Digital Society.at

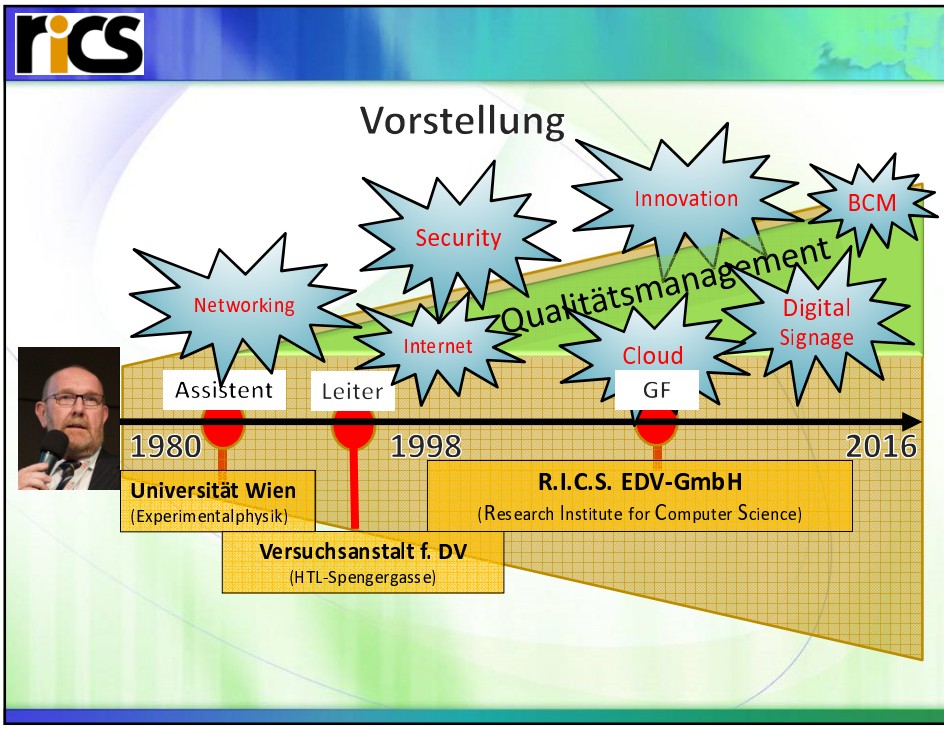
Digitalk

11. Mai 2016

Sicher im Netz und in der Cloud (Verschlüsselung)

Dr. Manfred Wöhrl
Manfred@Woehrl.at

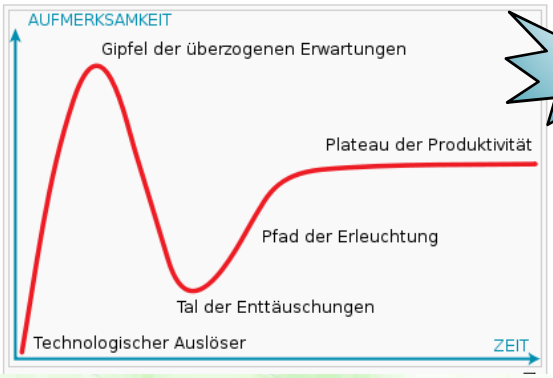
R.I.C.S.EDV-GmbH
Schönbrunner Schloßstr. 5/2
A-1120 Wien
http://www.rics.at



Die nahe Zukunft

Was kommt auf uns zu?

Zuerst die Technik, viel später das Risikomanagement!



Cloud

IoT

Big Data

Industrie 4.0

Neue Risiken….kommt jetzt auch der Hacker 4.0 ?

Hype-Zyklus nach Gartner Inc.

Jackie Fenn

Das Goldrausch-Theorem

Big-Data: Das Klondyke von heute

Claims abstecken und Geld machen – über den Rest reden wir später…..

- Wer sorgt für meine Privatsphäre ?
- Wer schützt mich vor kriminellen Angriffen ?

- Wie schnell reagiert die Gesetzgebung ?
- Wer hat Interesse daran, meine Privatsphäre zu schützen ?

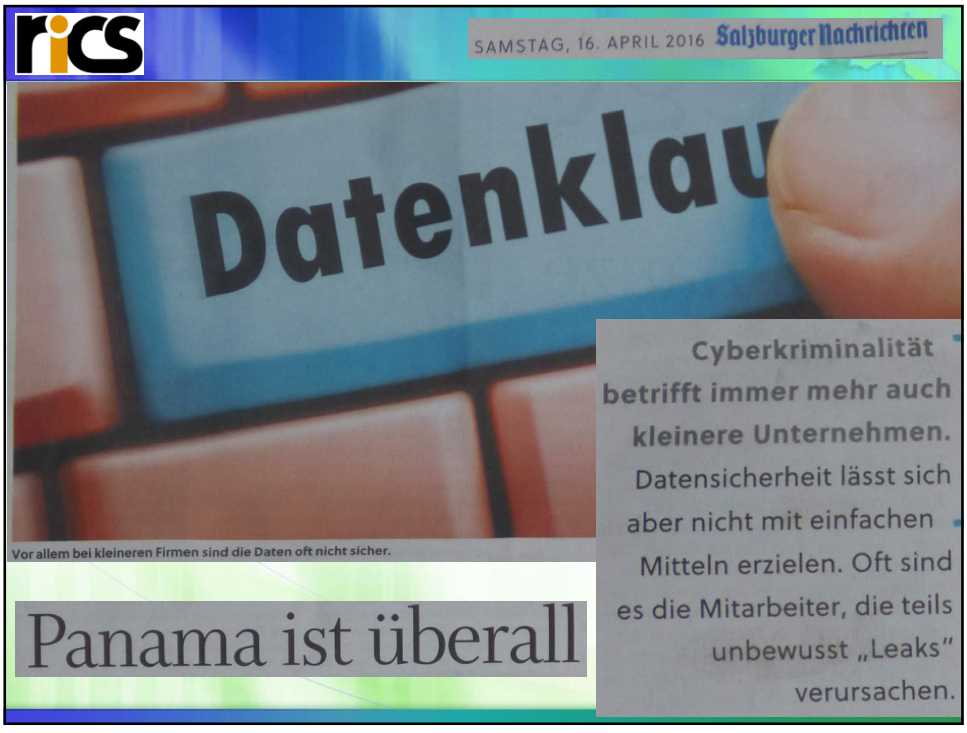
Schütze Dich selbst !

Zitat

Süddeutsche Zeitung, 3. Mai 2016

Wie TTIP zum Schlachtfeld im Krypto-Krieg wurde

In den Verhandlungen über TTIP wehrt sich die EU gegen den Versuch der Vereinigten Staaten, Minimal-Standards für IT-Sicherheit festzuschreiben. Das geht aus Dokumenten hervor, die Greenpeace *Süddeutscher Zeitung*, WDR und NDR vor ihrer Veröffentlichung zur Verfügung gestellt hat. Es geht darum, ob der Staat über sogenannte Hintertüren - bewusst eingebaute Schwachstellen im Programmcode von Informationstechnik - auf verschlüsselte Daten zugreifen kann, etwa auf einem iPhone von Apple. Solche Hintertüren und vergleichbare Vorschriften können Staaten zur Voraussetzung für den Verkauf von Produkten machen. Das wollen die USA verbieten. Europäische Regierungen wollen das Thema Verschlüsselung nicht in TTIP sehen und weiter national regeln. Manche fürchten wohl auch um ihre Möglichkeiten, ihre Bürger zu überwachen. Denn "Regulierung von Verschlüsselung" heißt auch: Der Staat entscheidet mit, wie sicher Smartphones und Apps sind, die die Bevölkerung nutzt.



Awareness

„Der **Bedarf** an Sicherheitsmaßnahmen ist unendlich,
das **Bedürfnis** der Benutzer ist gleich Null."

Zitate:

- Meine Daten interessieren niemanden.
- Ich habe nichts zu verbergen.
- Ich vertraue meiner EDV (meinem Betreuer).
- Es trifft immer die Anderen.

Anmerkung: …bis mir selbst das Handy gestohlen wird
oder ich meinen USB-Stick verliere…..

Awareness

Österreichisches Informationssicherheitshandbuch
V4.0.1 vom 19.1.2016 Kapitel 2.3.2

- Nur durch Verständnis und Motivation ist eine dauerhafte Einhaltung und Umsetzung der Richtlinien und Vorschriften zur Informationssicherheit zu erreichen

8

Grundlagen

Computerdaten, die uns nützen
muss man vor fremdem Zugriff schützen.
Die vielen Infos, die dort liegen
darf nicht problemlos jeder kriegen.
M.Wöhrl

Datenschutz ⟺ Datensicherheit

Recht ⟺ Praxis

Zukunft ⟺ Gegenwart

If privacy is outlawed, only outlaws will have privacy.

Diskussion

Europäische Gerichtshof für Menschenrechte (EGMR)

In der Sache Barbulescu v. Romania (application no. 61496/08) entschied der EGMR im **Jänner 2016** zugunsten eines Arbeitgebers, der den Yahoo-Messenger-Account eines Arbeitnehmers ohne vorherige Information überwachte und das **Dienstverhältnis dann wegen privater Chats in der Arbeitszeit beendete**. Der Messenger-Account wurde auf Wunsch des Arbeitgebers für die Bearbeitung von Kundenanfragen eingerichtet, vom Arbeitnehmer dann aber während der Arbeitszeit privat benutzt. **Die private Nutzung war verboten**. Der Arbeitgeber überwachte aufgrund eines Verdachts die Messenger-Kommunikation und konfrontierte den Arbeitnehmer mit dem Ergebnis der Kontrolle im Nachhinein. Der EGMR entschied, dass es nicht unrechtmäßig sei, dass ein Arbeitgeber überprüfen möchte, ob seine Arbeitnehmer ihre dienstlichen Aufgaben während der Arbeitszeit verrichten. Auch die Beendigung des Dienstverhältnisses wurde als rechtmäßig angesehen.

Private E-Mails? Private Telefonate ? „Rest an Privatsphäre am Arbeitsplatz?“
Private Daten auf einem Firmenrechner ?

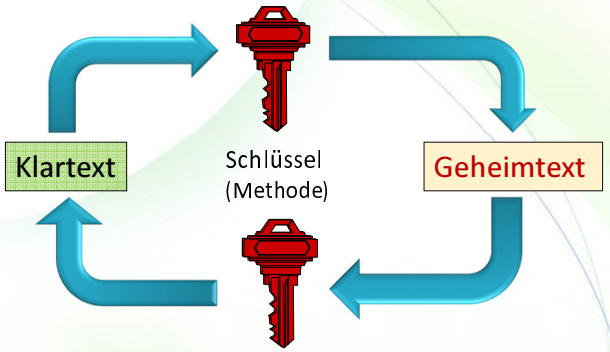
Methoden

Verschlüsselungsmethoden

1 : 1 Zuordnung Buchstabenshift Buchstabenmaske	Entschlüsselung einfach bei Kenntnis eines Orginaltextes und dazu gehörigem Geheimtextes
Symmetrische Verfahren (Key)	Data Encryption Standard DES, 3DES Advanced Encryption Standard AES
Asymmetrische Verfahren (Key)	Public/Private-Key Technik

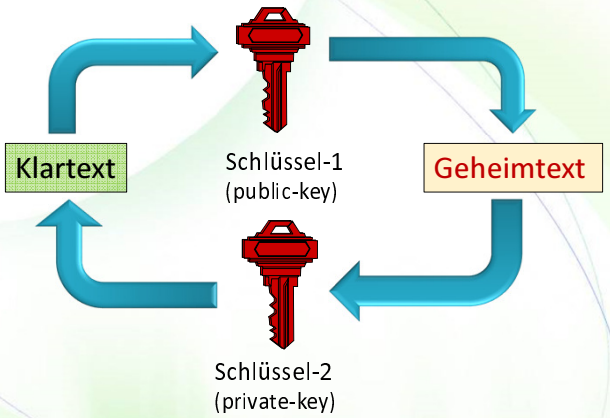
Kritische Faktoren:
Key-Länge, Algorithmen (Startvektor)
Rechenzeit (Realzeitverhalten)
Länderspezifische Gesetzeslage

Symmetrische Verschlüsselung



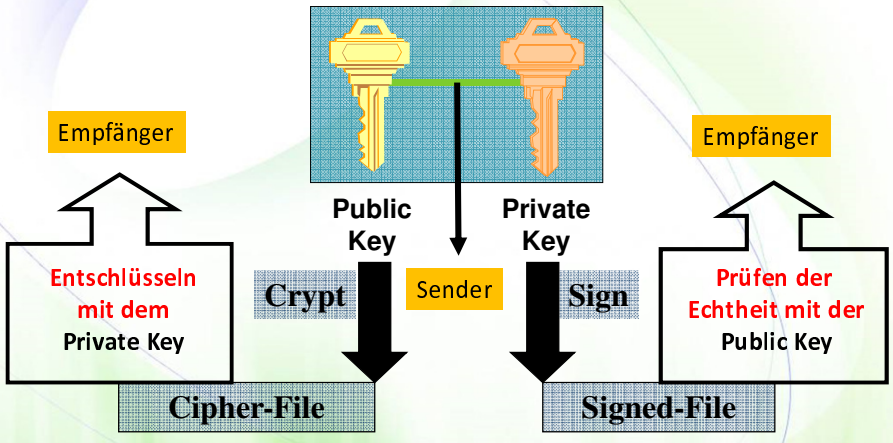
Problem: Umgang mit dem Schlüssel

Asymmetrische Verschlüsselung



Problem: Wer erzeugt den Schlüssel

Zusatz: Signatur



Passwort

Was ist ein sicheres Passwort ?

- **Länge**
  20+
- **Zeichen mischen, Merksatz**
  Ziffern, Buchstaben, Sonderzeichen
- **Keine Verbindung zur Person**
  Geburtstag, Haustier…..
- **Nach Möglichkeit Wechsel zur HW-Lösung**
  „Token“
- **Anti-Lexikon-und-Phrasen-Prüfung**
  „Brute-Force-Checker“
  http://password-checker.online-domain-tools.com/

PIN

Wie merke ich mir einen PIN ?

- **Niemals aufschreiben**
  Umfeld Arbeitsplatz….Bankomartkarte
- **Umkehrbare pers. Algorithmen definieren**
  Spiegeln
  3412 → 2143 → 3412
  Positionstausch (z.B. aussen)
  3412 → 2413 → 3412
  Rotieren im Kreis um x Positionen
  (1 x rechts) 3412 → 2341 → 3412 (1 x links)
  9-Komplement
  3412 → 6587 → 3412
- **Algorithmen kombinieren**
  zB. Spiegeln + 9-Komplement 3412 → 2143 → **7856**
- **Coded-PIN 7856 notieren**
  Verwenden auch als Teil eines Passwortes

Wo liegen meine Daten ?

- Lokal am Arbeitsplatz
  (Zutrittsschutz ?)
- Auf einem Server im LAN oder Internet
  (in meiner Administration ?)
- Auf einem Backup ?
  (wo abgelegt ? Per SYNC ?)
- In der Cloud z.B. auf Dropbox
  (public oder privat ?)
- Auf einem „Transferrechner“
  (z.B. bei Mail-Versand)

Ende-zu-Ende-Verschlüsselung
(„end-to-end encryption“, „E2EE“)

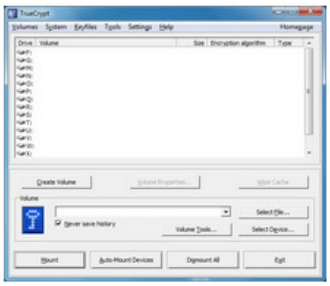
Stufen der lokalen Versschlüsselung

- File
- Container
  (File als Laufwerk)
- Partition
- Systempartition
  (Pre-Boot-Authentication)

Die CHIP Redaktion sagt:

TrueCrypt ist ein kostenloses Open-Source-Programm zum sicheren Verschlüsseln einzelner Daten oder des ganzen Systems.

Achtung: TrueCrypt wird seit Juni 2014 nicht mehr weiterentwickelt, die Entwickler warnen vor dem Einsatz ihrer Software. Allerdings gilt die hier angebotene Version 7.1a weiterhin als annähernd unknackbar. Den aktuellen Stand rund um TrueCrypt decken wir in dieser News ab. Als Alternative empfehlen wir die Windows-7-Versionen Enterprise und Ultimate sowie Windows 8/8.1 Pro und Enterprise, in denen BitLocker eingebaut ist oder die quelloffene Alternative DiskCryptor.



TrueCrypt

Alternative Downloads

ArchiCrypt Live 8.9.2

"ArchiCrypt Live" versteckt sensible Dateien in virtuellen Laufwerken.

CHIP-BEWERTUNG
Gut

Zum Download

WinSCP 5.7.7

WinSCP ist ein kostenloser Client, der es erlaubt, Secure Copy unter Windows zu nutzen.

CHIP-BEWERTUNG
Sehr gut

Zum Download

VeraCrypt 1.17

VeraCrypt ist ein neues Verschlüsselungsprogramm, das besser und sicherer sein will, als TrueCrypt.

CHIP-BEWERTUNG
Sehr gut

Zum Download

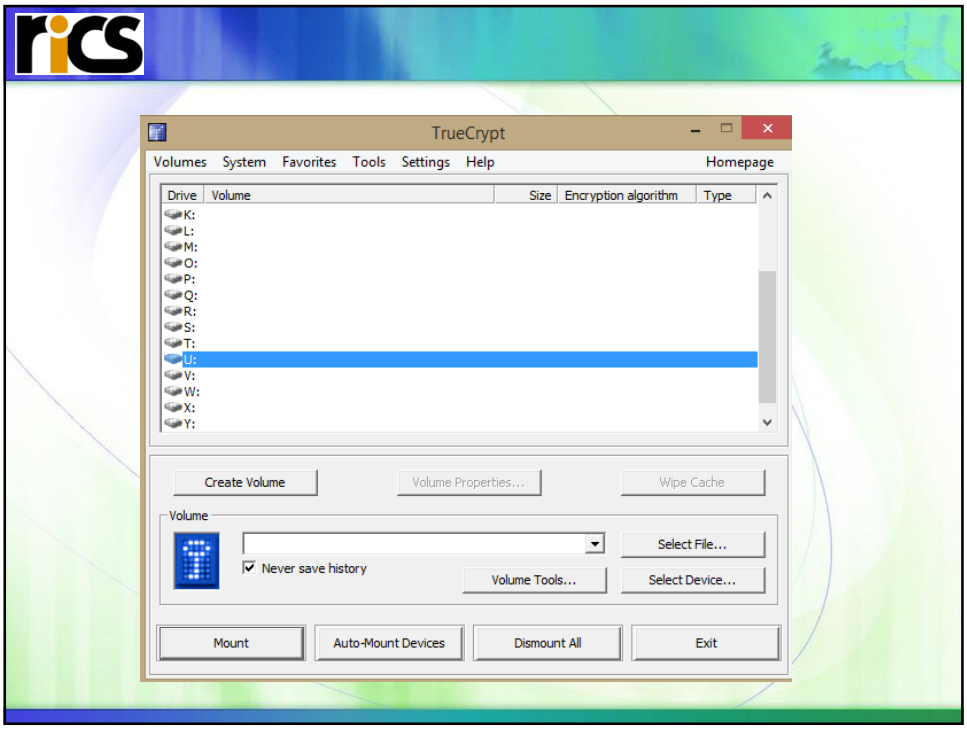
OpenVPN 2.3.10

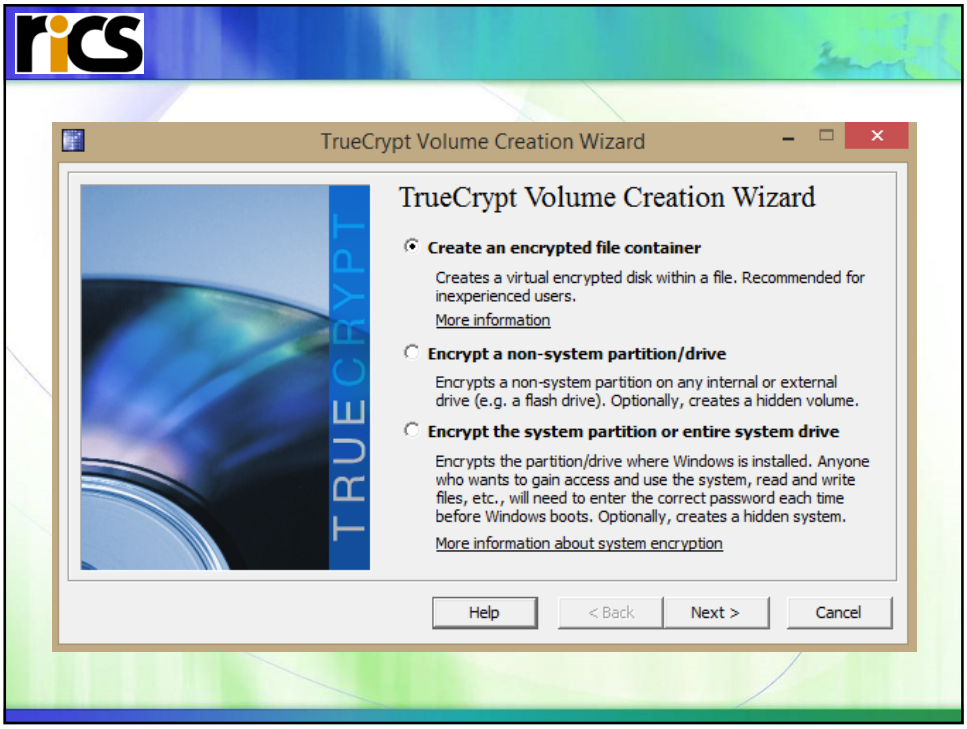
Mit OpenVPN errichten Sie ein virtuelles und verschlüsseltes Netzwerk.

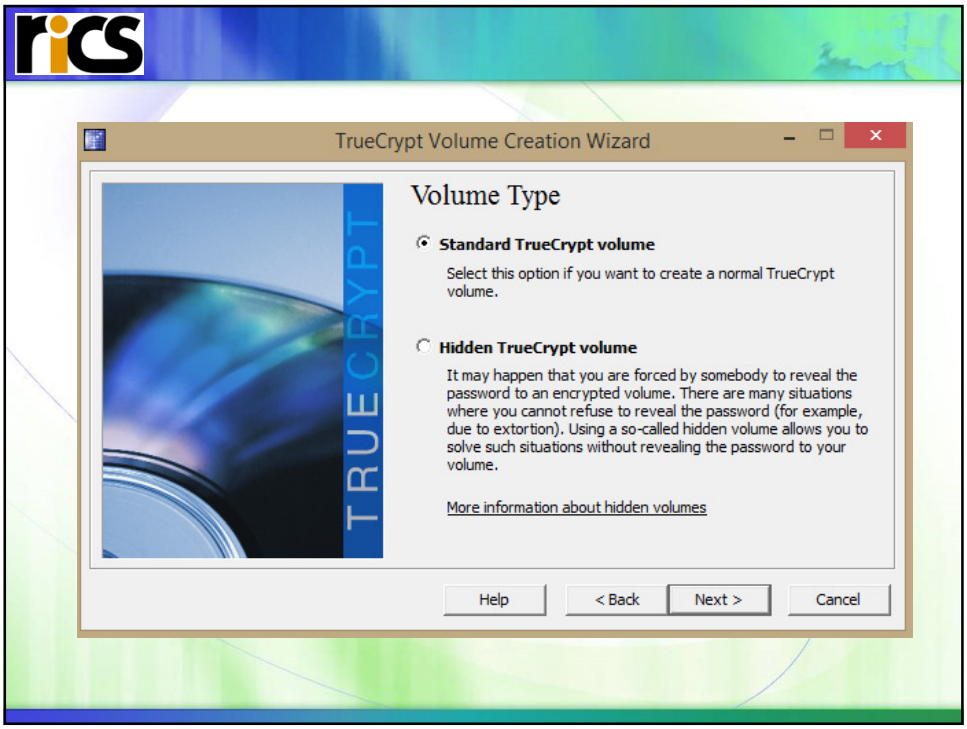
CHIP-BEWERTUNG
Sehr gut

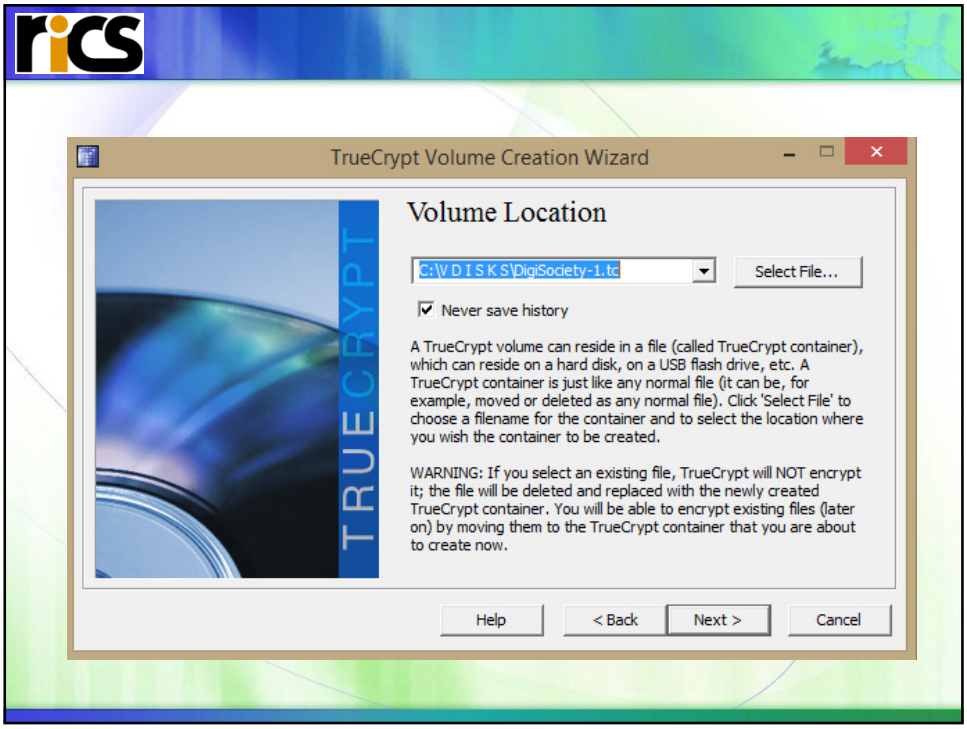
Zum Download

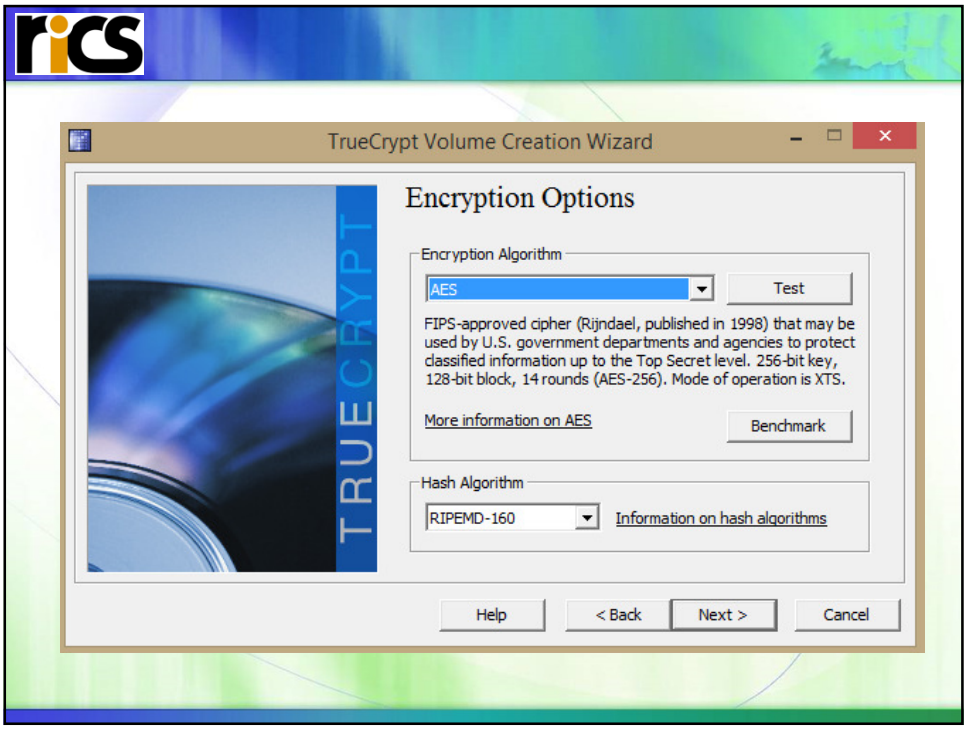

About TrueCrypt
TRUECRYPT
TrueCrypt 7.1a
Released by TrueCrypt Foundation on February 7, 2012
www.truecrypt.org
Portions of this software are based in part on the works of the following people: Paul Le Roux, Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson, Lars Knudsen, Ross Anderson, Eli Biham, Joan Daemen, Vincent Rijmen, Phillip Rogaway, Hans Dobbertin, Antoon Bosselaers, Bart Preneel, Paulo Barreto, Brian Gladman, Wei Dai, Peter Gutmann, and many
OK


TrueCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption algorithm Type
K:
L:
M:
O:
P:
Q:
R:
S:
T:
U:
V:
W:
X:
Y:
Create Volume
Volume Properties...
Wipe Cache
Volume
Never save history
Select File...
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

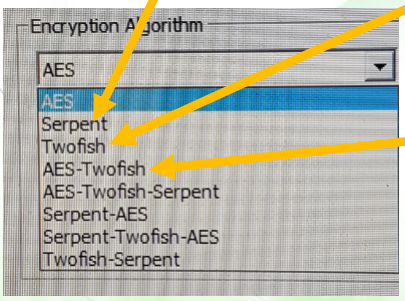

TrueCrypt Volume Creation Wizard
TrueCrypt Volume Creation Wizard
TRUECRYPT
Create an encrypted file container
Creates a virtual encrypted disk within a file. Recommended for inexperienced users.
More information
Encrypt a non-system partition/drive
Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.
Encrypt the system partition or entire system drive
Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.
More information about system encryption
Help
< Back
Next >
Cancel


TrueCrypt Volume Creation Wizard
Volume Type
TRUECRYPT
Standard TrueCrypt volume
Select this option if you want to create a normal TrueCrypt volume.
Hidden TrueCrypt volume
It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.
More information about hidden volumes
Help
< Back
Next >
Cancel


TrueCrypt Volume Creation Wizard
Volume Location
C:\V D I S K S\DigiSociety-1.tc
Select File...
Never save history
A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.
WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.
TRUECRYPT
Help
< Back
Next >
Cancel

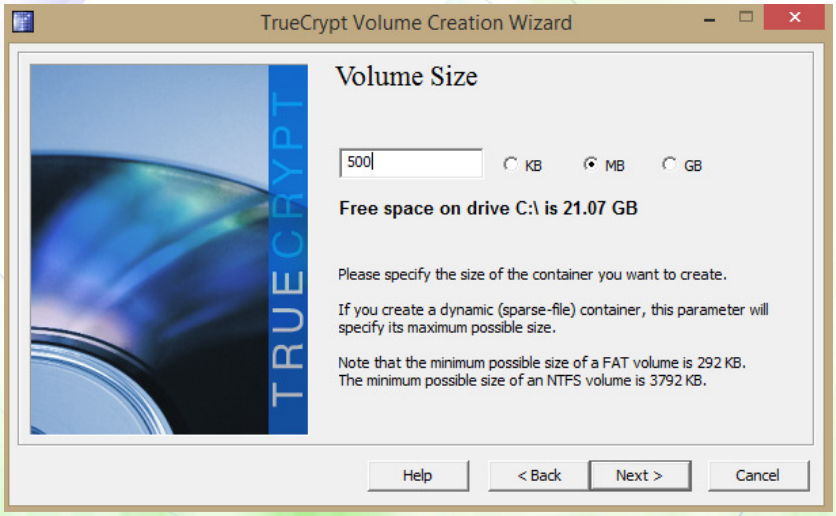

TrueCrypt Volume Creation Wizard
Encryption Options
Encryption Algorithm
AES
Test
FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.
More information on AES
Benchmark
Hash Algorithm
RIPEMD-160
Information on hash algorithms
TRUECRYPT
Help
< Back
Next >
Cancel

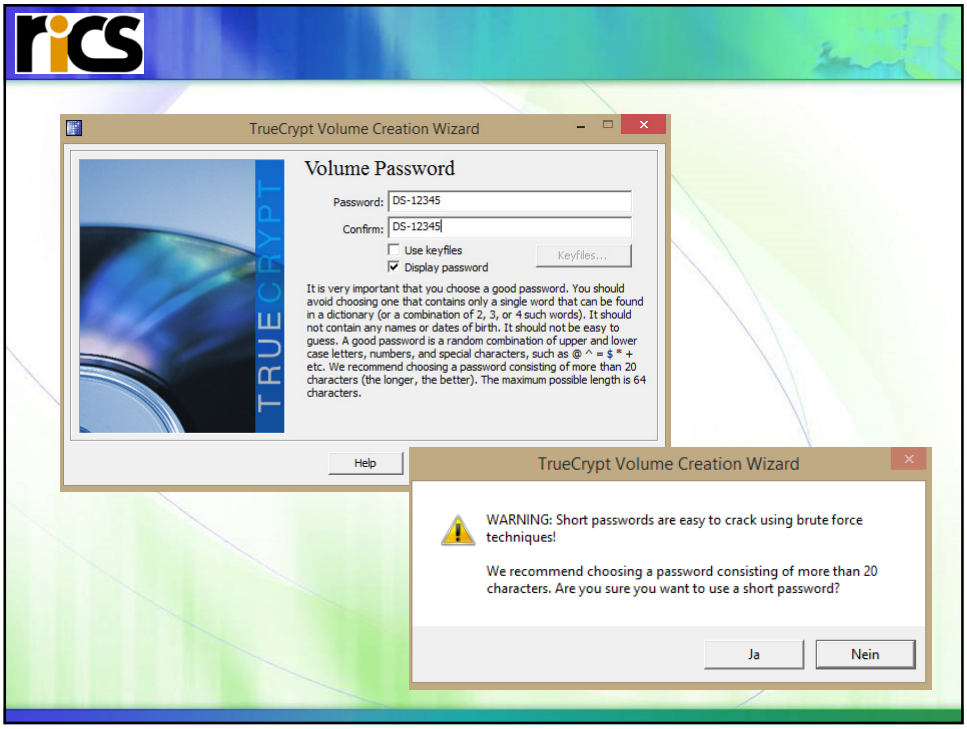
Elliptic curve cryptography
http://www.youtube.com/watch?v=HHFFvfDoTK4.

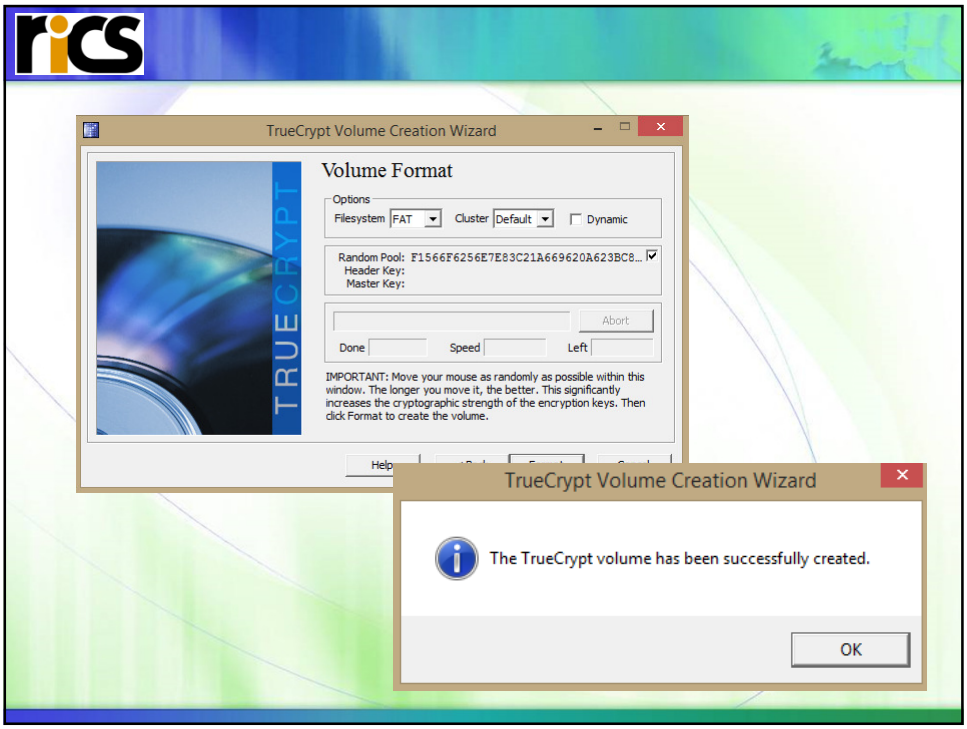


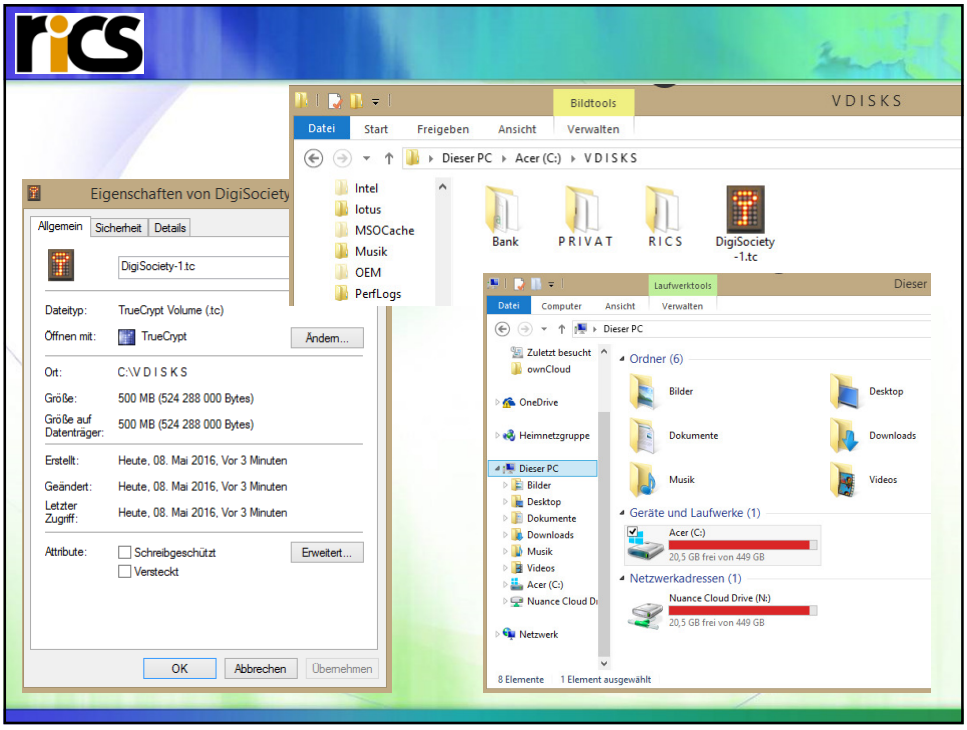
Symmetrischer Verschlüsselungsalgorithmus, der von Bruce Schneier et.al. entwickelt wurde. Es handelt sich um eine Blockchiffre mit einer Blockgröße von 128 Bit und 16 Runden, Schlüssellängen : 128
192 oder 256 Bit.

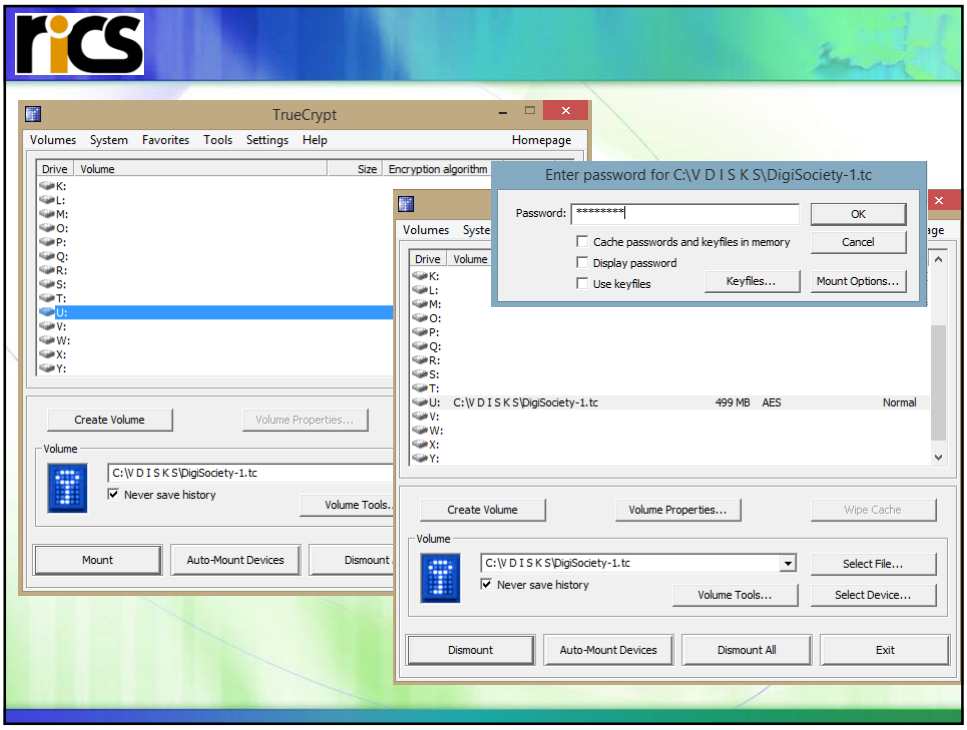
Twofish basiert auf Blowfish einem symm. Blockverschlüsselungsalgorithmus, der 1993 von Bruce Schneier entworfen und erstmals im April 1994 in *Dr. Dobb's Journal* publiziert wurde.

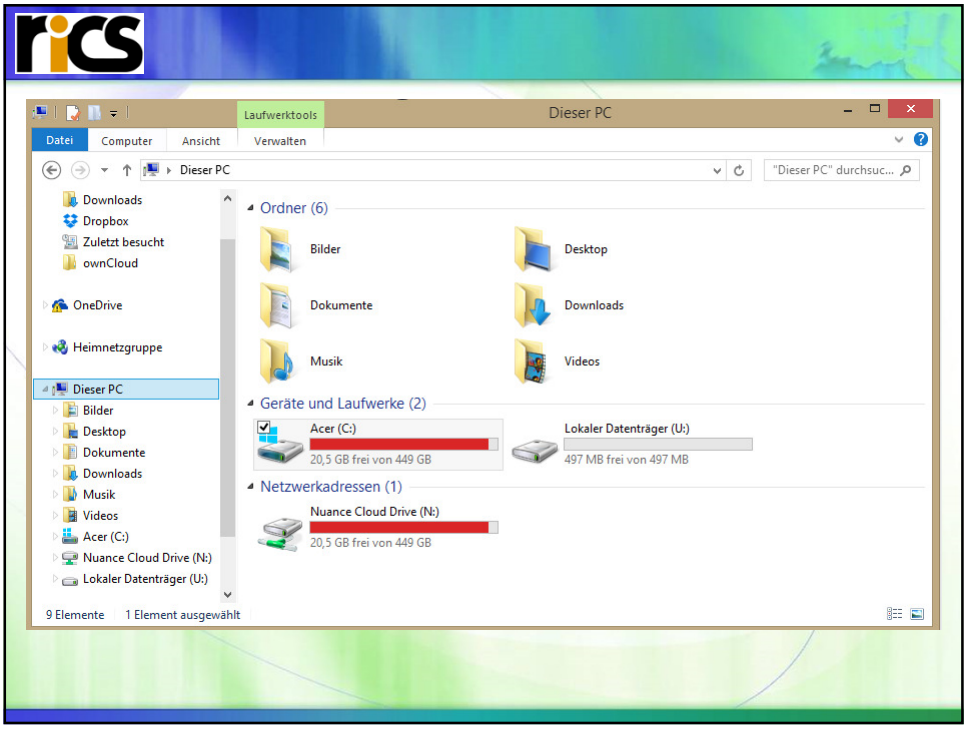



TrueCrypt Volume Creation Wizard
Volume Password
Password: DS-12345
Confirm: DS-12345
Use keyfiles
Display password
Keyfiles...
It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum possible length is 64 characters.
Help
TrueCrypt Volume Creation Wizard
WARNING: Short passwords are easy to crack using brute force techniques!
We recommend choosing a password consisting of more than 20 characters. Are you sure you want to use a short password?
Ja
Nein

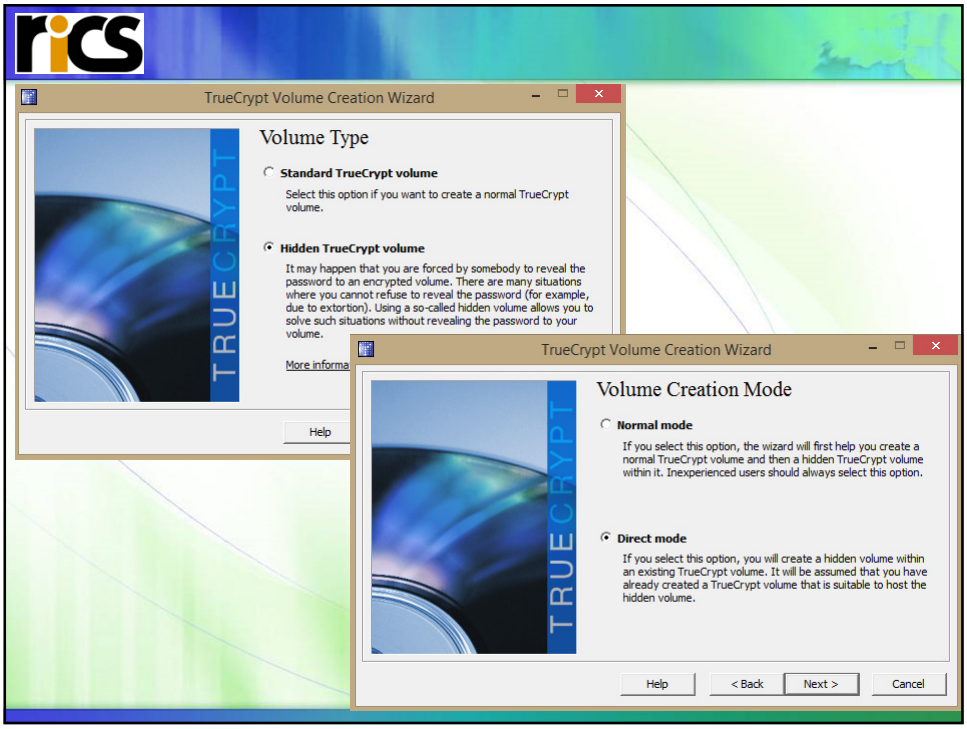

TrueCrypt Volume Creation Wizard
Volume Format
Options
Filesystem FAT
Cluster Default
Dynamic
Random Pool: F1566F6256E7E83C21A669620A623BC8...
Header Key:
Master Key:
Abort
Done
Speed
Left
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.
TrueCrypt Volume Creation Wizard
The TrueCrypt volume has been successfully created.
OK

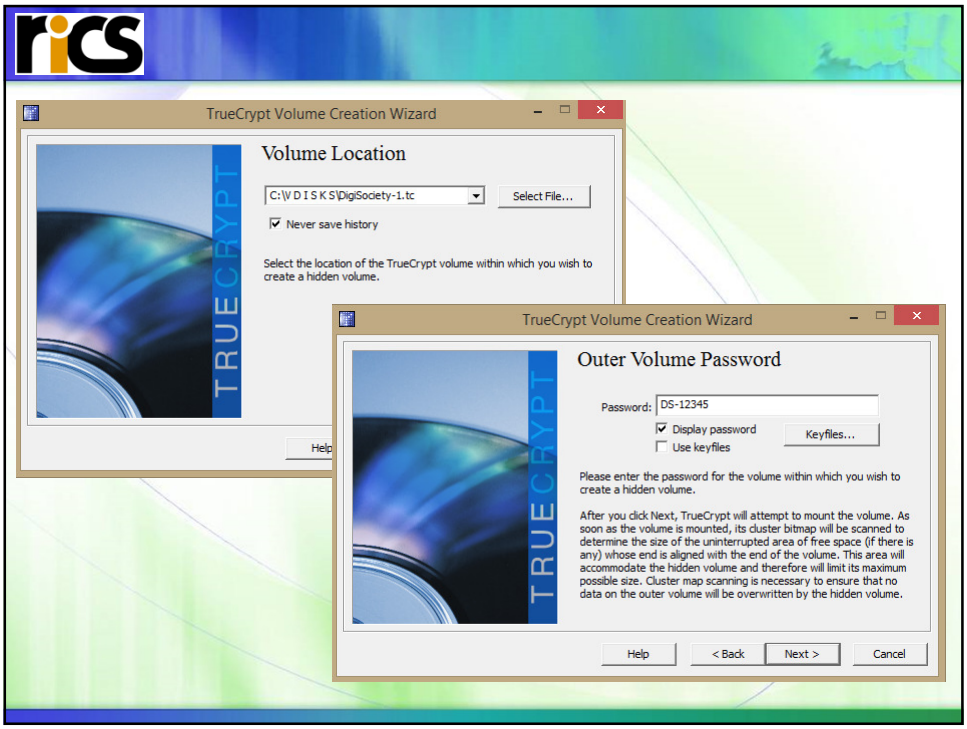

VDISKS
Bildtools
Datei
Start
Freigeben
Ansicht
Verwalten
Dieser PC ▸ Acer (C:) ▸ VDISKS
Intel
Iotus
MSOCache
Musik
OEM
PerfLogs
Bank
PRIVAT
RICS
DigiSociety -1.tc
Eigenschaften von DigiSociety
Allgemein
Sicherheit
Details
DigiSociety-1.tc
Dateityp: TrueCrypt Volume (.tc)
Öffnen mit: TrueCrypt
Ändern...
Ort: C:\VDISKS
Größe: 500 MB (524 288 000 Bytes)
Größe auf Datenträger: 500 MB (524 288 000 Bytes)
Erstellt: Heute, 08. Mai 2016, Vor 3 Minuten
Geändert: Heute, 08. Mai 2016, Vor 3 Minuten
Letzter Zugriff: Heute, 08. Mai 2016, Vor 3 Minuten
Attribute: Schreibgeschützt
Versteckt
Erweitert...
OK
Abbrechen
Übernehmen
Laufwerktools
Dieser
Computer
Ansicht
Verwalten
Zuletzt besucht
ownCloud
OneDrive
Heimnetzgruppe
Dieser PC
Bilder
Desktop
Dokumente
Downloads
Musik
Videos
Acer (C:)
Nuance Cloud Dr
Netzwerk
Ordner (6)
Geräte und Laufwerke (1)
20,5 GB frei von 449 GB
Netzwerkadressen (1)
Nuance Cloud Drive (N:)
20,5 GB frei von 449 GB
8 Elemente
1 Element ausgewählt

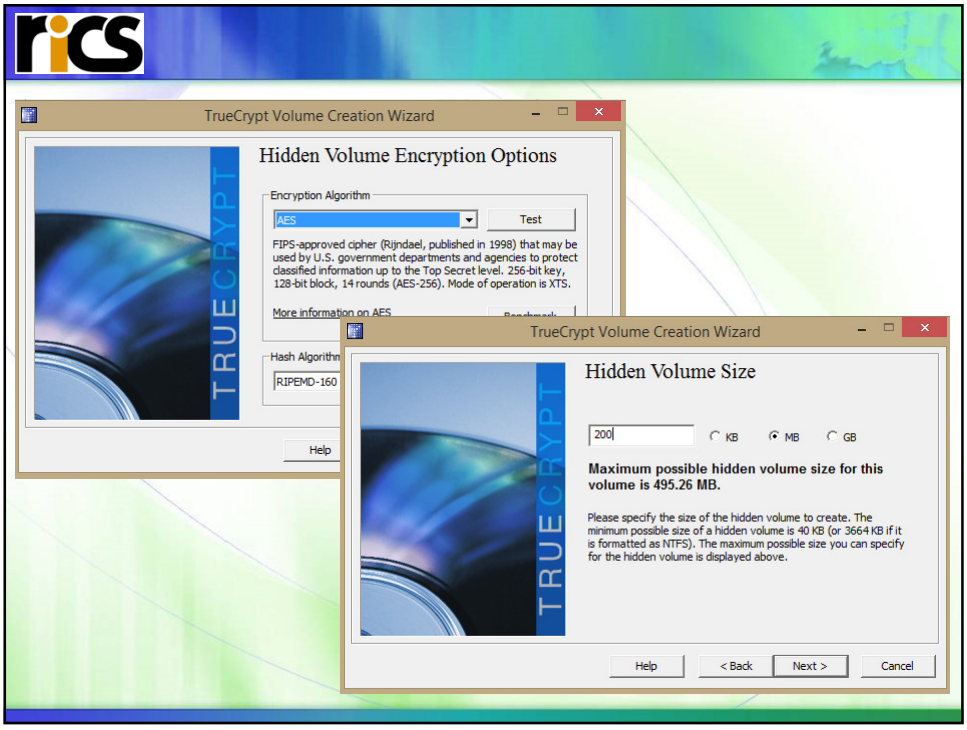

TrueCrypt
Volumes
System
Favorites
Tools
Settings
Help
Homepage
Drive
Volume
Size
Encryption algorithm
K:
L:
M:
O:
P:
Q:
R:
S:
T:
U:
V:
W:
X:
Y:
Create Volume
Volume Properties...
Volume
C:\VDISKS\DigiSociety-1.tc
Never save history
Volume Tools...
Mount
Auto-Mount Devices
Dismount
Enter password for C:\VDISKS\DigiSociety-1.tc
Password:
OK
Cancel
Cache passwords and keyfiles in memory
Display password
Use keyfiles
Keyfiles...
Mount Options...
C:\VDISKS\DigiSociety-1.tc 499 MB AES Normal
Wipe Cache
Select File...
Select Device...
Dismount All
Exit

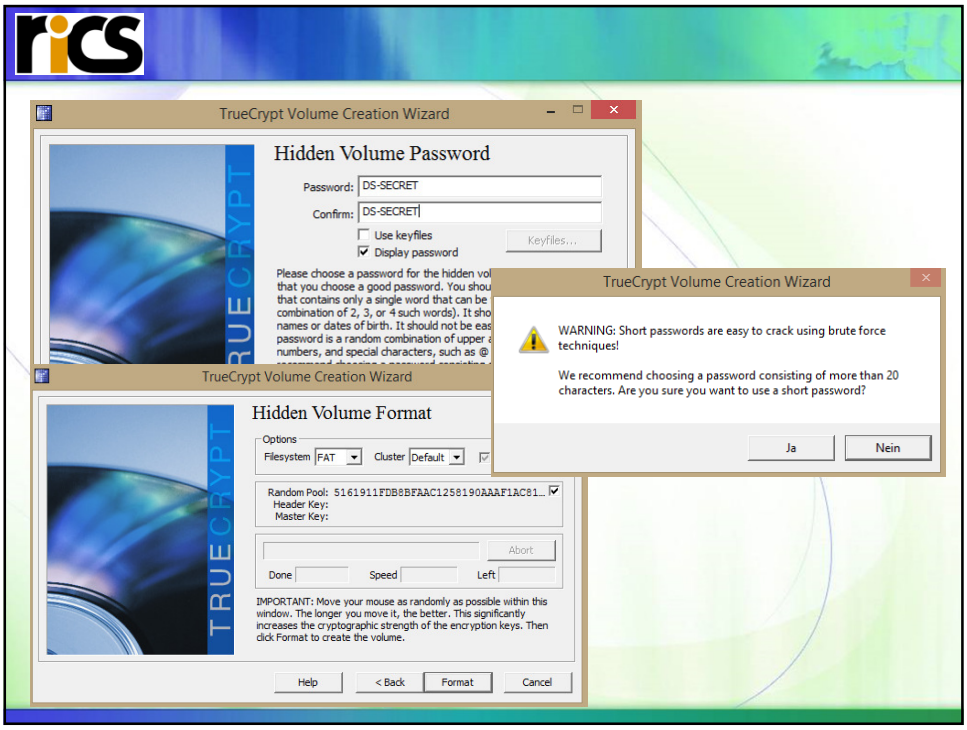

Laufwerktools
Dieser PC
Datei
Computer
Ansicht
Verwalten
Dieser PC
"Dieser PC" durchsuc...
Downloads
Dropbox
Zuletzt besucht
ownCloud
OneDrive
Heimnetzgruppe
Dieser PC
Bilder
Desktop
Dokumente
Downloads
Musik
Videos
Acer (C:)
Nuance Cloud Drive (N:)
Lokaler Datenträger (U:)
Ordner (6)
Bilder
Desktop
Dokumente
Downloads
Musik
Videos
Geräte und Laufwerke (2)
Acer (C:)
20,5 GB frei von 449 GB
Lokaler Datenträger (U:)
497 MB frei von 497 MB
Netzwerkadressen (1)
Nuance Cloud Drive (N:)
20,5 GB frei von 449 GB
9 Elemente
1 Element ausgewählt

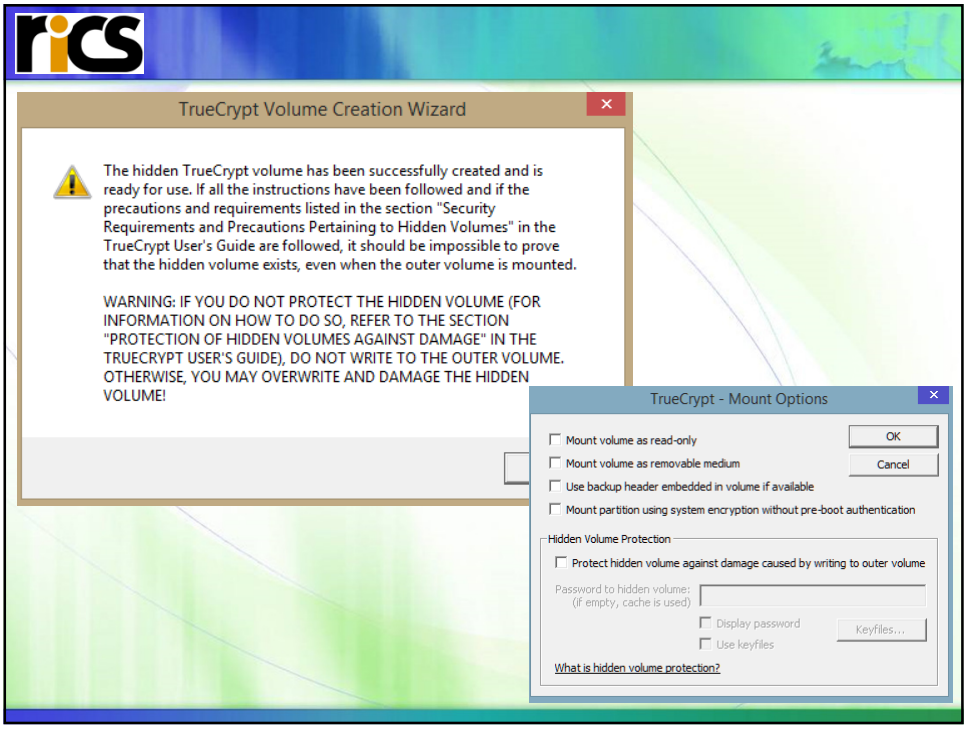

Top Secret

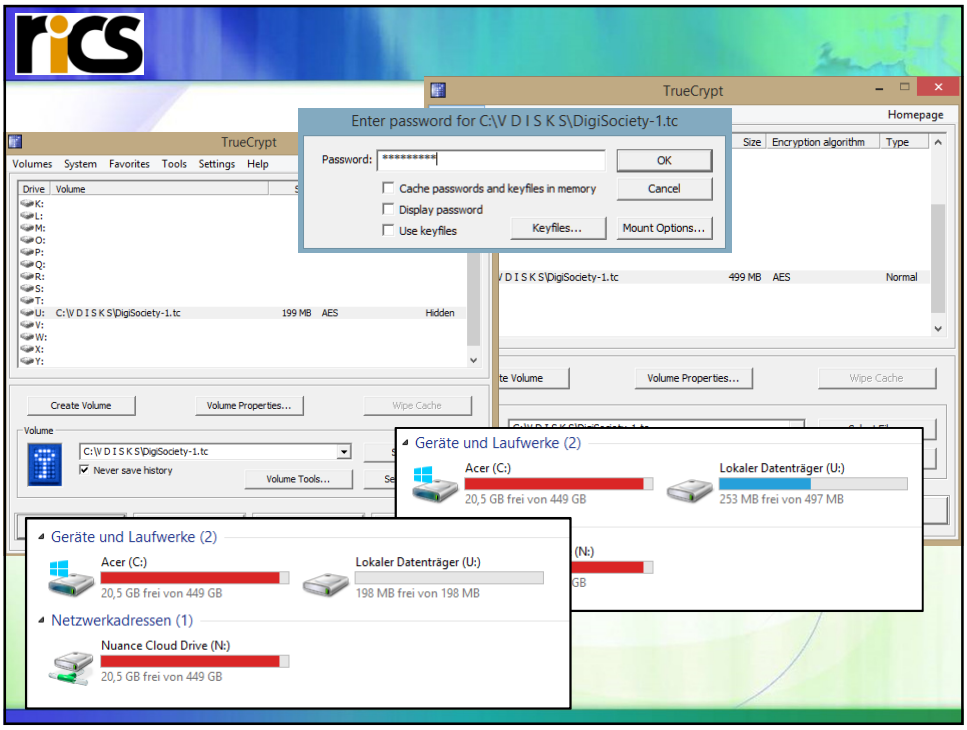

TrueCrypt Volume Creation Wizard
Volume Type
Standard TrueCrypt volume
Select this option if you want to create a normal TrueCrypt volume.
Hidden TrueCrypt volume
It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.
More informa
Help
TrueCrypt Volume Creation Wizard
Volume Creation Mode
Normal mode
If you select this option, the wizard will first help you create a normal TrueCrypt volume and then a hidden TrueCrypt volume within it. Inexperienced users should always select this option.
Direct mode
If you select this option, you will create a hidden volume within an existing TrueCrypt volume. It will be assumed that you have already created a TrueCrypt volume that is suitable to host the hidden volume.
Help
< Back
Next >
Cancel
TRUECRYPT


TrueCrypt Volume Creation Wizard
Volume Location
C:\V D I S K S\DigiSociety-1.tc
Select File...
Never save history
Select the location of the TrueCrypt volume within which you wish to create a hidden volume.
Help
TrueCrypt Volume Creation Wizard
Outer Volume Password
Password:
DS-12345
Display password
Use keyfiles
Keyfiles...
Please enter the password for the volume within which you wish to create a hidden volume.
After you click Next, TrueCrypt will attempt to mount the volume. As soon as the volume is mounted, its cluster bitmap will be scanned to determine the size of the uninterrupted area of free space (if there is any) whose end is aligned with the end of the volume. This area will accommodate the hidden volume and therefore will limit its maximum possible size. Cluster map scanning is necessary to ensure that no data on the outer volume will be overwritten by the hidden volume.
Help
< Back
Next >
Cancel
TRUECRYPT


TrueCrypt Volume Creation Wizard
Hidden Volume Encryption Options
Encryption Algorithm
AES
Test
FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.
More information on AES
Hash Algorithm
RIPEMD-160
Help
TrueCrypt Volume Creation Wizard
Hidden Volume Size
200
KB
MB
GB
Maximum possible hidden volume size for this volume is 495.26 MB.
Please specify the size of the hidden volume to create. The minimum possible size of a hidden volume is 40 KB (or 3664 KB if it is formatted as NTFS). The maximum possible size you can specify for the hidden volume is displayed above.
Help
< Back
Next >
Cancel
TRUECRYPT

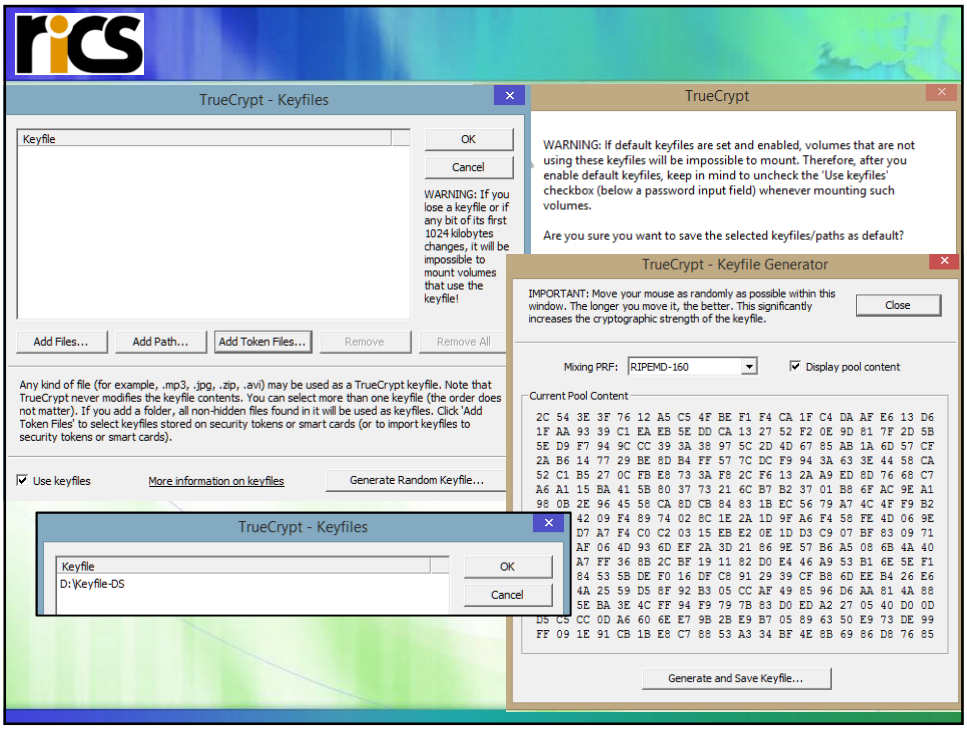

TrueCrypt Volume Creation Wizard
Hidden Volume Password
Password: DS-SECRET
Confirm: DS-SECRET
Use keyfiles
Keyfiles...
Display password
TrueCrypt Volume Creation Wizard
WARNING: Short passwords are easy to crack using brute force techniques!
We recommend choosing a password consisting of more than 20 characters. Are you sure you want to use a short password?
Ja
Nein
TrueCrypt Volume Creation Wizard
Hidden Volume Format
Options
Filesystem FAT
Cluster Default
Random Pool: 5161911FDB8FAAC1258190AAAF1AC81...
Header Key:
Master Key:
Abort
Done
Speed
Left
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.
Help
< Back
Format
Cancel
TRUECRYPT


TrueCrypt Volume Creation Wizard
The hidden TrueCrypt volume has been successfully created and is ready for use. If all the instructions have been followed and if the precautions and requirements listed in the section "Security Requirements and Precautions Pertaining to Hidden Volumes" in the TrueCrypt User's Guide are followed, it should be impossible to prove that the hidden volume exists, even when the outer volume is mounted.
WARNING: IF YOU DO NOT PROTECT THE HIDDEN VOLUME (FOR INFORMATION ON HOW TO DO SO, REFER TO THE SECTION "PROTECTION OF HIDDEN VOLUMES AGAINST DAMAGE" IN THE TRUECRYPT USER'S GUIDE), DO NOT WRITE TO THE OUTER VOLUME. OTHERWISE, YOU MAY OVERWRITE AND DAMAGE THE HIDDEN VOLUME!
TrueCrypt - Mount Options
Mount volume as read-only
Mount volume as removable medium
Use backup header embedded in volume if available
Mount partition using system encryption without pre-boot authentication
OK
Cancel
Hidden Volume Protection
Protect hidden volume against damage caused by writing to outer volume
Password to hidden volume: (if empty, cache is used)
Display password
Use keyfiles
Keyfiles...
What is hidden volume protection?

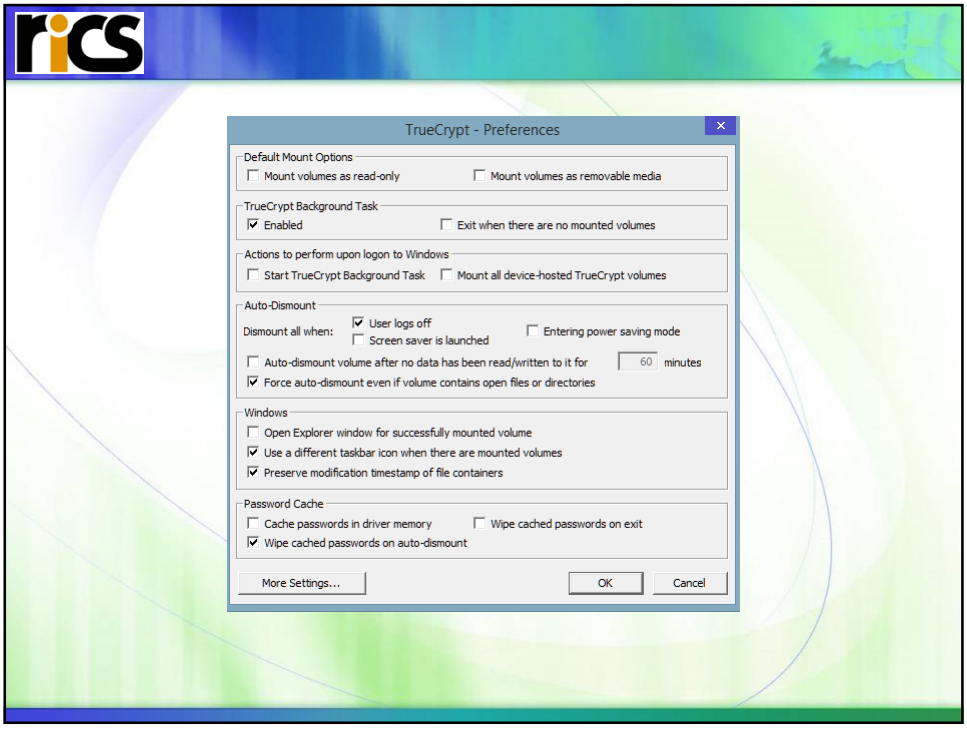

TrueCrypt
Enter password for C:\V D I S K S\DigiSociety-1.tc
Password:
OK
Cancel
Cache passwords and keyfiles in memory
Display password
Use keyfiles
Keyfiles...
Mount Options...
Volumes System Favorites Tools Settings Help
Homepage
Create Volume
Volume Properties...
Wipe Cache
Volume
Never save history
Volume Tools...
Geräte und Laufwerke (2)
Acer (C:)
20,5 GB frei von 449 GB
Lokaler Datenträger (U:)
198 MB frei von 198 MB
253 MB frei von 497 MB
Netzwerkadressen (1)
Nuance Cloud Drive (N:)
20,5 GB frei von 449 GB

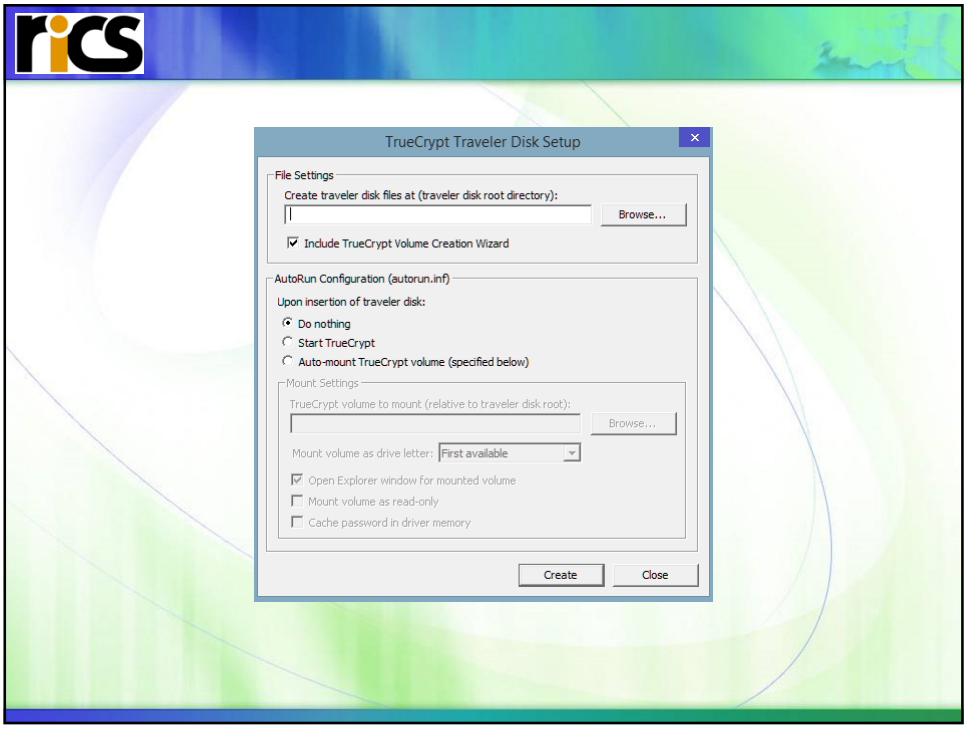
USB-TOKEN

„Wissen und besitzen“



Settings


TrueCrypt - Preferences
Default Mount Options
Mount volumes as read-only
Mount volumes as removable media
TrueCrypt Background Task
Enabled
Exit when there are no mounted volumes
Actions to perform upon logon to Windows
Start TrueCrypt Background Task
Mount all device-hosted TrueCrypt volumes
Auto-Dismount
Dismount all when:
User logs off
Screen saver is launched
Entering power saving mode
Auto-dismount volume after no data has been read/written to it for
60
minutes
Force auto-dismount even if volume contains open files or directories
Windows
Open Explorer window for successfully mounted volume
Use a different taskbar icon when there are mounted volumes
Preserve modification timestamp of file containers
Password Cache
Cache passwords in driver memory
Wipe cached passwords on exit
Wipe cached passwords on auto-dismount
More Settings...
OK
Cancel



Conclusion

Zusammenfassung

Verschlüsselungstechnik ist Bestandteil von Smartphones, chipbasierten Kreditkarten, Reisepässen und Webseiten. Damit sie sicher bleiben und weder Polizei noch Kriminelle Zugriff auf entsprechende Daten bekommen, muss das kryptografische Schloss unknackbar bleiben. Die Verschlüsselung muss auch für meinen PC, Notebook und Tablet so gut sein, dass moderne Computer Hunderte Jahre rechnen müssen, um die mathematische Gleichungen zu lösen, mit der die Daten geschützt sind.

Der Mensch

- Sicherheit bedeutet Aufwand
  - Ohne Einsicht werden Methoden umgangen
  - Unerkannter „Mehrwert“ des SEC-Prozesses
- Der Mensch lebt monoton
  - Veränderungen im tägl. Ablauf sind unbeliebt
  - Token werden abgelehnt (Verlust?)
- Risiken werden verdrängt
  - „Mir wird schon Nichts passieren“
- Der Mensch braucht Leitfiguren
  - Die Chefetage muß Security vorleben
  - (und nicht „over-rulen“)

Danke für Ihre Aufmerksamkeit !

Sie haben Fragen ?
Wir haben die Antwort !

R.I.C.S.EDV-GmbH
Schönbrunner Schloßstr. 5/2
A-1120 Wien
http://www.rics.at

Dr. Manfred Wöhrl
Manfred@Woehrl.at