PASSWORT TRESOR V3.0 mit Start PIN

USB Gerät zum „Hackersicheren“ abspeichern und automatischen ausgeben von Texten. Wie Passwörter, Login-Daten, Internet Lesezeichenliste, wiederkehrende Text usw.

Damit die Daten nicht via USB Laufwerk sichtbar sind, wird die »USB Stick-funktion« beim Start des Passwort Tresors ausgeschaltet.

Im Auslieferzustand ist der Passwort Tresor mit Demodaten geladen.
Änderung der Demodatei wird auf den nächsten Seiten beschrieben.

Anwendung des Demomodus.

1. Passwort Tresor im USB Port des Computers einstecken.
   Der Passwort Tresor kann an dem USB Port eingesteckt bleiben.
   Damit der PC sicher auf startet ist der Passwort Tresor mit einer Startverzögerung von 3 Minuten eingerichtet. Die Startzeitverzögerung kann durch 2 x Drücken des Drehknopfes am Passwort Tresor abgebrochen werden.

2. Die PIN Eingabe ist in der Demo ausgeschaltet.
   Ist die PIN Abfrage eingeschaltet und wird ein falscher PIN eingegeben, dann dauert es 30 Sekunden bis ein neuer PIN eingegeben werden kann.

3. Zum Ansehen der Datenausgabe, eine Textverarbeitung oder ein Editor am PC öffnen.

4. Das Textprogramm anklicken damit es für Texteingabe bereit ist.

5. Drehknopf am Passwort Tresor auf einen der Einträge einstellen und danach den Drehknopf einmal kurz drücken.

6. Auf dem Bildschirm erscheint die Ausgabe der gespeicherten Informationen.

Eigene Passwörter eingeben & PIN Abfrage einschalten.

Um die **Dateien PWData.txt und Lock.txt zu editieren** muss der »USB Stick« aktiviert werden. **Dazu muss während dem EINSTECKEN des USB Steckers der Drehknopf vom Passwort Tresor gedrückt sein. Bis die LED anfängt zu Blinken oder das Display eingeschaltet ist.**

Danach sind die Dateien via USB Laufwerk zugänglich.

ACHTUNG: der USB Speicherbereich ist nur wenige MB gross. Das reicht zwar für ein paar Tausend Texteinträge, aber andere Daten als **PWData.txt** und **Lock.txt** sollten nicht gespeichert werden. Ebenso sind in dem Modus der Programmcode sowie die zugehörigen Dateien sichtbar. Änderungen an den Dateien können das Gerät Funktionsunfähig machen. Es muss dann eventuell alles neu aufgesetzt werden.
(Die Systemdateien sind auf einem Windows PC als "nicht sichtbar" markiert.)

Die Passwortdateien sind in dem Textfile **PWData.txt** & **Lock.txt** geschrieben. **Der Text muss mit einem Editor** geschrieben werden. Z.B. Notepad, Word geht nicht weil dort Steuerzeichen mitgespeichert werden.

Die Dateien **PWData.txt** und **Lock.txt dürfen nicht in einen Ordner verschoben werden**.

Die Datei **Lock.txt** muss 4 Zahlen enthalten ohne ENTER. Also nur eine Zeile.
Die 4 Zahlen bilden den PIN zum Freischalten des Passwort Tresors.
Falls KEIN PIN am Start erwünscht ist, dann muss die Datei Lock.txt 0000 enthalten.

Auf dem »USB-Stick-Bereich« befinden sich im Lieferzustand die DEMO Files **PWData.txt** & **Lock.txt.** Der PIN Startschutz ist ausgeschaltet. *(Die Datei Lock.txt enthält 0000)*
Als Daten sind 5 Datensätze eingegeben.

Folgender **PWData.txt** Dateiaufbau pro Datensatz ist nötig:

° **Bezeichnung** der Dateifunktion (wird auf dem Display angezeigt)

° **PWSTARTx** Start des Datensatzes mit fortlaufender Nummer X

° Datentext Linie 1 Datenausgabetext

° Datentext Linie 2 Datenausgabetext

° usw.

° **PWENDx** Ende des Datensatzes mit gleicher Nummer X wie PWSTART.

° Am Ende der Datendatei **PWData.txt** muss noch eine Infolinie stehen. *Z.B.* ***Version 2.0***

Beispiel PWData.txt:

Email Demo PWSTART1 https://smf.pcaarburg.ch/zzzpwt/PasswordSafeTestDemo.html Smurfy@home.com hiThereThisiSMyNew12945%LonGPa%WordsSince983(use)(passworSaFe PWEND1	Datensatz 1
Wetterprognose PWSTART2 https://www.srf.ch/meteo PWEND2	Datensatz 2
Text in Word PWSTART3 Vielen Dank für Ihr Interesse am Passwort Tresor. PWEND3	Datensatz 3
PWS Version 2 DE	Ende

PWSTART mit fortlaufender Nummer ist zwingend notwendig.

PWEND mit fortlaufender Nummer ist zwingend notwendig.

Ein Datensatz dazwischen kann beliebig viele Zeilen haben.

Demo Dateien **PWData.txt** & **Lock.txt** kann man herunterladen unter:
https://smf.pcaarburg.ch/Smurfy_CH_Hardware_projects/SD_DemoDaten.zip

---

Anwendung:

Passwort Tresor in USB Port einstecken.
Der Passwort Tresor ersetzt die Tastatureingaben bis auf ENTER.
ENTER muss an der Tastatur eingegeben werden.

Beispiel Anwendung der Demodatei 1 / **Email Login Demo**.

Internetbrowser öffnen und einmal in die URL Eingabeleiste klicken.
Mit Drehknopf drehen bis auf Display steht < **Email Login Demo** >
Drehknopf am Passwort Tresor einmal drücken. *(Die URL wird im Explorer eingegeben.)*
Auf der Tastatur ENTER drücken. *(Die Testseite wird geöffnet.)*
Einmal mit der Maus in das Feld USERNAME klicken.
Drehknopf am Passwort Tresor einmal drücken. *(Der User-Name wird eingegeben.)*
In das Feld PASSWORD klicken.
Drehknopf am Passwort Tresor einmal drücken. *(Das Passwort wird eingegeben.)*
EINLOGGEN anklicken.
Drehknopf am Passwort Tresor einmal drücken. *(Damit ist das Gerät für weitere Auswahl bereit.)*

Bedeutung der LED Anzeigen:

Grün: Gerät ist bereit zum Auswählen eines Datensatzes.
Rot: Daten werden ausgegeben oder berechnet
Blau: Gerät wartet auf einen Druck auf Drehknopf um weitere Daten auszugeben.

PASSWÖRTER ERSTELLEN

Die Passwörter wo mit dem Passworttresor verwaltet werden können dürfen nur folgende Zeichen enthalten.

a b c d e f g h i j k l m n o p q r s t u v w x y z

0 1 2 3 4 5 6 7 8 9

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

@ # * § ! ? < ( ) % $ ¢ £ & = + - . , : ; _ « / ¦ ° ¬ | & § ü ä

Andere Zeichen werden eventuell falsch übersetzt oder blockieren den Passwort Tresor.

Ein YouTube Videos vom Passwort Tresor gebrauch ist unter folgendem YouTube Link vorhanden.

Video Anleitung Anwenden
https://youtu.be/Ct78FFIRmjg?feature=shared

Video Anleitung Datenerstellen
https://youtu.be/_ulSwlclmHk?feature=shared

Das Video ist ohne Abfrage von PIN Nummer am Start.
Der Passwort Tresor hat eventuell im Video ein anderes Gehäuse. Die Funktion ist jedoch bei allen Geräten gleich.

Haftungsausschluss:
Das Gerät ist nach bestem Wissen und Gewissen hergestellt. Zum Zeitpunkt der Herstellung ist mir kein Weg bewusst wie jemand via Internet auf die Passwortdatei Zugriff nehmen könnte. Die Passwörter sind jedoch bei Entwendung des Gerätes auslesbar. Die Speicherkarte kann in einem PC ausgelesen werden. Die Verwendung dieses Geräts erfolgt auf eigenes Risiko. Für die Verwendung kann ich keine Haftung übernehmen. Nichts ist 100% Sicher, die Passwörter sollten nicht nur auf diesem Gerät gespeichert werden. Bei einem Defekt ist es unter Umständen nicht mehr möglich die Passwörter zu rekonstruieren. Sollte ein PC bereits mit einem Virus infiziert sein, so ist dieses Gerät kein Schutz. Das Abfangen von Eingabedaten via „Tastaturlogger“ kann nicht verhindert werden. Wenn das Gerät geöffnet wird kann das ein Kurzschluss auf dem Mikroprozessor erzeugen. Das kann danach den USB Port vom PC überlasten und im schlimmsten Fall zerstören.

Technische Merkmale:
Das Gerät wird vom PC als Tastatur erkannt.
Maximale USB Portbelastung < 40mA

©Smurfys.CH ©August 2024©