* Einstellungen[86]) festlegen können.

Video Workshop ArchiCrypt Passwort Safe[23]



TOP[8]

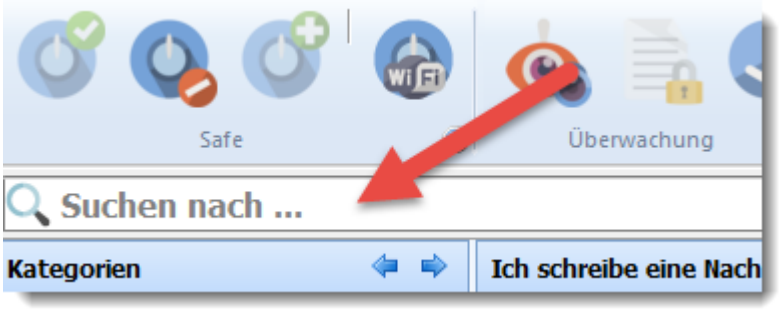
Folgende Themen könnten Sie ebenfalls interessieren:

Idee für ein Passwort[27]
So stellen Sie sicher, dass der Passwort Safe die Internetseite erkennt[17]
Menüleiste Bearbeiten[51]
Dialog für die Passworteingabe[28]
Informationen eines Passworteintrags[67]

10.2 Dialog zur Suche

In der Home Ansicht[27] haben Sie stets die Suchenleiste[43], mit der Sie in allen Feldern des Passwortsafes suchen können.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

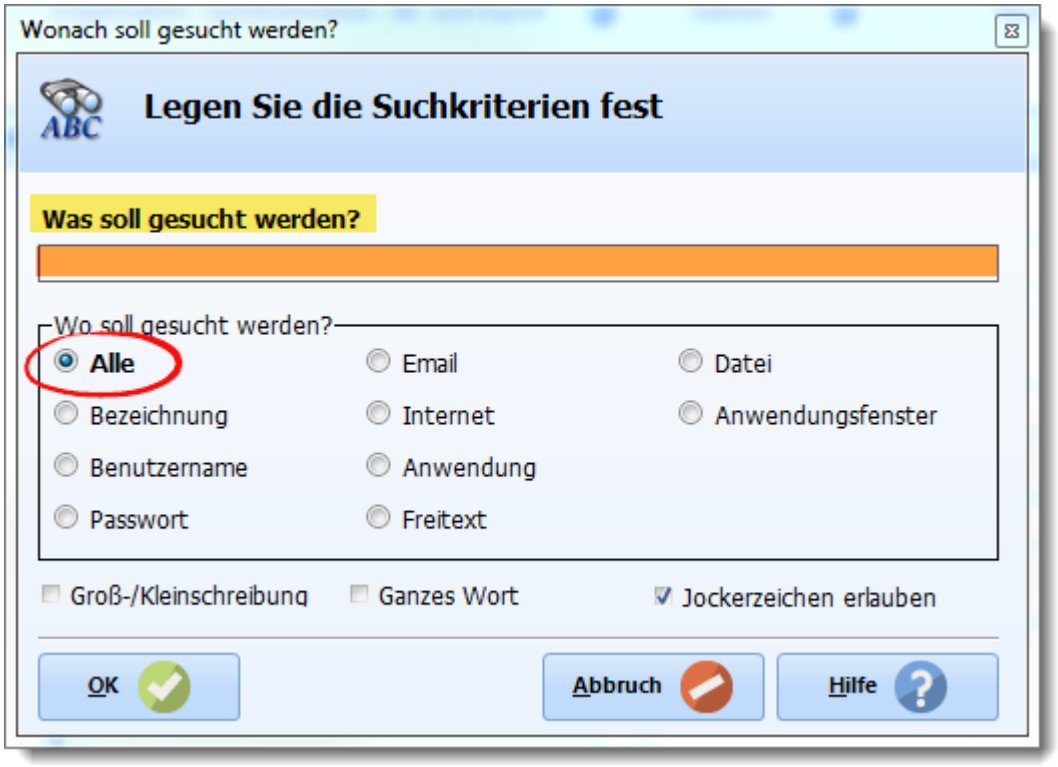


Sie können die Suche auf feinere Art durchführen, indem Sie bei Werkzeugen[54] die entsprechende Suchfunktion nutzen.

Den Dialog für die Suche erreichen Sie über die **Menüleiste Suchen**[54] , das **Hauptmenü Suchen**[46] oder, am schnellsten, über die Tastenkombination (Strg + F).

Alternativ können Sie aber auch direkt in der **HOME-Ansicht**[47] schnell in allen Feldern des Passworteintrags nach einem Begriff suchen[55].

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Wenn Sie **Alle** wählen, dann entspricht dies in der direkten Schnellsuche[55] in der **HOME-Ansicht**[47].

Folgende Themen könnten Sie ebenfalls interessieren:

Menüleiste Suchen[54]
Informationen eines Passworteintrags[67]
Schnellsuche[55]

10.3 Passworteingabe

Es gibt unterschiedliche Dialoge zur Eingabe von Passwörtern

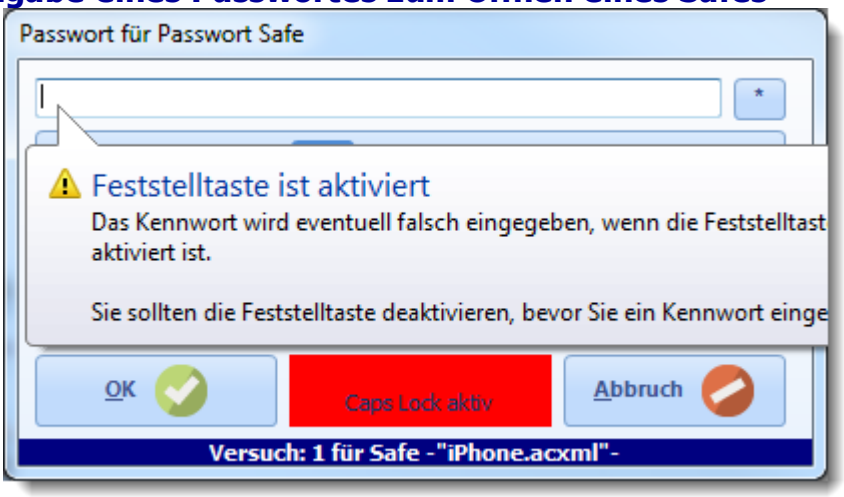
1. **Erstellen eines neuen Safes oder Änderung des Safe Passworts**
2. **Öffnen eines Safes**

Eingabe eines neuen Passwortes

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Geben Sie das gewünschte Passwort **1** ein. Um sicherzustellen, dass Sie sich nicht vertippt haben, geben Sie das Passwort zur Kontrolle nochmals in **2** ein. Sind beide Angaben identisch, können Sie das Passwort **Übernehmen**. Mit **3** rufen Sie die virtuelle Tastatur[31] auf.

Eingabe eines Passwortes zum Öffnen eines Safes

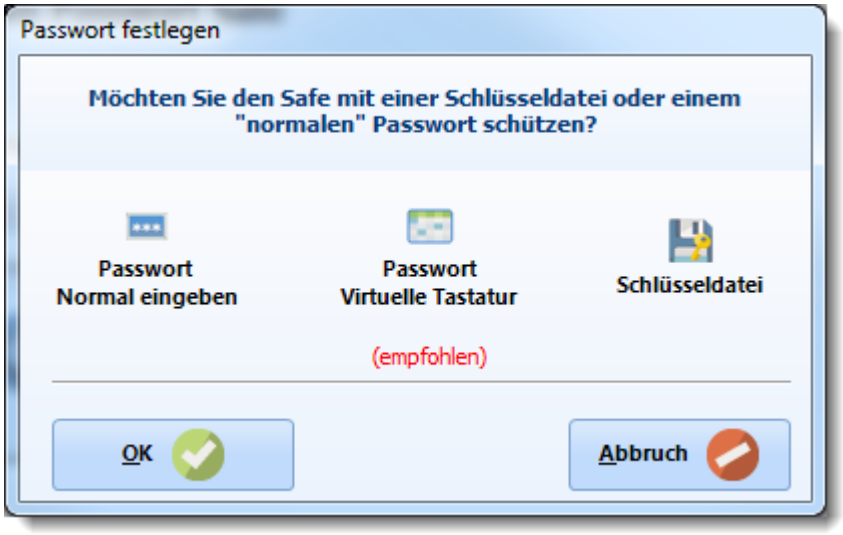


Dieser Dialog wird Ihnen angezeigt, wenn Sie einen Safe öffnen. Sie können das Passwort direkt eingeben, die virtuelle Tastatur nutzen, oder den Safe mit einer Schlüsseldatei[36] öffnen. Sie

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

erhalten eine Warnmeldung, falls ArchiCrypt Passwort Safe feststellt, dass die **Feststelltaste** aktiv ist.

Auswahl beim Erstellen eines neuen Safes

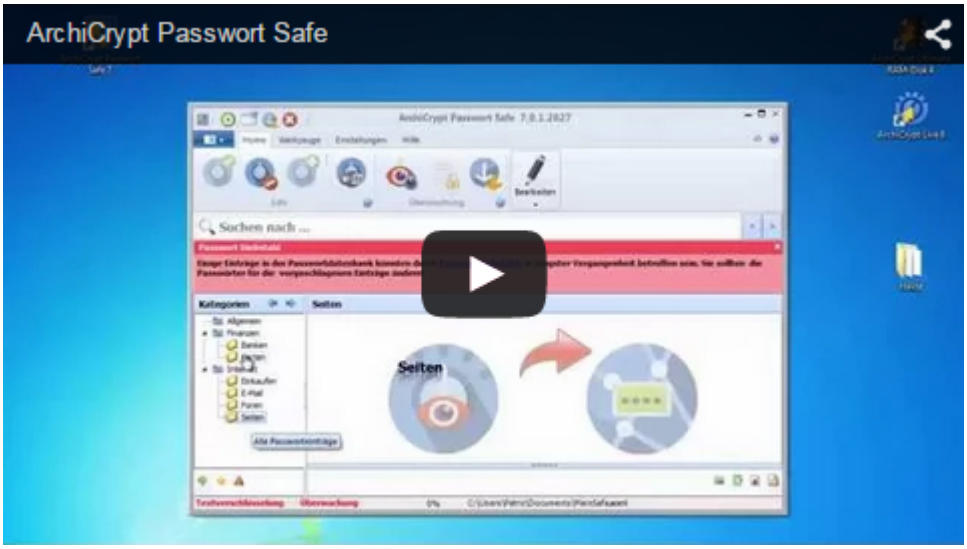


ArchiCrypt Passwort Safe bietet Ihnen beim Erstellen eines neuen Safes die Wahl, ob Sie den Safe mit einem **Passwort** oder einer s.g. **Schlüsseldatei** schützen möchten. Das Passwort können Sie entweder über die Tastatur eingeben (*Passwort Normal eingeben*) oder, sicher gegen **Keylogger** (*Programme die Tastatureingaben ausspionieren*), über die virtuelle Tastatur.

Je nach Wahl wird Ihnen der Dialog zur Eingabe eines neuen Passwortes[28] , die virtuelle Tastatur[31] , oder der Dialog zum Erstellen[33] oder Einlesen[36] einer Schlüsseldatei angezeigt.

Video Workshop ArchiCrypt Passwort Safe[23]

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



Folgende Themen könnten Sie ebenfalls interessieren:

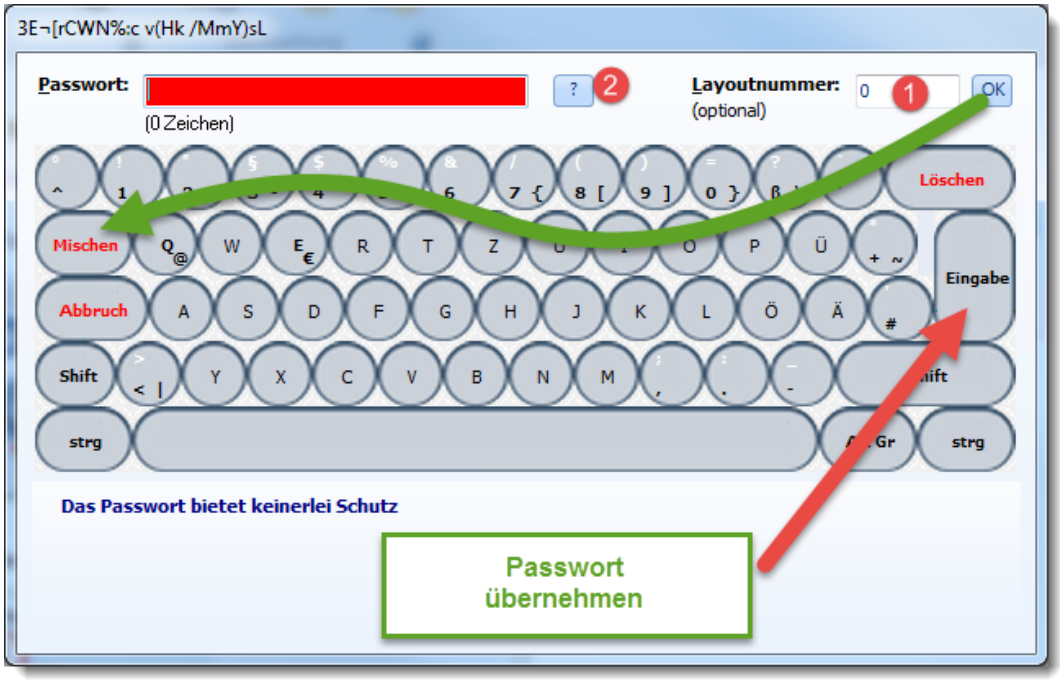
- So erstellen Sie einen Passwort Safe [30]
- Erster Start - So richten Sie ArchiCrypt Passwort Safe ein [27]
- So erstellen Sie einen Safeeintrag [8]
- So erzeugen Sie beim Surfen einen neuen Safe Eintrag [110]

10.4 Virtuelle Tastatur

So schützen Sie sich gegen Key-Logger

Die **virtuelle Tastatur** ist ein wirksames Mittel gegen s.g. Key-Logger (siehe Sicherheit [42]), die jede Eingabe in eine normale Tastatur protokollieren können.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt



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

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

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

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

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

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

10.5 Schlüsseldateien

Schlüsseldateien

Was ist eine Schlüsseldatei?

Eine Schlüsseldatei ist eine Datei, die Sie statt eines Passwortes nutzen können, um Zugang zu Ihrem Passwort Safe zu erhalten. Sie sparen sich so die Eingabe eines langen (*Schlüsseldatei entspricht ca. 32 Zeichen inkl. nicht druckbaren Zeichen*) und komplizierten Passwortes. Es gibt zwei Arten von Schlüsseldateien.

1. unverschlüsselte Schlüsseldatei (Schutz durch *physischen* Besitz)

Die unverschlüsselte Form der Schlüsseldatei ist vergleichbar mit Ihrem Hausschlüssel. Wer ihn besitzt, erhält Zugang zu Ihrem Haus. Zum Öffnen des Safes, Ver- und Entschlüsseln von Text und Dateien genügt entsprechend der Besitz der Schlüsseldatei. Sie müssen also sehr sorgfältig darauf achten, dass die Datei nicht in falsche Hände gelangt.

2. verschlüsselte Schlüsseldatei (Schutz durch Wissen und *physischen* Besitz)

Die verschlüsselte Variante ist mit Ihrer EC-Karte vergleichbar, mit der Sie nur Geld von Ihrem Konto abheben können, wenn Sie die Karte besitzen und die Geheimnummer kennen.
Zum Öffnen des Safes, Ver- und Entschlüsseln von Text und Dateien ist der Besitz der Schlüsseldatei und die Kenntnis des Passwortes notwendig. Ein Angreifer müsste Ihnen also die Schlüsseldatei entwenden und das Passwort ausspähen und stehlen. **Diese Variante bietet extrem hohen Schutz.**

Im Vergleich dazu handelt es sich bei einem normalen Passwort um einen reinen **Schutz durch Wissen**.

So erstellen Sie sich eine Schlüsseldatei

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Unverschlüsselte Schlüsseldatei

Betätigen Sie die Schaltfläche **Weiter >**, sammeln Sie nach Aufforderung, durch Bewegen der Maus, Zufallsdaten und legen Sie den Speicherort für die Schlüsseldatei fest.

Verschlüsselte Schlüsseldatei

Ähnlich wie bei Ihrer EC Karte, bei der nicht nur der Besitz der Karte genügt, sondern bei der Sie auch eine PIN kennen

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

müssen, benötigen Sie hier nicht nur die Schlüsseldatei, sondern zusätzlich auch ein Passwort.

Passwort eingeben

Schaltfläche **Weiter >** betätigen. Zeitliche Gültigkeit festlegen

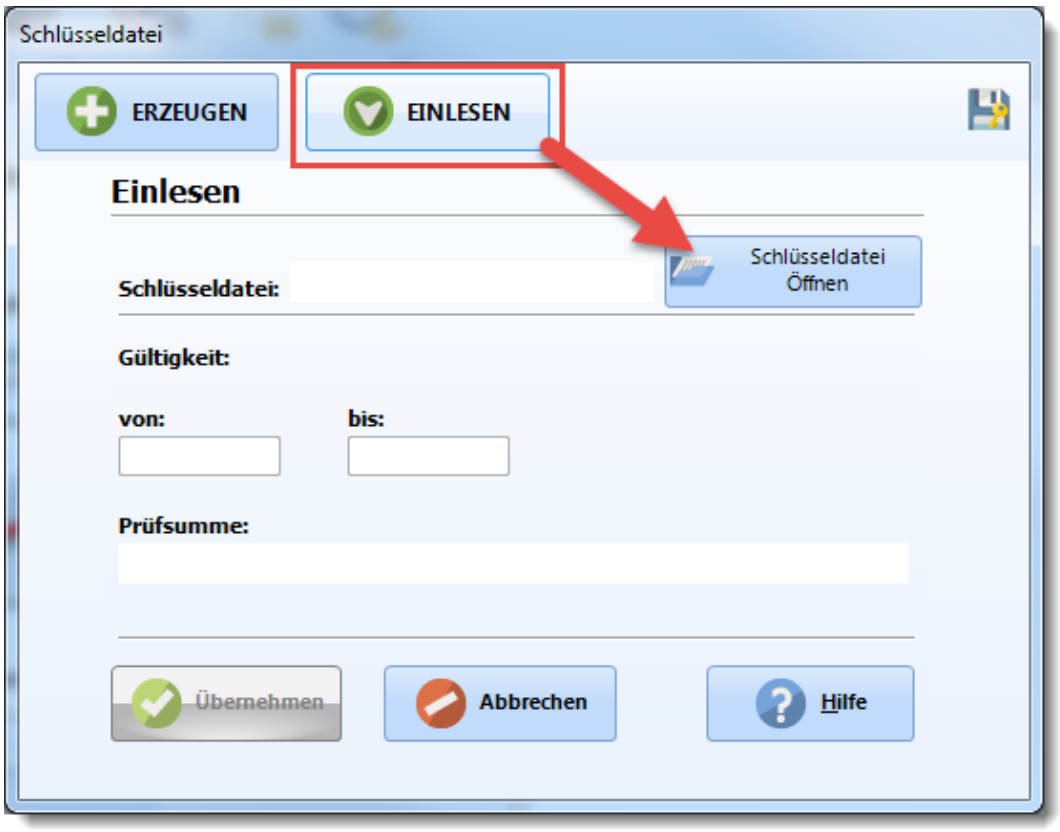
In diesem Schritt können Sie angeben, ob die Schlüsseldatei unbegrenzt, oder innerhalb zeitlicher Grenzen gültig ist. Beachten Sie bitte, dass es sich hierbei um keinen wirklichen Schutz handelt. Es ist lediglich eine Funktion, die **Sie** daran erinnert, ein Passwort nach einer bestimmten Zeit zu ändern.

Schaltfläche **Weiter >** betätigen und Speicherort für die Schlüsseldatei festlegen.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

TIPP: Legen Sie die Schlüsseldatei auf einem Wechselmedium (USB-Stick, CD, etc.) ab und fertigen Sie sich unbedingt eine Sicherungskopie an.

So lesen Sie Ihre Schlüsseldatei ein



Klicken Sie ggf. auf die Schaltfläche **Einlesen**. Klicken Sie dann auf Schlüsseldatei **Schlüsseldatei öffnen**. Falls die Schlüsseldatei mit einem Passwort geschützt ist, werden Sie zur Eingabe des Passwortes aufgefordert. Prüfsumme und ggf. vorhandenes Gültigkeitsdatum werden angezeigt. Klick auf **Übernehmen** schließt den Einlesevorgang ab.

Folgende Themen könnten Sie ebenfalls interessieren:

So stellen Sie sicher, dass immer in folgendem Verzeichnis nach einer Schlüsseldatei gesucht wird 93
Dialog für die Passworteingabe 28
Informationen eines Passworteintrags 67

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

11 Tastaturkürzel

In ArchiCrypt Passwort Safe können Sie nicht nur Funktionen mit Hilfe der frei definierbaren Hotkeys[101] aufrufen. Viele der Safe Funktionen selbst besitzen **vordefinierte Tastaturkürzel**.

Vordefinierte Tastaturkürzel	
Safe	
Neuer Passwort Safe	<STRG> + <ALT> + N
Öffne Passwort Safe	<STRG> + <ALT> + O
Schließe Passwort Safe	<STRG> + <ALT> + S
Kopieren nach ...	<STRG> + <ALT> + K
Passwort ändern	<STRG> + <ALT> + P
Import von Safedaten	<STRG> + <ALT> + Z
Export von Safedaten	<STRG> + <ALT> + X
Einstellungen	<F10>
Beenden	<STRG> + F4
Werkzeuge	
Passwort analysieren	<STRG> + <ALT> + U
Bearbeiten	
Neue Kategorie	<STRG> + K
Neuer Ordner	<STRG> + O
Neuer Safeeintrag	<STRG> + E
Safeeintrag bearbeiten	<F2>
Auswahl löschen	<STRG> + L
Suchen	
Suchen...	<STRG> + F
Weiter suchen	F3
Überwachung	
Text verschlüsseln	<STRG> + <W>
Überwachung starten	<STRG> + <I>
Standby	<STRG> + <R>
Hilfe	
Hilfe	<F1>
Ihre Hotkeys	

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Folgende Themen könnten Sie ebenfalls interessieren:

Menüleisten 45

12 Mobile Nutzung

12.1 Safe Portable

➡HINWEIS: Sie müssen, können und dürfen die Mobile USB Version mit Ihren Freischaltdaten aktivieren!

Was ist ein Safe Portable?

Ein Safe Portable ist eine spezielle Version, die auf einem Wechseldatenträger (*z.B. USB-Stick)*

➡Vorsicht: Einige USB-Sticks melden sich am System als lokales Laufwerk an. Auf diesen Sticks können Sie die mobile Version nicht installieren.

Somit können Sie die wesentlichen Funktionen von ArchiCrypt Passwort Safe auch unterwegs nutzen. Einfach USB-Stick an den jeweiligen Windows Rechner anschließen, ArchiCrypt Passwort Safe starten und los geht's. Alle Einstellungen und natürlich Ihre Passwort Datenbank werden auf Ihrem Wechseldatenträger gespeichert. Noch besser, wenn selbst die Datenbank nicht mitgeführt werden muss. Das können Sie zum Beispiel mit ArchiCrypt Passwort Safe Online erreichen.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Übersicht:

1. Der Safe Portable fragt beim Start das Passwort für den mitgeführten Passwort Safe oder den Passwort Safe im Internet[35] ab und stellt die Funktionen Überwachung[79], Textverschlüsselung[81] und Drag Drop Verschlüsselung[83] bereit.
2. Ein Safe Portable speichert seine Einstellungen (*Hotkeys, Autofill, etc.*) auf dem Wechselmedium.
3. Auf dem System auf dem Sie den Safe Portable nutzen, ist keine Installation nötig.
4. Das System bleibt nach Beenden des Programms und Entfernen des USB-Sticks unberührt.

Einschränkungen eines Safe Portable

Keine Möglichkeit selbst wieder einen Safe Portable zu erstellen.
Die portable Version kann nur eine **Safe Datenbank** verwalten (*Mob.acxml*)

So erstellen Sie einen Safe Portable

Zunächst müssen Sie mit Ihrer registrierten ArchiCrypt Passwort Safe Version den Safe laden[48], den Sie mobil nutzen möchten. Wechseln Sie zu den Werkzeugen[54] und betätigen Sie die Schaltfläche Safe Portable[62].

➡ ACHTUNG: SIE benötigen ca. 50 MB freien Speicherplatz auf dem Wechsellaufwerk!

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Legen Sie fest, wo der Safe Portable gespeichert werden soll. Das Ziel **MUSS** auf einem **Wechsellaufwerk** (*USB-Stick, SD-Speicherkarte*) liegen. ArchiCrypt Passwort Safe erzeugt jetzt Ihren Safe Portable.

Neben dem Safe Portable [**Datei ArchiCryptSafe.exe**] finden Sie im gleichen Verzeichnis weitere Module, die Sie jedoch nicht manuell aufrufen sollten. Der aktuelle Passwort Safe wurde als Kopie [**Datei Mob.acxml**] ebenfalls in diesem Verzeichnis abgelegt.

Sicher wissen Sie, dass man ArchiCrypt Passwort Safe nur genau einmal starten kann. Zum Testen des **Safe Portable** müssen Sie daher **ArchiCrypt Passwort Safe** (*PC-Installation*) zunächst beenden.

TIPP: Selbstverständlich ist es möglich, den Safe Portable auf einen Passwort Safe im Internet[35] zugreifen zu lassen. Dadurch entfällt dann (vor allem bei Zugriff via FTP[36]) die Notwendigkeit, verschiedene Versionen des Passwort Safes zu synchronisieren[56].

Sie können Passwort Datenbanken über das Safe Sender-Empfänger Modul[122] mit anderen Rechnern und mobilen Geräten austauschen. Da die mobile Version nur einen Passwort Safe verwalten kann, wird der auf dem mobilen Speicher abgelegte Safe Mob.acxml beim Empfang nach Rückfrage überschrieben!

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Folgende Themen könnten Sie ebenfalls interessieren:

Menüleiste Safe Portable (USB) erstellen 62
ArchiCrypt Passwort Safe - Online 128

13 Umgang mit der Software

13.1 Datenverlust vorbeugen

ArchiCrypt Safe ist kein Kinderspielzeug. Verschlüsselte Daten sind **unwiederbringlich verloren**, wenn das **Passwort nicht mehr verfügbar** ist.

Merken Sie sich das zum Schutz der Daten im Passwort Safe verwendete Passwort gut. Selbst wir als Hersteller der Software sind nicht in der Lage verschlüsselte Daten ohne Kenntnis des Passwortes zu entschlüsseln.

Informationen zur Sicherheit und über die eingesetzten Verfahren 42

Automatische Sicherungskopien (Backups)

Der Safe legt bei jedem Öffnen eines Safes eine **Sicherheitskopie** an. Die Sicherheitskopie wird im Verzeichnis der Safe Datei angelegt.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Sicherungen tragen den gleichen Namen wie der Safe zu dem sie gehören, gefolgt von einer Nummer in Klammern und der Dateiendung **bacxml**.

BEISPIEL:
Safe Datei
D:\Daten\MeinPasswortSafe.acxml
Automatische Sicherung:
D:\Daten\MeinPasswortSafe(2).bacxml

Es werden so immer mehrere Versionen eines Safes aufbewahrt. Bei einem Fehler oder versehentlichem Löschen können Sie so auf die gesicherte Version zurückgreifen. Einfach die Dateiendung von **bacxml** auf **acxml** ändern und Datei zum Beispiel per Doppelklick als Safe laden.

➡ **HINWEIS: Bei Passwort Safes, die im Nur-Lesen Modus geöffnet wurden, werden keine automatischen Sicherungen erstellt. Auch dann, wenn Sie in den Einstellungen unter Allgemeines - Backups das Erzeugen von Sicherungen deaktiviert haben, werden keine automatischen Sicherungen erzeugt.**

Bitte sichern Sie sich grundsätzlich regelmäßig die Safe Daten auf einem anderen Medium. Bei einem Hardware-Defekt nützen Ihnen die Sicherungen auf dem defekten Medium nichts.

13.2 Sicherheit

➡ **Trotz aller Maßnahmen, die bei der Gestaltung von ArchiCrypt Passwort Safe ergriffen wurden, raten wir dringend davon ab, die Software auf einem System zu nutzen, über deren Sicherheit Sie nicht informiert sind. Insbesondere in schlecht geführten Internet Cafés im Ausland könnte Schadsoftware installiert sein, die nicht nur Tastatureingaben protokolliert sondern auch den Netzwerkverkehr abhört, Bildschirmmitschnitte anfertigt etc. Auch Ihr heimischer PC sollte stets mit aktueller Antivirensoftware ausgestattet sein.**

MERKE: Auf einem unsicheren System nützt die beste Sicherheitssoftware nichts

Grundsätzliches

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Alle Daten *(Passwörter, Zugangsdaten, Bilddaten, Dateien, Freitext, etc.)* werden in einer Datei im so genannten **XML Format** abgelegt. Sie können diese Datei prinzipiell mit jedem Textprogramm öffnen. Alle Inhalte sind jedoch mit den unten aufgeführten Verfahren verschlüsselt, **zu jedem Zeitpunkt**. Auf dem Datenträger liegen somit **niemals** Klartextdaten Ihrer Passwortdatenbank. Auch dann nicht, wenn Sie die Passwortdatenbank mit Ihrem Passwort geöffnet haben. Bei offenem Passwortsafe werden die Einträge im Hauptspeicher Ihres Rechners gehalten, dort aber mit einem zufälligen Sitzungsschlüssel verschlüsselt. Erst, wenn auf die Daten im Passwort Safe zugegriffen wird, werden diese entschlüsselt. Wenn die Daten aus dem Safe an andere Anwendungen übertragen wurden, obliegt die Sicherheit der Daten diesen Anwendungen.

Die **Sicherheit in der Cloud** ist durch die Verschlüsselung der Passwortdatenbank gewährleistet. Diese bleibt in der Cloud zu jedem Zeitpunkt verschlüsselt. **Ihr Safe Passwort** wird weder in der Cloud noch auf Ihrem Rechner abgelegt.

Eingesetzte Verfahren

ArchiCrypt Passwort Safe setzt ausschließlich auf standardisierte Verfahren.

- Advanced Encryption Standard (AES; in der 256 BIT Version; CFB (*Cipher Feedback*) Modus)
- Hashverfahren SHA512
- Schlüsselableitungsfunktion PBKDF2
- Maskengeneratorfunktion MGF1.

Informationen zu AES finden Sie unter
http://de.wikipedia.org/wiki/Advanced_Encryption_Standard

Zufallszahlenpool

ArchiCrypt Passwort Safe sammelt ab Start Daten für einen **Zufallszahlenpool**. Dabei werden viele nicht deterministische Systemzustände und das Anwenderverhalten mit einbezogen. Die Änderung eines einzelnen Bits ändert den kompletten Datenpool. Bei Entnahme wird der Pool neu berechnet.

Vorgänge beim Erzeugen einer Passwortdatenbank

Folgende Werte werden aus dem Zufallszahlenpool erzeugt:

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Saltwert 1 der Größe 80 BIT

Saltwert 2 der Größe 80 BIT

Masterkey der Größe 800 BIT (*entspricht Passwort der Länge 100 Zeichen inkl. Groß-,Kleinbuchstaben, Ziffern,Sonderzeichen und nicht druckbare Zeichen. Mit diesem Masterkey werden die alle sensiblen Daten im Passwort Safe verschlüsselt.)*

Folgende kryptografische Berechnungen werden durchgeführt:

Der vom Anwender eingegebene Schlüssel (*Passwort/Schlüsseldatei*), **UserKey** genannt, wird mit Hilfe des Salt 1 Wertes in einer Schlüsselableitungsfunktion (*KDF;Key Derivation Function*) zum so genannten abgeleiteten Nutzerschlüssel (**Derived UserKey**). Zum Einsatz kommt PBKDF2 gemäß PKCS#5. Als Hashfunktion wird **SHA512** eingesetzt. Die Anzahl **Iterationen** (*iterations*) beträgt 50000.

Aus dem abgeleiteten Nutzerschlüssel, **DerivedUserKey**, wird zusammen mit dem Salt 2 Wert zunächst mit PBKDF2 und einer Iterationszahl von 1000 ein **Prüfwert A** (*checksum A*) berechnet.

Aus diesem **Prüfwert A** wird mit Hilfe einer **Mask Generation Function** (*MGF1 aus PKCS#1*) ein **Prüfwert A'** berechnet. Als Hashfunktion kommt SHA512 zum Einsatz.

Dieser **Prüfwert A'** wird mit dem Saltwert 2 konkateniert. Man erhält den **Prüfwert A''**=**Salt 2 + Prüfwert A'**

Abschließend wird der **Prüfwert A''** mit dem abgeleiteten Nutzerschlüssel zu **Enc(Prüfwert A'')** verschlüsselt.

Der **Masterkey** wird mit dem abgeleiteten Nutzerschlüssel verschlüsselt (**Encrypted MasterKey**).

Im Passwort Safe werden folgende Werte abgelegt:

Saltwert 1, Saltwert 2, Enc(Prüfwert A'') und der verschlüsselte Masterkey.

Vorgänge beim Öffnen einer Passwort Datenbank

Der Anwender gibt den potentiellen Schlüssel (*Passwort/Schlüsseldatei*) ein. Man erhält den **UserKey?**.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Anm.: Alle Werte, die mit einem Fragezeichen ? versehen sind, sind nur dann korrekt, wenn der eingegebene Schlüssel mit dem beim Erzeugen verwendeten Schlüssel übereinstimmt. Erst am Ende der Prüfroutine steht fest, ob dem so ist.

Folgende Daten werden aus der Passwortdatenbank eingelesen:

Saltwert 1
Enc(Prüfwert A'')
Verschlüsselter Masterkey

Folgende kryptografische Berechnungen werden ausgeführt:

Der **UserKey?** wird zusammen mit dem **Saltwert 1** an die Schlüsselableitungsfunktion **PBKDF2** übergeben. Genau so, wie beim Erzeugen der Datenbank. Man erhält **Derived UserKey?**. Dieser ist nur korrekt, falls **UserKey?** korrekt eingegeben wurde.

Jetzt wird mit Hilfe von **Derived UserKey?** der Wert **Enc(Prüfwert A'')** entschlüsselt zu **Prüfwert A'' ?** Auch hier erhält man nur dann den korrekten Wert, wenn die Eingabe korrekt war.

Dieser Wert wird aufgeteilt in
Salt 2?
und
Prüfwert A'?

Derived UserKey? und **Salt 2?** werden an die Schlüsselableitungsfunktion PBKDF2 übergeben und man erhält den **Prüfwert B**
Mit Hilfe der Mask Generation Function **MGF1** wird daraus der **Prüfwert B'** berechnet.

An dieser Stelle wird **Prüfwert A'? mit Prüfwert B'** verglichen. Sind beide identisch, ist **UserKey?** korrekt und stimmt mit **UserKey** beim Erzeugen der Datenbank überein. Wir können den UserKey verwenden um den verschlüsselten Masterkey zu dechiffrieren. Mit diesem entschlüsselten Masterkey werden die Einträge der Passwortdatenbank entschlüsselt.

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Index

- _ -

_FF_AutoLogin 16

- 2 -

256 BIT 42

- A -

Activate on startup 86
acxml 41
Add On 86
Advanced Encryption Standard 30, 42
aef 83
AES 30, 42
Aktivschutz 86
Aktualisieren 120
Alarm bei Passwort Diebstahl 9
Allgemeines 86
ALMailSlot 16
Änderung des Passworts 45
Änderung des Safe Passworts 28
Android 9, 120
Anti Spyware 86
Anti-Keylogger 24, 86
Anti-Keylogger umschalten 86
Antivirensoftware 42
Anwendung 67, 8
Anwendungsfenster 45, 67, 79, 8
Anwendungsspion 8
Anzeige der Kurzhilfe in Sekunden 86
ArchiCrypt Easy Encryption 81
ArchiCrypt FTE 81
ArchiCrypt im Internet 45
ArchiCrypt Live 45
ArchiCrypt Online-Disk 30
ArchiCrypt Online-Shop 3
ArchiCrypt PassOnPaper 45
ArchiCrypt Passwort Safe - über das Internet laden 128
ArchiCrypt Passwort Safe bei Inaktivität schließen nach 86
ArchiCrypt Passwort Zentrale 120
auf neue Version prüfen 86
Auflösung 1, 8
Aufnahme starten 8
Aufruf Passwort Safe 86
Ausgabe der ArchiCrypt PassOnPaper Karte 1
Ausgabeart 1
Ausgabeformat 1
Ausgehende Safes 120
Aussehen 86
aussprechbare Passwörter 24, 86
Austausch mit SmartPhone und Tablet 23
Austausch ohne Drittanbieter 120
Austausch über Drittanbieter 120
Austausch von Passwortdatenbanken 23
Auswahl beim Erstellen eines neuen Safes 28
Auswahl Favoriten im Infobereich führt keine Aktion aus 86
Auswahl löschen 45
Autofill 86
Autoit 16
Automatisch letzten Passwort Safe öffnen 86
Automatische Sicherungskopien 41
Automatisches Ausfüllen der Login Daten versuchen 86
Automatisches Login 23

- B -

Backups 86, 41
bacxml 86, 41
Bauzeichnungen 8
Bearbeiten 9
Bearbeiten Menü 23
Bei FTP geänderte Daten im Hintergrund übertragen 86
Bei FTP grundsätzlich keine automatischen Backups erzeugen 86
Beim Öffnen History als Auswahl anzeigen 86
Beim Start Favoriten anzeigen 86
Beim Start prüfen, ob neue Version verfügbar ist 86
Beim Start Überwachung starten 86
Benutzername 23, 67, 8
Benutzername 1. Teil 8
Benutzername 2. Teil 8

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Benutzeroberfläche 23
Bequemlichkeit 6
Bestellmöglichkeiten ArchiCrypt Passwort Safe 3
Besuchen aktiviert Überwachung 86
Betriebssystem 15
Bezeichnung 23, 8
Bild 67, 8
Bild laden 8
Browser 86
Browser überwachen 23

- C -

CFB 42
Cipher Feedback 42
Cloud Anbindung 9
Cloud Dienste 30, 120
Coud Anbieter 9
CSV Datei 45

- D -

Datei 67
Dateiendung acd 27
Dateiendung aef 83
Dateiendung bacxml 41
Daten importieren 45
Datenbank senden 45
Datendiebstahl 9
Der klassische Passwortgenerator 86
Derived UserKey 42
Detailansicht 23
Diebstahl Alarm 9
Diebstahl von Nutzer- und Passwortdaten 9
Diebstahl von Nutzerdaten 6
Dienstanbieter 9
Diese Zeichen können Sie noch nutzen 1
Download als .ZIP Archiv 128
Drag & Drop Verschlüsselung 83
Drag and Drop Component Suite 16
Drag&Drop 39, 45
Dropbox 120

- E -

EC-Karte 33
Edge Browser 86
eigene WEB-Seite 30
Eigener Zeichensatz 86
Ein gutes Passwort 126
Eine Safe Datei senden 120
Eine Safe-Datenbank versenden 120
Eingabe des Masterpasswortes 1
Eingabe eines neuen Passwortes 28
Eingabe eines Passwortes zum Öffnen eines Safes 28
Eingabe von Bezeichnung und Passwort bzw. PIN 1
Eingabe von Passwörtern 28
Eingesetzte Verfahren 42
Einschränkungen eines Safe Portable 38
Einstellungen 45
Einstellungen anpassen 23
Eintrag als Favorit 45
Eintrag löschen 23
Eintrag suchen 86
Eintrag verschieben 23
Einträge organisieren 23
E-Mail 8
E-Mail Adresse 67
E-Mail erstellen lassen 67
Endlosschleife 86
Entfernen-Taste 45
Erkennen einer Internetseite 23
Erstelle neuen Safe Eintrag 86
Erstellen einer Kopie 39
Erstellen von Safe Portable 45
Erweiterte Kurzhilfe anzeigen 86
Erzeugen aussprechbarer Passwörter 86
Es gibt mehrere Seiten, auf denen Sie die Daten dieses Safeeintrags nutzen 8
Export 45, 67
Export components for Delphi. 16
Export der Safedaten 45

- F -

Fahrrad 5
Farbcode 1
Fast Text Encryption 81
Favorit 39, 45
Favorit festlegen 23
Favoriten 23
Featurematrix Browser 86

Federal Information Processing Standards Publication 181 86
Fehlermeldungen des FTP Servers 30
Fenster- und Anwendungsspion 8
Feststelltaste 28
FF.au 16
FIPS PUB 181 86
Firefox 86
Formular 67, 8
Formularfelder aus aktueller Internetseite auslesen 8
Formularfüller 86
Formularfunktion 8
Formularwerte 67
Freitextfeld 67, 8
FTP Login 30
Fülle Formular aus 86

- G -

Ganzes Wort 26
GDrive 120
Geeignetheit verschiedener Passwortarten für PassOnPaper 5
Gehe zur nächsten Fundstelle 86
Geheimnummer 33
generische Modus 86
Google Chrome 86
Google Drive 120
Grafik 67
Graustufenbild 8
Groß-/Kleinschreibung 26
gute Passwörter 126
gutes Passwort 24

- H -

Hardware-Defekt 41
Hashverfahren 42
Hauptmenü 39, 45
Hilfe 23
History 30, 86
History Auswahlfeld 30
History Liste 9
History löschen 86
Home 45
Hotkeys 86, 37
Hotkeys einrichten 23
Hotkeys verwenden 23
htaccess 30
HTTPS 30

- I -

im eigenen Netzwerk 120
Import 45
importieren Sie Passwort-Daten 45
Indizierte TAN Verfahren 8
Infobereich 45, 79
Internet 67, 8
Internet Explorer 86
Internet und Anwendungsfenster 8
Internetseite für Safeeintrag 23
Internetseiten 67, 79
Internetseiten besuchen 67
internetsicher 86
Internetverbindung 30
iOS 120
iPhone 9

- J -

Jetzt auf neue Version prüfen 86

- K -

Kategorie erstellen 23
Kategorie-Ansicht 39
Kategorie-Kontextmenü 45
Kategorien 39, 45
Kategorien automatisch erweitern 86
Kategorien und Ordner 23
KDF 42
Keine automatische Sicherung von Passwort Safes anlegen 86
Kennwort 67
Key Derivation Function 42
Keylogger 28
Key-Logger 31
Klartextansicht 67
klassischen Passwortgenerator 86
kleinere Dateien 67
Koffer 5
Kombination 5

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Kompatibilitätsmodus 86
Kontextmenü 8
Kontextmenü Systemtray 23
Kontextmenü-Systemtray 86
Konverter 27
Kopieren nach 45
kryptografische Berechnungen 42
Kurzhilfe 8

- L -

LAN 9, 45, 120
Layoutnummer 31
letzte Datenbank 86
Link-Generator 128
Listen 67, 8
Listen mit Hotkeys drucken 23
LogBuch 86
Lösche Dateien 128
Lösche Zwischenablage 86
Lupe 8

- M -

Makro 67, 8
Makro abspielen 86, 8
Makro ausführen 67
Makro-Aufnahme 8
MAPI 67
Mask Generation Function 42
Maskengeneratorfunktion 42
Masterkey 42
Masterpasswort 1, 5
Mehrfachverwendung 24
Menüleiste Bearbeiten 45
Menüleiste Dateien 45
Menüleiste Organisation 45
Menüleiste Safe 45
Menüleiste Suchen 45
Menüleiste Überwachung 45
Menüleisten 23, 39
MGF1 42
Minileiste 45
Minimale Anforderungen 15
Mit Windows starten 86
Mob.acxml 38
Mobile Versionen 24
MozRepl 86
MozRepl Installation für Firefox 86

- N -

Nach Index des Listenelements fragen 86
Nachricht bei Überwachung 86
Nachrichtenfenster 79
Navigations-Menü 128
Netzwerk-Kommunikation 86
Netzwerk-Kommunikation anzeigen (hilfreich bei Fehlersuche) 86
Neue Kategorie erstellen 45
neue Version 45, 86
Neuer Ordner 45
Neuer Passwort Safe 45
Neuer Safeeintrag 45
Neuerungen 9
Neues Passwort zur Zwischenablage 86
Notizzettel 8

- O -

Öffne Passwort Safe 45
Online-Banking 8
Optik 86
Ordner 45
Ordner erstellen 23
Overbyte ICS InternetComponent Suite 16

- P -

PassOnPaper 24
PassOnPaper Karte 1
Passwort 23, 67, 8
Passwort & Co. 8
Passwort an Archicrypt Live senden 45
Passwort ändern 45
Passwort Datenbank aufräumen 9
Passwort Dialog 23
Passwort Diebstahl Warnung 23
Passwort Eintrag suchen 23
Passwort für Internetseite erzeugen 23
Passwort Generator 126
Passwort Generator nutzen 23
Passwort im Klartext anzeigen 67
Passwort mit Benutzername koppeln 86

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Passwort Safe aufräumen 45
Passwort Safe beenden 45
Passwort Safe im Alltag 23
Passwort Safe laden 23
Passwort Safe schließen 23
Passwort Safe Upload 128
Passwortdetails 39, 67
Passwortdiebstahl-Warnung 39
Passworteintrag 39
Passworteintrag erstellen 23
Passwörter bewerten 45
Passwörter für Internetseiten. 126
Passwortgenerator 23, 86
Passwortlänge 86
Passwortliste erzeugen 86
PBKDF2 42
PC Version 120
Permanentschutz 86
Persönliche Dateien einsehen 128
PIN 1
PKCS#1 42
PKCS#5 42
portable Passwort Safe Version 3
Portable Version 38
Portable Version registrieren 38

- Q -

QR Code 45
QR Passcode 45
QR Passcode Generator 45

- S -

Safari Browser 86
Safe Datenbank von PC zu PC 23
Safe erstellen 23
Safe Passwort ändern 45
Safe Portable 45
Safe Portable erstellen 45
Safe senden 120
Safe Sender-Empfänger 38
Safe Sender-Empfänger Modul 38
Safe ToGo 27
Safedatenbank kopieren 45
Safeeintrag 67
Safeeintrag bearbeiten 45
Safeeintrag klonen 45
Safeeintrag kopieren 45
Safeeinträge erstellen 23
SafeXChange Tool 45
Salt 42
Saltwert 42
Schaltfläche Download 128
Schaltpläne 8
schlechte Passwörter 126
Schließe Passwort Safe 45
Schlüsselableitungsfunktion 42
Schlüsseldatei 30, 67, 86
Schlüsseldatei auf einem Wechselmedium 33
Schlüsseldatei entspricht ca. 33
Schlüsseldatei immer suchen unter 86
Schlüsseldatei öffnen 33
Schlüsseldateien 33
Schnelle Variante für ein neues Passwort 8
Schutz 86
Schutz durch Besitz 33
Schutz durch physischen Besitz 33
Schutz durch Wissen und Besitz 33
Seriennummer ArchiCrypt Passwort Safe 3
SHA512 42
Shift-Taste 31
sicheres Passwort 86
Sicherheit der Daten 30
Sicherheit in der Cloud 42
Sicherheit von PassOnPaper 5
Sicherheitsbewußtsein 6
Sicherheitscode 1
Sicherheitskopie 41
Sicherungskopie 86, 33
Sie ändern Sie Einstellungen 86
Sie befinden sich gerade auf der Internetseite, zu der Sie einen Eintrag erstellen möchten 8
Sie haben ein Passwort in der Windows Zwischenablage 8
Sie möchten an einem bestimmten Datum erinnert werden 8
Sie möchten die Seite manuell eingeben 8
Sie möchten eine Schlüsseldatei erzeugen oder nutzen 8
Sie möchten sehen, was im Passwortfeld steht 8
Sie möchten selbst ein Passwort eingeben 8
Signal bei Überwachung 86
Signale bei Textverschlüsselung 86

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Sitzungsschlüssel 42
So ändern Sie das Passwort für Ihren Passwort Safe 45
So ändern Sie Einstellungen 45
So bringen Sie ArchiCrypt Passwort Safe bei, beim Erscheinen eines Dialogs ein bestimmtes Passwort bereit zu stellen 8
So entschlüsseln Sie Dateien mit ArchiCrypt Passwort Safe 83
So entschlüsseln Sie Ihre Passwörter mit der ArchiCrypt PassOnPaper Karte 1
So erstellen Sie eine Kopie Ihres Safes 45
So erstellen Sie einen neuen Passwort Safe 30
So erstellen Sie einen Safe Portable 38
So erstellen Sie sich ein sicheres Passwort für eine Internetseite 86
So erstellen Sie sich eine Schlüsseldatei 33
So finden Sie rasch einen bestimmten Safeeintrag 45
So importieren Sie Passwort-Daten 45
So können Sie die Grafik wieder unverschlüsselt speichern 67
So können Sie eine verschlüsselte Textnachricht entschlüsseln 81
So laden Sie Ihren Passwort Safe aus dem Internet 30
So lesen Sie Ihre Schlüsseldatei ein 33
So nutzen Sie ArchiCrypt Passwort Safe - Online 128
So nutzen Sie den Passwort Safe um ein ArchiCrypt Live Laufwerk zu laden 67
So nutzen Sie den Safe beim iTAN-Verfahren 8
So richten Sie die Formularfunktion ein 8
So rufen Sie die Hilfe zu einer Funktion auf 45
So schützen Sie sich gegen Key-Logger 31
So sehen Sie sich die Informationen zu einem Passworteintrag an 67
So sicher sind Ihre Daten im Safe 30
So speichern Sie die Datei unverschlüsselt auf Ihrem Rechner 67
So starten Sie die Überwachung 79
So stellen Sie sicher, dass der Passwort Safe die Internetseite erkennt 8
So stellen Sie sicher, dass immer in folgendem Verzeichnis nach einer Schlüsseldatei gesucht wird 86
So stellen Sie sicher, dass sich der Safe schließt, wenn Sie Ihren Rechner verlassen 86
So tauschen Sie sicher Textnachrichten per E-Mail aus 81
So übertragen Sie die Daten per Tastenkombination in Ihren Browser 86
So verbinden Sie ein Formularfeld mit einem Wert aus Ihrem Passwort Safe 8
So verschlüsseln Sie Dateien mit ArchiCrypt Passwort Safe 83
So versenden Sie verschlüsselte Daten per E-Mail 83
So zeichnen Sie Tastatur- und Mauseingaben auf 8
Social Engineering 24
Sofortiges Speichern 9
Speicherort 30
Spionageprogramme 31
SSL 30
Standardmaße 45
Standby 45
Standby Modus 23
Standby-Modus 45
Suchbegriff 9, 39, 26
Suche 9, 39
Suchenleiste 26
Suchfeld 39
Suchfunktion 26
Suchkriterien 45
Symbol 8
Symbol im Infobereich 45
Symbol im Systemtray 23
Symboltastatur 31
Synchronisation 45
Systemtray 45

- T -

TAN 1
Tastaturkürzel 86, 37
Tastenkombination 86
Tausendsassa 23
Telefonbanking 1
Testpasswort erzeugen 86
Text verschlüsseln 45
Textinformationen 67
Textverschlüsselung 67, 81
Tipp zum Aufzeichnen von Makros 8
Tipps zum Passwort 23
Trenner nutzen 86
Tresor 5
Trick 1 (Portalseite) 8

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt

Trick 2 (Platzhalter) 8

- U -

Übernehmen 33
Übertragen von Passwort Safes im LAN 9
Überwachung 45, 79
Überwachung starten 45
unterschiedliche Dialoge zur Eingabe von Passwörtern 28
unverschlüsselte Schlüsseldatei 33
URL in Title 86
URL per E-Mail 128
USB Version 38
USB Version aktivieren 38
UserKey 42

- V -

Verbrauchten Listeneintrag verschieben 86
verdeckte Eingabe 31
Verfalldatum 9
VERHALTEN 86
VERKNÜPFUNG 8
verschlüsselte Schlüsseldatei 33
Verschlüsselung 83
Verschlüsselung von Texten 24
Versuch nach Eingabe automatisch Login abzuschließen 86
Vielen Dank, dass Sie sich für ArchiCrypt Passwort Safe entschieden haben! 6
virtuelle Tastatur 28, 31
Vollverschlüsselung 24
vordefinierte Tastaturkürzel 37
Vordergrund-Modus 45

- W -

Warnungen 23
Was funktioniert mit welchem Browser? 86
Was ist eine Schlüsseldatei? 33
Was ist ein Safe Portable 38
Was soll gesucht werden 26
Was tun, wenn der Empfänger keinen ArchiCrypt Passwort Safe besitzt 81
Was tun, wenn Sie einen Passwort Safe via FTP geöffnet haben und die Verbindung zum Internet abbricht? 30
Wechseldatenträger 38
Weitere Bestellmöglichkeiten 5
Welche Angaben müssen beim Erstellen eines Passworteintrags gemacht werden? 8
Werkzeuge 45
WiFi 45
WiFi LAN WLAN Modul 23
WiFi Modul 120
Windows 10 9
WLAN 9, 45, 120
Wo möglich, Virtuelle Tastatur zur Eingabe von Passwörtern nutzen 86
Wo soll gesucht werden 26
Wörterbuchattacken 24
www.Passwort-Zentrale.de 126

- X -

XML Format 42

- Y -

Youtube 23

- Z -

Zahlenschloss 5
Zahlenschlösser 1
Zeichensatz vorschlagen 86
Zeige Bild an 86
Zufallsdaten 86, 33
Zufallszahlenpool 42
Zugangsdaten 9
Zugangsdaten zu E-Mail Postfächern 9
Zugriff über http oder https 30
Zugriff via FTP 30
Zusammenarbeit mit Browser sicherstellen 23
Zwischenablage 67

© 2002-2017 Softwareentwicklung Patric Remus - ArchiCrypt