FIfF Regionalgruppe München
Vortragsreihe Datenschutz und IT-Sicherheit
Hochschule München
05.05.2010

Privacy Tools - aber sicher!

Lizenzbedingungen/Copyright

Die von uns verwendeten Inhalte stammen ebenfalls aus öffentlichen Quellen, die im Vortrag vermerkt sind. TrueCrypt und Tor sowie deren Logos sind eingetragene Warenzeichen!

Wir danken der Hochschule München für die Einladung!

Agenda

1.	**Begrüßung und Vorstellung**
2.	**Einleitung – Kurzvorstellung der Tools**
3.	**GnuPG**
4.	**TRUECRYPT**
5.	**Tor**
6.	**Zusammenwirken der Tools**
7.	**Fragen und Diskussion**

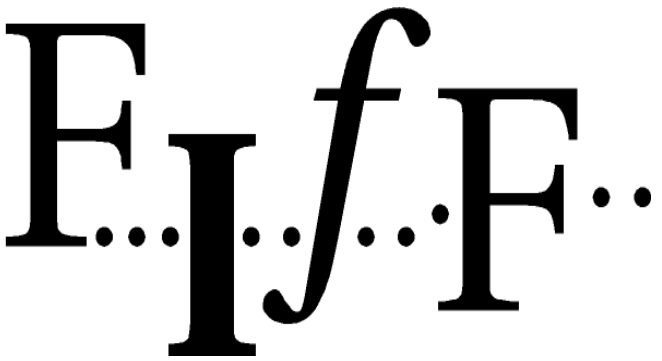
Vorstellung

- Sylvia Johnigk
- Diplom-Informatikerin TU-Berlin
  - Schwerpunkt Informatik & Gesellschaft, Software Technik
- 5 Jahre Forschung IT-Sicherheit
- 8 Jahre IT-Sicherheit für einen Finanzdienstleister
- Seit Juli 2009 selbständige Beraterin für mittelständige Unternehmen

Kontakt: sylvia.johnigk (at) secucat (dot) de

secucat

- Kai Nothdurft
- Diplom-Informatiker Uni-Bremen
  - Schwerpunkt Datenschutz
- 4 Jahre selbstständiger Berater
- Seit 1998 IT-Sicherheit für einen Versicherer



Agenda

1. Begrüßung und Vorstellung
2. **Einleitung – Kurzvorstellung der Tools**
3. GnuPG
4. TRUECRYPT
5. Tor
6. Zusammenwirken der Tools
7. Fragen und Diskussion

Einleitung/Motivation

Privatheit oder Privacy ist ein (Menschen)Recht.

Artikel 1 Abs. 1 GG

Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

Artikel 2 Abs.1 GG

Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit (...).

Artikel 5 Abs. 1 GG

Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt.

Einleitung/Motivation

Artikel 10 Abs. 1 GG

Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

Artikel 13 Abs. 1 ff. GG

Die Wohnung ist unverletzlich.

Informationelles Selbstbestimmungsrecht

bezeichnet das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.

Gemäß dem Bundesverfassungsgericht handelt es sich um ein Datenschutz-Grundrecht, das im Grundgesetz nicht ausdrücklich erwähnt wird.

Der Vorschlag, ein Datenschutz-Grundrecht in das Grundgesetz einzufügen, fand bisher nicht die erforderliche Mehrheit.

Einleitung/Motivation

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informations-technischer Systeme (umgangssprachlich auch als IT-Grundrecht, Computer-Grundrecht oder Grundrecht auf digitale Intimsphäre bezeichnet [1]) ist ein in der Bundesrepublik Deutschland geltendes Grundrecht, welches vornehmlich dem Schutz von persönlichen Daten dient, die in informationstechnischen Systemen gespeichert oder verarbeitet werden. (Wikipedia)

www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html

Werden meine Grundrechte ausreichend umgesetzt? Bin ich u*ngehemmt, ist mein Recht verwirklicht*, wenn ich (weiß):

- dass meine Korrespondenz von „jedem“ gelesen werden kann?
- dass „jeder“ der auf meinen Speicher zugreifen kann, weiß, was ich gespeichert habe?
- dass „jeder“ weiß wann ich wo im Internet nach welchen Informationen recherchiert habe?
- dass die Polizei demnächst das Internet mit autonomen Agenten überwacht?

Einleitung - GnuPG

- GnuPG oder auch GPG ist ein *freies* Kryptographiesystem, das seinen Einsatz findet, wenn Daten/Informationen „*vertraulich*“ und „*sicher*“ **übertragen** werden sollen.

- Es eignet sich insbesondere beim Einsatz von E-Mail, da so E-Mails und Anhänge
  - verschlüsselt versendet werden können und
  - nur vom gewünschten Empfänger wieder entschlüsselt werden können
- Es eignet sich weiterhin zum Signieren von E-Mails. Die Signatur kann vom Empfänger geprüft werden.

TrueCrypt/Tor

- TrueCrypt
  - ist ein Open-Source-Programm zur Verschlüsselung von Festplatten, Teilen davon oder Wechseldatenträgern.
  - schützt die Daten, die verschlüsselt wurden vor dem Verlust der Vertraulichkeit.
- Tor
  - ist ein Netzwerk zur Anonymisierung der Verbindungsdaten.
  - kann beispielsweise für Web-Browsing, Instant Messaging, IRC, SSH, E-Mail, P2P und andere benutzt werden.
  - schützt vor der Analyse des Datenverkehrs seiner Nutzer.
  - kann helfen, Zensur zu umgehen.

Einleitung - Passphrase

- Nur eine starke Passphrase und ein Rechner frei von Schadsoftware machen den Einsatz von GnuPG und TrueCrypt sinnvoll. Das schwächste Glied in einer Kette von Sicherheitsmaßnahmen bestimmt die Stärke.
- Voraussetzungen für eine sichere Passphrase
  - Viele Zeichen (absolutes Minimum 8 Empfohlen 20)
  - Mischung aus Groß- und Kleinbuchstaben a...z, A...Z
  - Mindestens ein Zeichen aus 0...9
  - Mindestens ein Sonderzeichen !,“,..,§,$,...?,'
- No Goes
  - Worte aus dem Duden
  - Tastaturfolge 'qwert'
  - Geburtsdaten, Kontonummer
  - Allgemein geläufige Abkürzungen IBM, SAP, GnuPG

Wie komme ich zu einer sicheren Passphrase/Mantra

Wie komme ich zu einer sicheren Passphrase/Mantra

Wie komme ich zu einer sicheren Passphrase/Mantra

Agenda

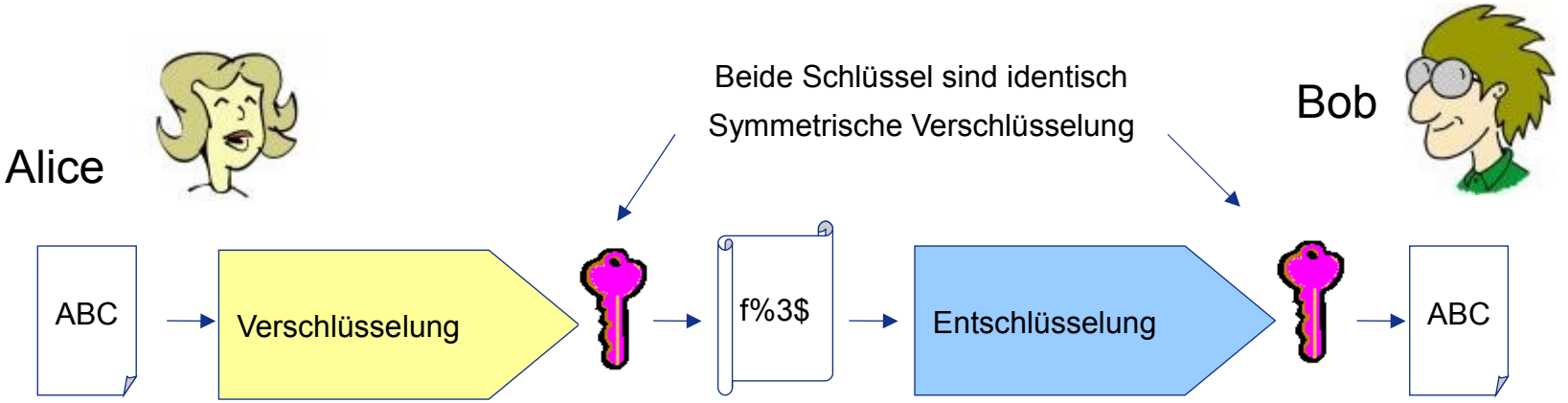
1. Begrüßung und Vorstellung
2. Einleitung – Kurzvorstellung der Tools
3. **GnuPG**
4. TRUECRYPT
5. Tor
6. Zusammenwirken der Tools
7. Fragen und Diskussion

GnuPG - Allgemeines

- GnuPG oder GPG (GNU Privacy Guard, Privatsphärenschutz) ist ein freies Kryptographiesystem, d.h., es wird eingesetzt
  - zum Verschlüsseln und Entschlüsseln von Daten
  - zum Erzeugen und Prüfen elektronischer Signaturen.
- Es implementiert den OpenPGP-Standard nach RFC 4880 – ersetzt PGP
- Versionen ab 2.0 implementieren auch den S/MIME-Standard.
- GnuPG benutzt standardmäßig nur patentfreie Algorithmen und wird unter der GNU-GPL vertrieben.
- Es kann unter GNU/Linux, Mac OS X (eingeschränkt) und diversen anderen unixoiden Systemen sowie unter Microsoft Windows betrieben werden.
- Läuft nicht unter
  - iPhone, ...

Symmetrische Verschlüsselung hat ein Problem

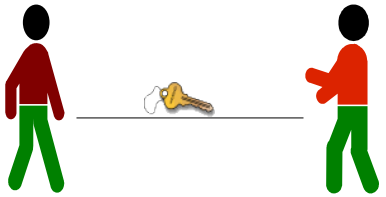
- Klassische Verfahren nutzen einen Schlüssel: Sender verschlüsselt mit dem selben Schlüssel, den der Empfänger zum Entschlüsseln nutzt – symmetrische Verschlüsselung.
- Hauptprobleme sind der sichere Austausch des genutzten Schlüssels, Anzahl der Schlüssel, Einmalnutzung des Schlüssels.
- Sie werden trotzdem benutzt, weil sie einfach und schnell sind.



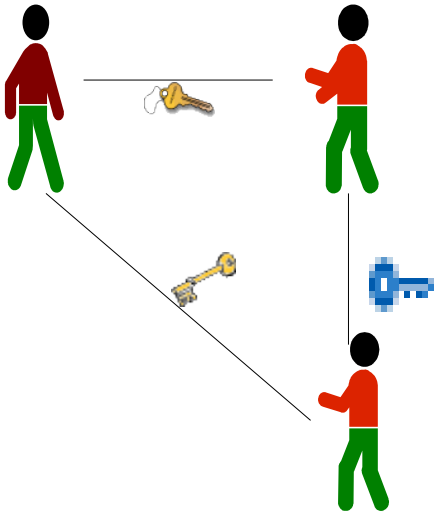
Symmetrisches Verschlüsselungssystem

Problem: Für n Personen, die alle untereinander geheim kommunizieren möchten, werden insgesamt **S = n(n-1) / 2** Schlüssel benötigt.

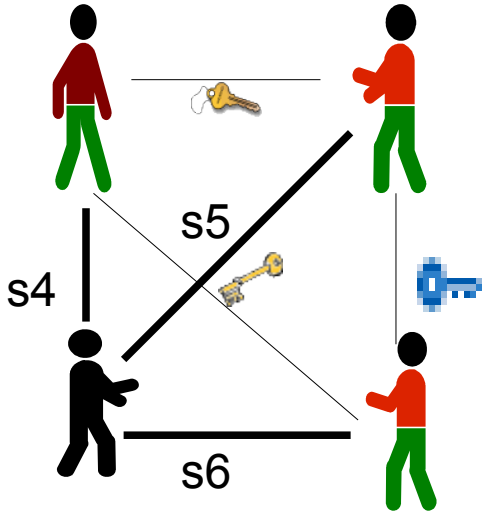
2 Personen = 1 Schlüssel



3 Personen = 3 Schlüssel



4 Personen = 6 Schlüssel



5 Personen = 10 Schlüssel
50 Personen = 1225 Schlüssel
1000 Personen = 499.500 Schlüssel

Public Key Verschlüsselung (GnuPG)

- Public Key Verfahren beseitigen das Problem des Austauschs, indem zwei Schlüssel generiert werden: ein öffentlicher Schlüssel  und ein geheimer Schlüssel. 
- Der öffentliche Schlüssel kann bedenkenlos an die Kommunikationspartner verteilt  werden. Diese nutzen den öffentlichen Schlüssel, um E-Mails/Anhänge an den Besitzer zu verschlüsseln.
- Der geheime Schlüssel verbleibt beim Besitzer und wird sicher verwahrt.

  - Der Besitzer kann alleinig mittels seines geheimen Schlüssels die E-Mail wieder entschlüsseln, die mit dem öffentlichen verschlüsselt wurde.
  - Der Besitzer nutzt den geheimen Schlüssel, um seine E-Mails/Anhänge zu signieren. Damit stellt er sicher, dass die gesandten Daten von ihm sind (Authentizität) und die Daten nicht manipuliert wurden.
  - Der Empfänger kann dies überprüfen, indem er die Signatur mittels dem öffentlichen Schlüssel des Senders prüft (Hashfunktion)
- Der Entschlüsselungsschlüssel kann nicht aus dem Verschlüsselungsschlüssel abgeleitet werden.

Public Key Verschlüsselung (GnuPG)

- Versenden einer Nachricht
  - Alice nutzt Bobs öffentlichen (grünen) Schlüssel, um die Nachricht an Bob zu verschlüsseln

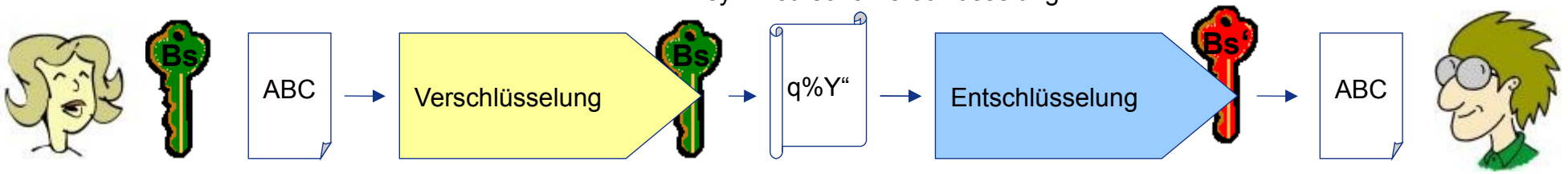
  - Nur Bob kann die Nachricht entschlüsseln, da er als Einziger den passenden/geheimen/privaten (roten) Schlüssel besitzt.

Alice

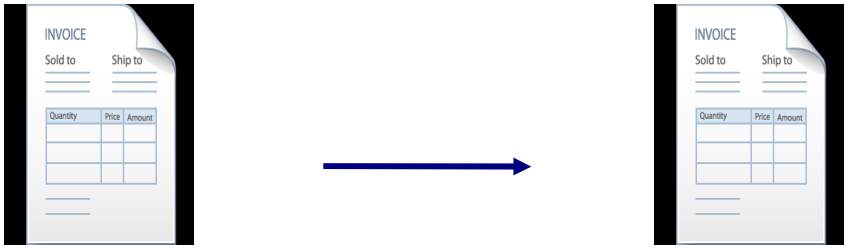
Bob

s‘ kann nicht mit vertretbarem Aufwand aus s abgeleitet werden.

Asymmetrische Verschlüsselung



Signaturverfahren (RSA) für Nachvollziehbarkeit und Integrität



MD5/SHA1 Verfahren erzeugt einen Hash

3A37EB5E 2288B830

MD5/SHA1 Verfahren erzeugt einen Hash

3A37EB5E 2288B830

identisch ???

Verschlüsselt den Hash

Privater Schlüssel von Alice

3A37EB5E 2288B830

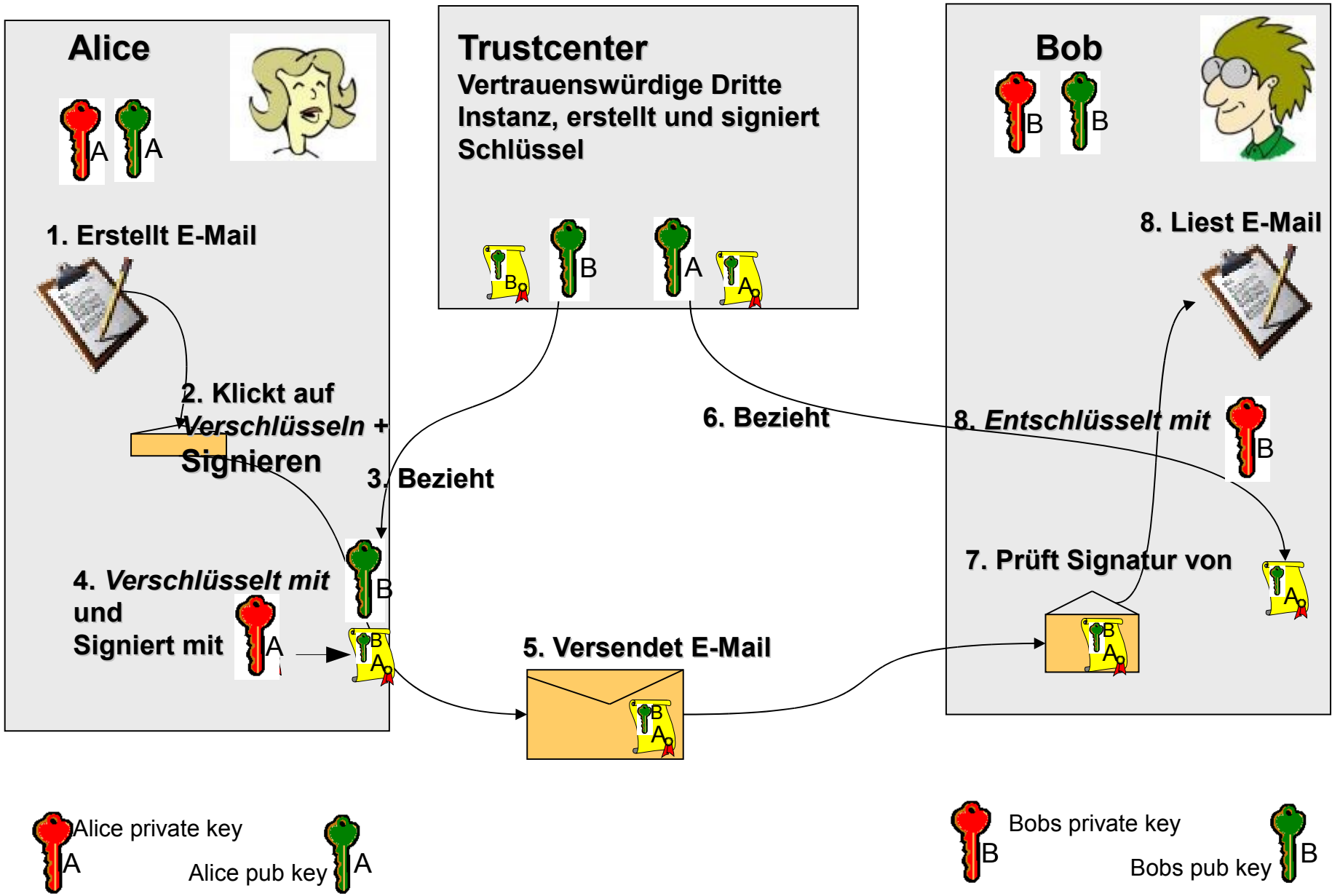
Entschlüsselt den Hash

Öffentlicher Schlüssel von Alice

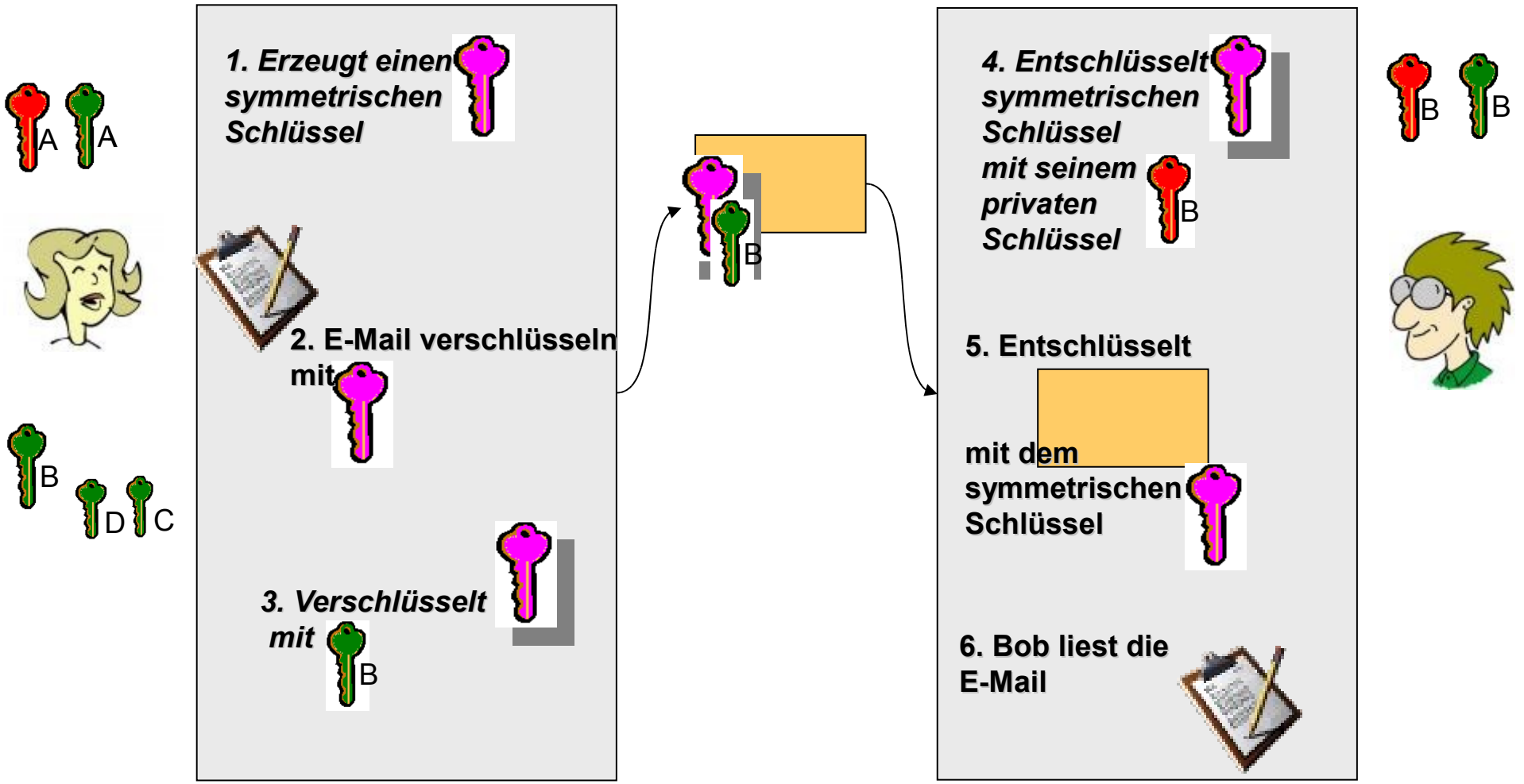
02F72BF5 747AB807

02F72BF5 747AB807

S/Mime E-Mail mit digitaler Signatur und Verschlüsselung



Hybride Ver- und Entschlüsselung



GnuPG im Alltag

- GnuPG ist nicht nur eine komplexe Software, es gibt auch technische, gesellschaftliche und rechtliche Aspekte, die berücksichtigt werden sollten:
  - Die eingesetzte Technik muss in verschiedenen Situationen mit drastisch unterschiedlichen Sicherheitsanforderungen umgehen können. Das macht die Schlüsselverwaltung kompliziert.
  - Der Einsatz von GnuPGP ist keine alleinige persönliche Entscheidung, sondern erfordert, dass es mindestens einen Kommunikationspartner gibt, der dies auch einsetzen will.
  - Die Haltung der Gesetzgeber ist länderspezifisch. Die legale Nutzung von GnuPG respektive Verschlüsselung wird in vielen Ländern national diskutiert

Warum und wie sollte ich GnuPG nutzen

- Der wichtigste Grund ist der Schutz der Privatsphäre
  - Ich will mit anderen korrespondieren, ohne dass Dritte mitlesen können.
  - Ich will meine Daten auf meinem Rechner vor dem unbefugten Zugriff Dritter schützen.
  - Ich will meine Daten (E-Mail) durch digitale Signaturen authentifizieren und deren Integrität gewährleisten.
- Wie und mit welchem Aufwand ich es tue, hängt davon ab, wie zielstrebig und findig der „Dritte“ ist.
  - Ist es „nur“ ein neugieriger Systemadministrator?
  - Ist es „nur“ der/das neugierige Partner, Kind oder Mitbewohner?
  - Ist es ein Industriespion, der Ihr Firmengeheimnis ausspähen möchte?
  - Ist es ein Geheimdienst, in einem Land in dem Sie als Journalist arbeiten?
  - Ist es der Staatsanwalt, der ihnen auf den Fersen ist?
- Der Aufwand, den man für Verschlüsselung treiben sollte, hängt vom vermuteten Angreifer ab.

Der Aufwand muss den Wert der Daten rechtfertigen.

Wie oder was ist wichtig bei der Verschlüsselung

- Die Wahl der Schlüssellänge Ihres öffentlichen und privaten Schlüsselpaars
  - Je länger der Schlüssel, desto besser der Schutz gegen Brute-Force-Angriffe
  - Je länger der Schlüssel, desto länger dauert der Ver- und Entschlüsselungsvorgang
- Der Schutz Ihres geheimen Schlüssels
  - hindert Angreifer daran, einfach Ihren geheimen Schlüssel zum Entschlüsseln verschlüsselter Nachrichten zu verwenden oder aber Nachrichten in ihrem Namen zu unterschreiben.
- Die Verfallsdaten Ihrer Schlüssel und die Benutzung von Unterschlüsseln
- Der Aufbau Ihres Web of Trust
  - verhindert, dass sich ein Unbefugter als einer Ihrer Korrespondenzpartner ausgeben kann.

Wahl der Schlüssellänge

- Hängt von der Art des Schlüssels ab
  - OpenPGP nutzt gewöhnlich ein Schlüsselbund aus mehreren öffentlichen und geheimen Schlüsseln.
  - Mindestens ein Hauptschlüssel zum Signieren und einen oder mehrere Unterschlüssel zum Verschlüsseln.
    - GnuPT ist ein hybrides Verfahren, d.h., der öffentliche Schlüssel wird benutzt, um den 128-Bit symmetrischen Sitzungsschlüssel zu verschlüsseln und der private Schlüssel wird für die Entschlüsselung genutzt.
    - Schlüssellänge beeinflusst Zeit zum Ver- und Entschlüsseln, Rechenaufwand steigt exponentiell zur Schlüssellänge – 1024 Bit sollten reichen
    - Praktischer Nutzen eines längeren Schlüssels zweifelhaft, da es andere Möglichkeiten gibt als Durchprobieren (Brute Force)

Ist der Sicherheitsbedarf so groß? – Einen Sicherheitsexperten fragen.

Schutz des geheimen Schlüssels

- Ist wichtig, denn
  - wenn ein Dritter Ihren geheimen Schlüssel hat, vorausgesetzt er „errät“ oder „erfährt“ Ihre Passphrase/Mantra, dann
    - kann er alle E-Mails entschlüsseln, die mit ihrem öffentlichen Schlüssel verschlüsselt wurden
    - kann er Dateien in Ihrem Namen signieren
  - wenn Sie Ihren geheimen Schlüssel „verlieren“ oder ähnliches, dann
    - können Sie all Ihre verschlüsselten Daten nicht mehr entschlüsseln und so nicht mehr lesen – die Daten sind quasi wertlos
    - können sie keine Unterschrift mehr leisten

Der Verlust des geheimen Schlüssels

ist aus Sicht der Datensicherheit eine Katastrophe.

Schutz des geheimen Schlüssels

- Das sollten Sie auf jeden Fall tun:
  - Widerrufsurkunde des öffentlichen Schlüssels und
  - Sicherheitskopie Ihres geheimen Schlüssels auf einen schreibgeschützten Datenträger (der die Gültigkeitsdauer ihres Schlüssels überlebt) speichern und
  - an einem sicheren Ort aufbewahren (Bankschließfach, gut verstecken, auf jeden Fall getrennt vom „eigentlichen System“. Sorgfältiger aufbewahren als die Kopie Ihres täglich genutzten geheimen Schlüssels.)
  - Zusätzlich kann es von Nutzen sein, einen ASCII Ausdruck auf Papier aufzubewahren.

Widerrufsurkunde

- Widerrufsurkunden
  - Nach dem Erzeugen Ihres Schlüsselpaars
  - eine Widerrufsurkunde für Ihre Schlüssel erzeugen.
  - Haben Sie Ihr Mantra vergessen oder
  - ist Ihr privater Schlüssel kompromittiert oder verloren gegangen,
  - so können Sie mit dieser Widerrufsurkunde andere davon in Kenntnis setzen, dass der dazugehörige öffentliche Schlüssel nicht mehr benutzt werden soll.
  - Ein zurückgerufener öffentlicher Schlüssel kann noch benutzt werden,
    - um Unterschriften zu prüfen, die Sie vor dem Widerruf abgegeben haben.
    - Sofern Sie noch Zugang zu Ihrem widerrufenen geheimen Schlüssel haben, so können Sie selbstverständlich noch Daten entschlüsseln, die vor dem Widerruf für Sie verschlüsselt worden sind.
    - Das Verschlüsseln mit dem öffentlichen Schlüssel ist nicht mehr möglich.

Schutz des geheimen Schlüssels

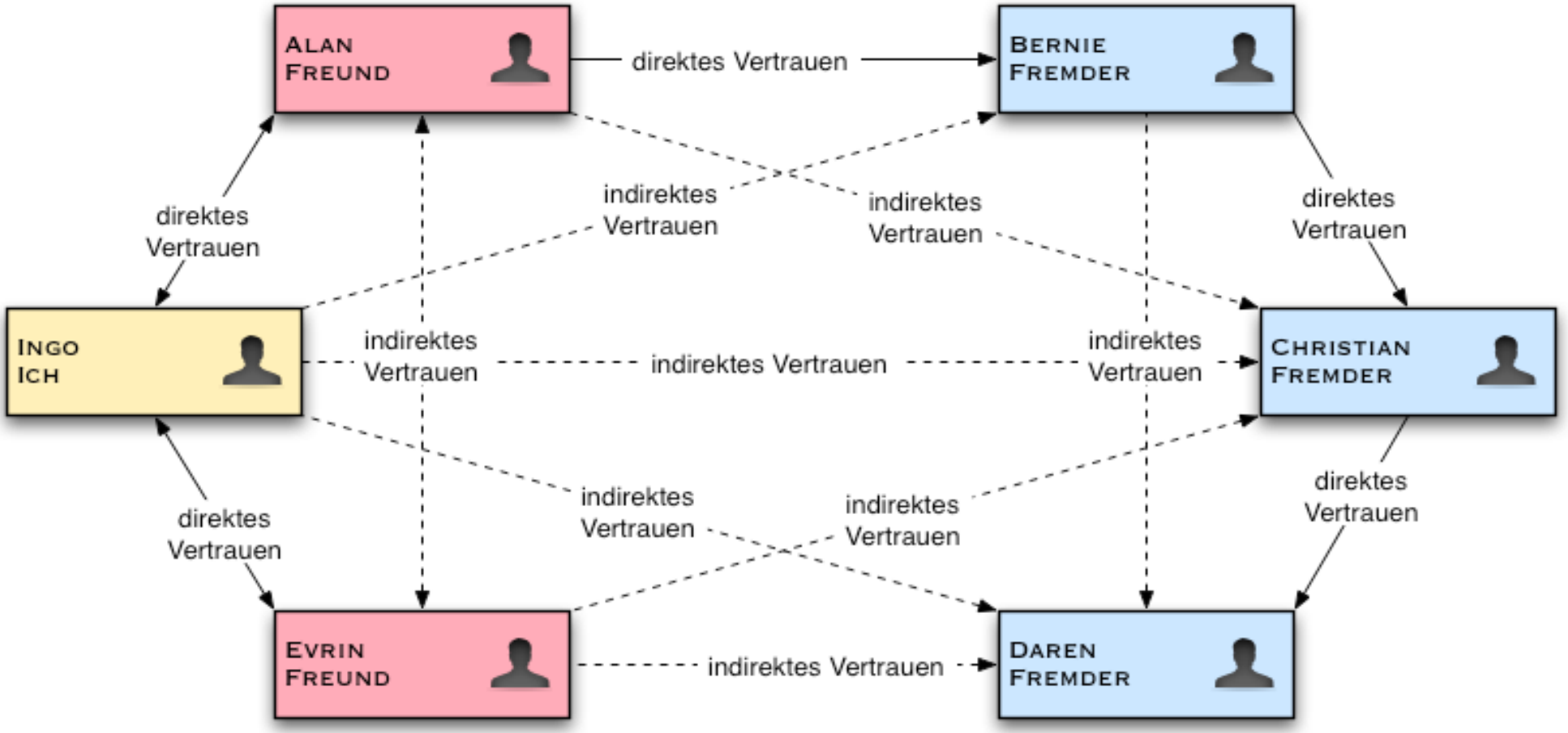
- GnuPG speichert Ihren privaten Schlüssel nicht in „roher" Form ab, sondern verschlüsselt ihn
  - unter Benutzung eines symmetrischen Verschlüsselungsverfahrens.
  - Sie brauchen das „Mantra“ oder die Passphrase, um mit Ihrem geheimen Schlüssel zu entschlüsseln oder zu signieren.
- Ein Angreifer muss also zwei Probleme lösen, um Zugang zu Ihrem geheimen Schlüssel zu bekommen:
  - Er muss den geheimen Schlüssel bekommen.
  - Er muss entweder
    - dessen Verschlüsselung knacken oder
    - an das Mantra kommen.

Schutz des geheimen Schlüssels

- Die sichere Aufbewahrung Ihres geheimen Schlüssels ist wichtig, doch auch mit einigem Aufwand verbunden.
  - Idealerweise gehört der geheime Schlüssel auf einem mobilen, schreibgeschützten Datenträger
  - oder auf einen *nicht vernetzten* Computer, zu dem nur Sie Zugang haben.
- Das heißt aber nicht, dass Sie nun GnuPG anders nicht benutzen können oder sollten.
- Sie haben sich nur entschieden, dass Ihnen Ihre Daten zwar wichtig genug sind, um sie zu verschlüsseln,
- aber nicht so wichtig, dass Sie besondere Maßnahmen treffen müssten, um die erste Barriere sicherer zu machen. Es ist letztlich Ihre Entscheidung, ob Ihr Sicherheitsanspruch damit schon erfüllt ist oder nicht.

Web of Trust – Graphische Darstellung

Graphik: wikipedia Jens Kohl



Web of Trust

- Verwaltung des Web of Trust erfordert Abwägung zwischen Aufwand und Nutzen
  - Beim Schutz gegen mehr oder weniger zufälliges Mitlesen und Dokumentenfälschungen kann man relativ vertrauensvoll hinsichtlich der digitalen Signaturen anderer Leute sein.
  - Firmen, die Angst vor Spionage haben, sollten die Unterschriften anderer sorgfältig prüfen.
- Trotzdem immer sorgsam mit dem Signieren von fremden Schlüsseln umgehen.
  - Im Sinne des Web of Trust ist es nicht ratsam, einen Schlüssel zu unterschreiben, dessen Authentizität Sie gerade noch so weit vertrauen, wie es für Ihr eigenes Sicherheitsbedürfnis ausreichend ist. Andere, die einen höheren Sicherheitsbedarf haben, sollten sich auf Ihre Unterschrift verlassen können.
  - Wenn man sich auf Ihre Signatur nicht verlassen kann, dann schwächt dies das Web of Trust und macht die Kommunikation für alle Benutzer von GnuPG schwieriger.

Web of Trust

- Tipp: Lassen Sie also beim Unterschreiben von Schlüsseln dieselbe Sorgfalt walten, die Sie von anderen auch angewandt sehen möchten, wenn Sie sich auf deren Unterschriften verlassen.

- Bei der Verwaltung Ihres Web of Trust sollten Sie sich auf zwei Dinge konzentrieren: Einerseits auf die Frage, wessen Schlüssel Sie genügend vertrauen, um sie selber zu signieren, und andererseits auf das Abstimmen der Optionen --marginals-needed und --completes-needed. Jeder Schlüssel, den Sie persönlich signieren, wird als gültig betrachtet, deshalb ist es - außer in kleinen Gruppen - keine gute Praxis, persönlich den Schlüssel jeder Person zu unterschreiben, mit der Sie kommunizieren. Sinnvoller ist es, sich daran zu gewöhnen, den Unterschriften anderer zu vertrauen.

Web of Trust

- Es ist wahrscheinlich die beste Strategie, beim Unterzeichnen von Schlüsseln genau die Authentizität des Schlüssels bzw. die Identität des Schlüsselbesitzers zu überprüfen und ansonsten durch Optionen zu bestimmen, wie sorgfältig GnuPG bei der Authentisierung sein soll.
- Ein konkretes Beispiel: Sie mögen einigen wenigen engen Freunden voll vertrauen, von denen Sie wissen, dass diese beim Unterschreiben von Schlüsseln sorgfältig vorgehen; den weiteren Schlüsselbesitzern in Ihrem Schlüsselbund vertrauen Sie in dieser Hinsicht nur teilweise. Danach können Sie --completes-needed auf 1 und --marginals-needed auf 2 setzen. Wenn Sie hinsichtlich der Sicherheit stärker besorgt sind, können Sie auch die Werte 1 bzw. 3 oder 2 bzw. 3 wählen. Wenn Sie allerdings mit einem weniger großen Vertrauen hinsichtlich der Authentizität auskommen wollen und nicht so sehr mögliche Angriffe auf Ihre Privatsphäre oder Firmendaten befürchten, dann können Sie die Werte 1 und 1 einsetzen. Je höher die Werte für diese Optionen sind, desto schwieriger ist es, Ihnen einen gefälschten Schlüssel unterzuschieben.

Rechtliche Aspekte der Verschlüsselung/Signatur

- Grundsätzlich ist dieses Thema Ländersache – es gibt keine umfassende globale Regulierung, aber diverse internationale Regulierungen.
- Gesetze ändern sich schnell, jeder muss sich aktuell informieren – Holschuld.
- Allgemeine Themen sind dabei
  - Export von Crypto-Verfahren
  - Nutzung bestimmter Crypto-Verfahren/Schlüssellänge
  - Hinterlegung des privaten Schlüssels
  - Grundsätzliches Handling
  - Signaturgesetz (SigG)
- Eine mögliche Informationsseite ist die von Bert-Jaap Koops

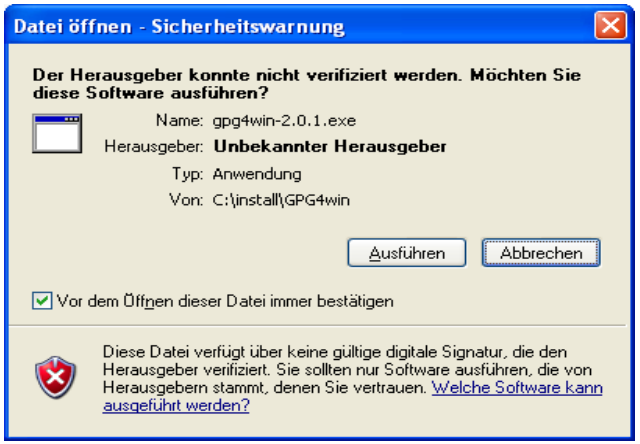
http://rechten.uvt.nl/koops/cryptolaw/

Restrisiken

- Personen mit physikalischem Zugriff auf die Hardware können Keylogger in den PC einbauen, die die Passphrase mitschneiden.
- Die Abstrahlung von Hardwarekomponenten (Tempest), z.B. Grafikkarten, kann mit empfindlichen Empfängern abgehört werden.
- Man kann beim Eingeben der Passphrase beobachtet werden (z.B. durch Überwachungskameras, Shouldersurfing).
- Jede Software kann durch das Betriebssystem, auf dem sie läuft, kompromittiert werden (z.B. durch ein Rootkit).
- Malware kann die Passphrase oder den Inhalt einer verschlüsselten E-Mail Dritten zugänglich machen.
- Das Web of Trust funktioniert nicht immer, manchmal kann man Public Keys nicht zuverlässig einer vertrauenswürdigen Person zuordnen.
- Der Einsatz auf einem System, über das man nicht vollständige Kontrolle besitzt, birgt Risiken (Internet Cafe, Firmenrechner, auf dem man nicht selbst Administrator ist), wenn unklar ist, ob man dem Betreiber vertrauen kann.
- Die Einschätzung der Vertrauenswürdigkeit von Partnern kann trügerisch sein, etwa wenn jemand unvorsichtig mit GnuPG umgeht.
- Das Enigmail Plugin war zum Zeitpunkt des Vortrags unsigniert, damit ist das Programm nur eingeschränkt vertrauenswürdig.
- Die GnuPG Sourcen und Binaries sind mit public keys signiert, deren Echtheit man vertrauen muss, auch wenn man die dahinter stehenden Entwickler nicht kennt.

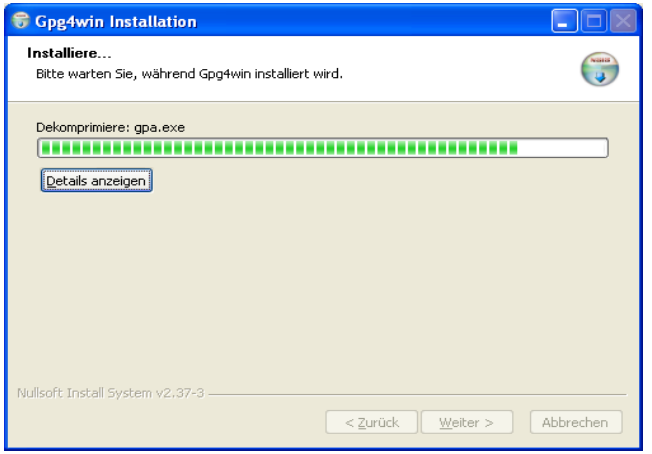
Installation - GnuPG

- http://www.gpg4win.org/ GPG4Win downloaden
- Installieren:
- Abfrage bestätigen (Die Signaturen liegen separat auf der Seite.)



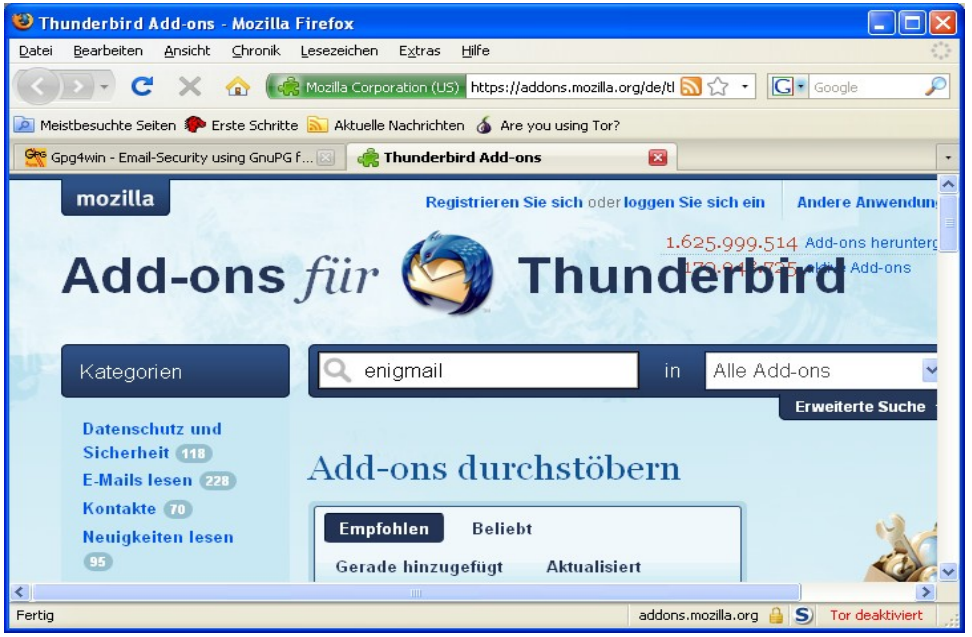
- Sprache auswählen

Installation - GnuPG



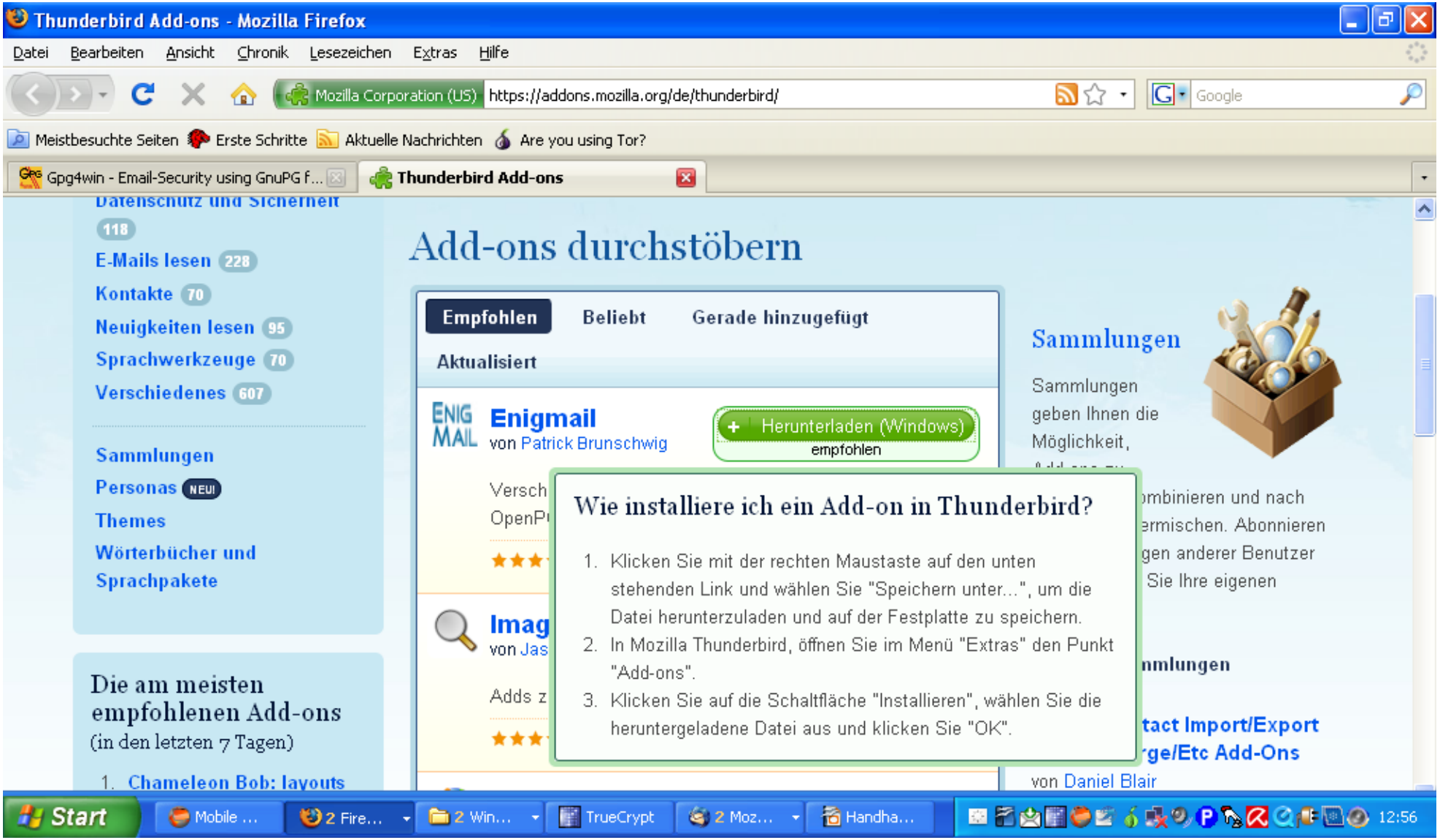
- Sprache auswählen
- Komplett installieren
- Im Thunderbird unter Extras → addons herunterladen (öffnet Browser)

Installation - GnuPG

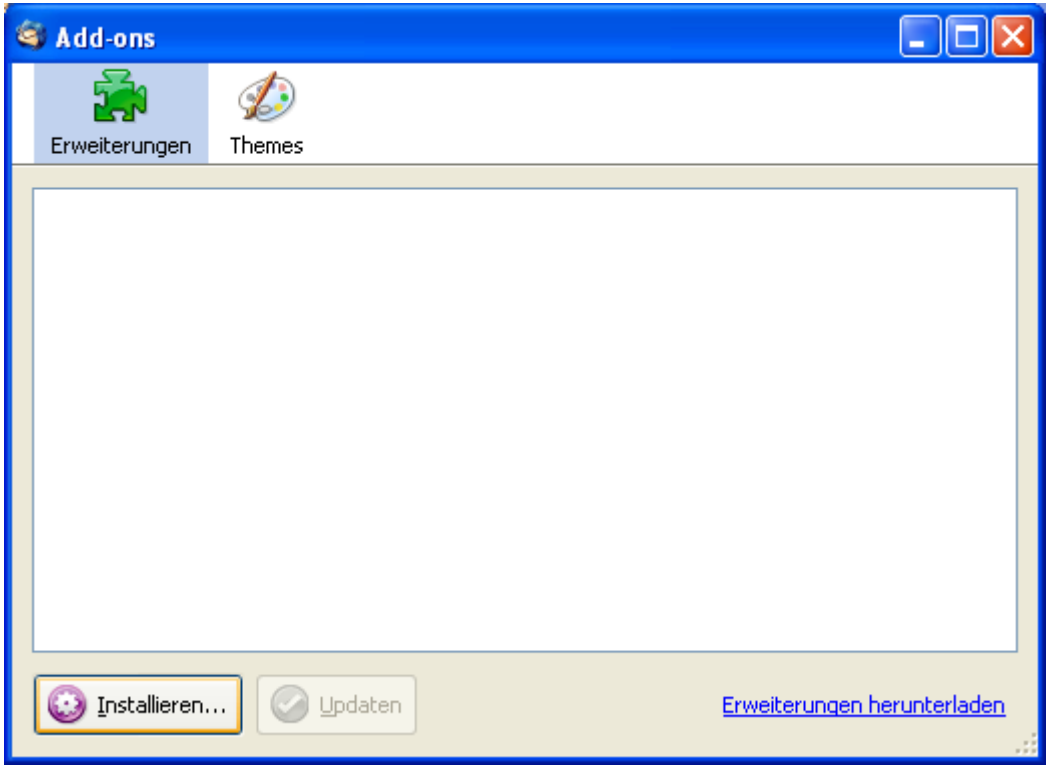


- Addon Suche: enigmail auswählen Sprache auswählen
- Komplett installieren
- Im Thunderbird unter Extras → addons herunterladen (öffnet Browser)

Installation - GnuPG

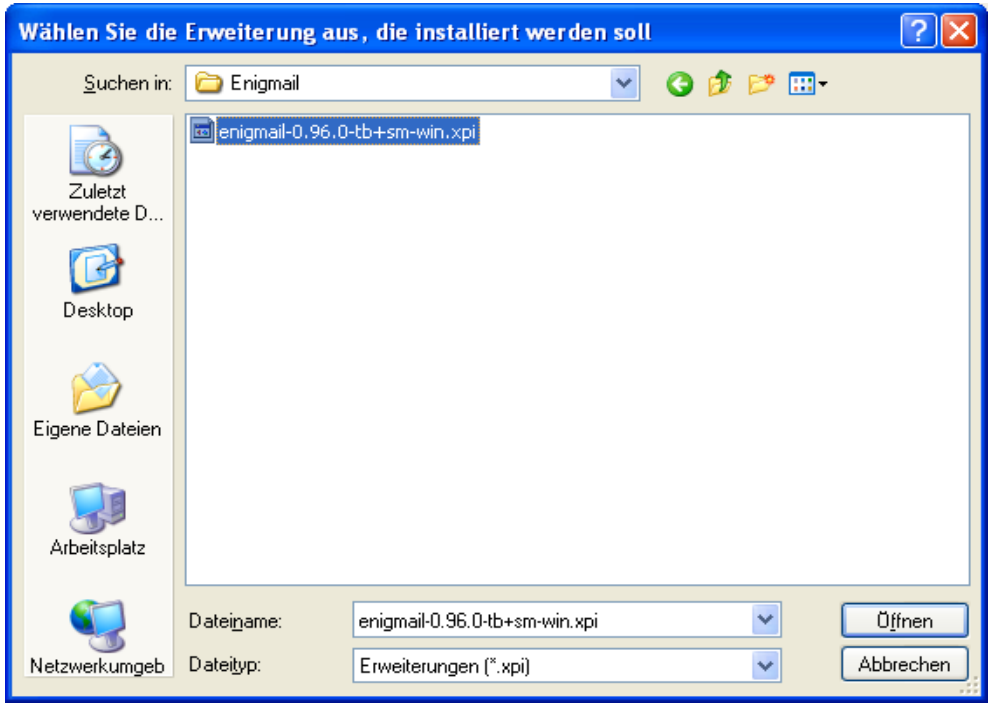


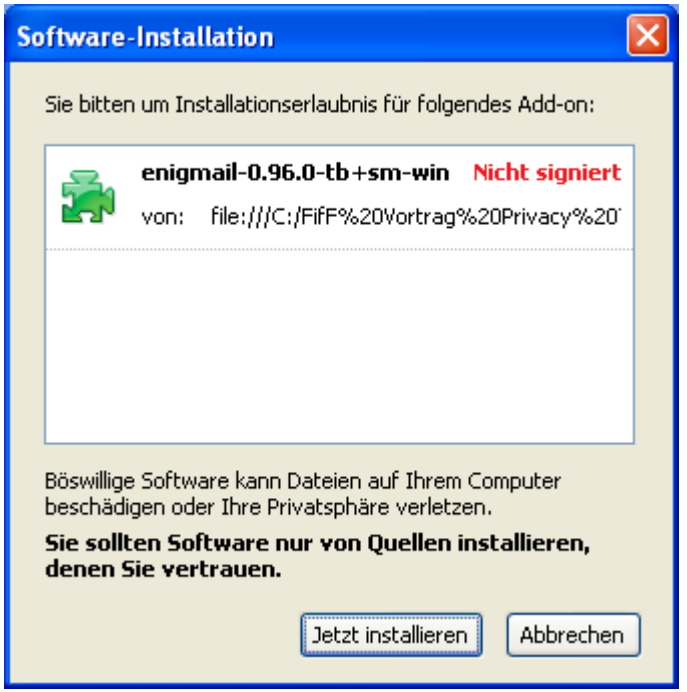
Installation - GnuPG



- Im Thunderbird Addon Menue (Extras, Addon) auf <installieren>
- Ins Verzeichnis wechseln, in das der Browser das heruntergeladene Addon (enigmail (...).xpi File abgelegt hat, und das Enigmail Addon auswählen

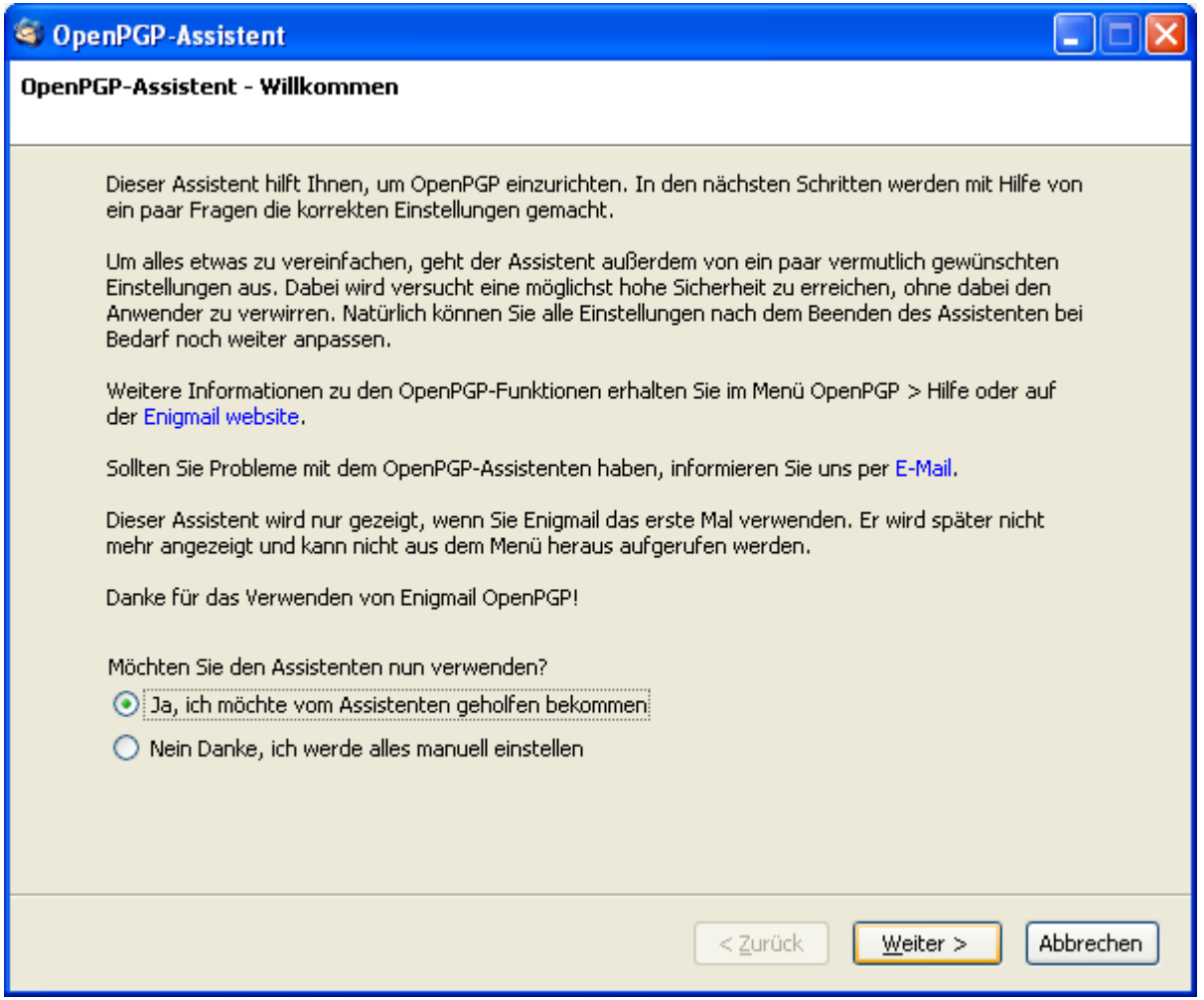
Installation - GnuPG





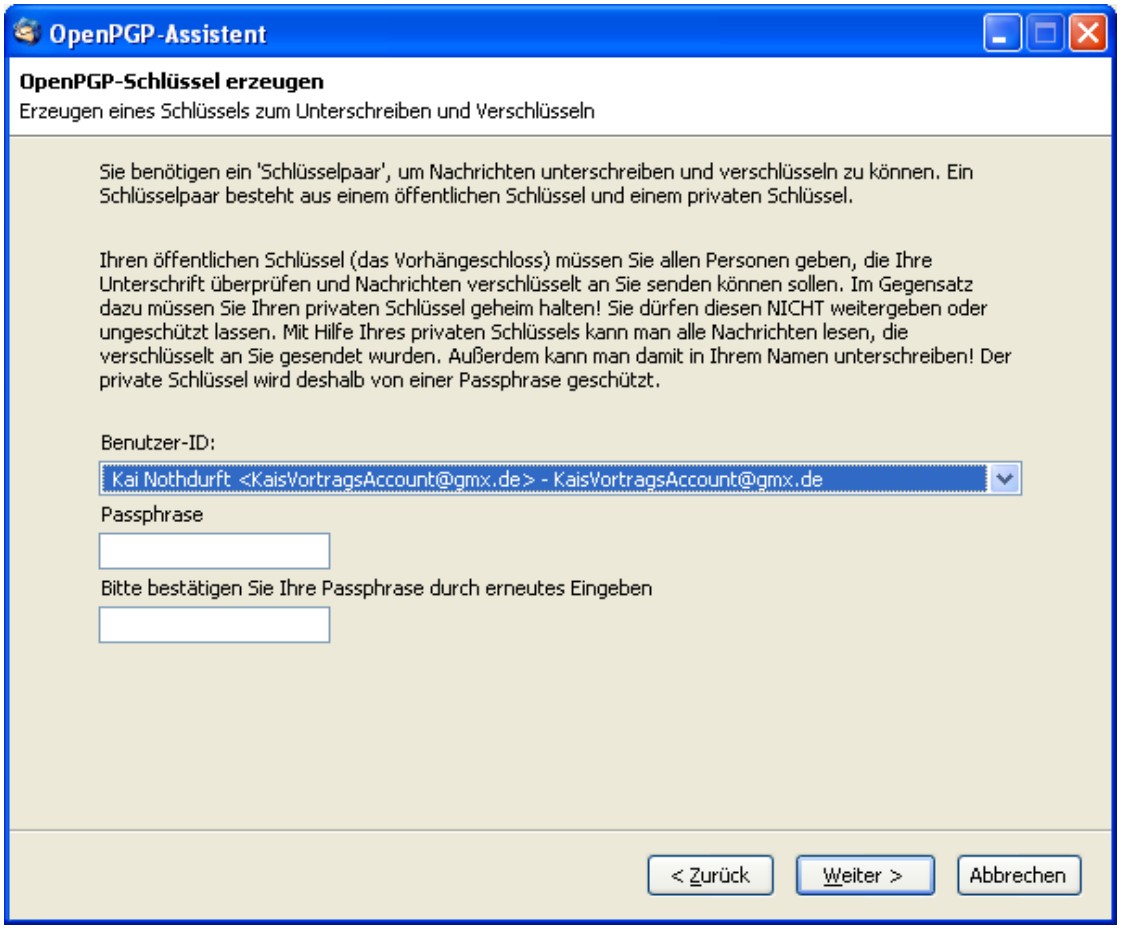
- Ins Verzeichnis wechseln, in das der Browser das heruntergelade Addon (enigmail (...).xpi File abgelegt hat und das Enigmail Addon auswählen
- <Jetzt installieren> und <Thunderbird neu starten>

Konfiguration von ENIGMAIL



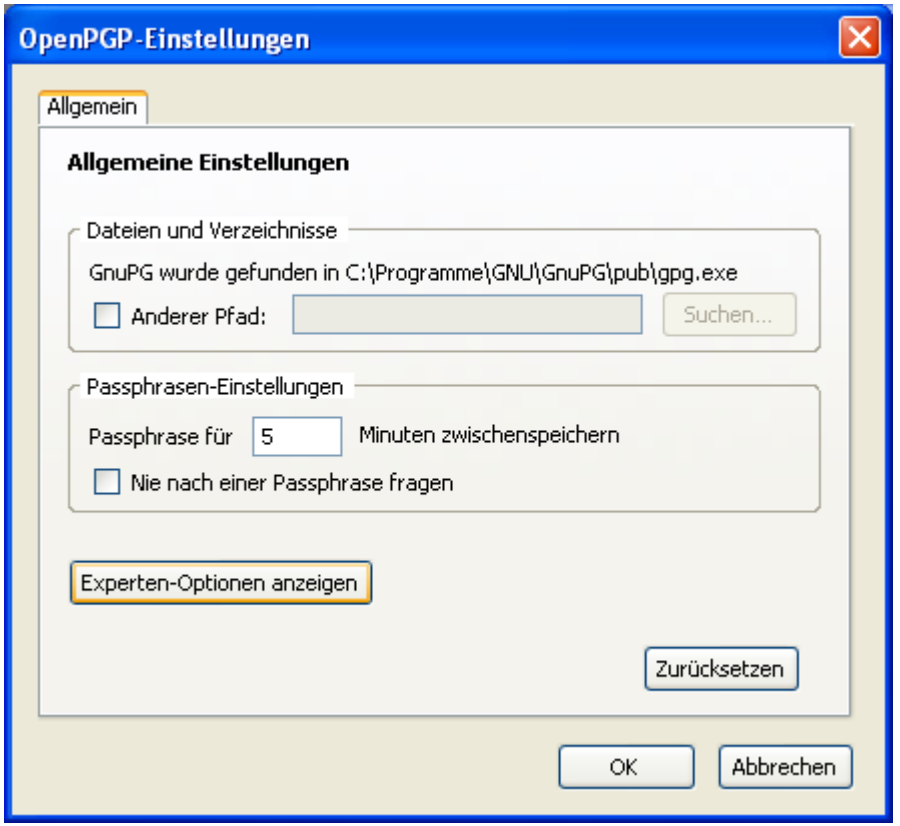
Konfiguration von ENIGMAIL

Die Schlüsselgenerierung kann entweder in Enigmail oder direkt mit GPA, der grafischen Benutzeroberfläche von GnuPG, durchgeführt werden.



Konfiguration von ENIGMAIL

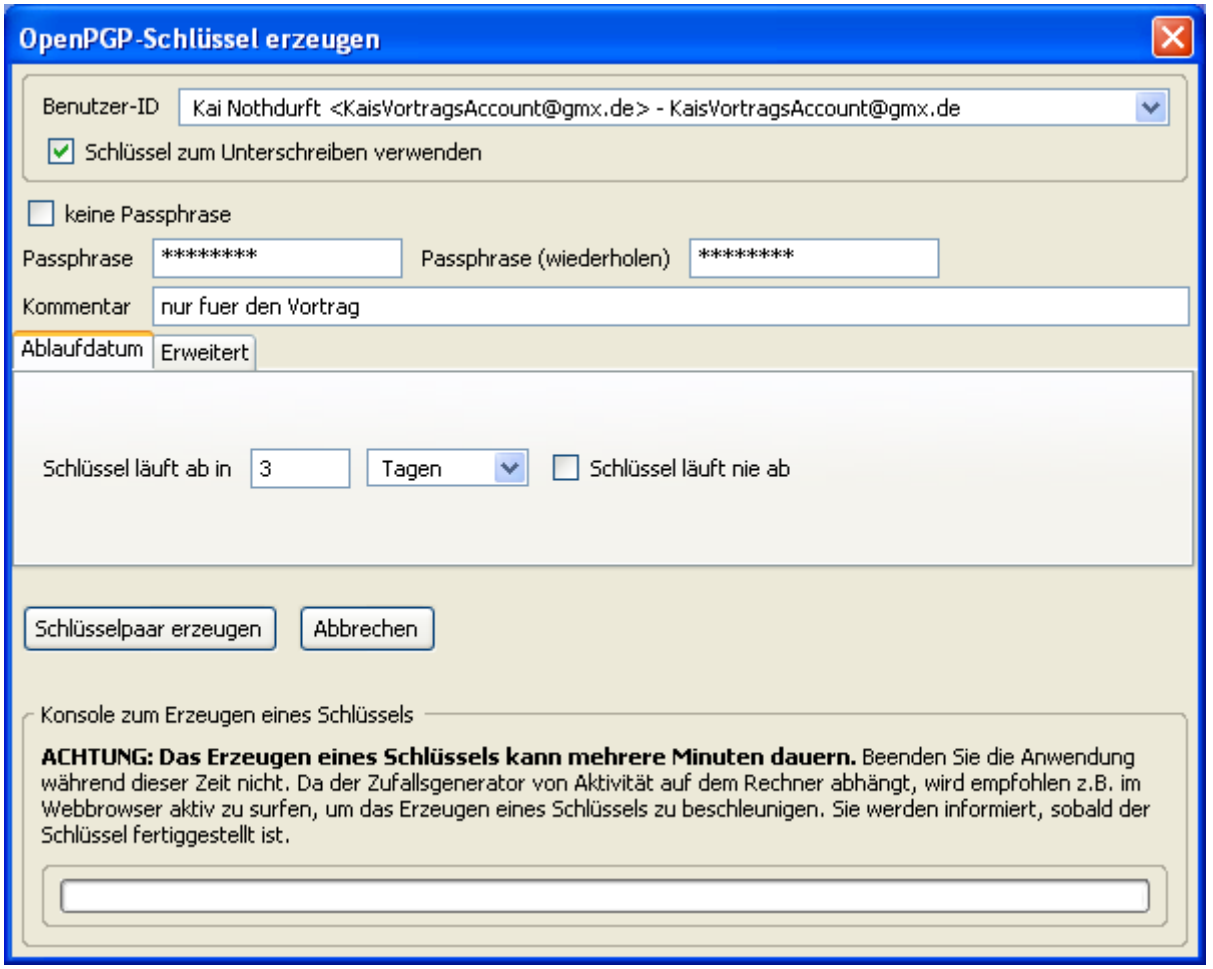
Einstellungen zu GnuPG:



Die Speicherzeit der Passphrase im Cache sollte nicht zu lange, schon gar nicht unendlich sein, damit sie nicht mit kompromittiert wird, falls das System einmal kompromittiert wird, z.B. durch Malware-Befall.

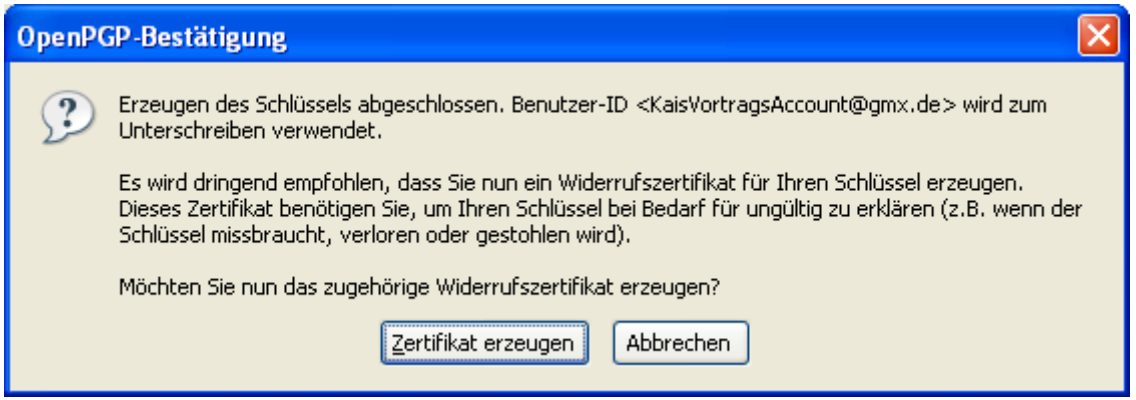
Konfiguration von ENIGMAIL

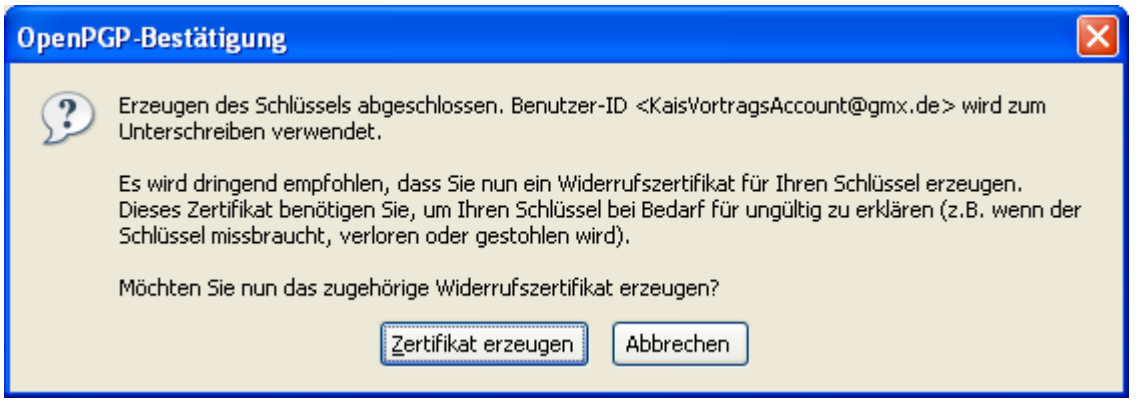
Schlüsselgenerierung mit Enigmail



Konfiguration von ENIGMAIL

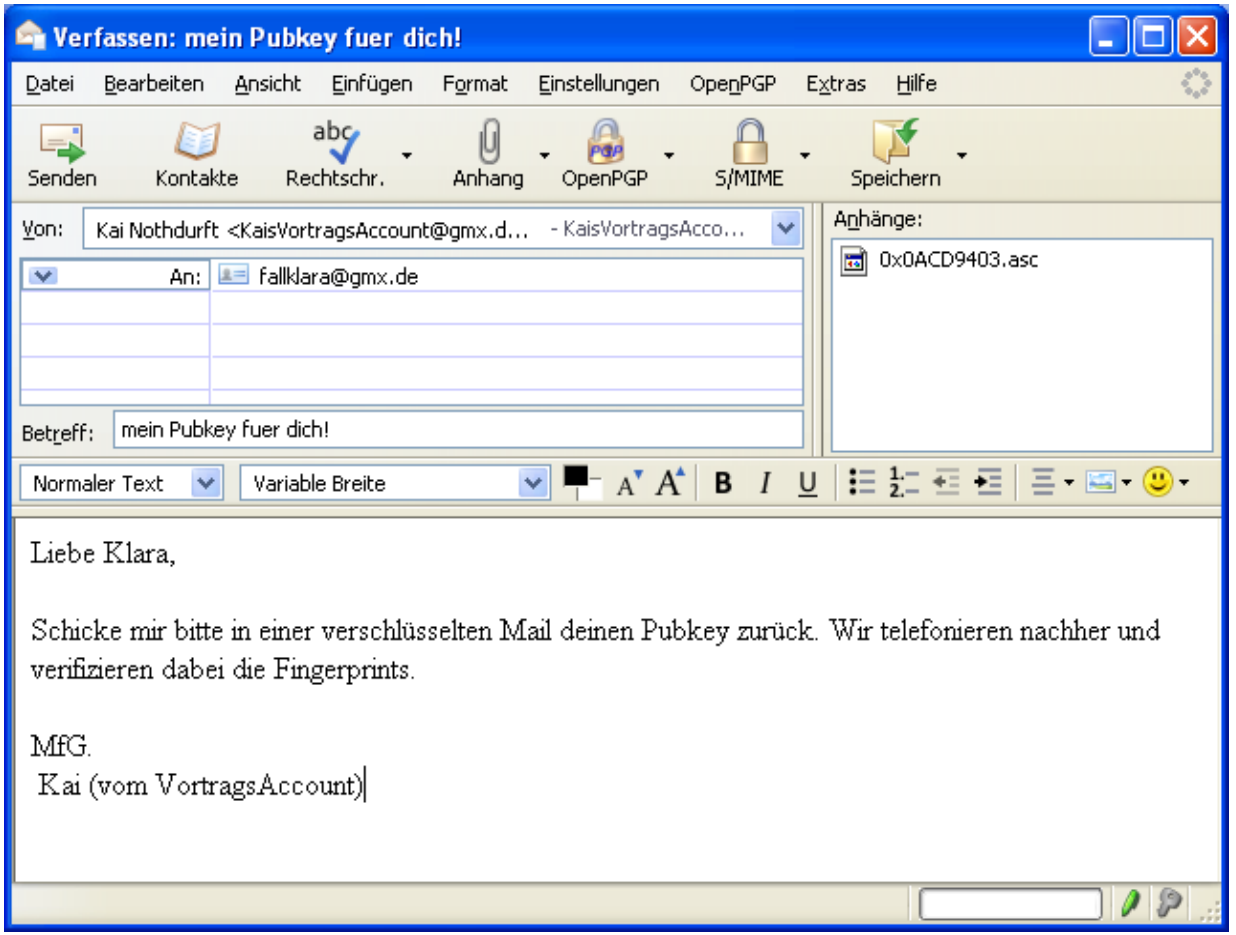
Schlüsselgenerierung mit Enigmail, Revokationszertifikat erzeugen und sichern





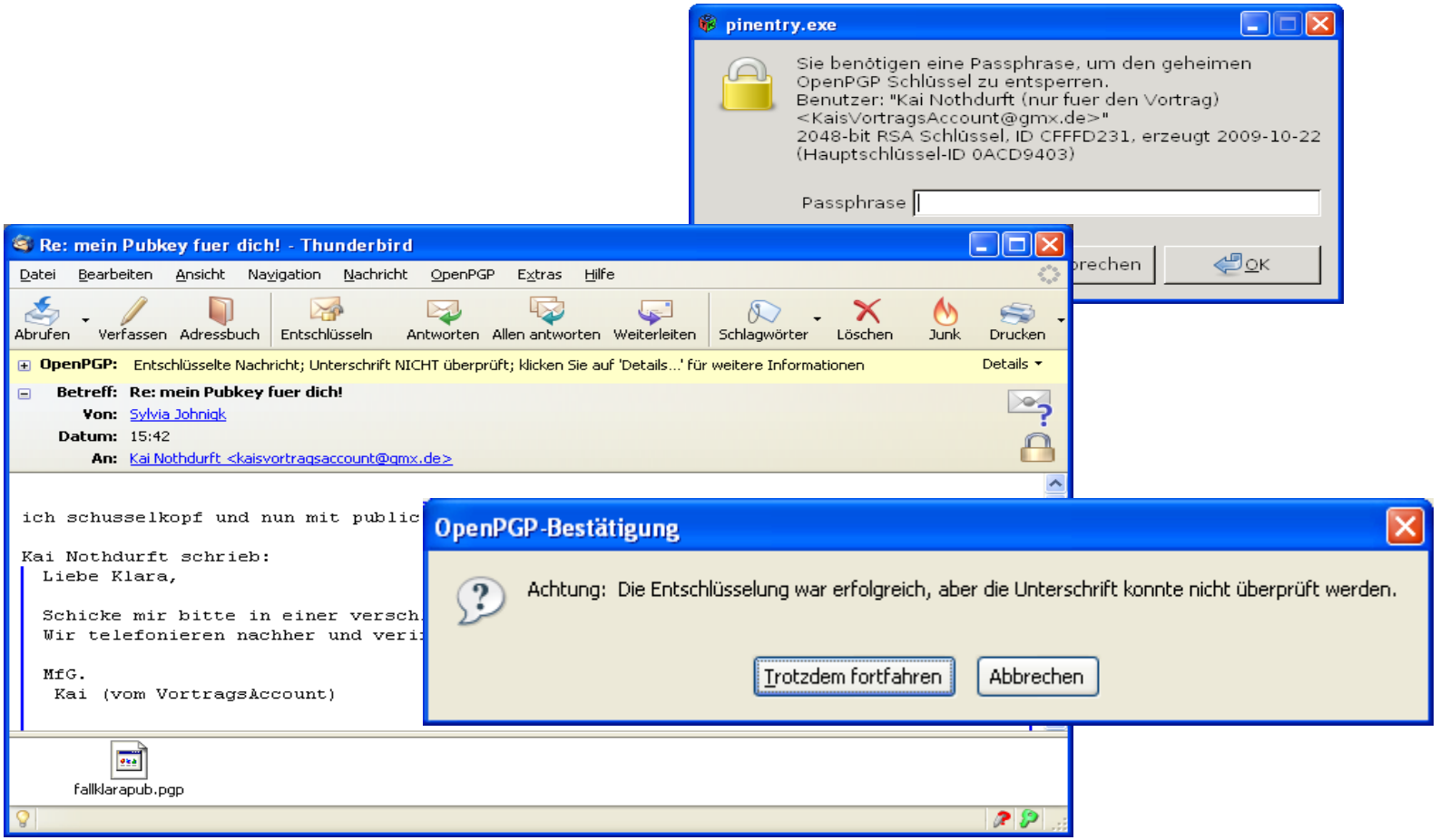
Übermittlung des Übermittlung des pubkey an einen Partner

Im Menü unter GnuPG die Einstellung: öffentlichen Schlüssel anhängen wählen und die E-Mail signieren.



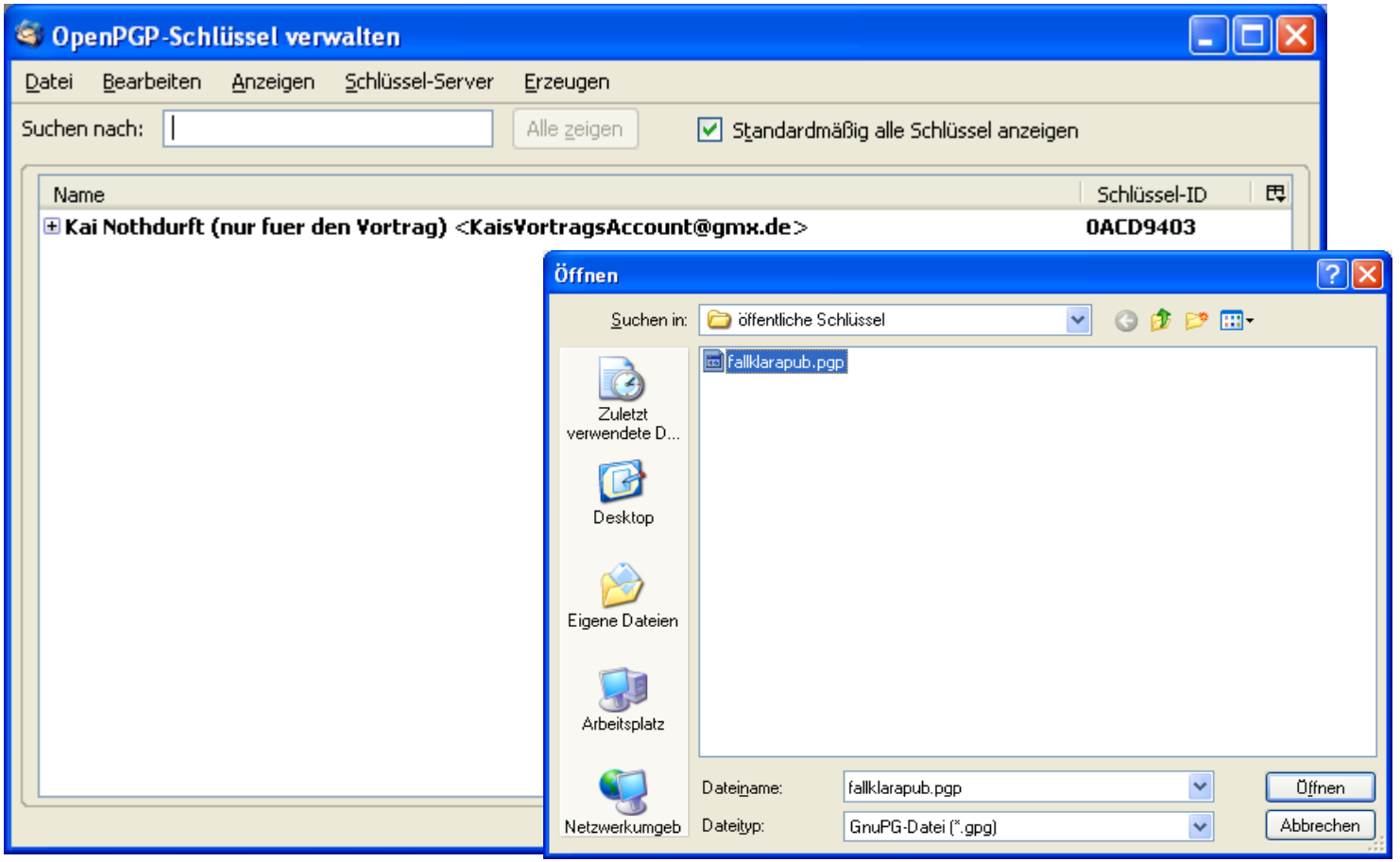
Übermittlung des Übermittlung des pubkey an einen Partner

Empfang einer verschlüsselten und signierten Mail



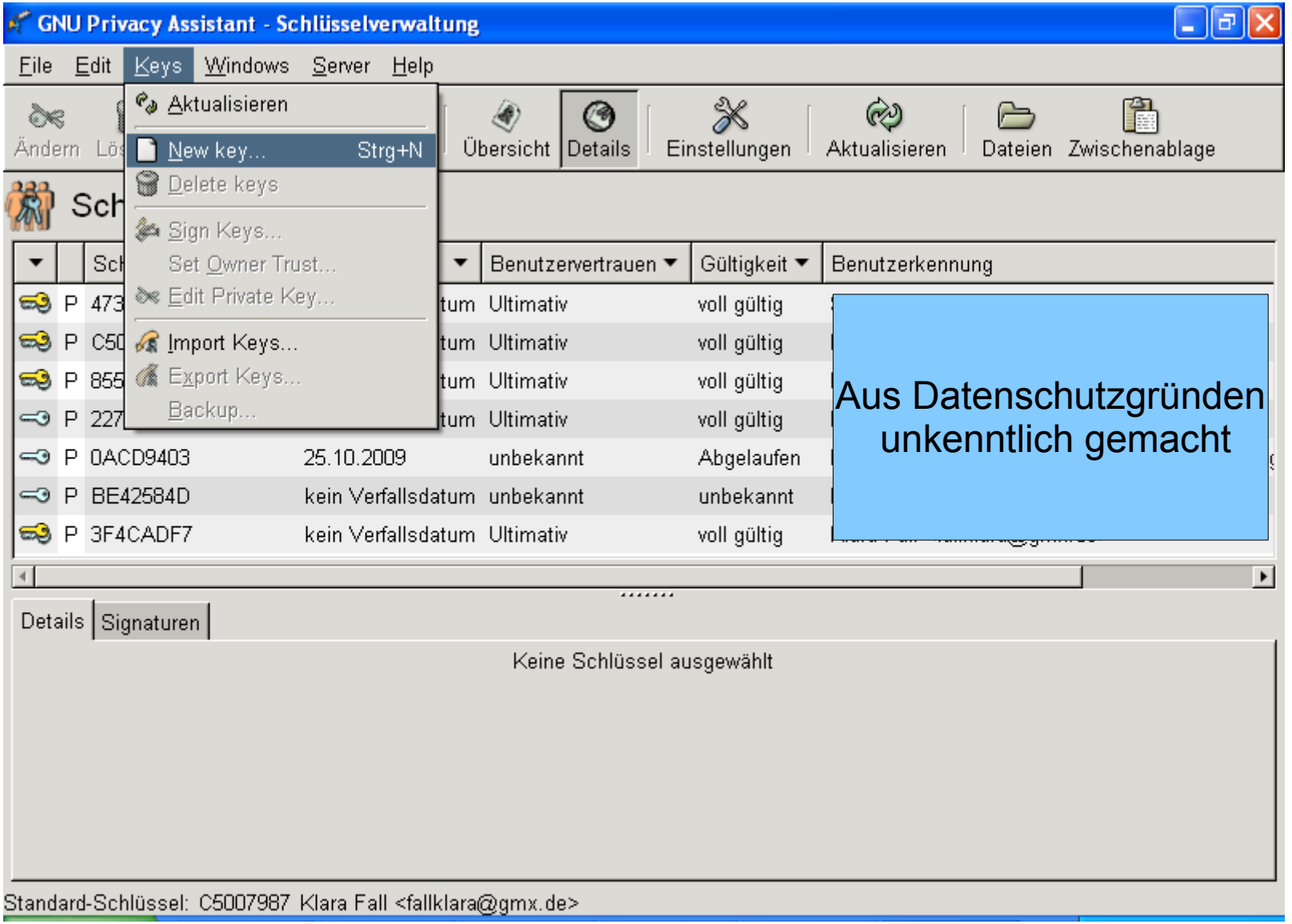
Übermittlung des Übermittlung des pubkey an einen Partner

Empfang einer verschlüsselten und signierten Mail



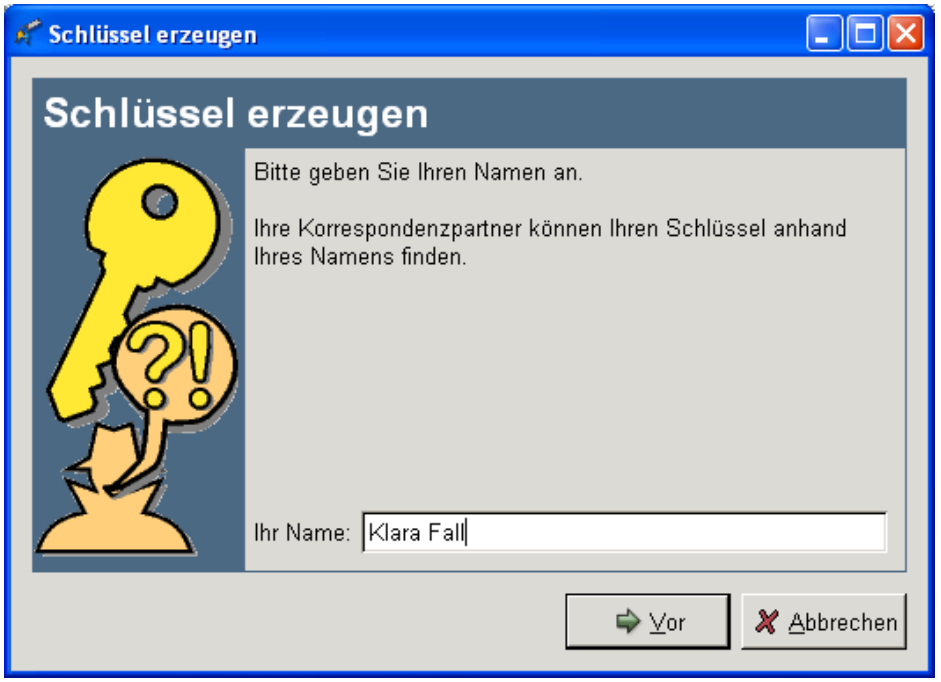
Schlüsselverwaltung Schlüssel importieren, Verzeichnis wählen, in das der Public Key gespeichert wurde.

PGP-Schlüssel mit GPA erzeugen



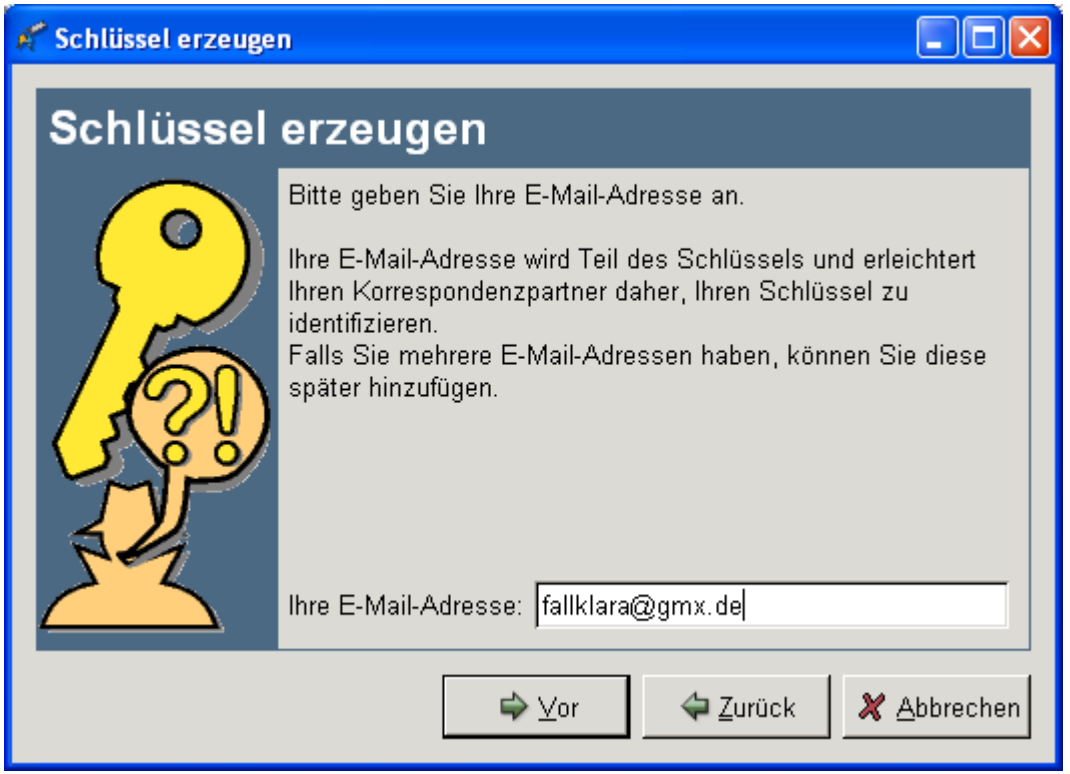
PGP-Schlüssel mit GPA erzeugen

- Nachdem das Programm gestartet wurde und man im Menü neuen Schlüssel erzeugen ausgewählt hat, muss man als erstes den Namen eingeben



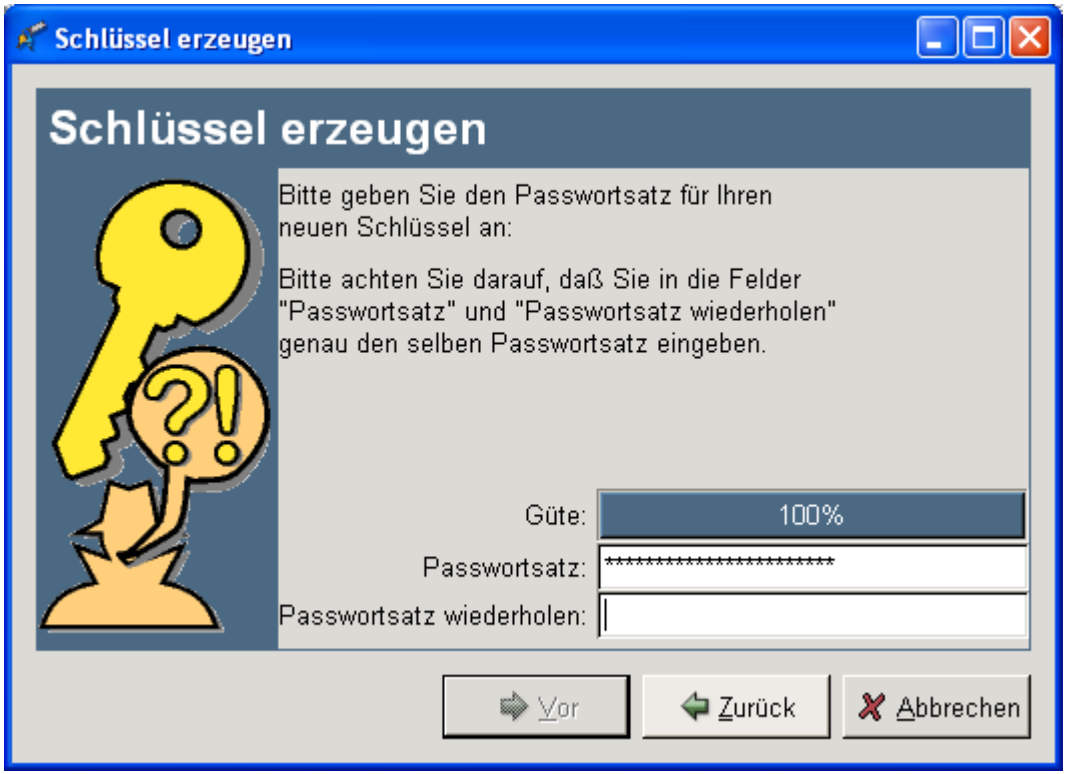
PGP-Schlüssel mit GPA erzeugen

- Als nächstes muss man die E-Mail-Adresse angegeben.



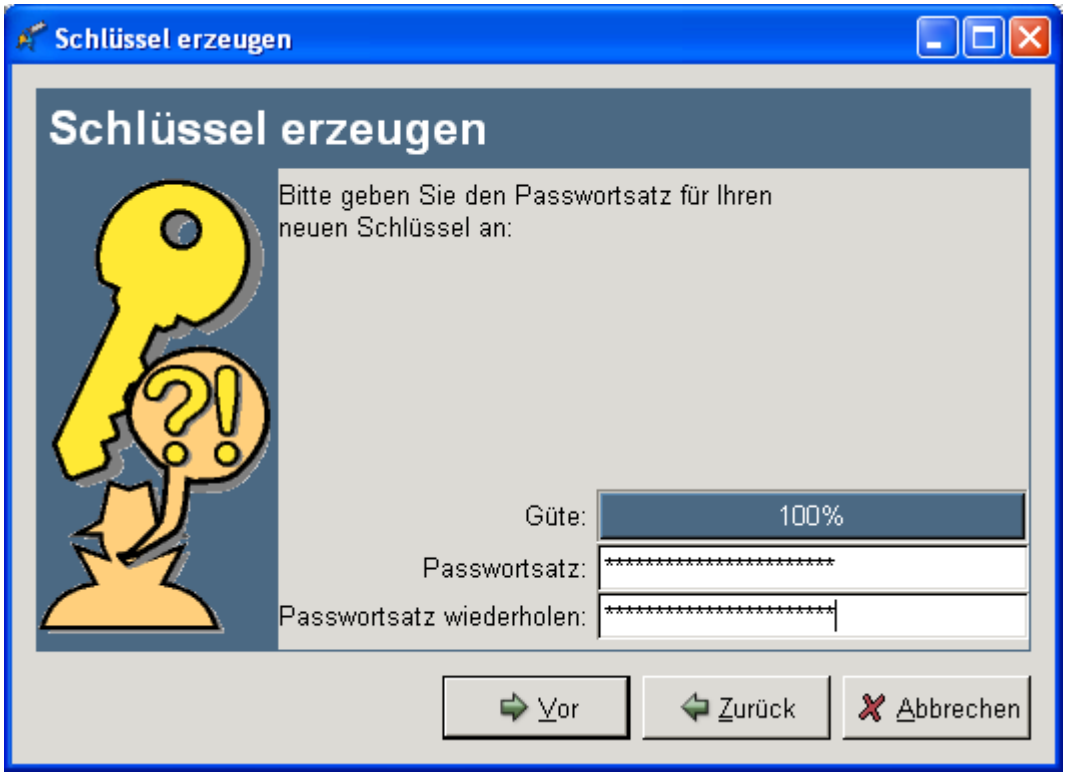
PGP-Schlüssel mit GPA erzeugen

- Im nächsten Schritt wird die Passphrase verlangt.
- GnuPG ist erbarmungslos, erst nach viel mehr Zeichen, als sich ein normaler Mensch merken kann, die zudem Sonderzeichen, Zahlen und Groß/Kleinschreibung enthalten müssen, vergibt er 100% Passphrase Sicherheit.



PGP-Schlüssel mit GPA erzeugen

- Dieses muss wiederholt werden. Dieser Schritt soll nicht Benutzer quälen, sondern verhindern, dass sich Benutzer einen ungültigen Schlüssel merken, wenn sie sich bei der erstmaligen Nutzung vertippt haben.



PGP-Schlüssel mit GPA erzeugen

Statt Laufwerk A: empfiehlt es sich, eine Sicherheitskopie auf CD ROM zu brennen, die danach nicht aus Versehen überschrieben oder von Malware infiziert werden kann.

Agenda

1. Begrüßung und Vorstellung
2. Einleitung – Kurzvorstellung der Tools
3. GnuPG
4. **TRUECRYPT**
5. Tor
6. Zusammenwirken der Tools
7. Fragen und Diskussion

Einleitung

- TrueCrypt ist ein Freeware und Open Source Kryptographiesystem. Der Name ist als Markenzeichen geschützt: Einsatzzweck ist der Schutz der Vertraulichkeit gespeicherter Daten. Optional fungiert TrueCrypt auch als steganographisches System, indem es gespeicherte verschlüsselte Daten versteckt.
- Typische Einsatzzwecke: Schutz der Vertraulichkeit gespeicherter Daten bei Diebstahl oder Verlust eines Notebooks, Wechseldatenträgers, Smartphones
- Verstecken von Informationen und glaubhaftes Abstreiten ihrer Existenz unter Zwang
- Nur bedingt geeignet für Einsatz in größeren Unternehmen, da folgende Funktionen fehlen: Key Escrow/Key Recovery, zentrales Key und User Management oder Schnittstellen zu entsprechende Systemen, z.B. IDM

Einleitung

- TrueCrypt ist ein symmetrisches Kryptosystem, das den selben Schlüssel für Ver- und Entschlüsselung nutzt.
- Unterstützte Algorithmen: AES, Twofish, Serpent sowie Kombinationen davon mit 256Bit im XTS Mode
- Hashverfahren für Random-Funtionen: RIPEMD-160, SHA512, Whirlpool
- Unterstützte Betriebssysteme: Win, Mac, Linux
  - Windows XP, Vista, Windows7, Win2000SP4 und neuere (32 und 64 bit)
  - Mac OS 10.4 Leopard,10.5 Tiger, 10.6 Snow Leopard (32 bit)
  - Linux (Kernel2.4, 2.6 oder kompatibel)

  (Stand TrueCrypt Version 6.3a November 2009)

Einleitung

- TrueCrypt erzeugt Volume genannte verschlüsselte Container auf beliebigen Speichermedien (HDD, Memorystick, DVD...). Nachdem das Volume gemountet wurde, erfolgt die Ver- und Entschlüsselung on the fly beim Zugriff, nahezu transparent für den Benutzer.
- Volumes können einzelne Files oder auch ganze Partitionen oder Storage Devices sein. Die Größe und Art des Volumes wird bei der Anlage durch den Benutzer festgelegt.
- Hidden Volumes werden erst nach Eingabe eines Passworts sichtbar und verbergen damit zusätzlich die Existenz einer verschlüsselten Information.
- Für Windows existiert zusätzlich die Option, die Bootpartition des OS zu verschlüsseln und damit eine komplette Festplatte mit Pre-boot Authentication-Schutz zu versehen. Ohne Eingabe des Passworts kann die Festplatte nicht entschlüsselt werden.
- In einem Hidden Volume kann wiederum ein Hidden Operating System versteckt werden.

Quelle und Installation

- WWW.Truecrypt.org, gewünschtes Betriebssystem auswählen, Sourcen oder Binary download
- Pgp signature bzw. Zertikat überprüfen
- Win: run setup, Linux Packetquellen installieren
- RTFM (Anleitung vor Gebrauch lesen, es lohnt sich!)
- Konzept entwickeln: Was soll für welchen Zweck verschlüsselt werden? Vor welchem Szenario eines unerwünschten Zugriffs will ich meine Informationen schützen (Verlust, Diebstahl, Nötigung bei Grenzübertritt, in einem Verhör, unter Folter)?
- Zunächst üben, Basisfunktionen nutzen (File Volumes, Partition eines Wechseldatenträgers, z.B. USB Memorystick)
- vor Nutzung einer Fulldisk Systemverschlüsselung unbedingt ein Backup anfertigen!
- Wahl einer sicheren Passphrase
- Passphrase merken, speichern oder aufschreiben und sicher verwahren (abhängig vom Konzept)?

Sicherheits-Konzept

- Konzept entwickeln: Was soll für welchen Zweck verschlüsselt werden? Vor welchem Szenario eines unerwünschten Zugriffs will ich meine Informationen schützen (Diebstahl, Nötigung in einem Verhör, Folter)?
- Szenario1: Schutz vertraulicher Informationen

  Besonderen Filecontainer als Datentresor anlegen, vertrauliche Informationen nur dort speichern,

  Nutzung nur bei besonderem Schutzbedarf, starke Passphrase, aufgeschrieben und an sicherem Ort getrennt vom speichernden System hinterlegt.

  Sonderfall: Eine gemeinsame Nutzung mit mehreren Personen (Teamarbeit,, Gruppe) erfordert einen zusätzlichen Container mit gemeinsam bekannter weiterer Passphrase (shared secret).
- Szenario2: Schutz mobiler Datenträger

  Komplette Partition (Drive, Device) verschlüsseln, ansonsten wie oben; standardmäßige Nutzung der Verschlüsselung; erfordert Verfügbarbeit von TrueCrypt, um Device zu nutzen; sinnvoll für kleine, mobil genutzte Datenträger wie USB Memorysticks oder SD/Mikro-SD Karten, die leicht verloren gehen

Sicherheits-Konzept #2

- Szenario3: Notebook HDD

  Systempartition verschlüsseln; unterstützt nur Windows OS; Pre-boot Authentication; kein Zugriff auf HDD ohne PW; schützt bei Verlust oder Diebstahl vor Zugriff auf tmp, Papierkorb etc.; unter LINUX nicht notwendig, da z.B. SWAP und /home/user von TrueCrypt zu verschlüsseln ausreicht.

- Szenario4: Auslandsreise, Schutz vor mit Gewalt erpresstem Zugriff durch staatliche Organe, Kriminelle etc.

  nur für Fortgeschrittene!!!

  Anforderung: Plausible deniability, glaubwürdig abstreiten können, etwas zu verbergen zu haben:

  Klares und vollständiges Sicherheitskonzept ausarbeiten inkl. Verhaltensregeln im Ernstfall, keine Mitnahme bei inländischer Gewalt, keine Niederschrift der Passwörter, Einübung der Nutzung vor Nutzung (Probephase), Datensicherungskonzept: Vertraulichkeit versus Verfügbarkeit, Nutzung von Hidden Volumes, bei Einreise in Folterstaaten Zwiebelschalenmodell nutzen: Hidden Operating System mit Hidden Volumes in Hidden Volumes, TrueCrypt Bootloader tarnen (keine Anzeige oder Standard Win Boot Menu / Fehlermeldung (Disk Failure, ...))

  Technik kann keine gesellschaftlichen Probleme lösen...

Erzeugen eines Volumes

Passphrase aufschreiben?

Hier müssen die Schutzziele Vertraulichkeit und Verfügbarkeit gegeneinander abgewogen werden. Aufschreiben beinhaltet das Risiko, dass die notierte Phrase von Unbefugten entdeckt wird, Nicht-Aufschreiben das Risiko, dass man die sichere, aber komplizierte Passphrase vergisst und selber nicht mehr an die verschlüsselten Daten herankommt.

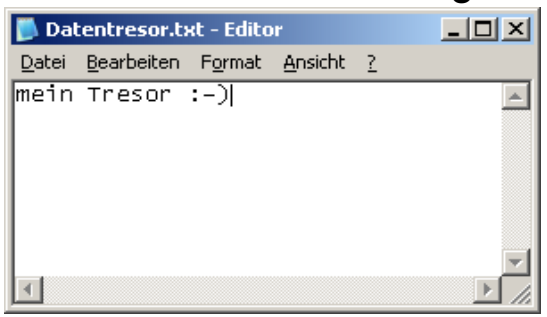
Für Szenario 1 ist m.E. Aufschreiben sinnvoll, da dieses Szenario ohnehin nur einen begrenzten Schutz bietet:

- Ob vertrauliche Daten im Tresor landen oder im Klartext im ungeschützten Bereich, hängt von der Sorgfalt des Benutzers ab. Wenn der Schutzbedarf einer Information falsch eingeschätzt wird oder sich der Bedarf ändert, aber die Datei nicht verschoben wird, liegt die Datei ungeschützt außerhalb des Tresors.
- Temporäre Dateien und der Inhalt des Zwischenspeichers werden nicht verschlüsselt.
- TrueCrypt wird selten, nur bei besonders heiklen Informationen benutzt, dadurch das Handling kaum geübt, was die Wahrscheinlichkeit von Bedienungsfehlern ebenso erhöht wie die Wahrscheinlichkeit, die Passphrase zu vergessen.

Erzeugen eines Volumes

Szenario1

1) Eine Pseudodatei erzeugen, diese wird später durch das TrueCrypt Volume ersetzt

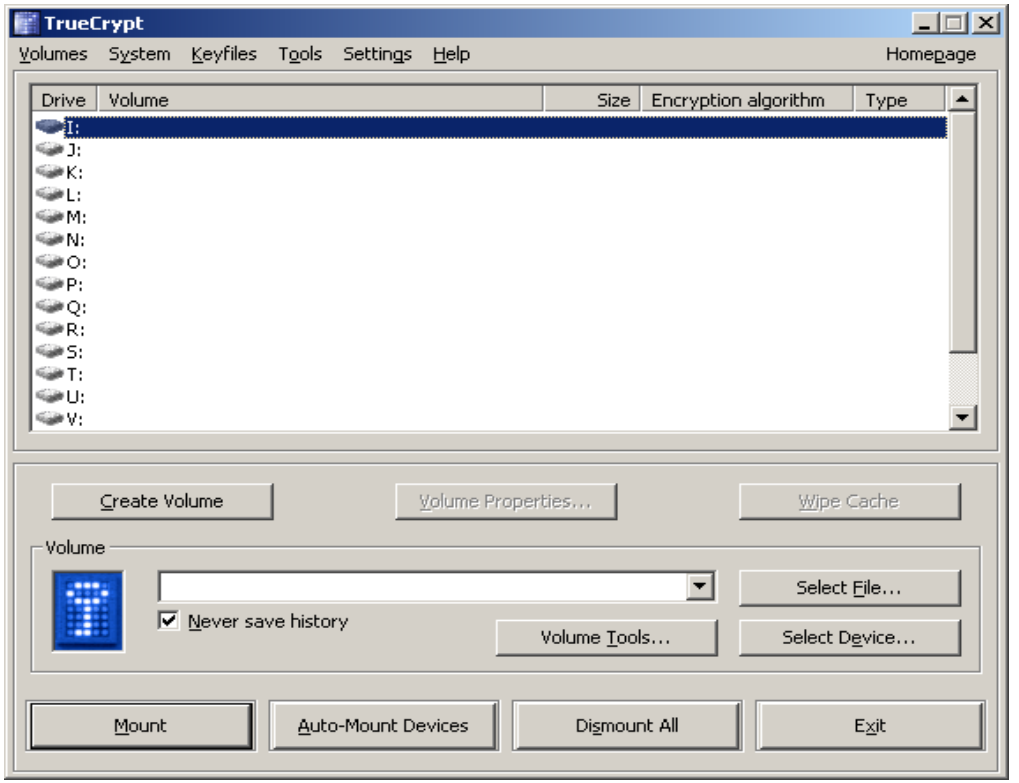


2) TrueCrypt starten

3) Im Menü Volumes:

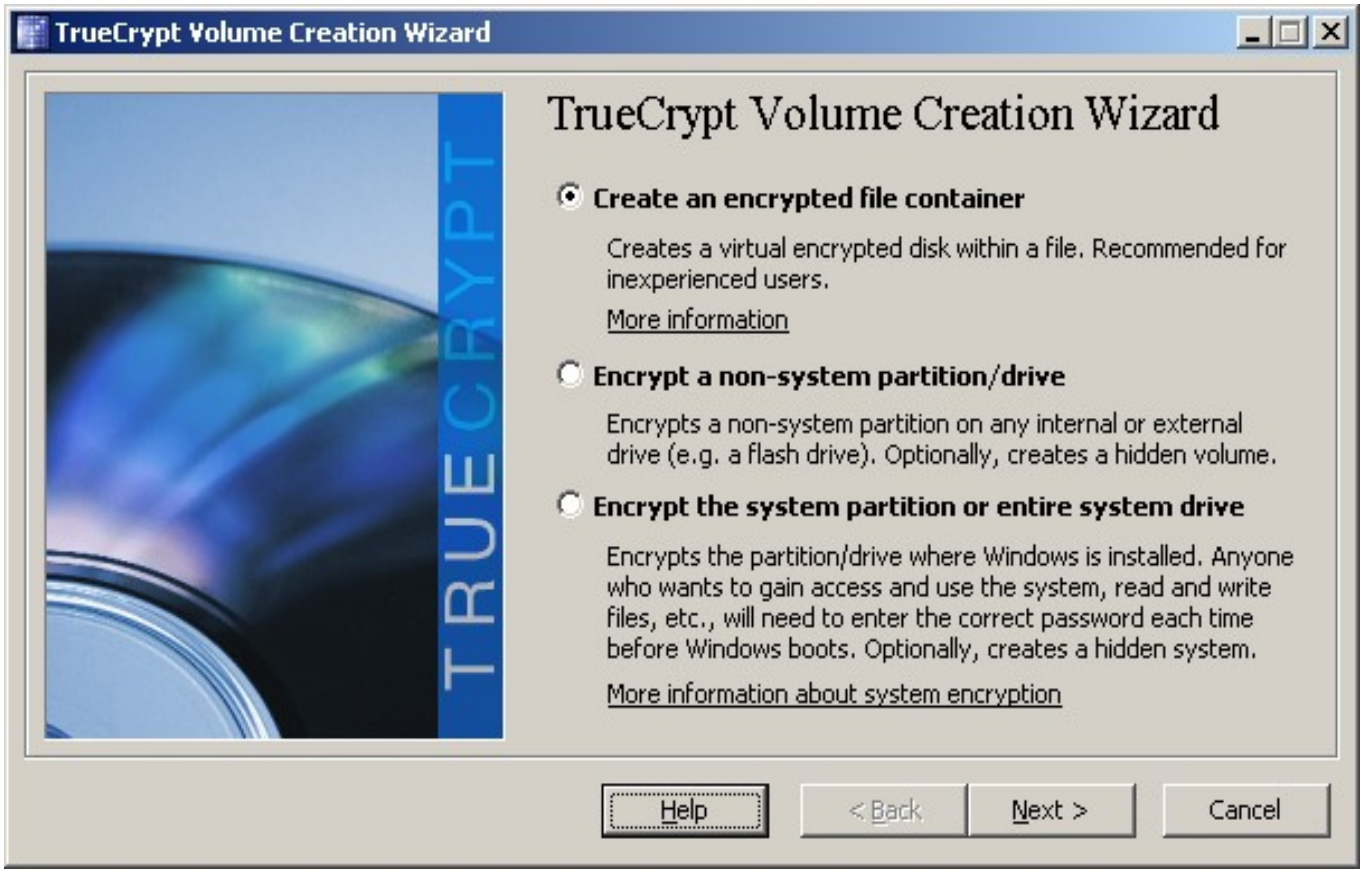
<create new volume>

Damit wird der Volume Creation Wizard aufgerufen.



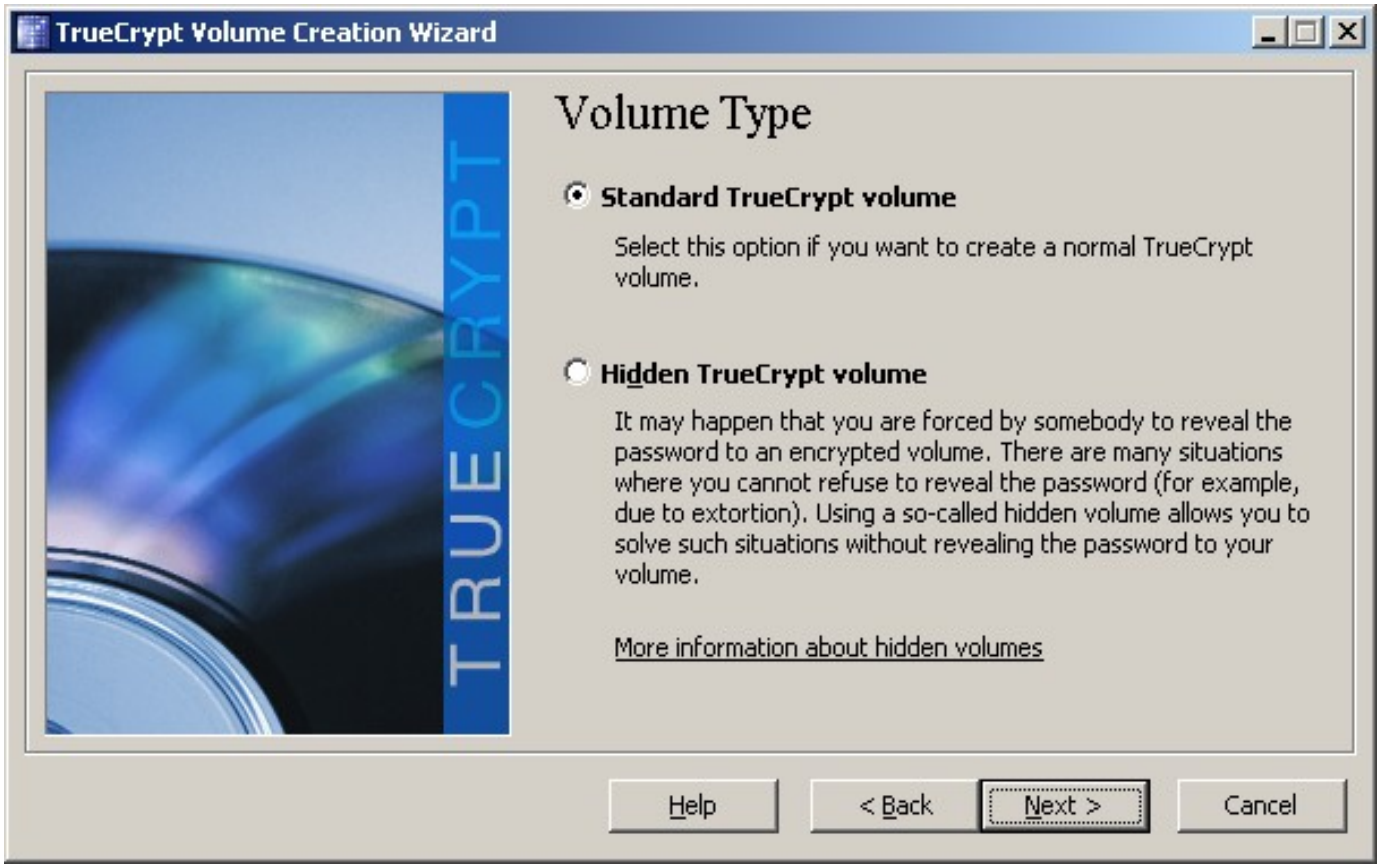
Erzeugen eines Volumes

Im Volume Creation Wizard Create an encrypted file container auswählen



Erzeugen eines Volumes

Standard TrueCrypt Volume wählen



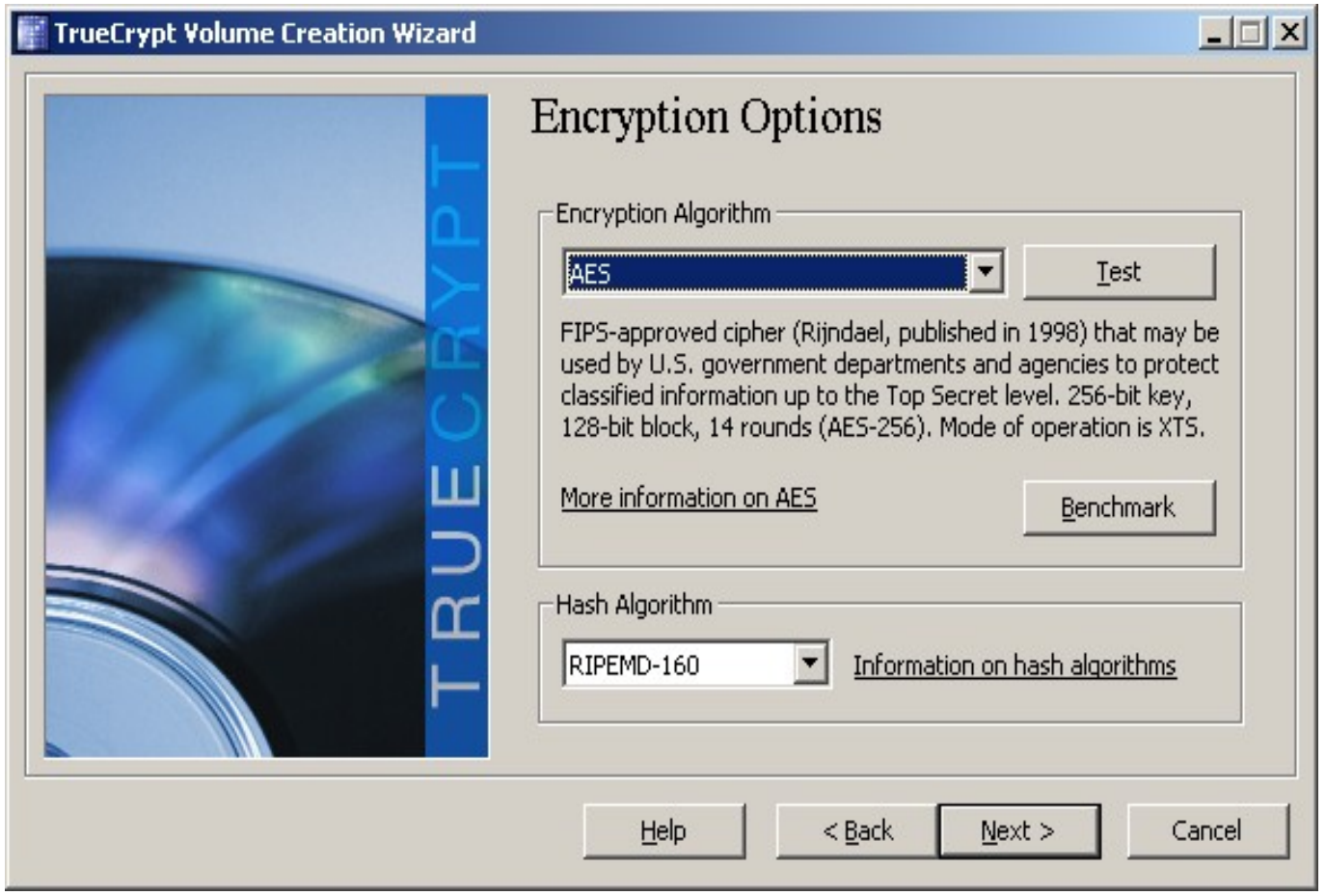
Erzeugen eines Volumes

die zuvor erzeugte Pseudodatei auswählen

Warnung, dass die Pseudodatei überschrieben wird, bestätigen

Erzeugen eines Volumes

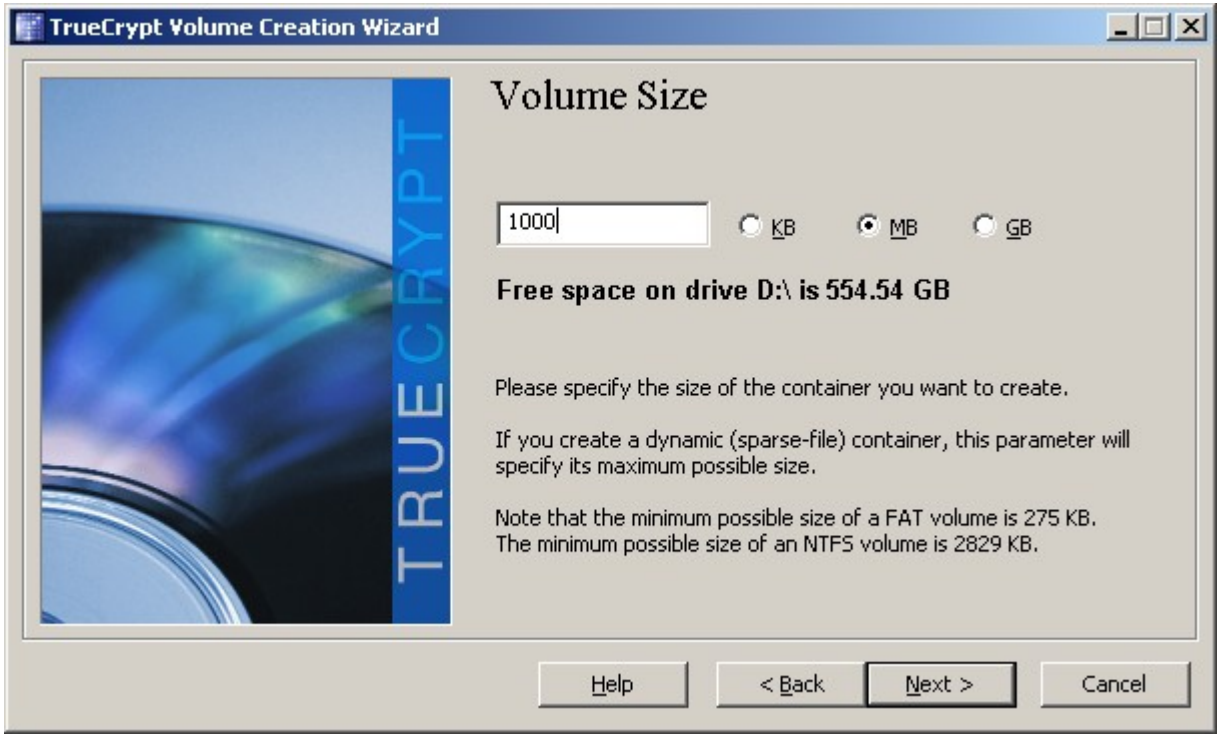
Default-Einstellungen übernehmen (AES, RIPEMD-160)



Erzeugen eines Volumes

Gewünschte Größe angeben

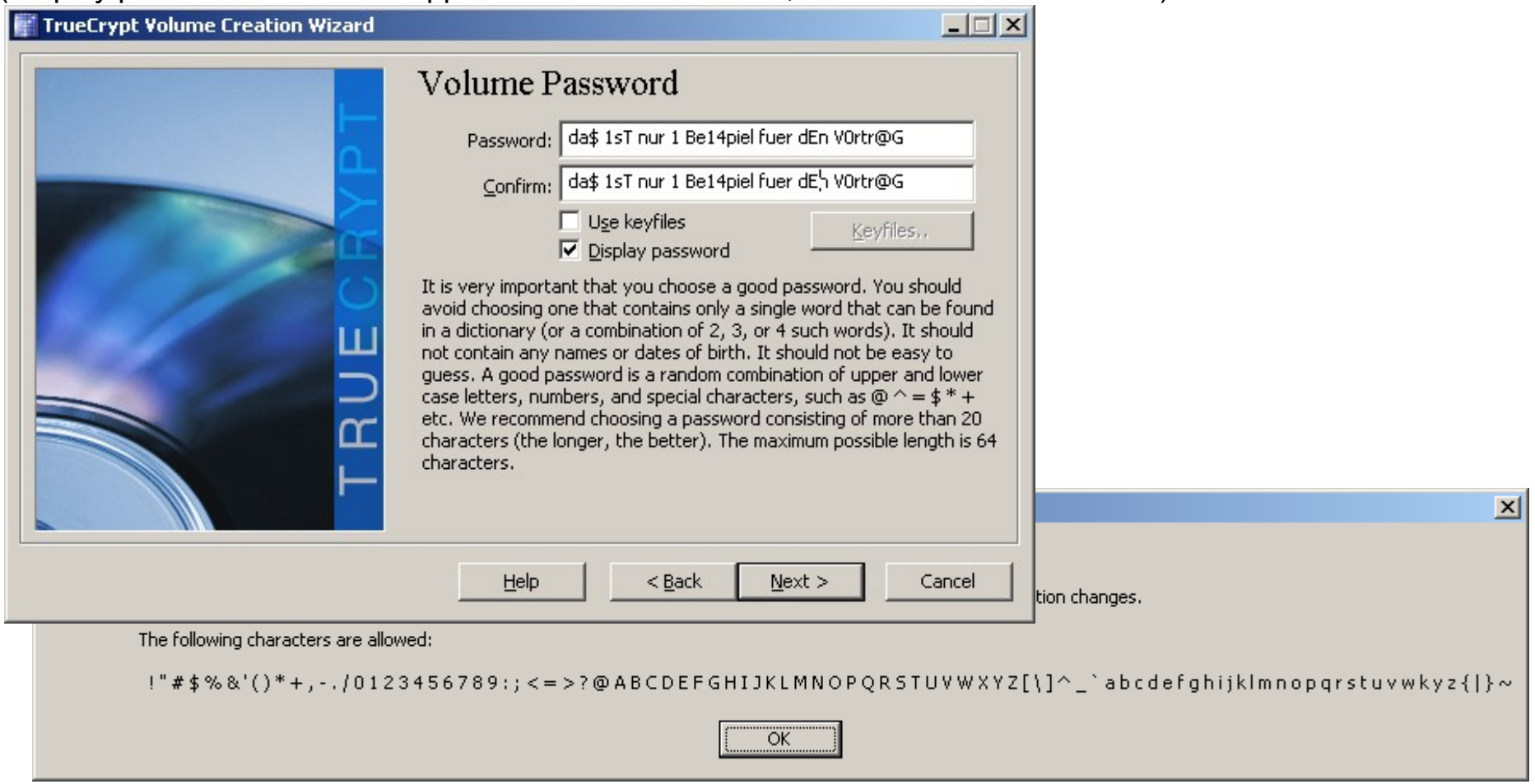
(abhängig von Bedarf und vorhandenem Platz auf dem Datenträger)



Erzeugen eines Volumes

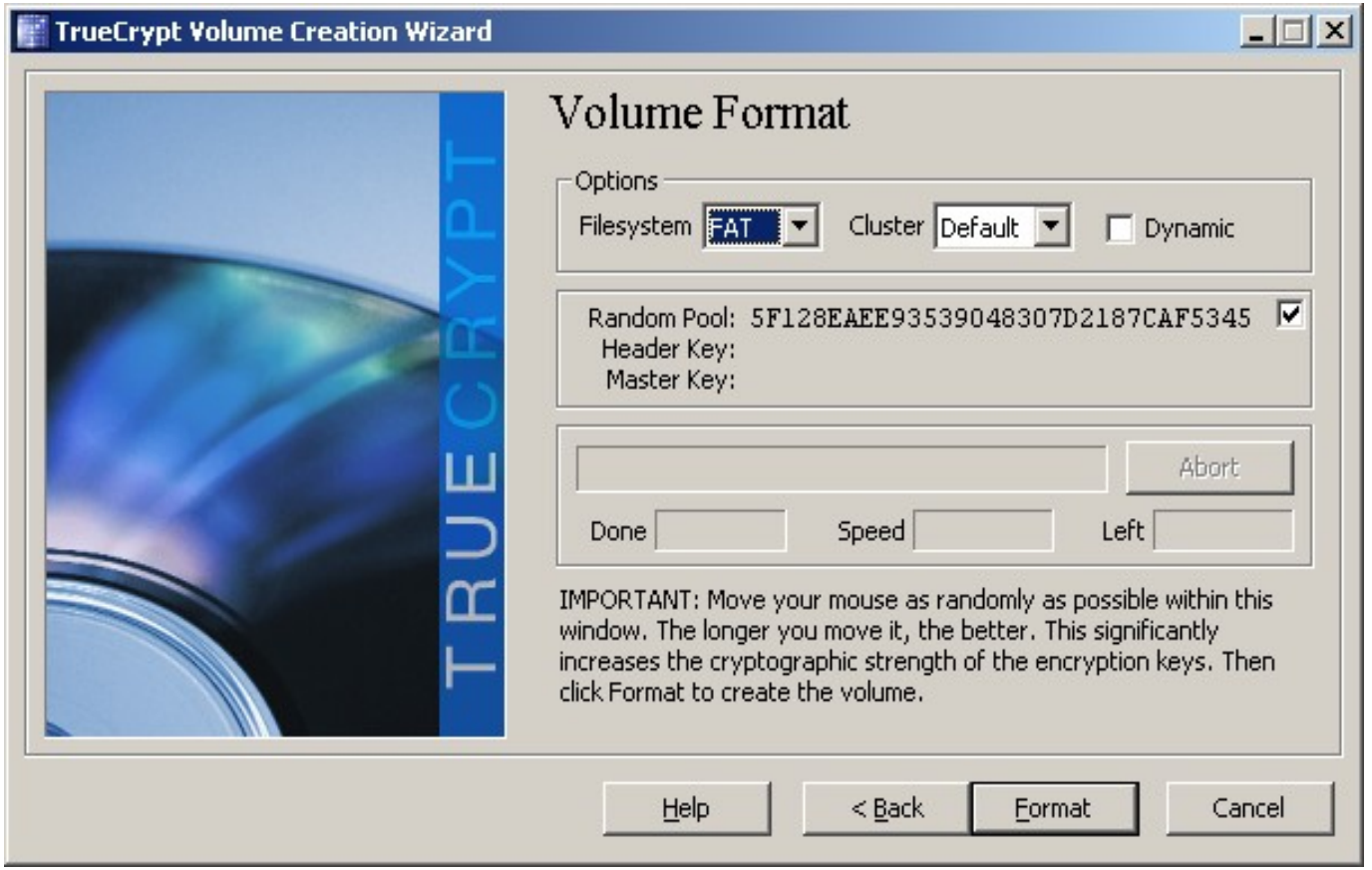
Sichere Passphrase aus ASCI Zeichen wählen

(Display password hilft bei Vertippen - aber nur einsetzen, wenn niemand zuschaut!!!)



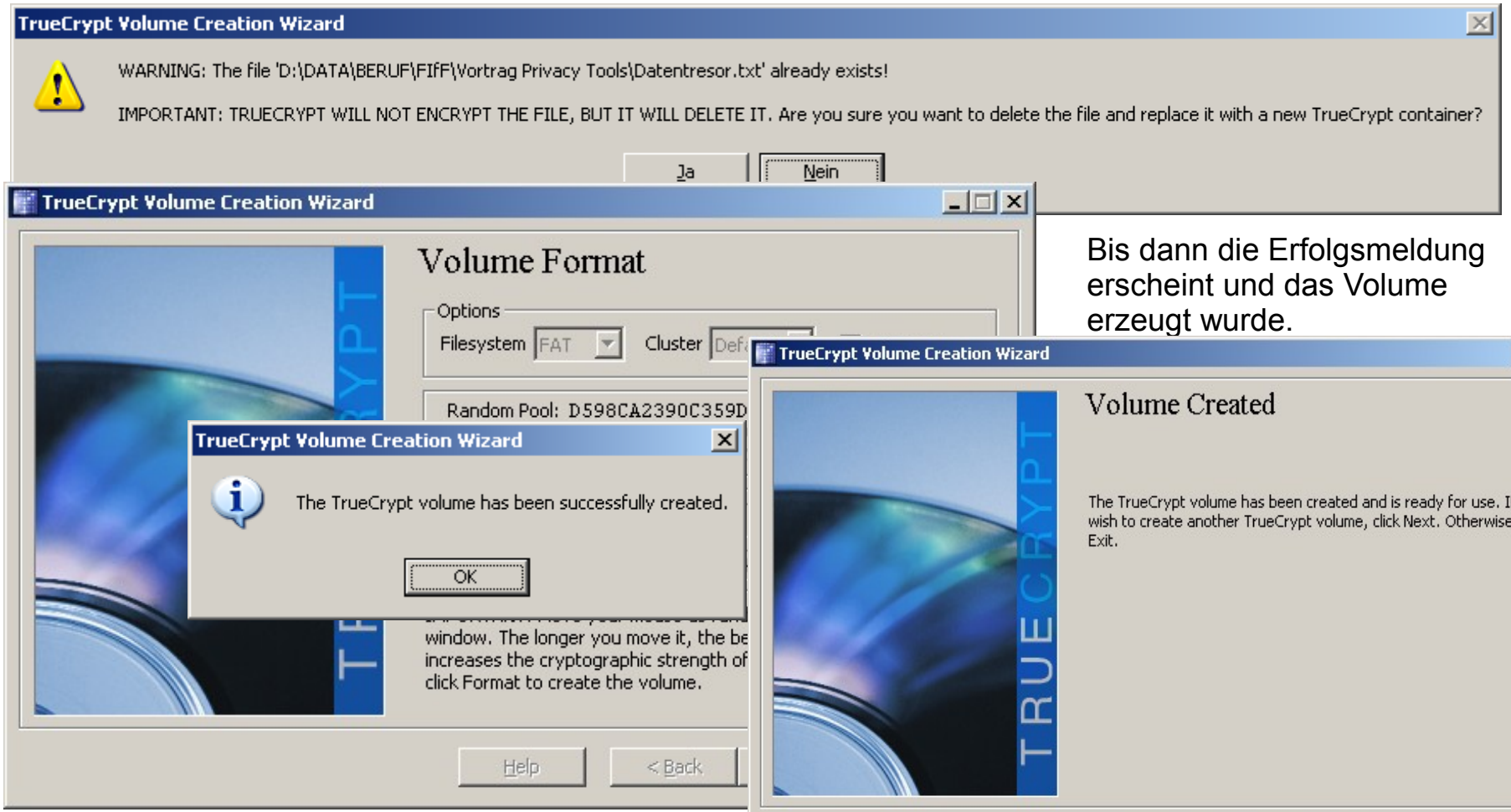
Erzeugen eines Volumes

Gewünschtes Dateisystem für das neue Volume wählen und mit der Maus spielen. Die Bewegungen werden genutzt, um Zufallszahlen zu erzeugen und den Schlüssel einmalig und nicht reproduzierbar zu machen



Erzeugen eines Volumes

TrueCrypt warnt noch einmal, dass die Pseudodatei überschrieben wird.

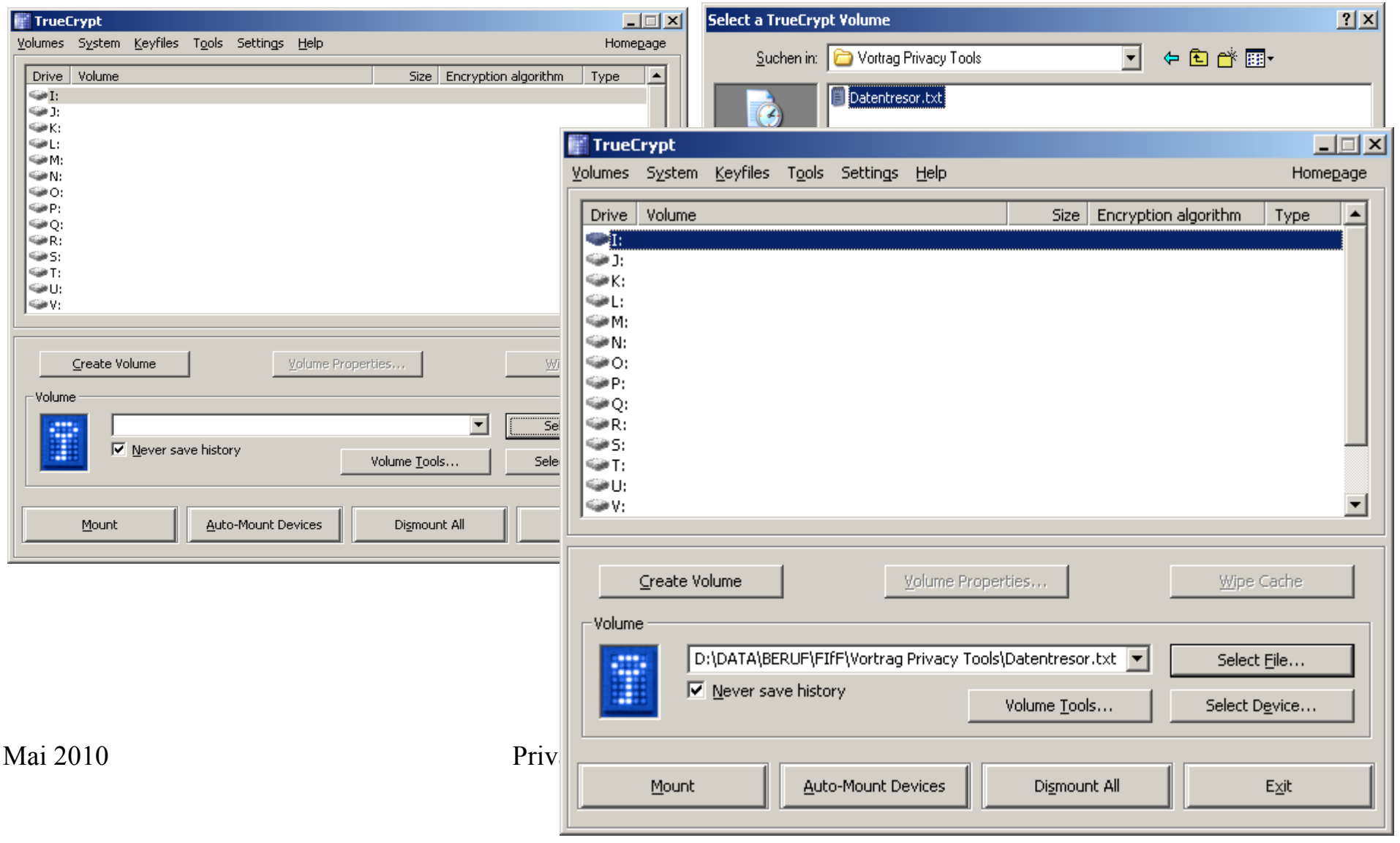


Bis dann die Erfolgsmeldung erscheint und das Volume erzeugt wurde.

Benutzung eines File Volumes

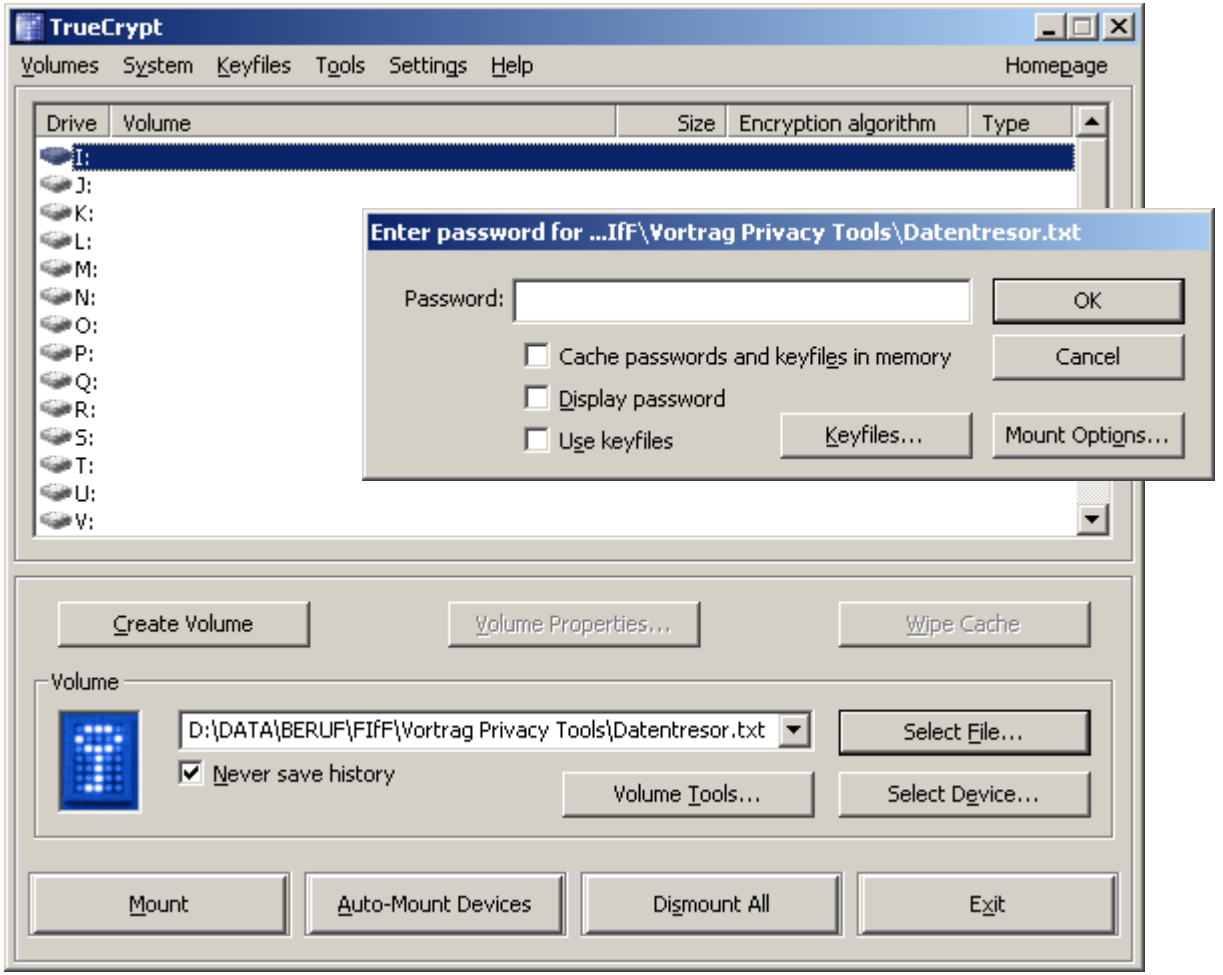
TrueCrypt starten, select file,

... dann die Containerdatei auswählen



Benutzung eines File Volumes

Der Containerdatei ein freies logisches Laufwerk zuordnen und auf <Mount> klicken.

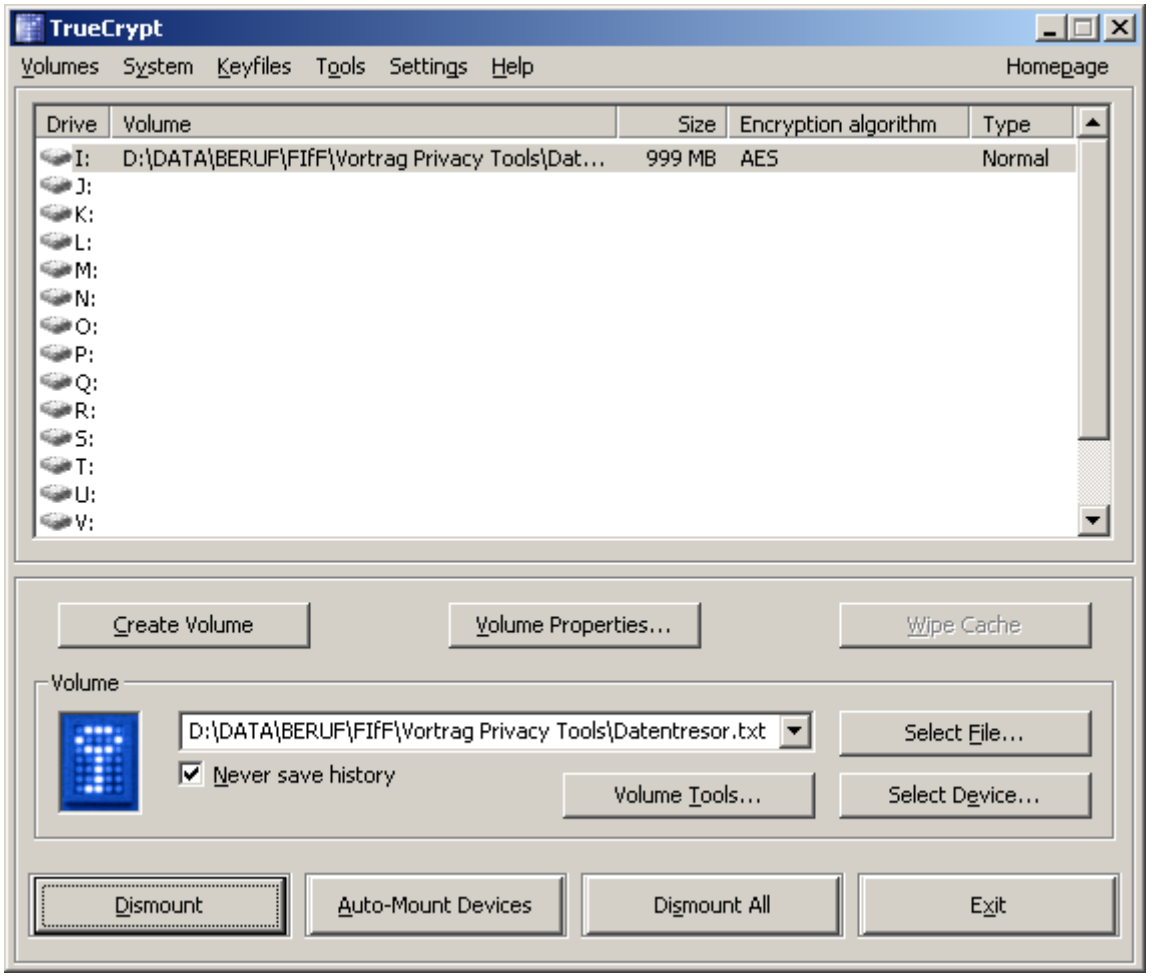


Die Passphrase wird zum Mounten abgefragt.

Für diese Aktion sind unter Win lokale Administratorrechte erforderlich, in LINUX muss der Mount Befehl durch zusätzliche Eingabe des Admin PW autorisiert werden.

Benutzung eines File Volumes

Die Containerdatei ist jetzt dem gewählten logischen Laufwerk zugeordnet und einsatzbereit.



Im Beispiel ist das TrueCrypt File das Laufwerk I: Solange das Laufwerk gemounted ist, lässt es sich wie ein normales Windows-Laufwerk benutzen. Alle Daten darin werden immer verschlüsselt abgelegt. Das Laufwerk kann mit Klick auf Dismount oder durch Abschalten oder Reboot des Rechners dismounted werden. Die Daten sind nur nach erneutem Mount mit Passwort-Eingabe lesbar.

Unter LINUX wird die Filecontainer-Funktion nahezu identisch genutzt.

Komplett verschlüsseltes Device (Drive/Partition) Volume

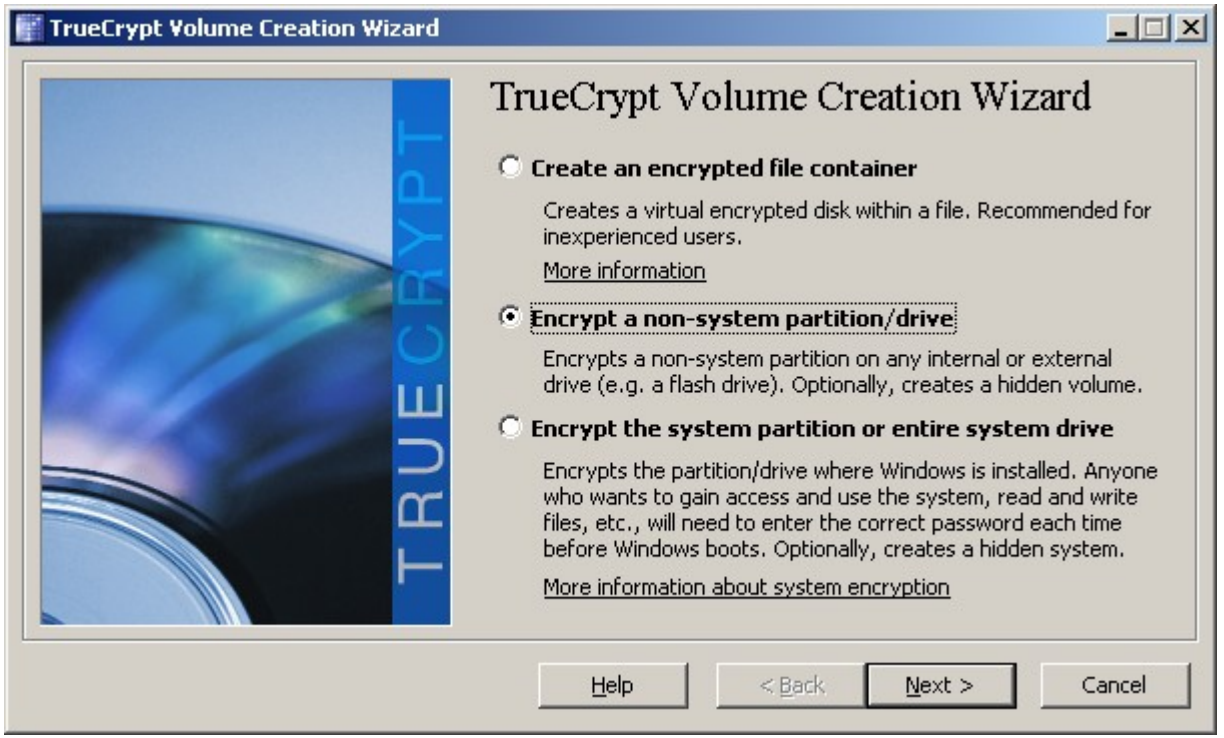
Szenario 2: Verschlüsseln eines USB Memorysticks oder einer ganzen HDD Partition

Zunächst sollte man das Device leeren und formatieren. Es besteht zwar auch die Möglichkeit, existierende Daten bei der initialen Verschlüsselung mit zu verschlüsseln, anstatt das Device einfach zu formatieren. Das dauert aber deutlich länger.

Im folgenden Beispiel wird ein leerer USB Memorystick verwendet.

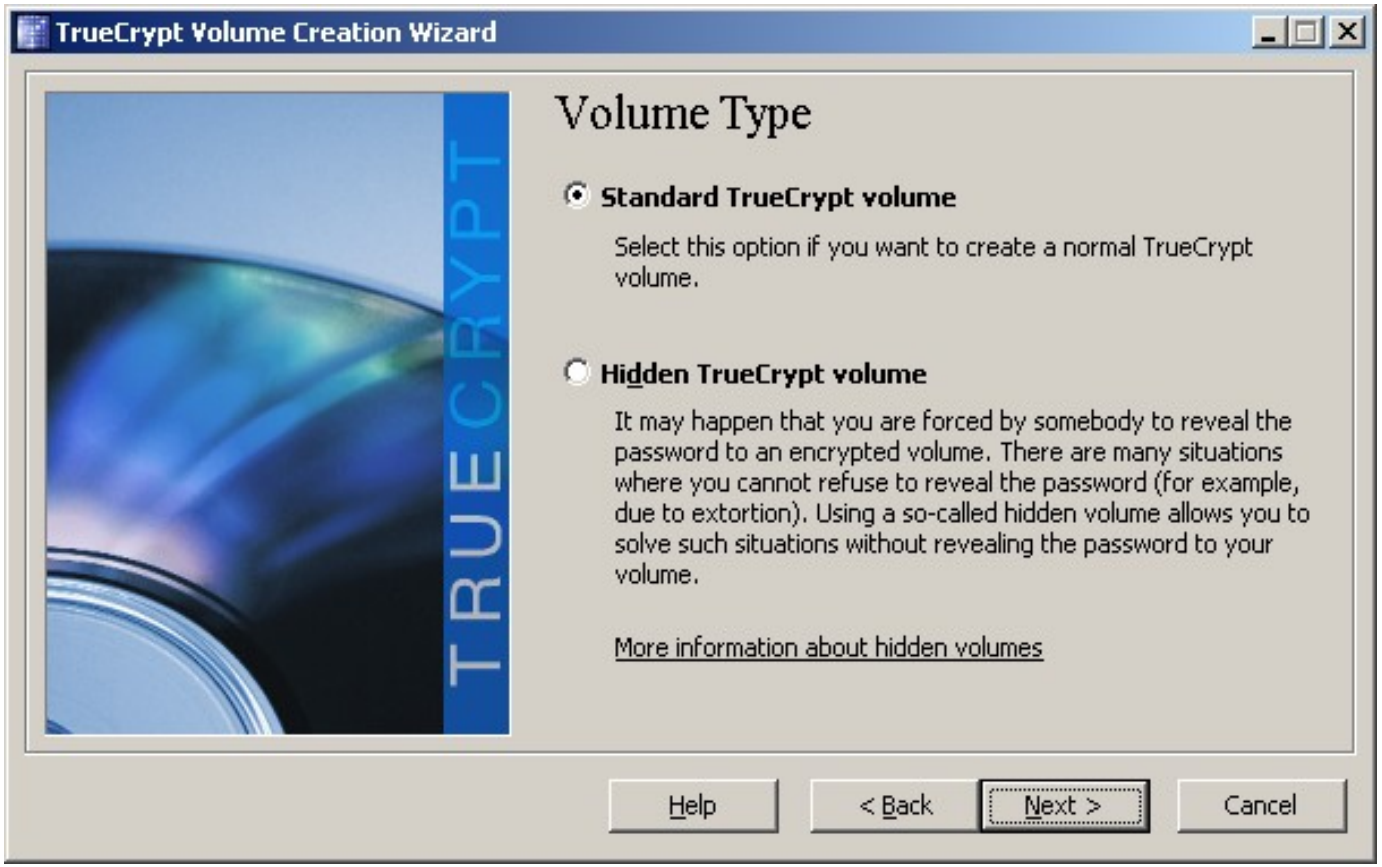
Komplett verschlüsseltes Device (Drive/Partition) Volume

Im Volume Creation Wizard diesmal die zweite Option encrypt a non-system device/drive wählen



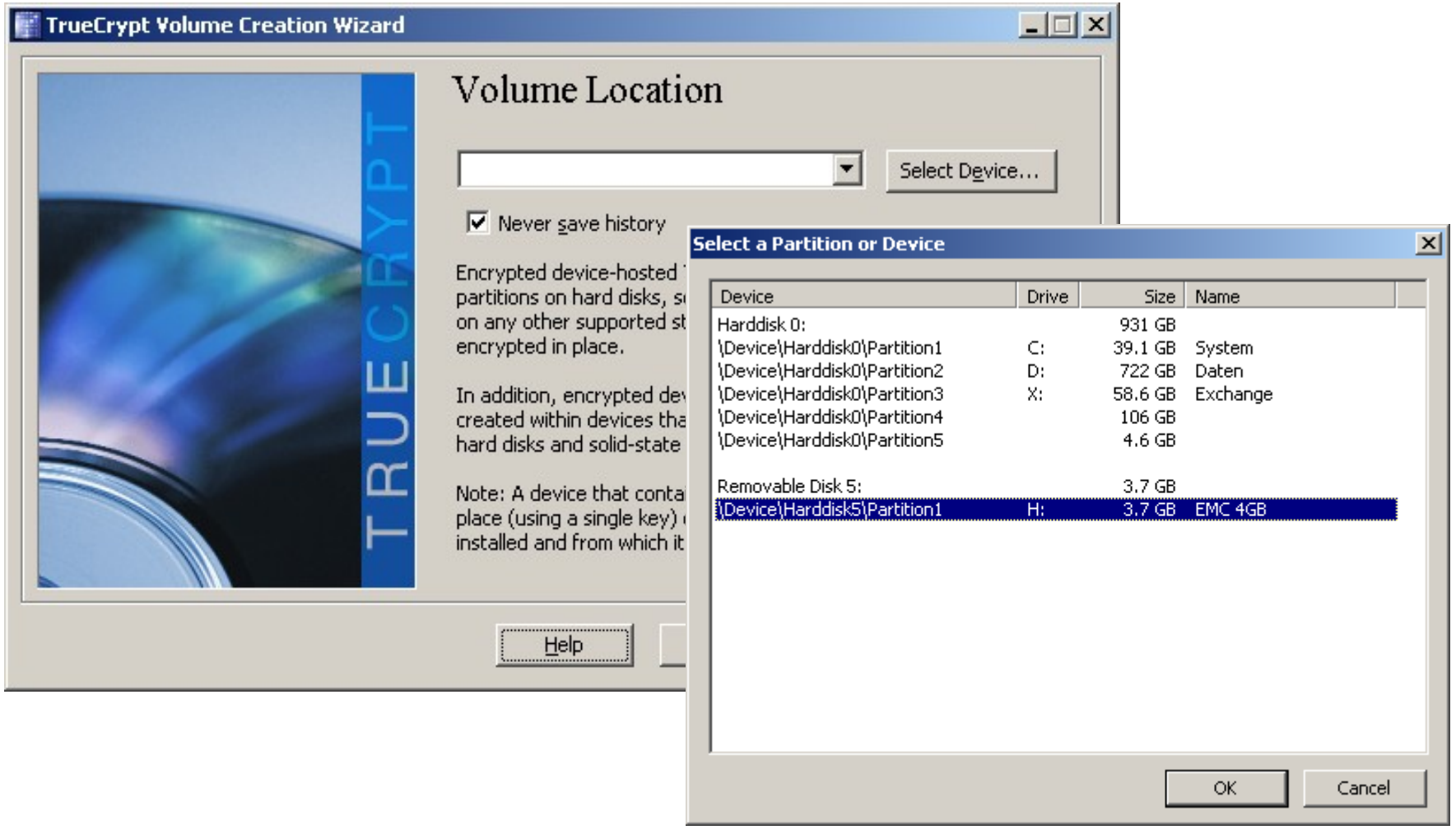
Komplett verschlüsseltes Device (Drive/Partition) Volume

Standard TrueCrypt Volume wählen



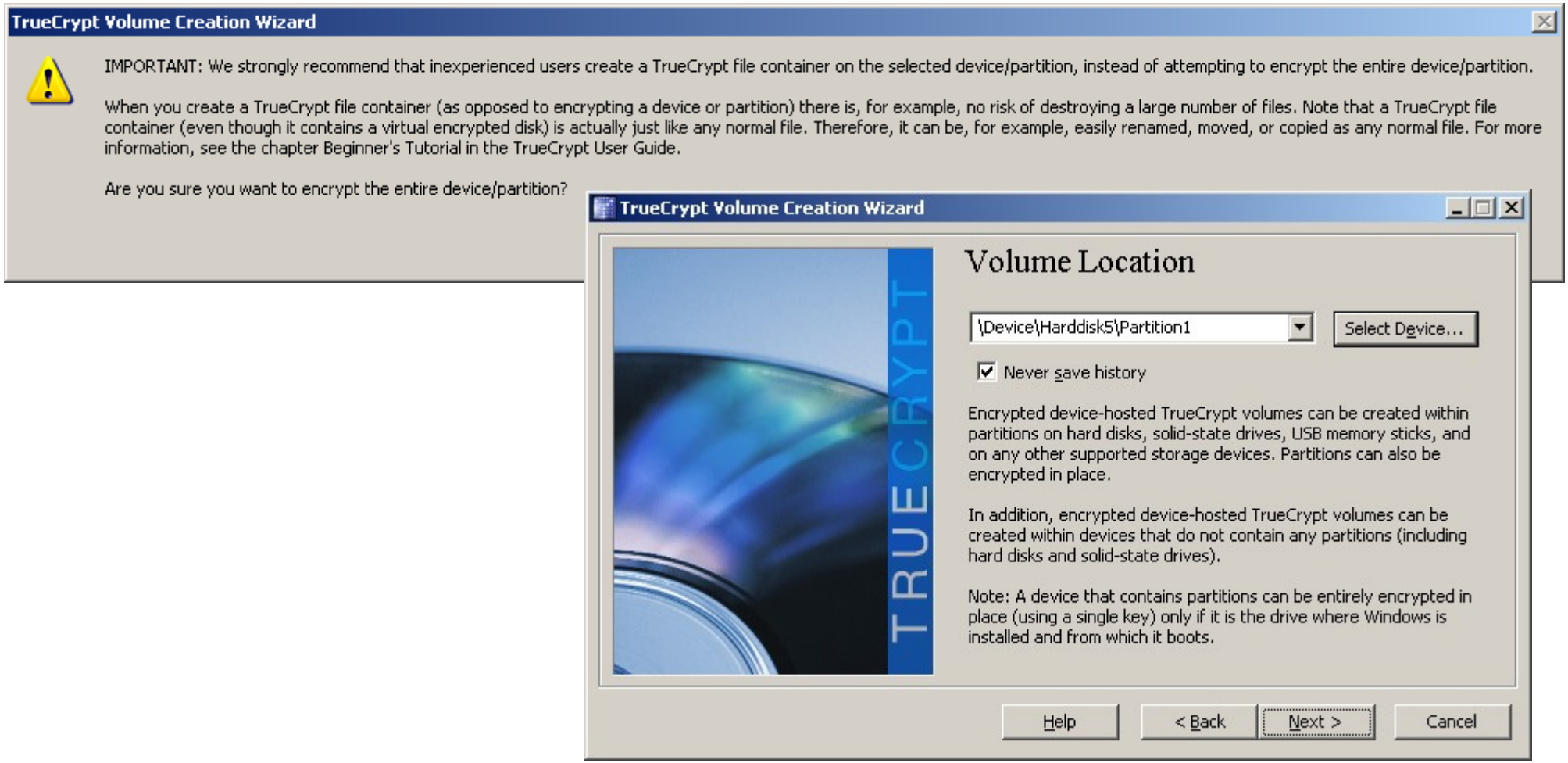
Komplett verschlüsseltes Device (Drive/Partition) Volume

Zu verschlüsselndes Device wählen (hier Laufwerk H, ein USB Stick)



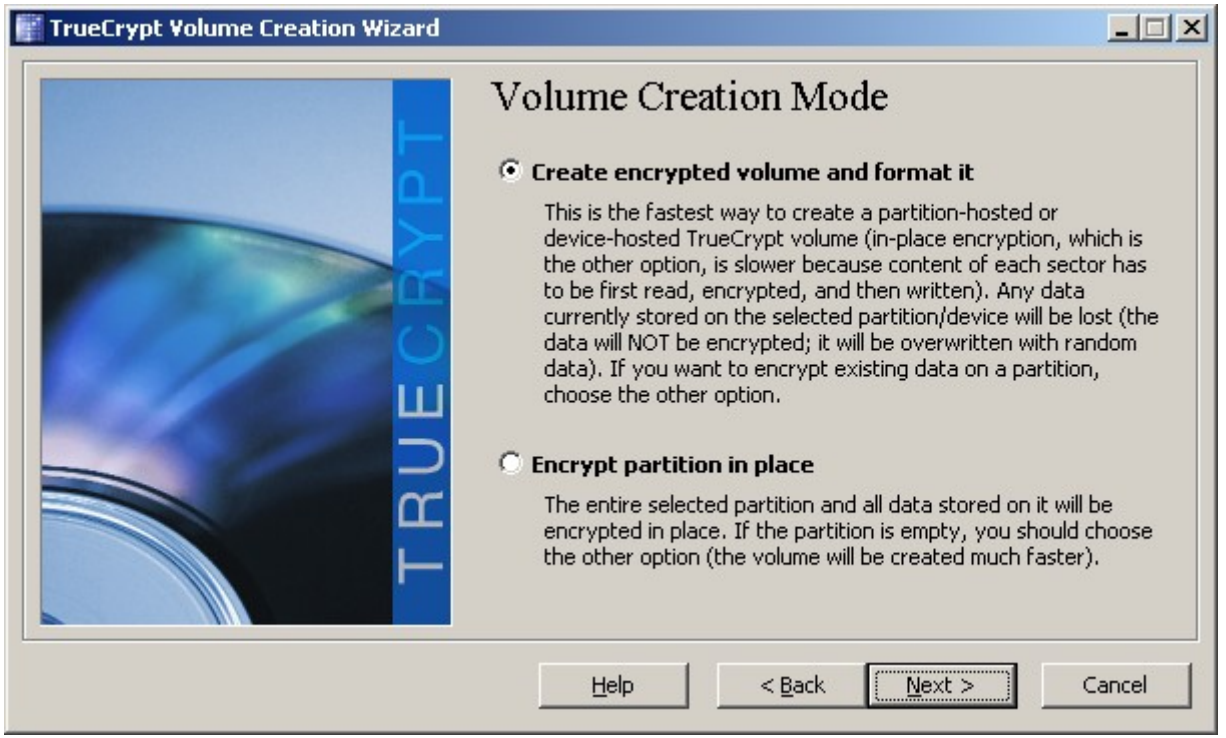
Komplett verschlüsseltes Device (Drive/Partition) Volume

Warnmeldung bestätigen, die empfiehlt, zunächst mit file encryption nach Szenario 1 zu üben



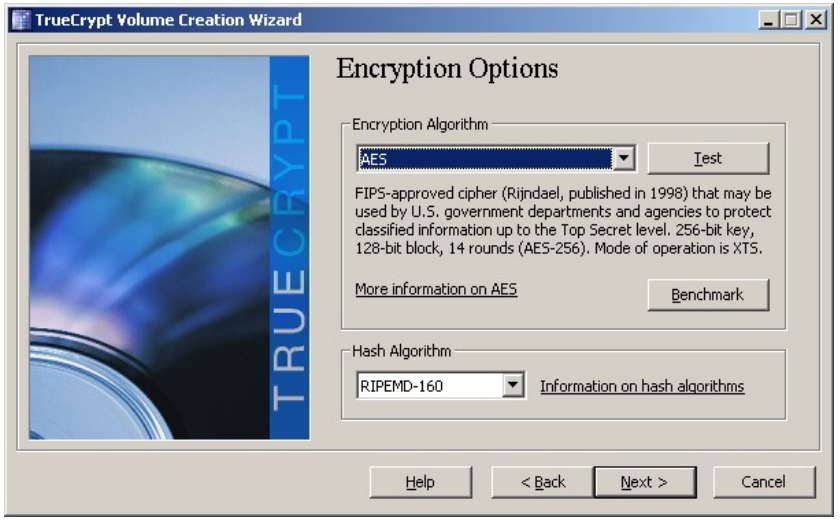
Komplett verschlüsseltes Device (Drive/Partition) Volume

Da der Datenträger leer war, kann hier die schnellere Option1 verwendet werden.

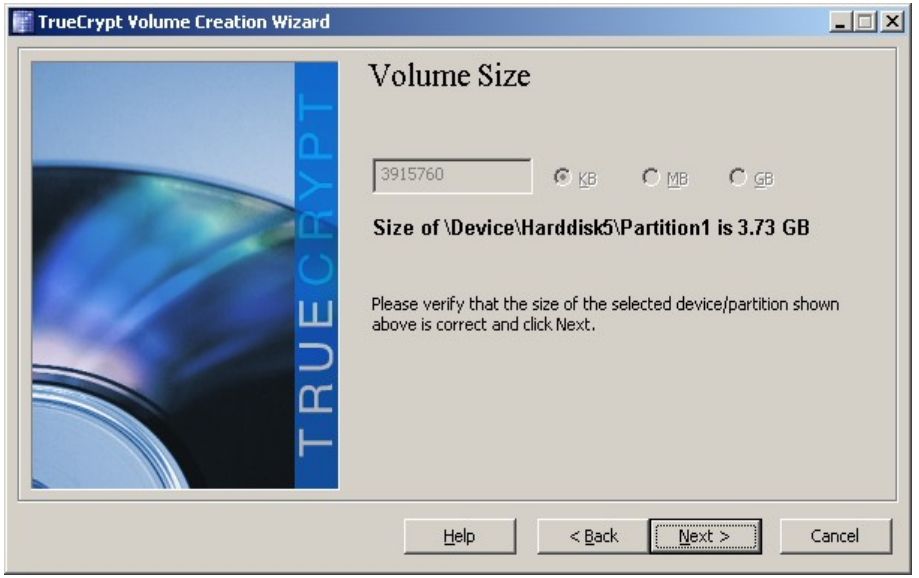


Komplett verschlüsseltes Device (Drive/Partition) Volume

Auch hier Default-Werte (AES, RIPEMD-160) verwenden

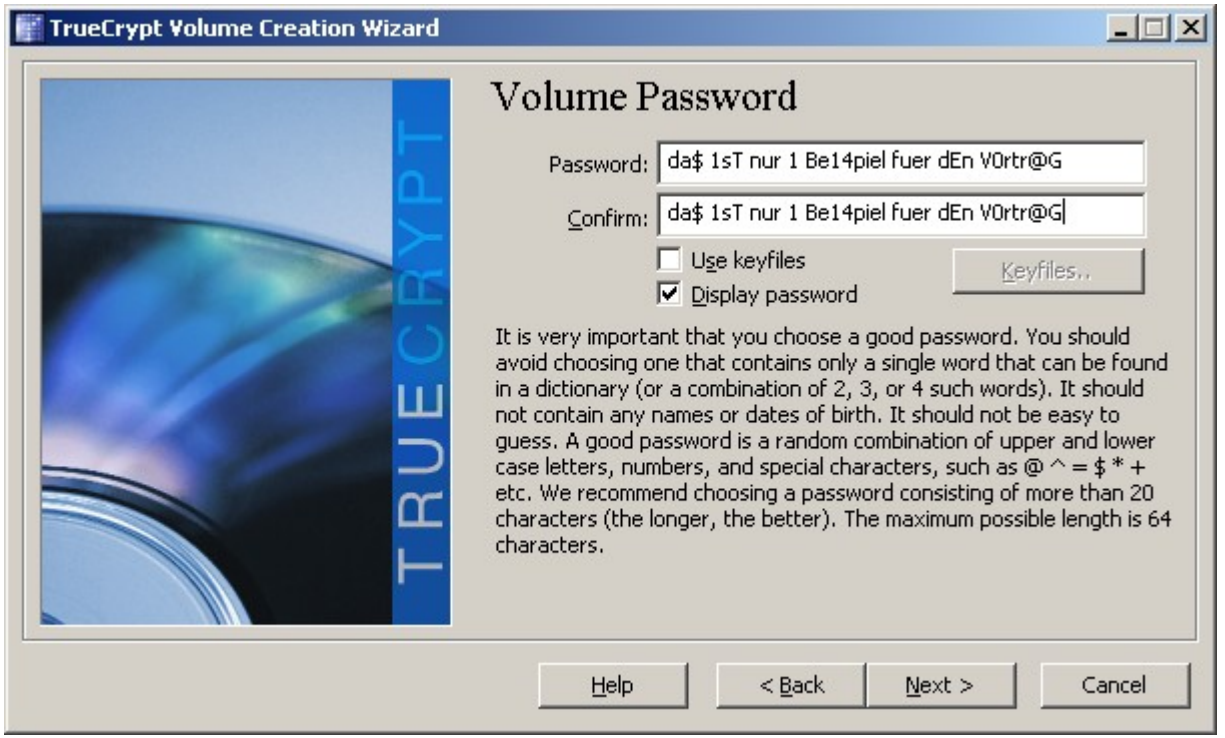


Die Größe des Volumes ist durch die Größe des Devices festgelegt, das ja komplett verschlüsselt werden soll.



Komplett verschlüsseltes Device (Drive/Partition) Volume

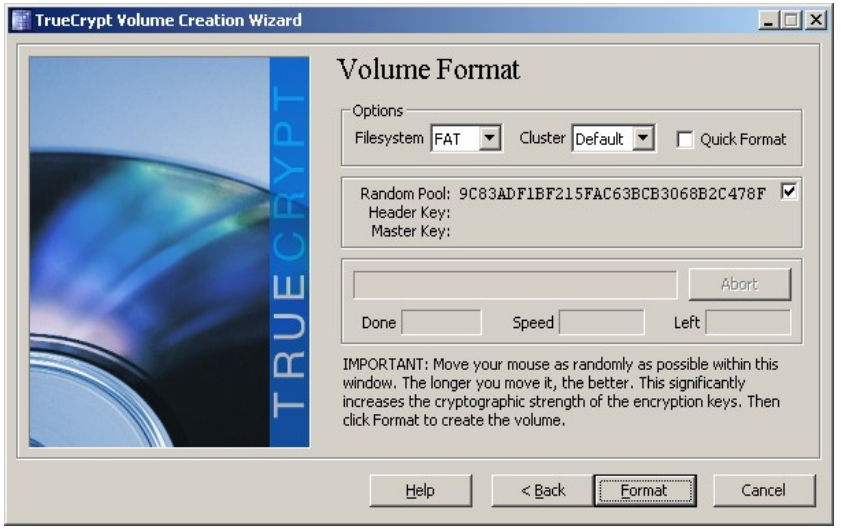
Sichere Passphrase wählen.

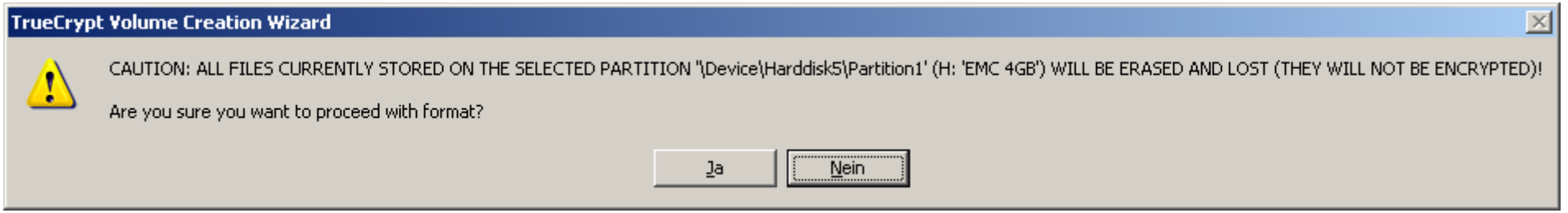


Da diese Phrase eventuell bei einer mobilen Nutzung eingegeben werden muss und man dabei dem Risiko ausgesetzt ist, beobachtet zu werden, könnte hier abweichend vom Beispiel eine separate, nur für diesen Zweck verwendetet Phrase sinnvoll sein, damit im Fall einer Kompromittierung nicht die Phrases aller anderen Volumes mit geändert werden müssen.

Komplett verschlüsseltes Device (Drive/Partition) Volume

Der Pool für Zufallszahlen wird wieder mit der Maus gefüllt

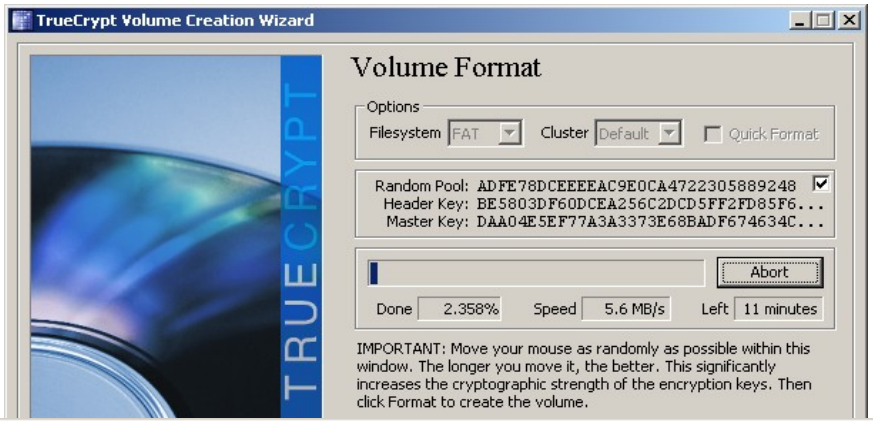


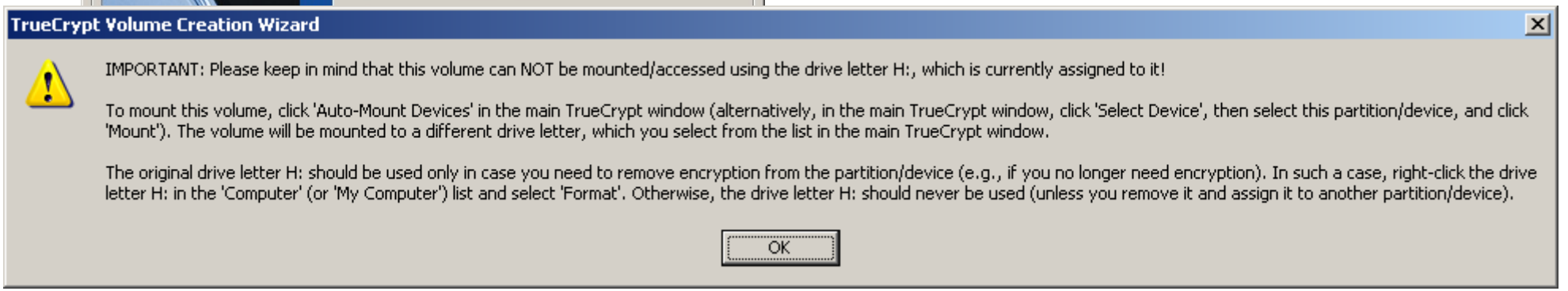


TrueCrypt warnt nochmal vor möglichen Datenverlusten

Komplett verschlüsseltes Device (Drive/Partition) Volume

Die Komplettverschlüsselung dauert, abhängig von der Größe des Devices einige Zeit.
Bei diesem USB 2.0 Stick werden etwa 6 MB/sec verschlüsselt.

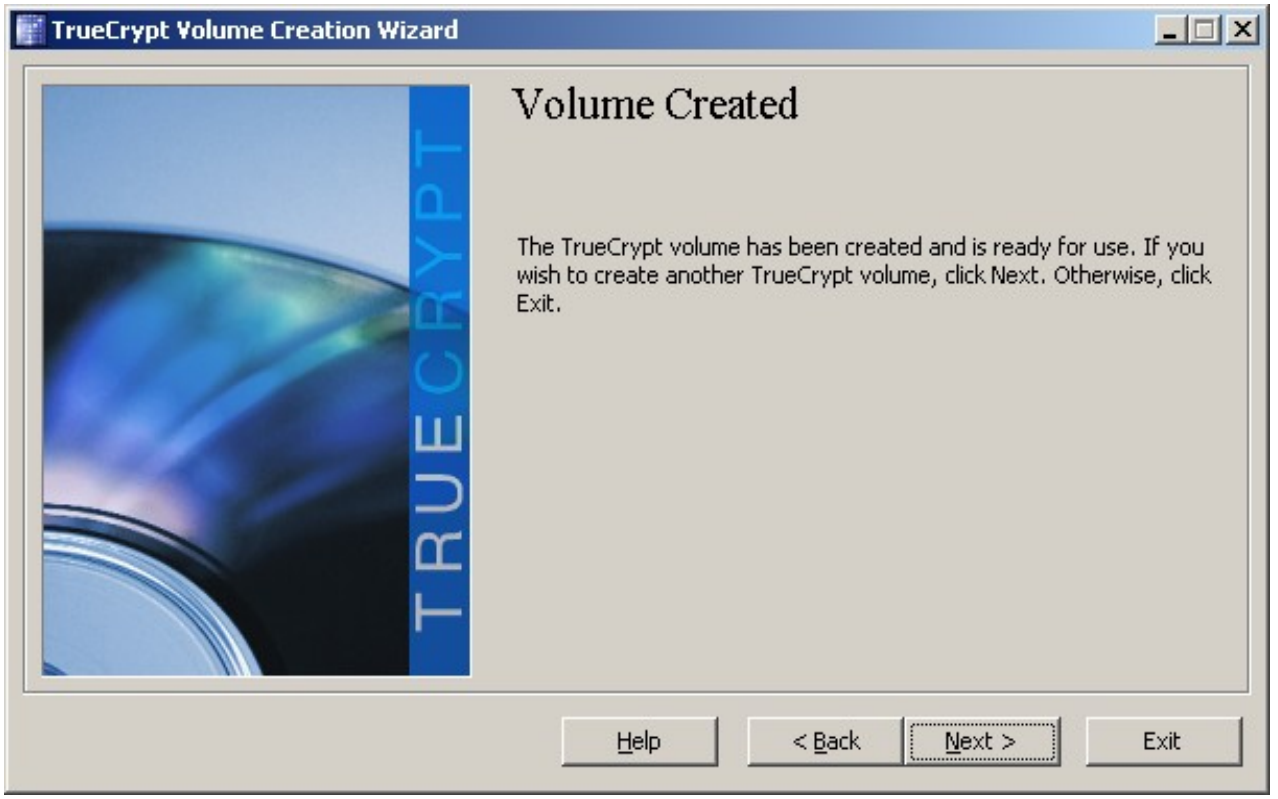




Es erscheint noch ein Hinweis, dass der bis zu diesem Zeitpunkt der Verschlüsselung genutzte Laufwerksbuchstabe des Devices nicht zum Mounten des Volumes wieder verwendet werden darf.

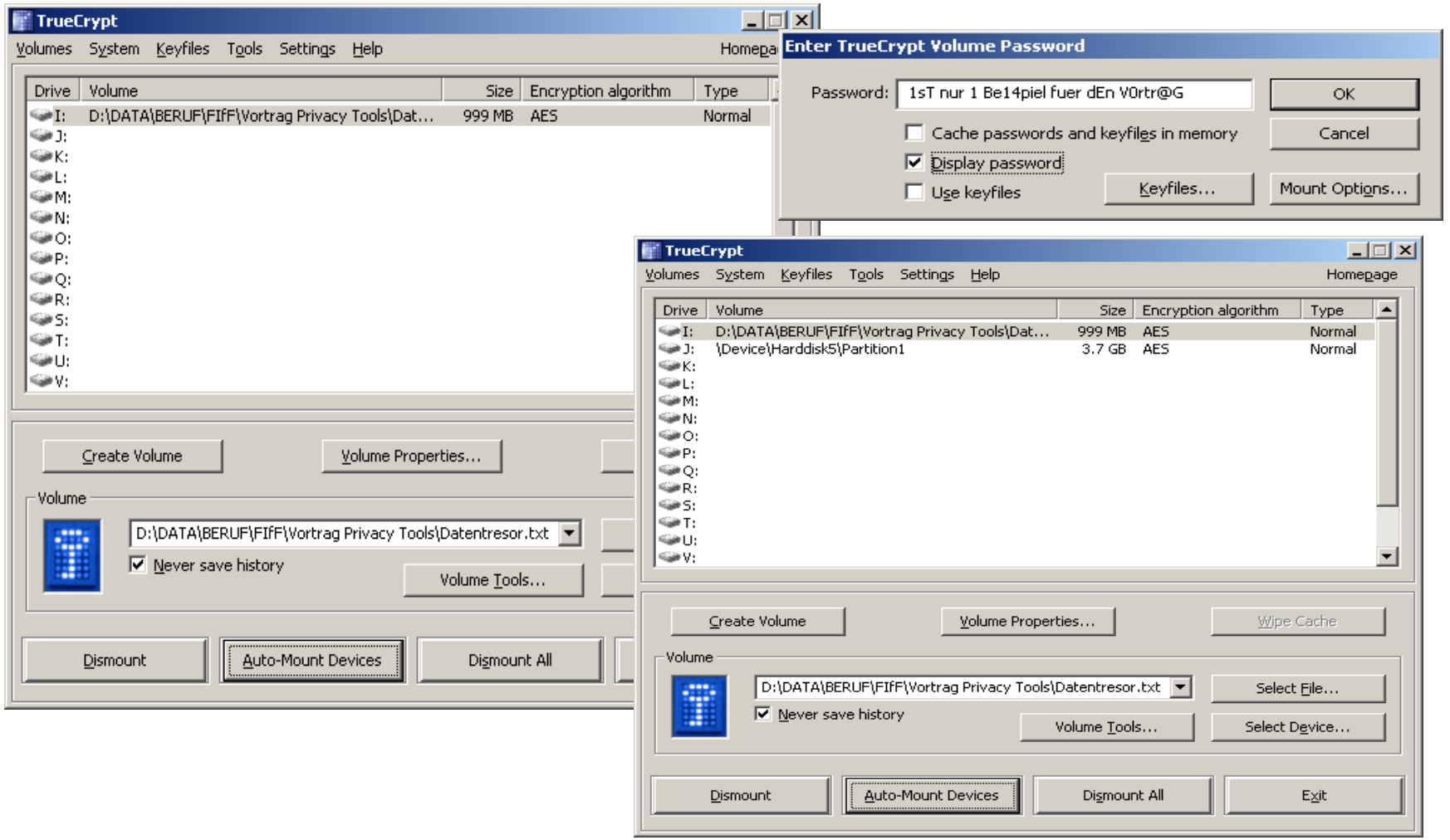
Komplett verschlüsseltes Device (Drive/Partition) Volume

Die Komplettverschlüsselung des Devices ist damit abgeschlossen. Das Device kann jetzt als Volume gemountet und genutzt werden.



Nutzung verschlüsselter Device (Drive/Partition) Volumes

Bei verschlüsselten Devices kann die Automount Funktion genutzt werden

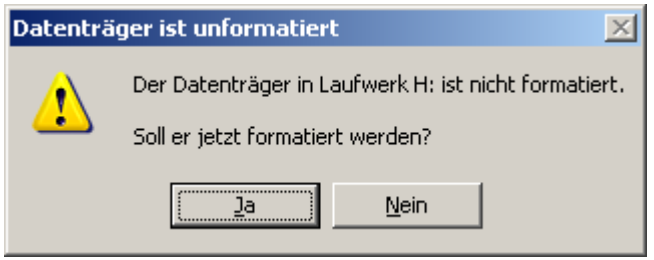


Nutzung verschlüsselter Device (Drive/Partition) Volumes

Um den USB Stick in Szenario 2 nutzen zu können, muss TrueCrypt ausgeführt werden. Für einen mobilen Einsatz etwa im Internetcafé oder an einem fremden PC, z.B. bei Bekannten, kann TrueCrypt als mobile Version auf einem zweiten Stick oder auf einer anderen unverschlüsselten Partition des gleichen Sticks verwendet werden.

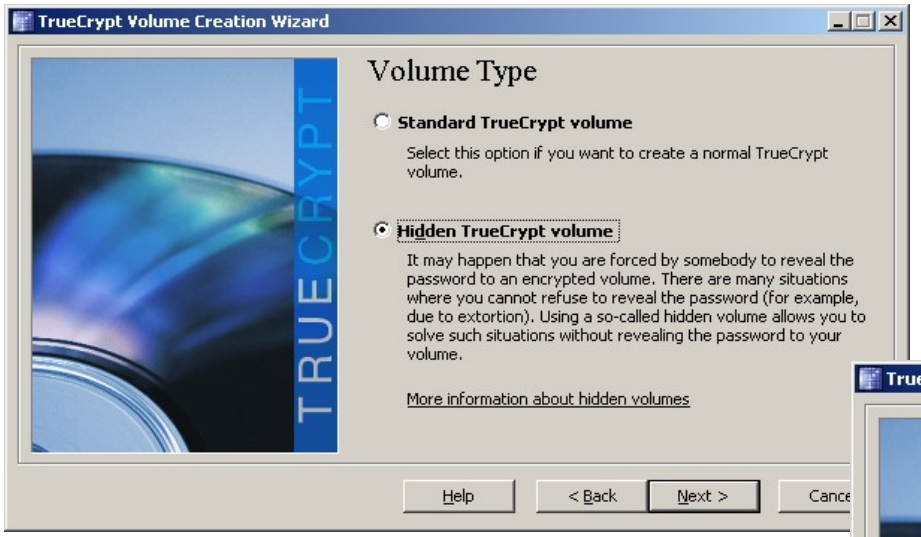
Da auch die Nutzung von Hidden Volumes TrueCrypt vorraussetzt, sind diese in Szenario 2 nur in seltenen Nutzungsfällen sinnvoll. Eine vorhandene TrueCrypt-Installation legt zumindest den Verdacht nahe, dass auch Hidden Volumes existieren könnten.

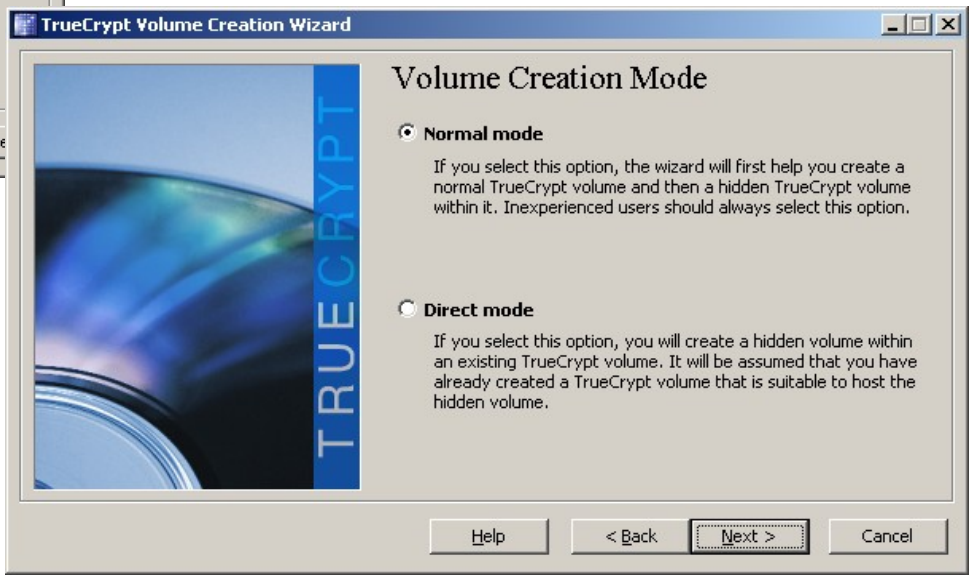
- Achtung: Wenn ein als Device Volume verschlüsselter USB Stick in einen Rechner gesteckt wird, sieht er für Windows wie ein unformatiertes Speichermedium aus, wenn auf den automatisch zugewiesenen Laufwerksbuchstaben (nicht den mit dem Mount in TrueCrypt verknüpften) zugegriffen wird. Die Formatierung würde das Volume mit seinen Daten zerstören!



Hidden Volumes

Aus dem Volume Creation Wizard die Option Hidden Volume wählen:

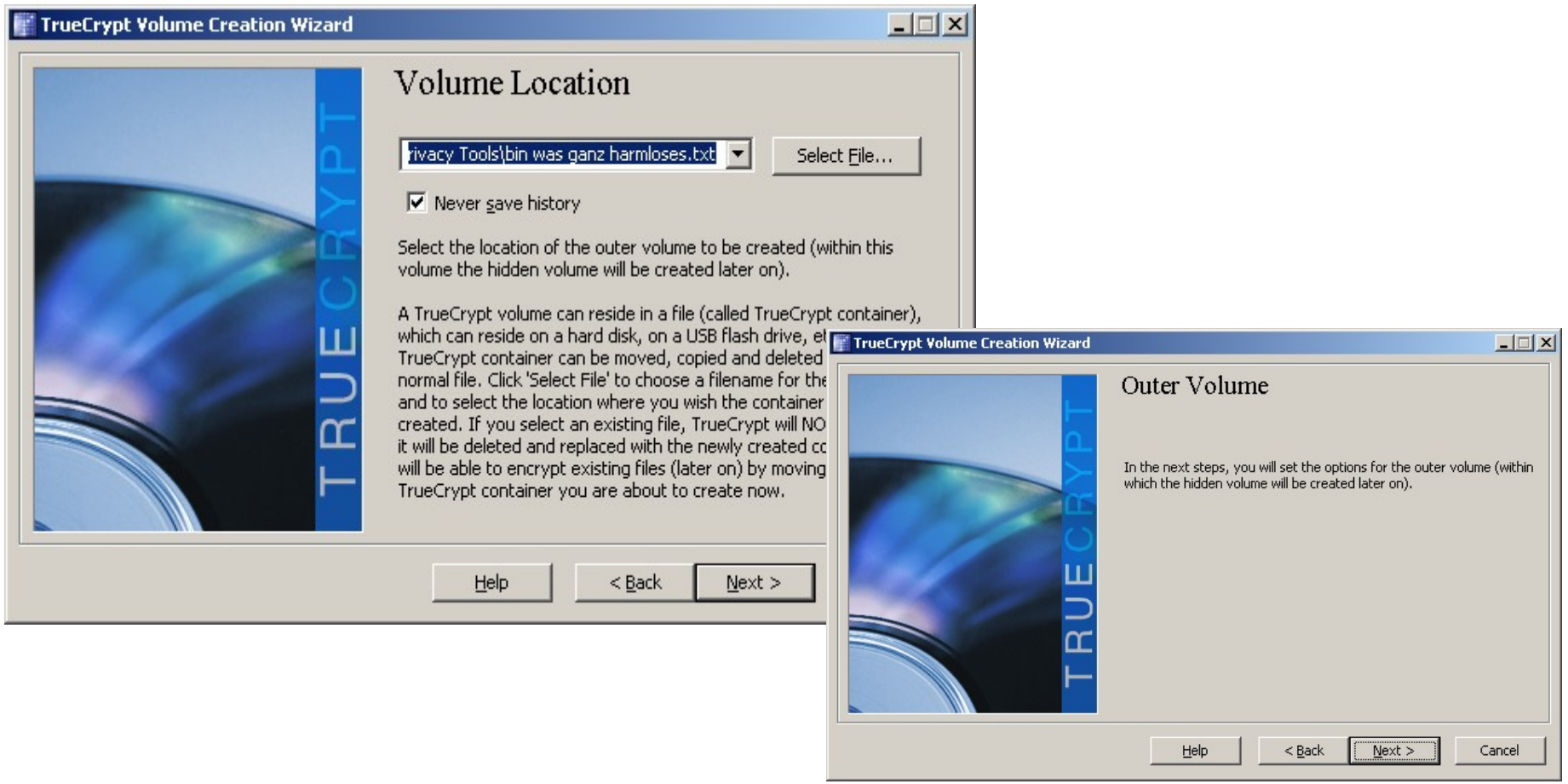




Hidden Volumes werden immer in normale TrueCrypt Volumes eingebettet. Im Normal Mode wird das äußere (outer) Volume in einem ersten Schritt erzeugt.

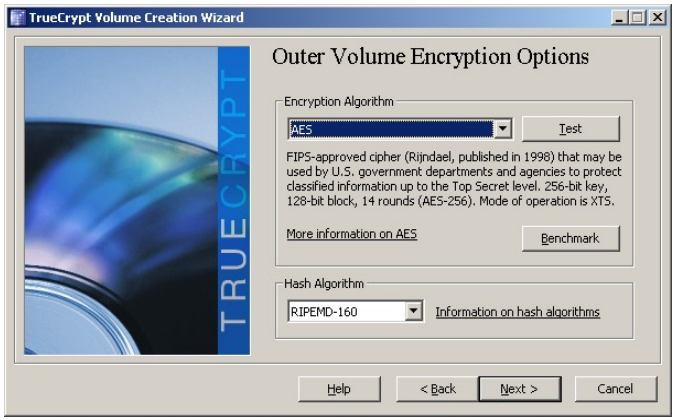
Hidden Volumes

Eine Pseudodatei wählen (oder neu erzeugen) als äußere Hülle (outer Volume) des Hidden Volumes:

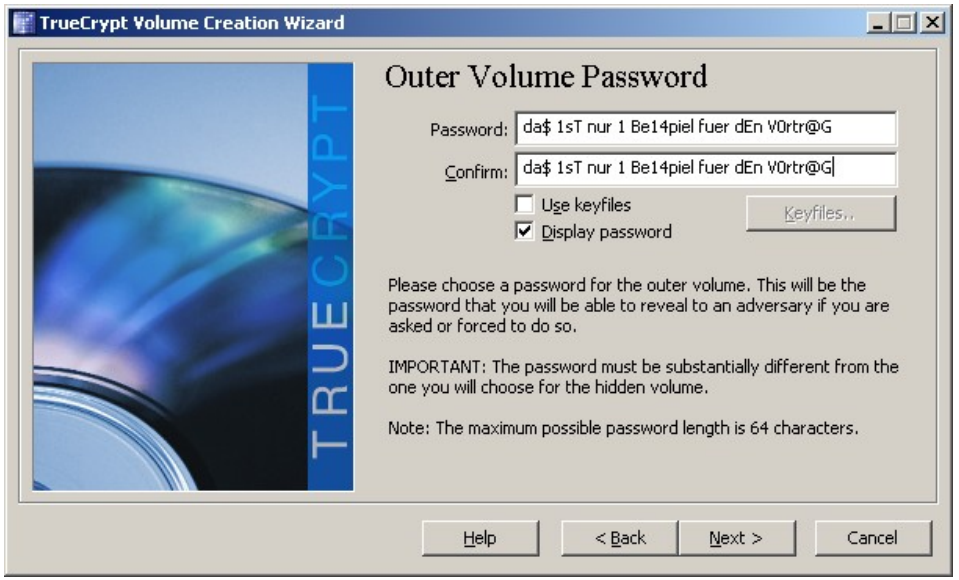


Hidden Volumes

Default-Einstellungen AES und RIPEMD-160



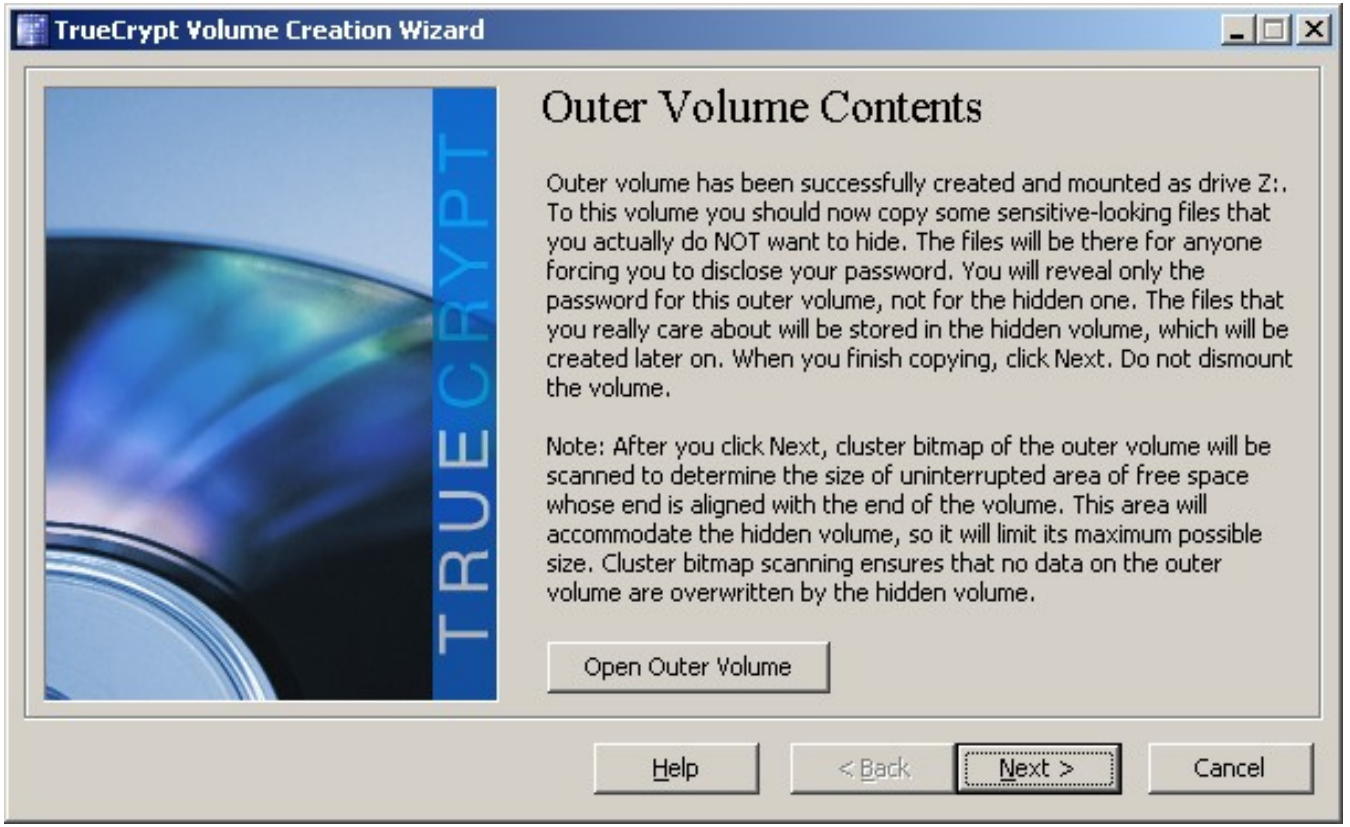
Größe festlegen (min 305 KB für outer Volume)



Passphrase für die äußere Hülle festlegen

Hidden Volumes

Pseudo-vertrauliche Daten erzeugen und in das Outer Volume kopieren. Die Daten sollten nur einen Teil des verfügbaren Platzes nutzen, um für die Hidden Daten Platz zu lassen, aber auch den Anschein erwecken, so vertraulich zu sein, dass es sich lohnt, sie zu schützen. Es könnten z.B. veraltete oder verfälschte Informationen der eigentlich schützenswerten Infos sein.



Hidden Volumes

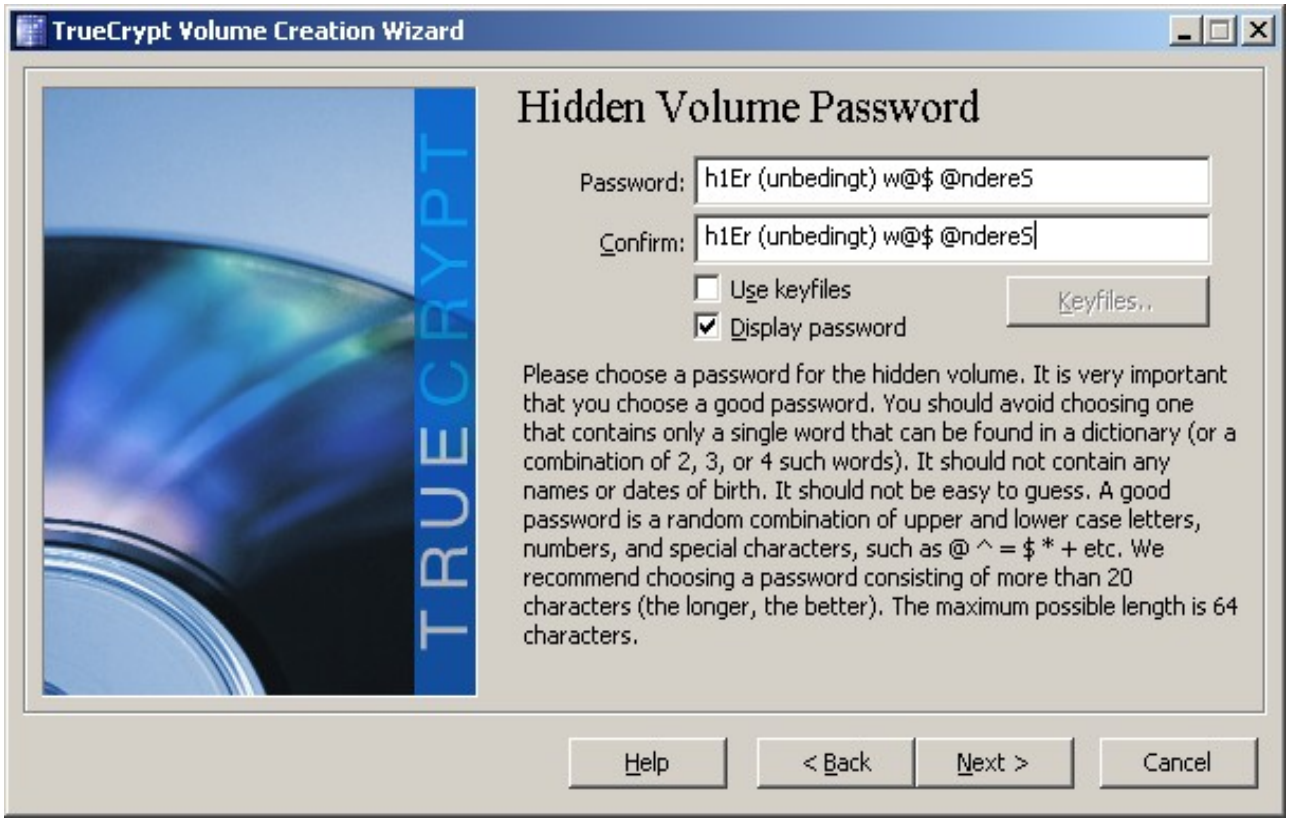
TrueCrypt ermittelt den maximal noch zur Verfügung stehenden Speicherplatz für das Hidden Volume.

Für das Hidden Volume können andere Algorithmen als für das Outer Volume verwendet werden.

Der zur Verfügung stehende Platz ist durch das Outer Volume nach oben begrenzt und sollte nicht voll ausgeschöpft werden, um noch Daten ins Outer Volume speichern zu können.

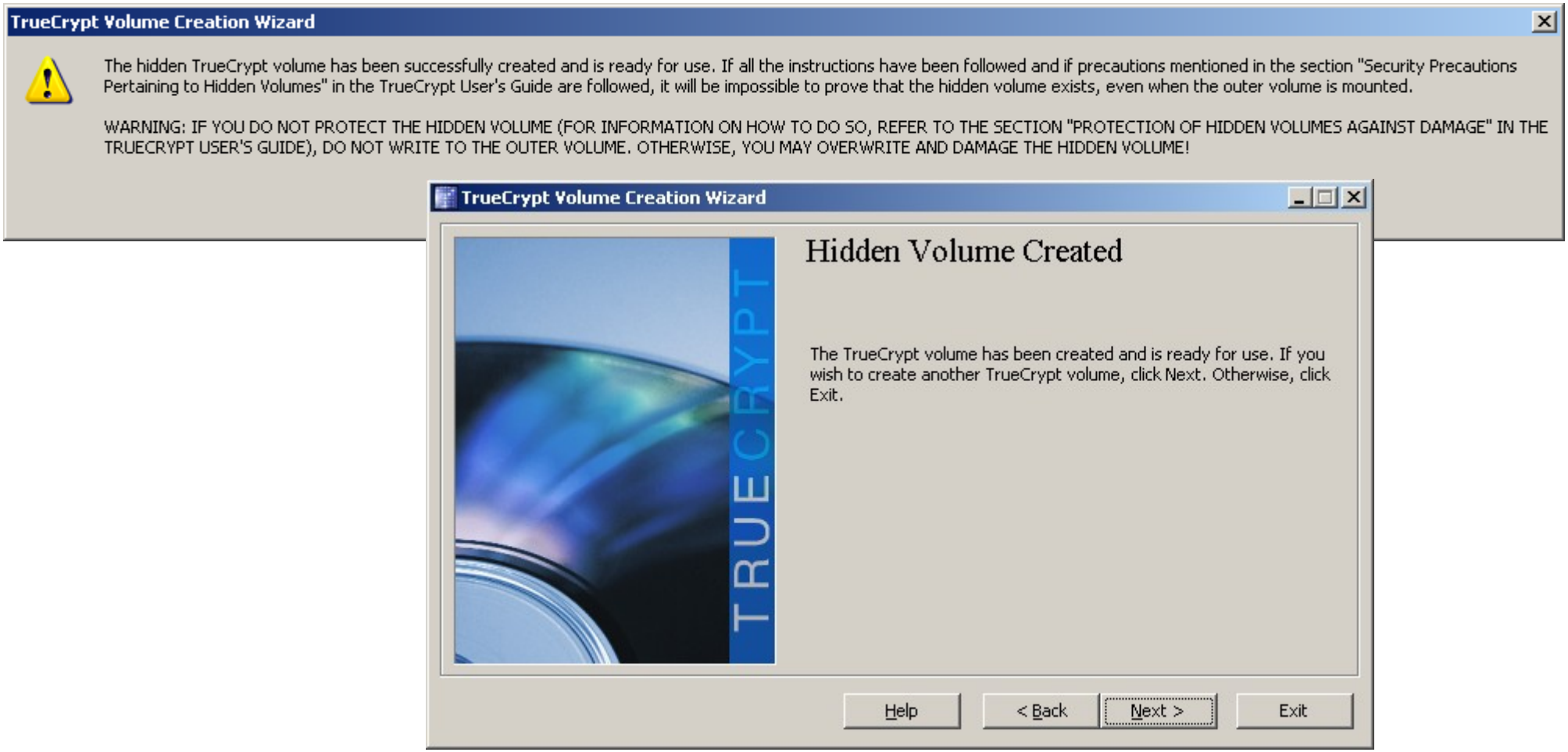
Hidden Volumes

Das Hidden Volume muss unbedingt eine eigene, separate Passphrase bekommen. Durch die verschiedenen Passphrases steuert der Benutzer, ob TrueCrypt das äußere oder das Hidden Volume mounten soll.



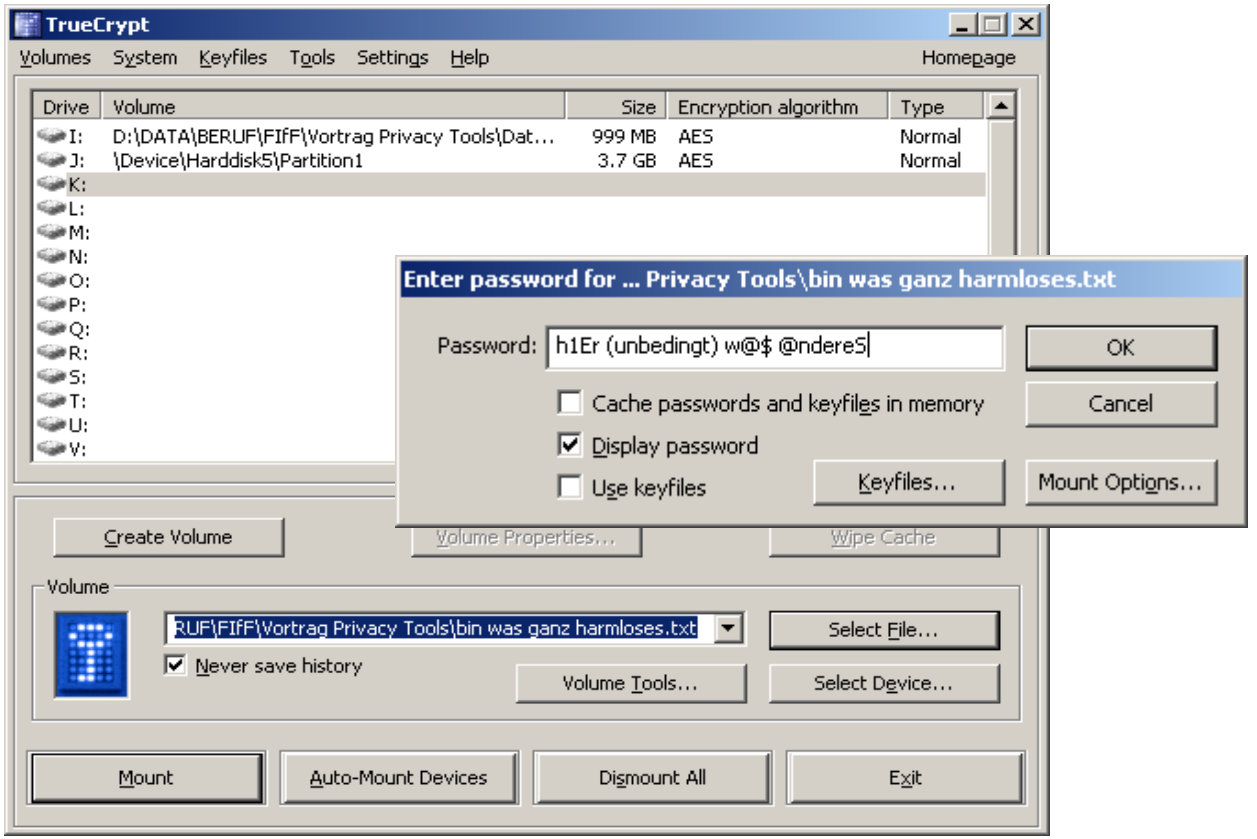
Hidden Volumes

Wie bei allen Volumes wird mit der Maus noch Zufallsmaterial erzeugt und anschließend das Volume erzeugt.



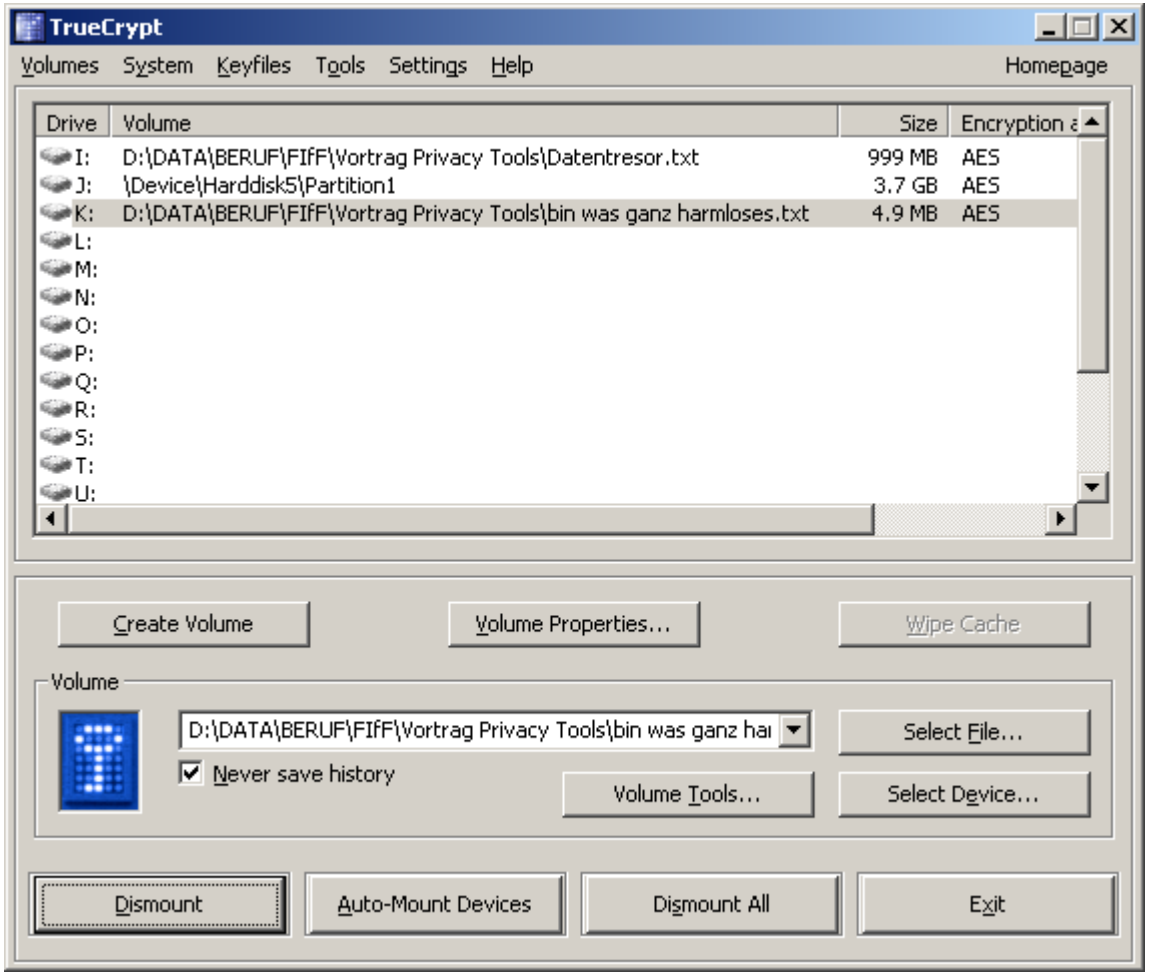
Nutzung Hidden Volumes

Zunächst muss das Outer Volume selektiert werden: Je nachdem welche Passphrase anschließend eingegeben wird (die des Outer oder des Hidden Volumes), wird entsprechend das Outer oder Hidden Volume gemountet. Achtung: Es darf immer nur entweder das Outer oder das Hidden Volume gemountet sein.



Nutzung Hidden Volumes

Danach kann das Hidden Volume wie ein normales Volume genutzt werden.



Restrisiken

Achtung, dies sind nur einige wichtige Beispiele ohne Anspruch auf Vollständigkeit!

- Data Leakage: Beim Arbeiten mit gemounteten Volumes können Metainformationen über Filenamen, zuletzt benutzte, geöffnete, geänderte, gelöschte Dateien usw., also Hinweise auf verschlüsselte oder versteckte Informationen, im Klartext auf die Festplatte geschrieben werden.

  Lösung: Wenn keine plausible deniabilty benötigt wird, komplette Systemplatte verschlüsseln oder Live CD nutzen und nur verschlüsselte oder read only Volumes nutzen

  Wenn plausible deniabilty benötigt wird: hidden operating system nutzen oder Live CD und Hidden Volumes nutzen

- File Paging, Swap File, Auslagerungsdatei: bei der Bearbeitung von Dateien werden Inhalte eigentlich verschlüsselt gespeicherter Informationen im RAM im Klartext zwischengespeichert. Wenn der verfügbare Hauptspeicher nicht ausreicht, wird ein Teil dieser Daten in die Windows-Auslagerungsdatei (bzw. den LINUX SWAP) geschrieben. Wenn nicht die gesamte Windows-Systempartition verschlüsselt ist, können sich dort vertrauliche Daten ansammeln. Daher als Lösung am besten Windows-Systempartition verschlüsseln.

- Hibernation, Power Safe Mode: beim Übergang in den Standby- oder Stromsparmodus werden bei längerer Inaktivität Speicherinhalte auf Festplatte geschrieben. TrueCrypt kann gerade geöffnete vertrauliche Daten nicht vor unverschlüsselter Ablage schützen.

  Lösung: Systemplatte verschlüsseln oder Stromspar- und Hibernation-Funktionen ausschalten

- Memory Dump Files: Fehlerberichte, Hexdump, … können sogar die Passphrases enthalten.
  Lösung: Auch hier Systempartition verschlüsseln oder Memory Dump abschalten.

Restrisiken #2

- TrueCrypt verschlüsselt nur Daten auf Datenträgern, Daten im RAM sind immer unverschlüsselt.
- Cold Boot Attack: Ein gesperrter Rechner hält Passphrases gemounteter Volumes im RAM. Einige RAM-Bausteine löschen sich erst nach Verzögerung, wenn die Stromzufuhr unterbrochen wird. Diese Verzögerung kann durch Herabkühlung soweit ausgedehnt werden, dass das RAM inkl. Dateninhalt in einer anderen Hardware wieder ausgelesen werden kann. Mit etwas Bastelei ist es auch möglich, die Stromzufuhr extern zu überbrücken und RAM aus einem laufenden System ohne Unterbrechung der Spannungsversorgung in ein anderes System zu verpflanzen und die dort gespeicherte Passphrase oder andere vertrauliche Informationen auszulesen.

  Lösung: Volumes bei Nichtbenutzung unmounten
- Physical Security, Kompromittierung des Systems durch Malware: Gelingt es einem Angreifer das System, auf dem TrueCrypt läuft, zu kompromittieren und unter seine Kontrolle zu bringen, kann er z.B. einen Hardware-Keylogger oder eine Malware (es wurde kürzlich ein speziell gegen TrueCrypt konzipiertes Bootkit vorgestellt) installieren und so die Verschlüsselung aushebeln oder die Passphrase erfahren.
- Multiuser Szenario: Password Cache wird von allen eingeloggten Usern geteilt. Switch User löst keinen Unmount aus. User ohne Admin-Rechte können Truecrypt unter Windows nutzen; unter UNIX sind normale Benutzer i.d.R. nicht berechtigt zu mounten.
- Passwortwechsel nach Kompromittierung der Phrase: Ein Angreifer könnte aus einer Kopie den Masterkey ziehen. Bei Verdacht der Kompromittierung der Passphrase (Beobachtung der Eingabe, Malware-Befall) neue Volumes (mit neuen Passphrases) anlegen, vertrauliche Daten aus alten Volumes herauskopieren und alte Volumes löschen.

Agenda

1. Begrüßung und Vorstellung
2. Einleitung – Kurzvorstellung der Tools
3. GnuPG
4. TRUECRYPT
5. **Tor**
6. Zusammenwirken der Tools
7. Fragen und Diskussion

Tor Anwendungszweck

Tor ist freie Open Source Software (für Win, Linux, MAC) und bezeichnet auch ein zugehöriges Netzwerk. Der Tor-Client dient dazu, anonyme TCP-Verbindungen über das Tor-Netzwerk herzustellen. Hauptanwendungsgebiet ist der anonyme Zugriff auf Webseiten und das anonyme Bereitstellen von Webservices im Internet. Es kann aber auch für andere TCP-basierte Dienste, z.B. zur anonymen Kommunikation per Chat genutzt werden. Mit Tor können auch Zensurbarrieren des eigenen Providers umgangen werden (Zugang zu gesperrten Webseiten).

Tor verhindert eine Verkehrsdatenanalyse der Verbindungsdaten, also eine Auswertung, wer mit wem wann und in welchem Umfang über das Netz kommuniziert hat. Die standardmäßig im Internet genutzten Verschlüsselungsverfahren (TLS/SSL, Ipsec, GnuPG) verschlüsseln und schützen lediglich den Inhalt der übertragenen Daten vor unerwünschten Mitlesern. Die Verbindungsdaten werden dabei nicht verborgen und sind z.B. durch staatliche Stellen, den Betreiber des Webservers oder die Provider auswertbar. Tor kann diese Lücke schließen und damit helfen, „die persönliche Freiheit und Privatsphäre wie auch vertrauliche Geschäftsbeziehungen und die allgemeine Sicherheit zu schützen.“ (www.torproject.org)

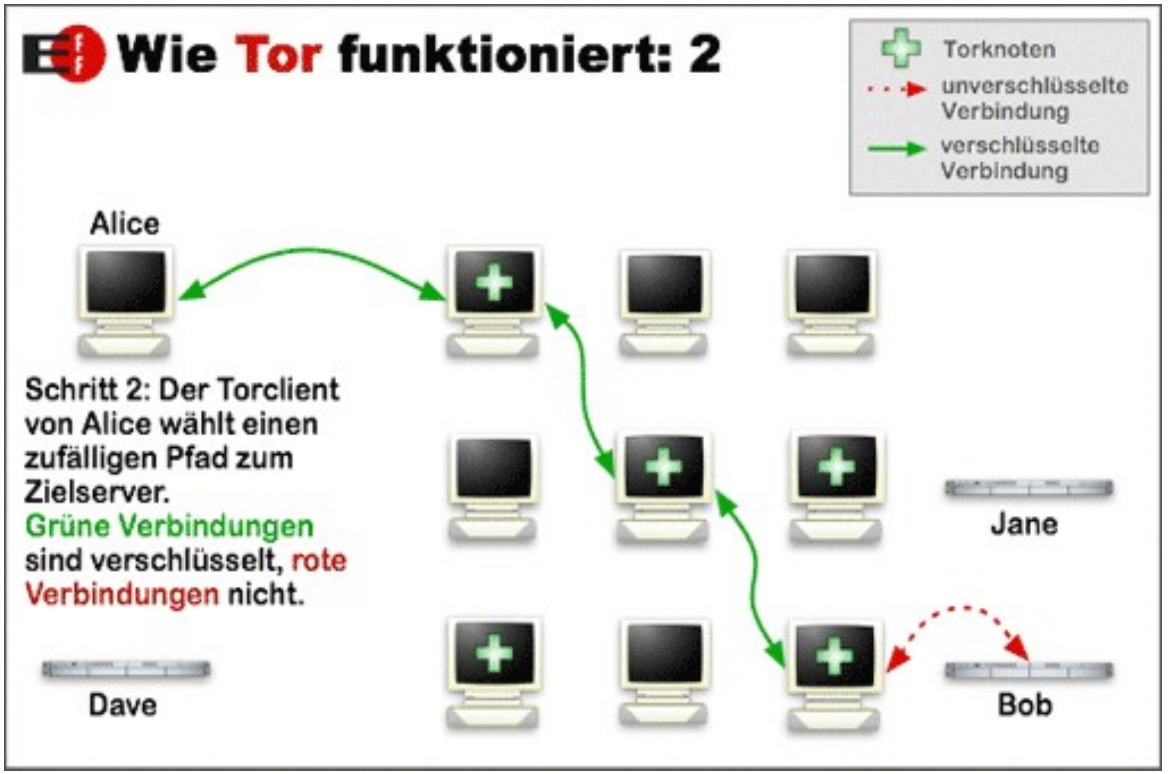
Tor bildet ein Onion Routing System, indem es das TCP-Datenpaket durch mehrere Verschlüsselungsschritte mit mehrere Schalen (wie bei einer Zwiebel) umgibt. Die äußerste Schale wird durch den öffentlichen Schlüssel des ersten Servers gebildet, die innerste Schale durch den öffentlichen Schlüssel des letzten Tor-Servers (auch Exit Node genannt). Auf dem Weg durch das Tornetzwerk entfernt jeder Server mit seinem privaten Schlüssel durch Entschlüsseln eine der Schalen und leitet das entschälte Datenpaket an den nächsten Tor-Server weiter. Er sieht nach Entfernung der Schale immer nur den nächsten vom Absender ausgewählten Tor-Server (bzw. als Exit Node die angesurfte Webadresse) sowie den vorherigen Server (bzw. als erster Server die IP des Surfers). Werden mindestens drei Server (drei Schalen) verwendet, kennt keiner allein mehr den ganzen Weg. Der erste Server kennt nur den Sender (der hier also nicht anonym ist) und den 2. Server. Der 2. Server kennt nur den 1. und 3. Server, der 3. Server kennt nur den 2. Server und das Ziel der Verbindung.

Tor Funktionsweise

Zur Zeit sind weit über 1000 Torknoten verfügbar, die in Schritt 1 geladen werden,...

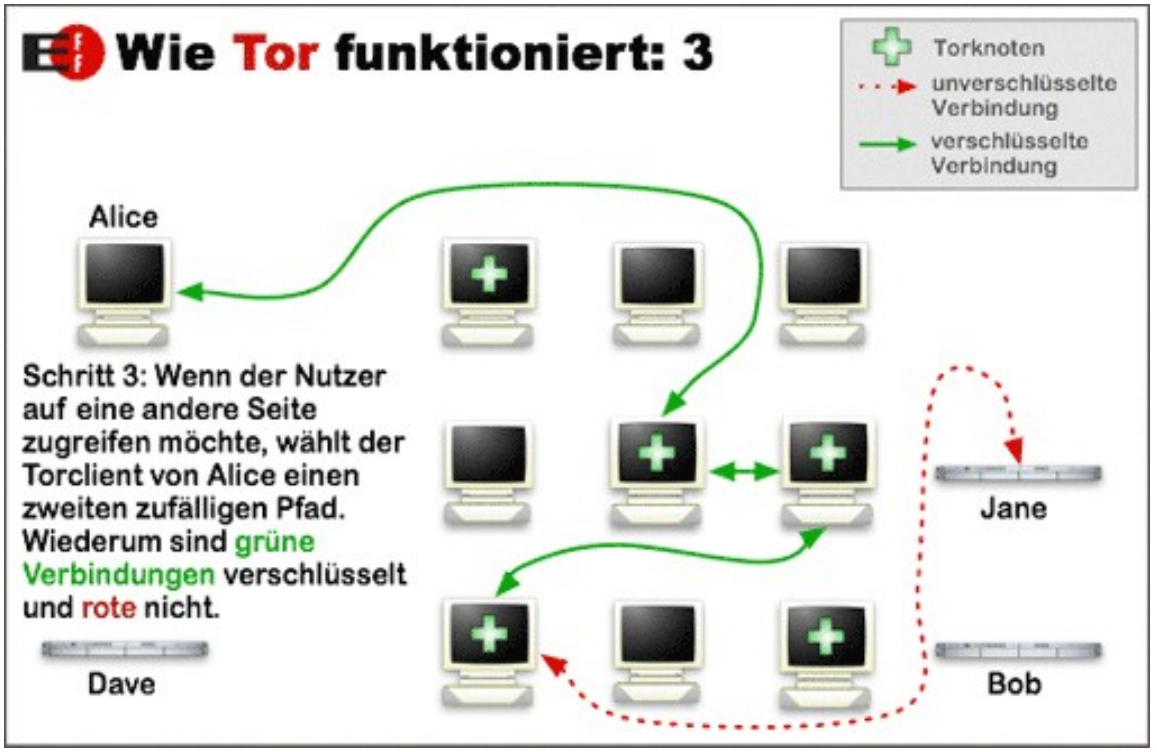
Tor Funktionsweise

… und aus denen der Client zufällig drei auswählt



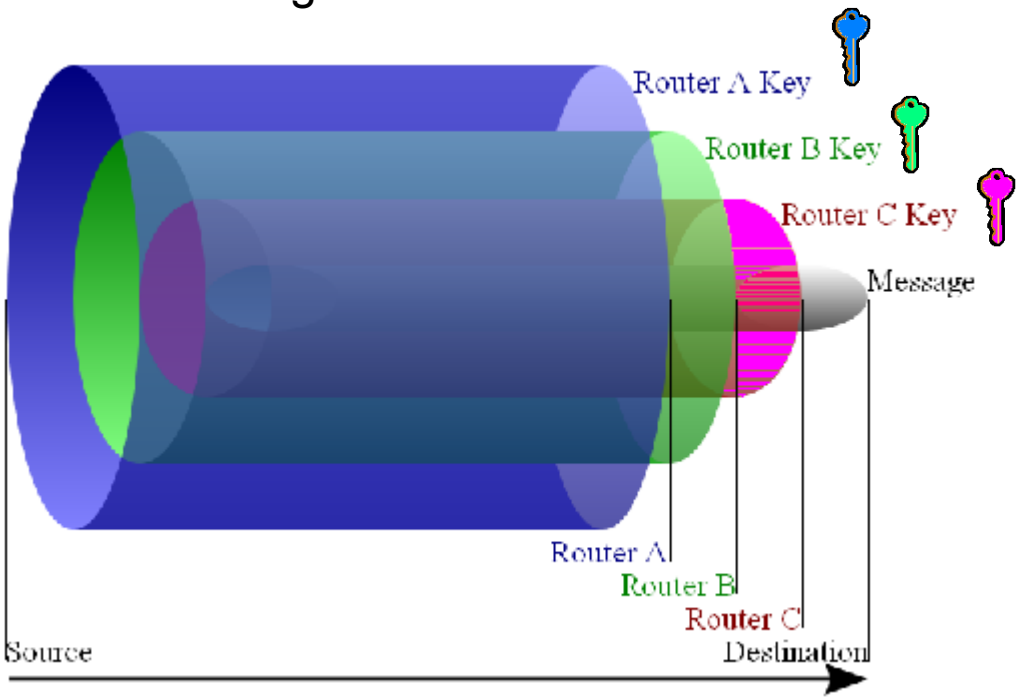
Tor Funktionsweise

… bei jedem Wechsel auf eine neue Seite, werden drei neue Server zufällig ausgesucht



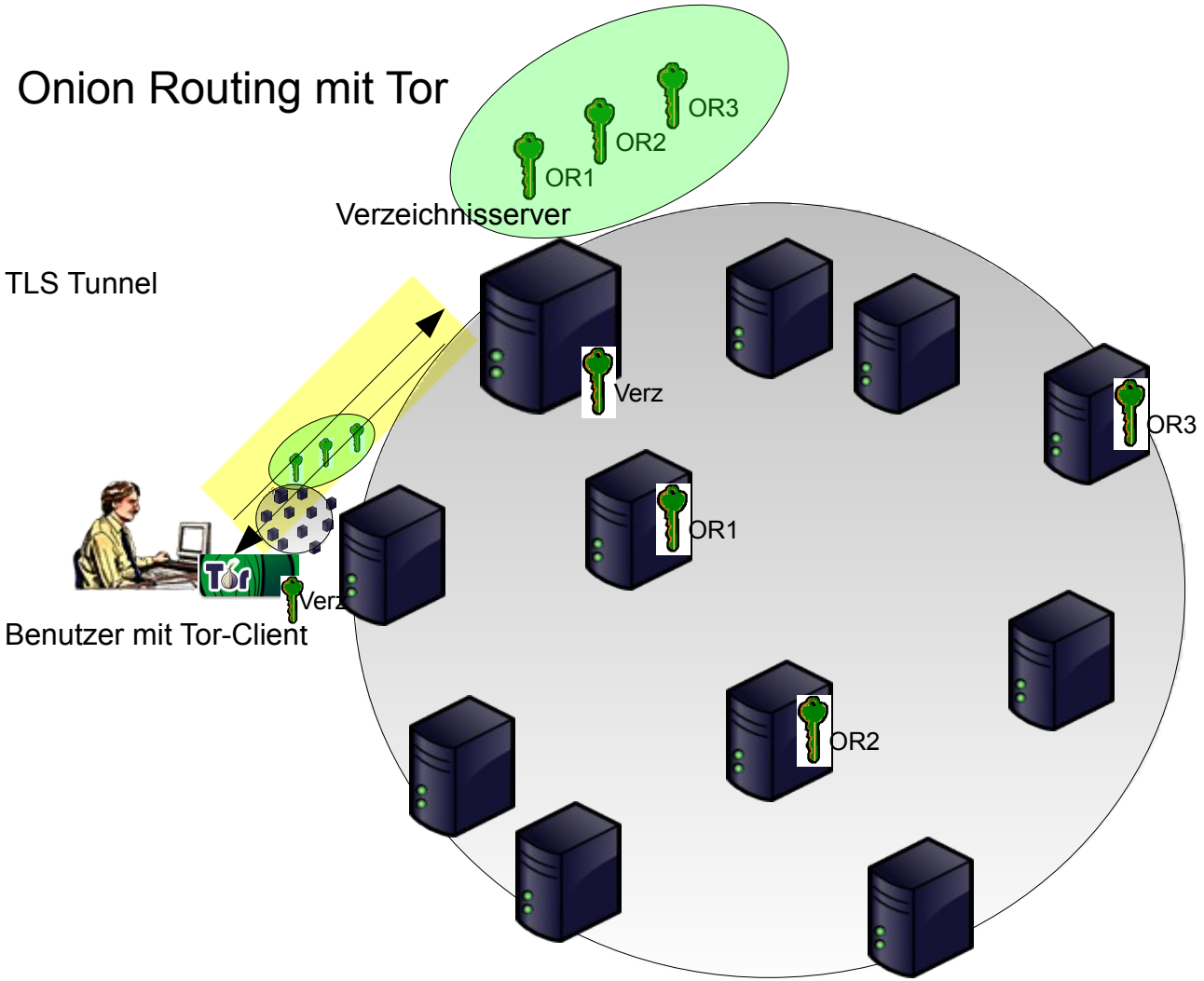
Tor Funktionsweise

Onion Routing mit Tor



http://de.wikipedia.org/wiki/Onion_Routing
(Urheber Harrison Neal)

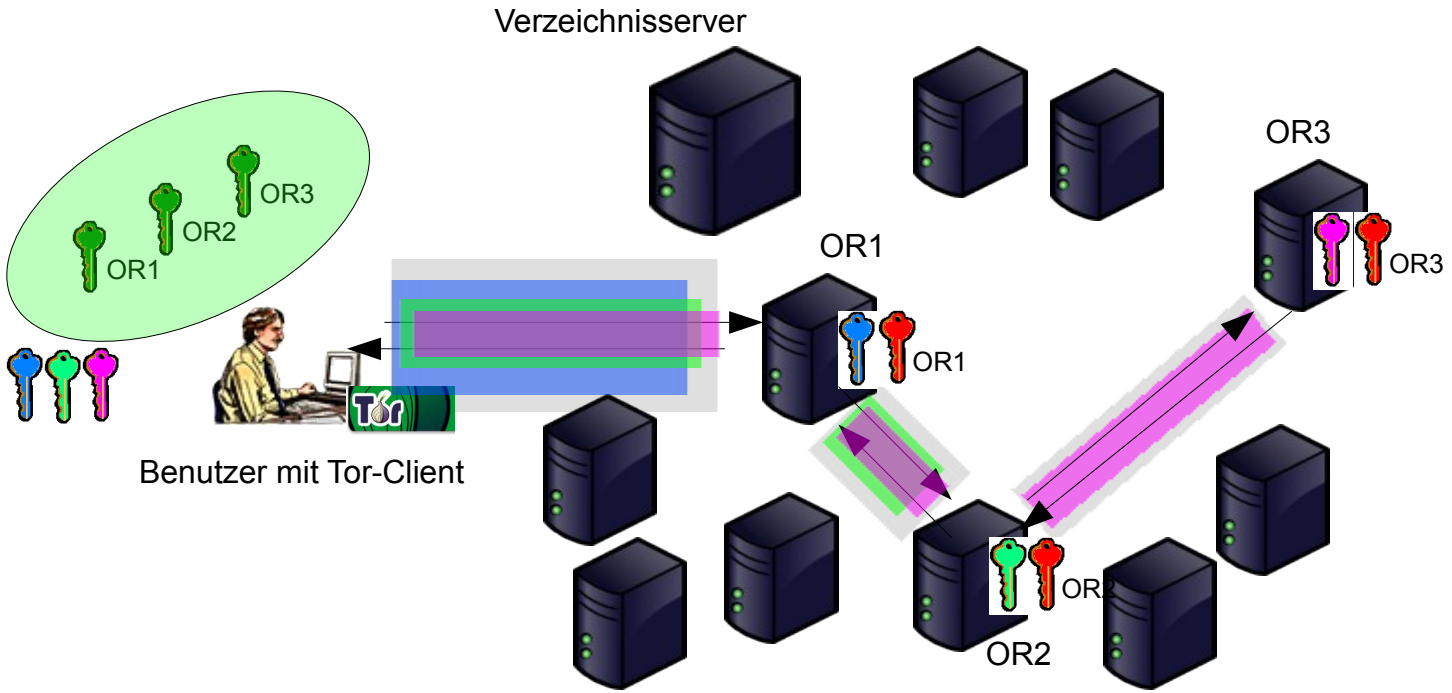
Tor Funktionsweise



Der Tor-Client stellt eine Anfrage an einen der Verzeichnisserver
Der Server authentisiert sich anhand seines im Sourcode des Clients hinterlegten Public Keys Verz
Der Tor-Client erhält vom Verzeichnisserver eine Liste aller verfügbaren Tor-Knoten-Server und zugehöriger Pubkeys.

Tor Funktionsweise

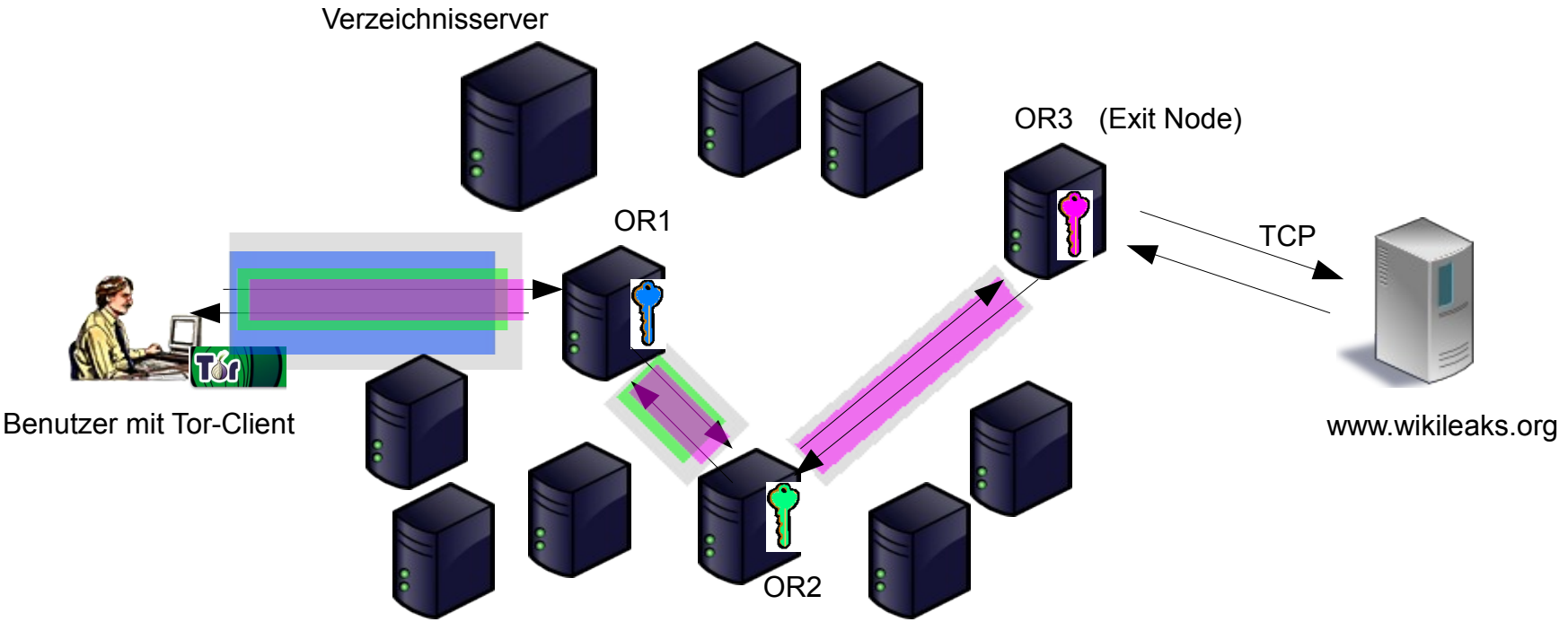
Aufbau des Circuits (Verbindungsweg)



Der Tor-Client (OP= Onion Program) wählt zufällig aus der Liste drei Knotenserver (OR=Onion Router) aus.
Er handelt über eine TLS-Verbindung mit dem 1. OR1 einen Session Key (blau) aus und gibt der Verbindung eine CircID OP-OR1.
Als nächstes übergibt er OR1 einen Befehl, eine weitere Verbindung zu OR2 zu etablieren.
OR1 benutzt einen TLS-Tunnel zu OR2 (über den weitere Torverbindungen multiplext werden) und vergibt eine eigene CircID OR1-OR2.
OP und OR2 vereinbaren, indirekt verbunden über OR1, ebenfalls einen Session Key (grün).
OP lässt OR1 ein pub(OR2) verschlüsseltes Paket an OR2 weitergeben, das den Befehl enthält, eine Verbindung zu OR3 aufzubauen.
OR2 etabliert über TLS eine Verbindung zu OR3 und vergibt eine eigene CircID OR2-OR3.
OP handelt mit OR3 (indirekt verbunden über OR1 und OR2) einen Session key aus (pink).

Tor Funktionsweise

Aufbau der Verbindung zum Zielserver



OP schickt OR1 den Befehl, pubOR2-verschlüsselte Daten weiterzuleiten an OR2,
Diese enthalten den pubOR3-verschlüsselten Befehl, Daten an OR3 weiterzuleiten.
Die Daten für OR3 enthalten das Kommando, eine TCP-Verbindung zum Zielserver aufzubauen (i.d.R. unverschlüsselt)
OR1 kennt die IP von OP und dessen CircID zu OR2.
OR2 kennt die zu dieser CircID gehörende CircID der Verbindung zu OR3
OR3 kennt diese CircID und die Zieladresse der Verbindung. Er fungiert damit als sogenannter Exit Node.
Das Ziel kennt die IP von OR3
Keiner außer OP kennt die gesamte Verbindung, weshalb OP anonym mit dem Ziel kommuniziert

Tor für Fortgeschrittene

Betreiben eines Tor-Servers

- Erfordert Konzeption einer Exit Policy, wohin Verbindungen erlaubt werden sollen, z.B. nur Verbindungen zu anderen Tor-Servern (kein Exit Node)
- Kann zu Abuse-Anfragen führen, da eigene IP Adresse im Rahmen von Verfahren ermittelt wird. (Kripo versteht inzwischen meistens, was TOR ist)
- Benötigt Bandbreite

Bridges

Mit dem Betreiben einer Bridge stellt ein Tor-Nutzer seinen Client als Verbindung zum Tor-Netzwerk zur Verfügung und leitet ebenfalls Tor-Datenverkehr weiter. Er betreibt aber keinen Server. Die Bridges werden über einen von drei Wegen (Web, Mailverteiler und persönlichen Kontakte) in Länder mit Zensurregelungen weitergegeben. Sie dienen dazu, Zensurmechanismen zu umgehen, die eine Verbindung zu bekannten Tor-Serven verhindern (große Nutzung in China und Iran).

Hidden Services

- Man kann über Tor auch anonym Dienste anbieten, z.B. eine Dissidenten-Website in einer Diktatur betreiben. Der Anbieter des Hidden Service befindet sich ebenso wie der anonyme Besucher hinter einem Onion Circuit im Tor-Netzwerk.
- Der Tor-Client des Anbieters wählt mehrere weitere Tor-Server davor als Einführungspunkte aus.
- Der Besucher setzt über einen dieser Punkte einen Kontaktwunsch ab und wählt einen weiteren Server als Rendezvouspunkt.
- Der Anbieter entscheidet, ob er dem Wunsch nachkommt, und verbindet sich ggf. mit dem Rendezvouzpunkt, wodurch die Verbindung zustande kommt.

Tor Risiken

Warnung: Willst du, dass Tor wirklich funktioniert?

… dann installiere es nicht nur einfach und denk nicht weiter drüber nach. Du musst ein paar deiner Verhaltensweisen ändern und deine Software überprüfen! Tor an sich ist NICHT alles, was du brauchst, um anonym zu sein. Es gibt mehrere, schwerwiegende Fallen, in die du geraten kannst:

1. Tor "schützt" nur Anwendungen, die so eingestellt sind, dass sie ihren Verkehr durch Tor leiten. Es anonymisiert nicht alle deine Daten, bloß weil du es installiert hast. Wir empfehlen dir, Firefox mit der Torbutton-Erweiterung zu benutzen.

2. Torbutton blockt Browser-Plugins wie Java, Flash, ActiveX, RealPlayer, Quicktime, Adobes PDF Plugin und andere: Diese können dazu gebracht werden, deine richtige IP-Adresse zu verraten. Zum Beispiel bedeutet das, dass YouTube nicht funktioniert. Wenn du wirklich YouTube benötigst, kannst du Torbutton umstellen, sodass es erlaubt wird; aber sei dir im Klaren darüber, dass du dich damit potenziell angreifbar machst. Außerdem: Erweiterungen wie die Google Toolbar suchen über Seiten, die du besuchst, weitere Informationen raus: Dabei könnten sie Tor umgehen und/oder sensible Informationen weitergeben. Es gibt Leute, die deswegen 2 Browser benutzen (einen für Tor und einen für unsicheres Browsing).

3. Pass auf Cookies auf: Wenn du jemals ohne Tor auf eine Seite gehst und diese dir einen Cookie einrichtet, könnte dich dieser Cookie identifizieren, wenn du wieder Tor benutzt. Torbutton versucht, deine Cookies dagegen abzusichern. CookieCuller kann dir helfen, Cookies zu sichern, die du nicht verlieren willst.

Tor Risiken

4. Tor anonymisiert die Herkunft deiner Daten und verschlüsselt alles zwischen dir und dem Tor-Netzwerk sowie alles im Tor-Netzwerk, aber es kann nicht die Daten zwischen dem Tor-Netzwerk und dem endgültigen Ziel verschlüsseln. Wenn du geheime Informationen verschickst, solltest du genauso viel Sorgfalt wie im normalen "bösen" Internet verwenden — benutze HTTPS oder andere End-To-End-Verschlüsselung und Authentifizierung.

5. Zwar schützt dich Tor davor, dass lokale Angreifer deine Daten beeinflussen oder mithören, aber es bringt auch neue Risiken: Böswillige Exit-Knoten können dich auf falsche Seiten leiten oder dir sogar verschleierte Applets schicken, die so aussehen, als kämen sie von einer vertrauenswürdigen Seite. Du solltest sehr vorsichtig sein, wenn du Programme oder Dokumente über Tor runtergeladen hast und deren Integrität nicht überprüfen kannst.

Quelle: http://www.torproject.org/download.html.de#Warning

Es gibt einige weitere Sicherheitsrisiken, die einen hohen Aufwand durch den Angreifer erfordern:

- Timing Analysen
- Eigenbetrieb oder Kompromittierung mehrerer Tor-Server durch den Angreifer

Eine gute Übersicht zu Risiken von Tor lieferte Roger Dingledine, einer der Entwickler von Tor in seinem Vortrag auf dem 25C3:

http://mirrors.dotsrc.org/congress/25C3/video_h264_720x576/25c3-2977-en-security_and_anonymity_vulnerabilities_in_tor.mp4

http://mirror.netcologne.de/25c3/audio_only/25c3-2977-en-security_and_anonymity_vulnerabilities_in_tor.mp3

Tor installieren

Empfohlene Konfiguration des Tor-Projekts: Tor in Kombination mit Firefox, dem Addon „Torbutton“ sowie dem lokalen Proxy „Privoxy“; Installation kann auf dem eigenen Arbeitsplatzrechner oder z.B. für Nutzung im Internetcafé auf USB-Stick erfolgen:

- Downloads von http://www.torproject.org
- USB portable Windows Version: http://www.torproject.org/torbrowser/dist/tor-im-browser-1.2.9_de.exe

Nach dem Download sollten zunächst die pgp-Signaturen geprüft werden. Die Entwickler signieren die bereitgestellten Sourcen und fertig kompilierten Binaries mit ihren private keys:

* Rogers (0x28988BF5) unterschreibt meist die Quellcode-Dateien

* Nicks (0x165733EA, oder sein Subkey 0x8D29319A)

* Andrews (0x31B0974B)

* Peters (0x94C09C7F, oder sein Subkey 0xAFA44BDD)

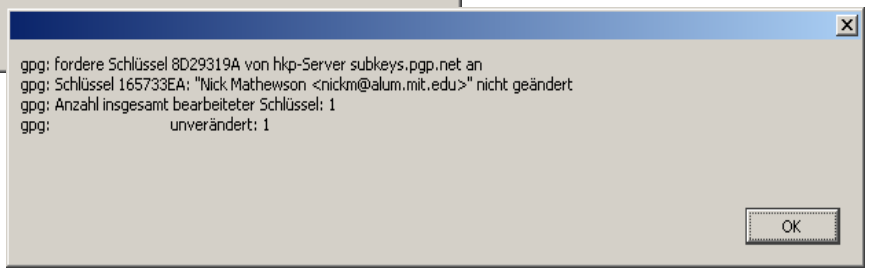
* Matts (0x5FA14861)

* Jacobs (0x9D0FACE4)

Diese Schlüssel müssen zunächst in den GnuPG Keyring importiert werden.

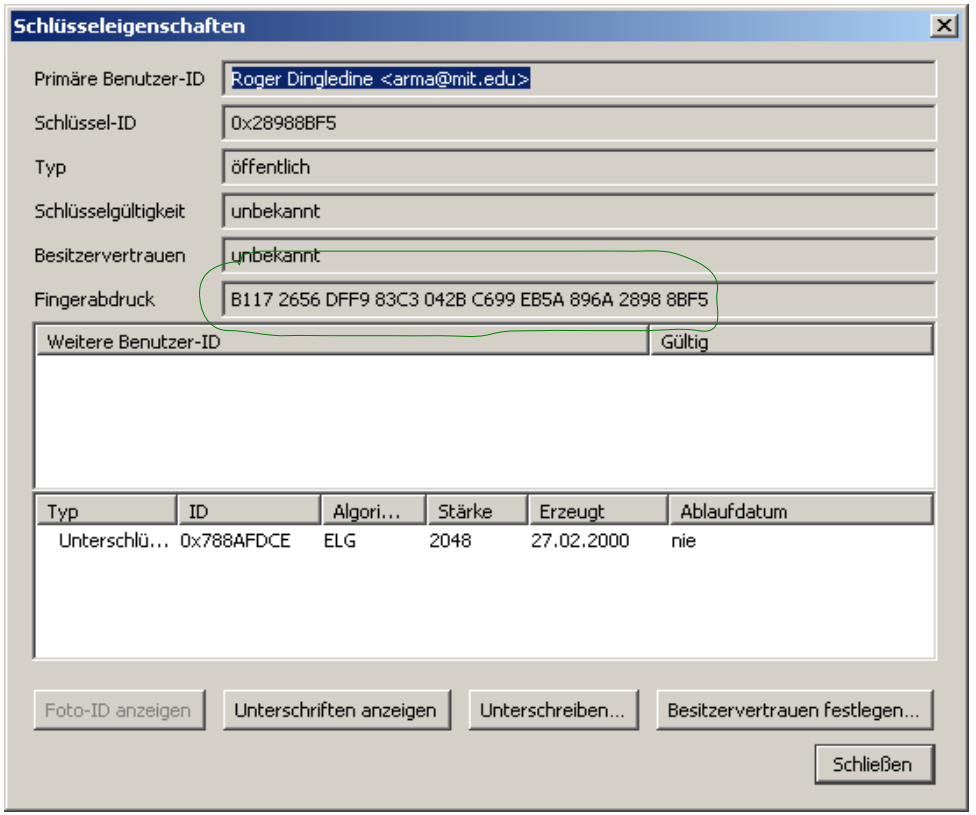
Tor Integrität prüfen

Am einfachsten ist, die Keys von einem der offiziellen Keyserver herunterzuladen, die Subkeys sind auf subkeys.pgp.net zu finden und in den eigenen keyring zu importieren.



Tor Integrität prüfen

Anschließend die Schlüsseleigenschaften der importierten Keys mit den Fingerprints auf den Torseiten http://www.torproject.org/verifying-signatures.html.de vergleichen

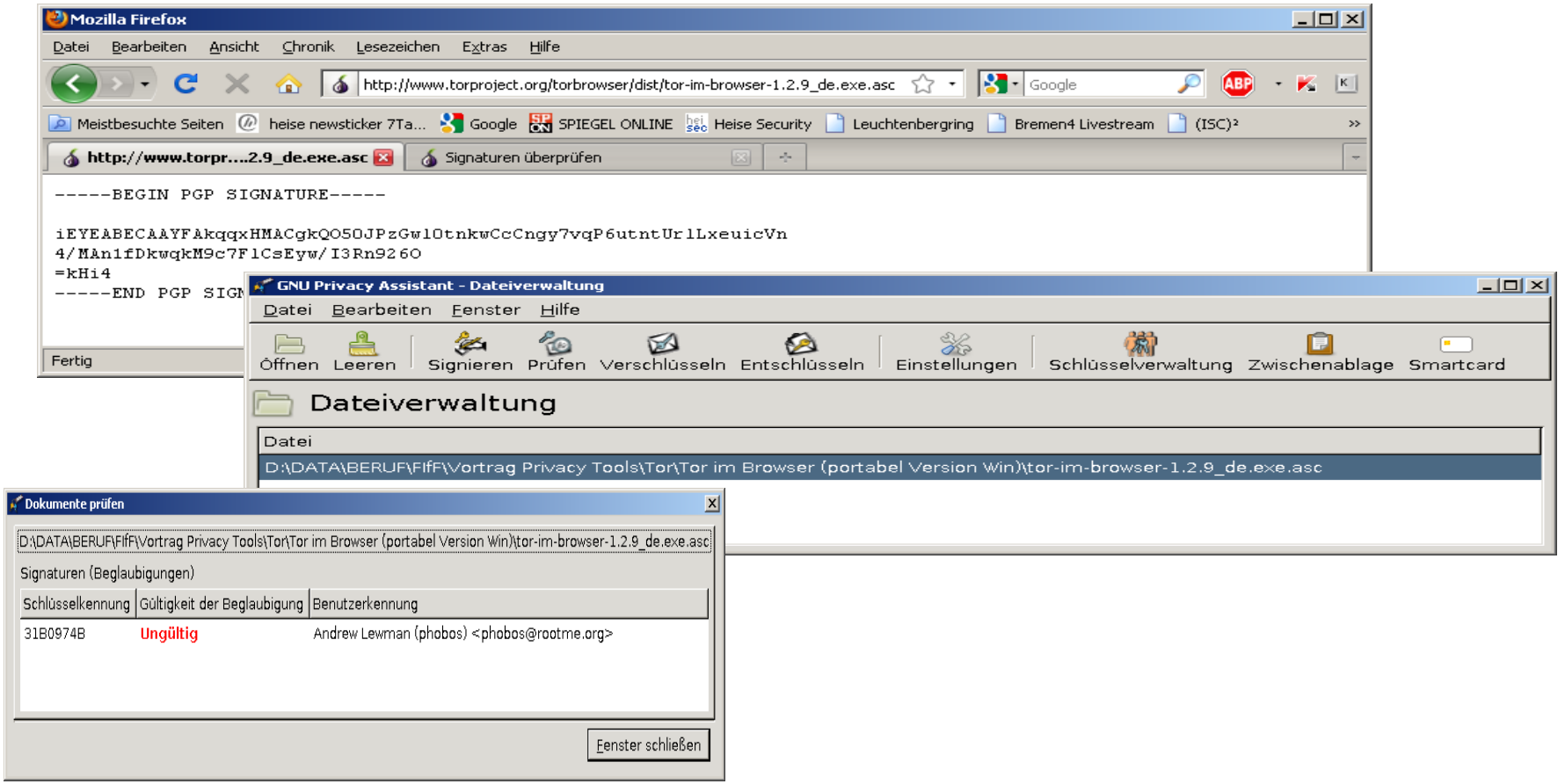


Damit hat man die Wahrscheinlichkeit erhöht, dass es sich tatsächlich um die echten Schlüssel handelt. Wirklich wissen, ob sie echt sind, kann man nur, wenn man den Key direkt von der Person erhalten hat oder über das Web of Trust jemandem vertraut, der jemandem vertraut, … der Roger kennt und die Echtheitsbestätigung über die Vertrauenskette weiterreicht.

```
pub   1024D/28988BF5 2000-02-27
      Key fingerprint = B117 2656 DFF9 83C3 042B  C699 EB5A 896A 2898 8BF5
uid                  Roger Dingledine <arma@mit.edu>
```

Tor Integrität prüfen

Anschließend die zugehörige veröffentlichte Signatur zur heruntergeladenen Torversion herunterladen und am besten im selben Verzeichnis ablegen. Mit GnuPG die Signatur prüfen. Solange die Schlüssel nicht als vertrauenswürdig eingestuft sind, wird bei der Prüfung eine Fehlermeldung ausgegeben.



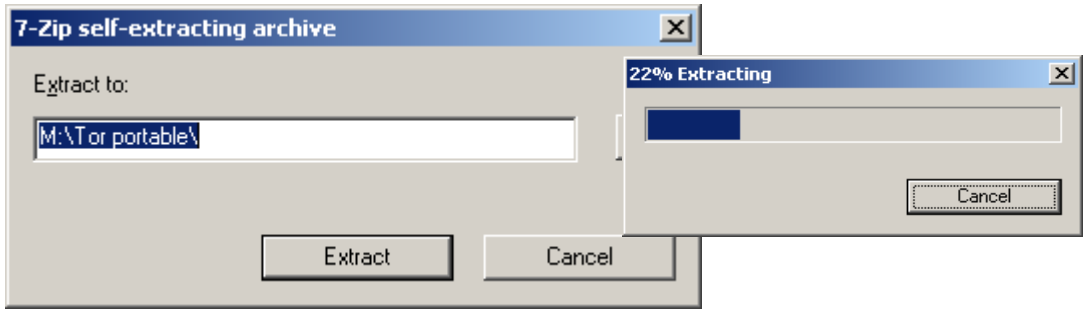
Tor installieren

Installation der Portable Version:

- Download und speichern auf ein Unterverzeichnis im Zielstick:

  http://www.torproject.org/torbrowser/dist/tor-im-browser-1.2.9_de.exe

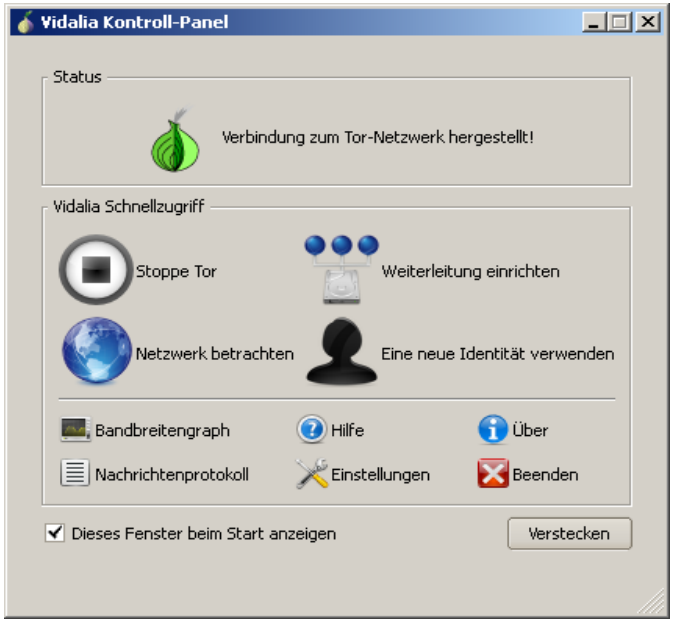
- Entpacken

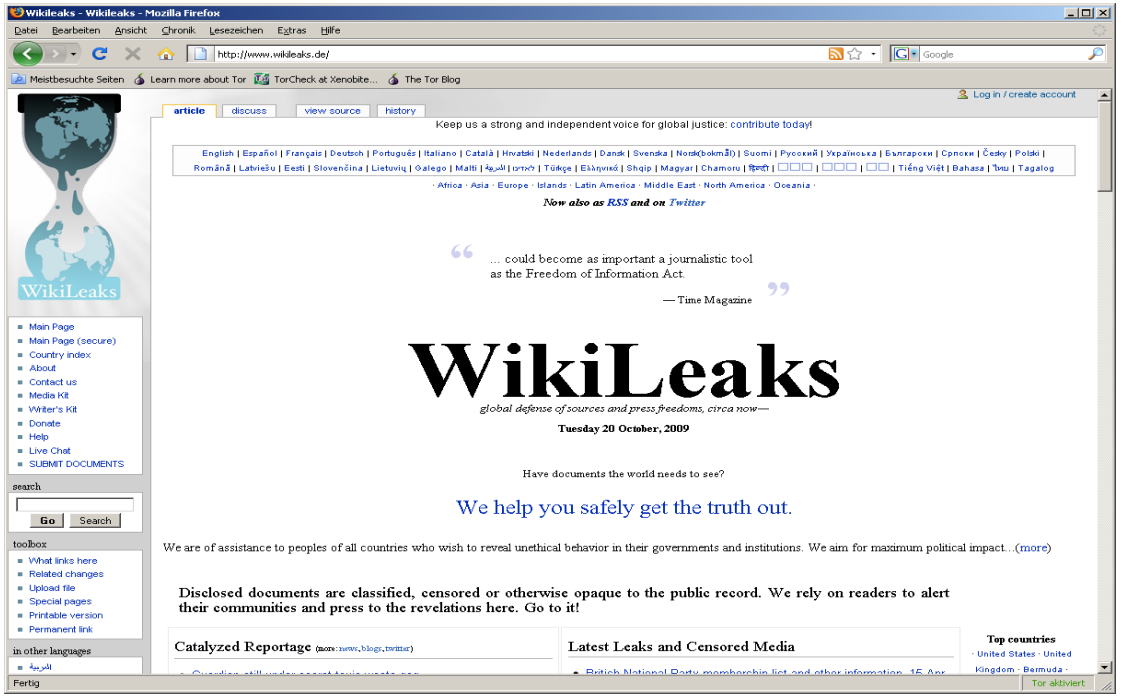


- Start Tor Browser.exe ausführen, fertig.

Tor installieren

Es erscheint das Vidalia Control Panel, mit dem grundlegende Einstellungen getroffen und die aktuelle Session beobachtet werden können:



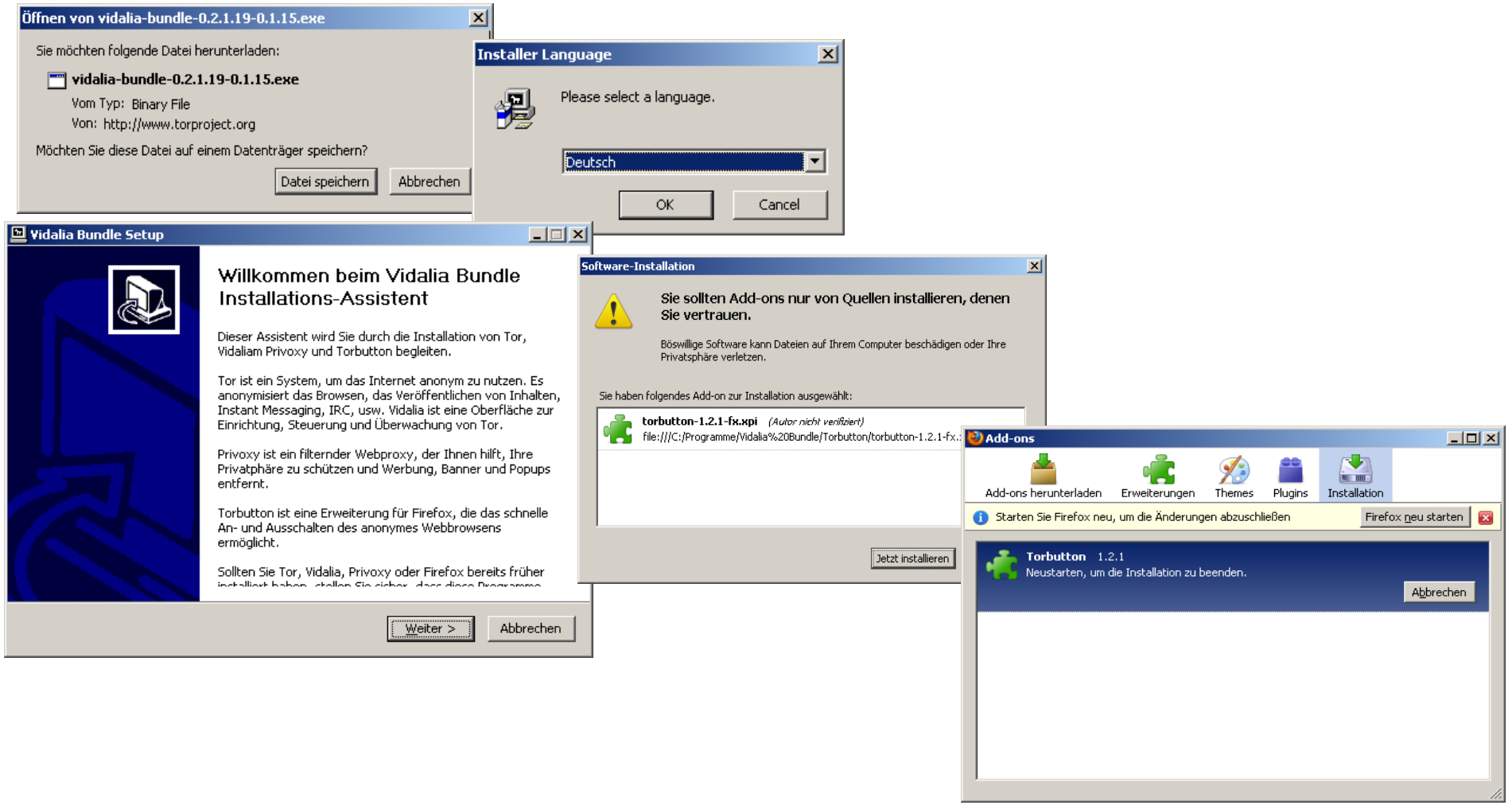


...dann wird der Firefox gestartet, rechts unten ist der Status zu sehen

Tor mobil nutzen

Tor auf eigenem Rechner installieren

Download von http://www.torproject.org/easy-download.html.de

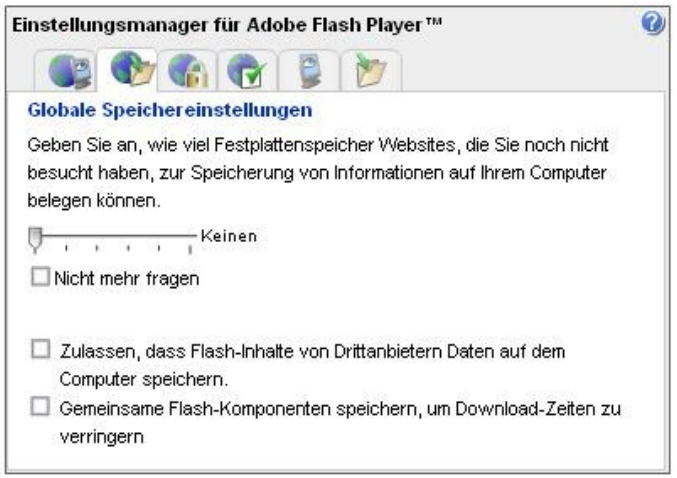


Browser sichern

Um Tor sicher betreiben zu können, müssen im Browser einige Sicherheitseinstellungen geändert werden. Der Internetverlauf (Referrer) und gespeicherte Cookies sollten vor der Nutzung entfernt werden.
Eine besondere Unart sind die sogenannten Flashcookies, die nicht im Browser direkt entfernt werden können. Man sollte die bereits gespeicherten aus deren Verzeichnis vor der Nutzung von Tor löschen:
XP: c:\Dokumente und Einstellungen\<aktueller Benutzer>\Anwendungsdaten\Macromedia\Flash Player\#SharedObjects (<aktueller Benutzer> ersetzen durch den eigenen Benutzer Namen, mit dem man sich am System anmeldet)

Vista: c:\Users\<aktueller Benutzer>\AppData\Roaming\Macromedia\Flash Player\#SharedObjects

Die Wiedereinnistung kann man über globale Einstellungen im Flash Player Manager verhindern:
http://www.macromedia.com/support/documentation/de/flashplayer/help/settings_manager.html

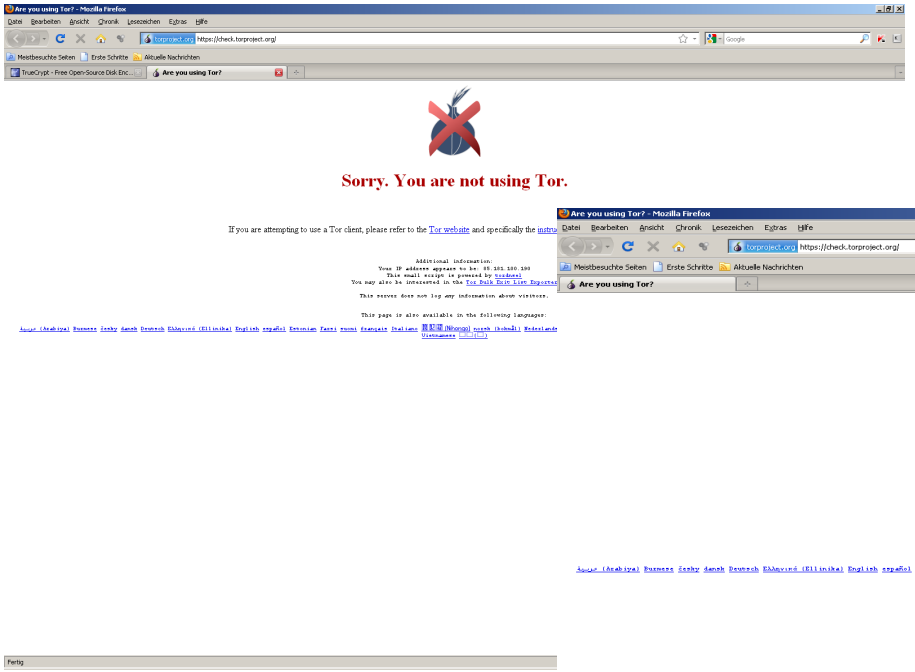


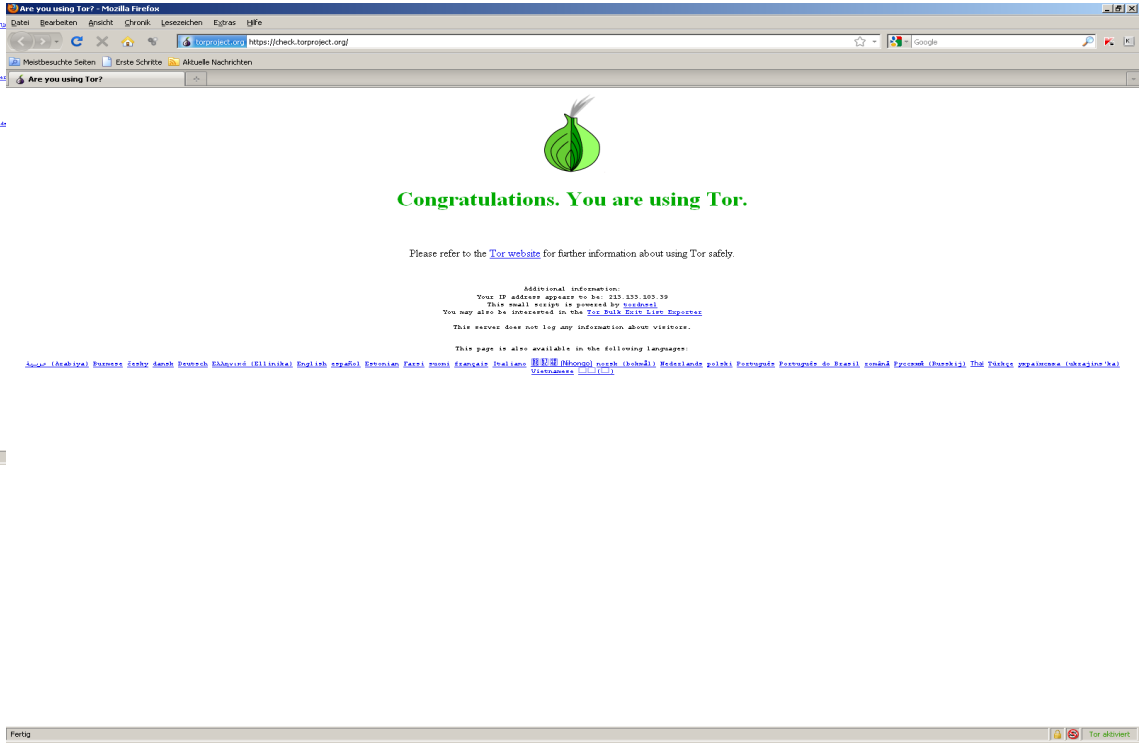
Auf der sicheren Seite ist man, wenn man bei der Nutzung von Tor einen separaten Firefox verwendet !

Eine Online-Checkseite verrät, ob bei der Installation und Konfiguration alles geklappt hat:
https://check.torproject.org/

Browser sichern

Eine Online-Checkseite verrät, ob bei der Installation und Konfiguration alles geklappt hat:
https://check.torproject.org/





Installation unter Ubuntu

Die portable Installation auf einem USB Stick für UNIXE ist hier beschrieben:
https://wiki.torproject.org/noreply/TheOnionRouter/TorUsb

Installation unter Ubuntu und anderen Debian-Systemen:
https://www.torproject.org/docs/debian

Rechtliche Aspekte der Tornutzung

Disclaimer: Wir sind keine Juristen. Dies ist keine Rechtsberatung, sondern lediglich allgemeine Hinweise!

Nutzung von Tor zum anonymen Surfen
In Deutschland ist die Nutzung zur Zeit legal (natürlich nur solange man die Anonymität nicht für die Vorbereitung oder Ausführung von Straftaten nutzt). In anderen Ländern kann die Nutzung aber strafbar sein, ebenso der Besitz oder die Verbreitung des Programms, also vorher informieren.

Betreiben eines Tor-Servers
Der letzte Tor-Server (Exit Node) in der Kette des Tor-Netzwerks kommuniziert in Klartext mit dem Zielserver. Dessen IP Adresse wird z.B. bei Ermittlungen von Strafverfolgern aus Logfiles extrahiert. Dadurch kann man ins Visier der Strafverfolgung gelangen. Man betreibt damit einen Webservice, der einen nach deutscher Rechtslage für darüber abgewickelte strafrechtliche Inhalte mit verantwortlich macht, wenn man davon Kenntnis erhält und nicht unverzüglich dagegen reagiert.
(Das gleiche Problem trifft übrigens auch Betreiber eines Web 2.0 Forums, etwa wenn sich dort jemand beleidigend äußert...)
Die Strafermittler können mit Log-Daten eines Tor-Servers in der Regel wenig anfangen, da Tor absichtlich Datenpakete einzelner User vermischt, um eine Rückverfolgung zu erschweren. Die Kripo ist übrigens, außer es ist Gefahr im Verzug nicht zugriffsberechtigt, nur die Staatsanwaltschaft.

Agenda

1. Begrüßung und Vorstellung
2. Einleitung – Kurzvorstellung der Tools
3. GnuPG
4. TRUECRYPT
5. Tor
6. **Zusammenwirken der Tools**
7. Fragen und Diskussion

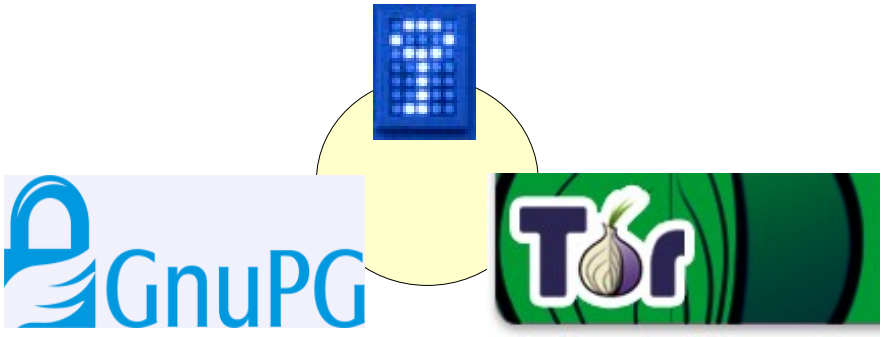
Zusammenwirken der Tools

Die drei vorgestellten Tools sind, obwohl sie alle Verschlüsselung zum Schutz des informationellen Selbstbestimmungsrechts nutzen, für sehr unterschiedliche Einsatzgebiete vorgesehen. Sie ergänzen und verstärken sich gegenseitig.

• GnuPG schützt die Vertraulichkeit von E-Mail und schützt vor falschen Absendern oder Manipulation von Inhalten. Seine Signaturen werden aber auch verwendet, um die Originalität, Echtheit und Unverfälschtheit der im Internet veröffentlichten Quellcodes und Binaries von TrueCrypt und Tor zu sichern.

• Mit TrueCrypt kann ein Anwender auf Reisen seine mitgeführten oder unterwegs empfangenen Daten verschlüsseln oder sogar verstecken, einschließlich des wertvollen privaten GnuPG Schlüssels oder der in unfreien Gesellschaften teilweise verbotenen, immer aber unerwünschten Privacy Tools TOR und GnuPG.

• Tor hilft, sich beliebige Informationen anonym aus dem Internet zu besorgen, auch Anleitungen und Hilfestellungen zur Nutzung der Privacy Tools. Durch Umgehen von Zensurfiltern gelangen diese Informationen und die Tools selber auch zu Benutzern, die sich durch deren Beschaffung erheblichen Risiken aussetzen, sofern sie trotz Zensur überhaupt an die Tools gelangen.



FRAGEN???