Datensicherung in der anwaltlichen Praxis

Rechtsanwalt
Dr. Alexander Koch

Koch & **Neumann**
RECHTSANWÄLTE

Gang des Vortrags

- Einführung in die Datenverschlüsselung.
- Schutz mobiler Geräte (Handys, Tablets, USB-Sticks, Laptops).
- E-Mail:
  - Transportverschlüsselung.
  - Verschlüsselung von Inhalten.
- Datensicherheit.

Einführung in die Datenverschlüsselung

Siegener Anwaltverein, 28. November 2014

Koch & Neumann
RECHTSANWÄLTE

Warum verschlüsseln?

- Schutz gegenüber neugierigen Kollegen/Familienangehörigen.
- § 43a Abs. 2 BRAO verpflichtet uns zur Verschwiegenheit.
  - Erfasst wird auch die fahrlässige Preisgabe — etwa durch verlorene USB-Sticks, Laptops oder fehlgeleitete E-Mails.
- Schutz von Mandantengeheimnissen gegenüber staatlichen Stellen.
  - Es sind schon Kanzleiräume durchsucht worden, um ***entlastendes*** Material in ***Beleidigungs***verfahren ***zugunsten*** des beschuldigten Anwalts zu finden.
    (BVerfG, Beschl. v. 5.5.2008 - Az. 2 BvR 1801/06.)
- NSA, BND & Co.

Im Alltag gehen die größten Gefahren nicht von mächtigen Geheimdiensten aus …

… praktisch relevanter ist der verlorene USB-Stick oder Laptop mit Mandantendaten!

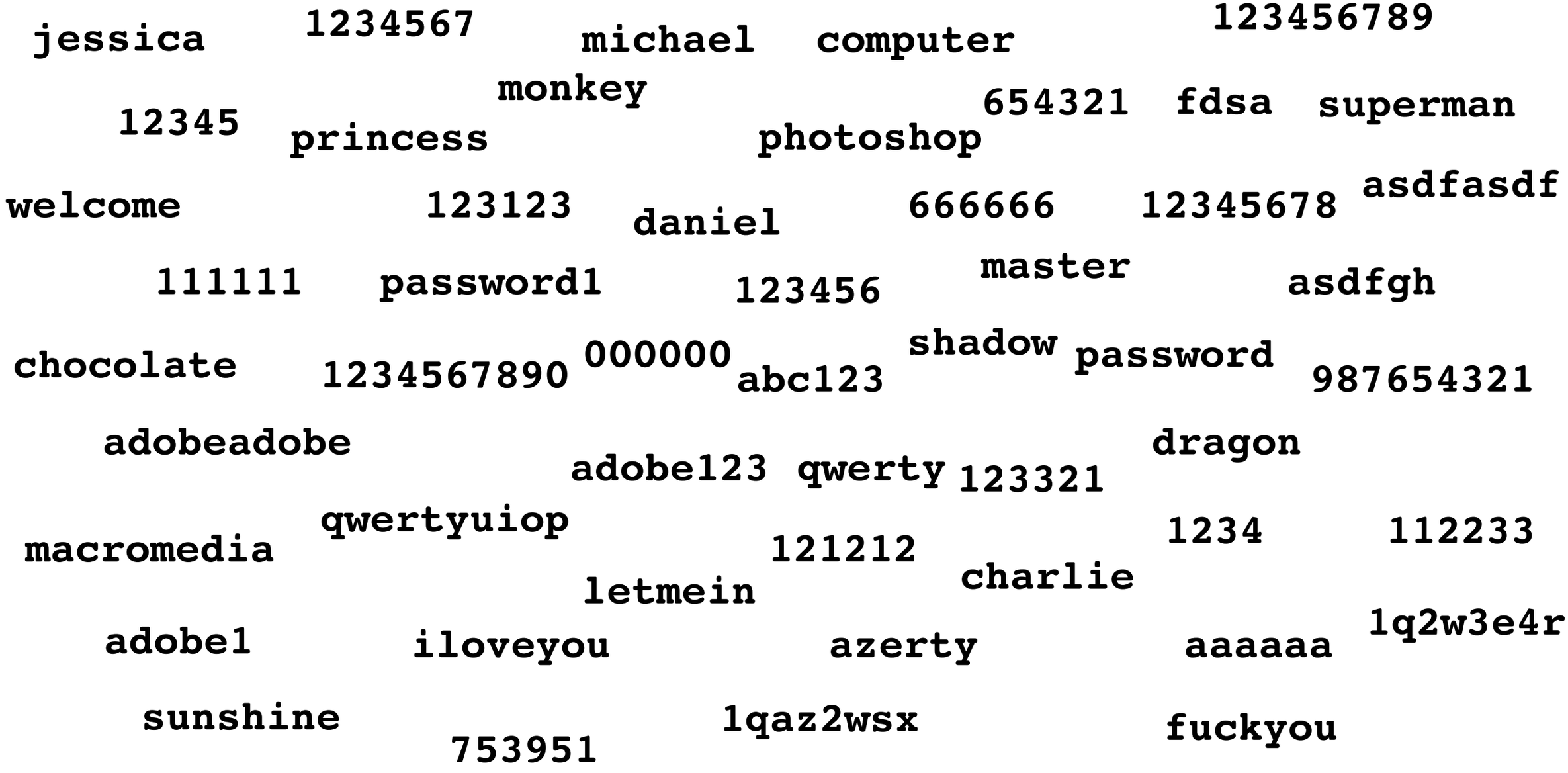
Risiken

- Daten sind bei Verlust des Kennworts/Schlüssels verloren.
- Verschlüsselung erschwert ggf. das Rekonstruieren von Daten.
- … solange die meisten E-Mails unverschlüsselt sind, fallen verschlüsselte E-Mails auf …
  - … was zu einer genaueren Analyse der Metadaten (also: Wer kommuniziert wann mit wem?) führen kann …

Schlussfolgerungen

- Alle Medien, die man verlieren kann (USB-Sticks, Handys, Laptops etc.), grundsätzlich verschlüsseln.
- Daten im Internet, wenn möglich, verschlüsseln.
- Backups nur verschlüsseln, wenn notwendig.
- Passwörter an einem sicheren Ort hinterlegen – soweit vertretbar.
  - (Die beste Verschlüsselung bringt nichts, wenn die StA den Zettel mit den Passwörtern auch beschlagnahmt ...)

Top-51-Passwörter des 2013er-Adobe-Hacks



Wörterbuchangriffe

- Programme sind im Internet frei verfügbar (und Bestandteil jeder vernünftigen Linux-CD).
- Wortlisten für sämtliche Sprachen, Namen u. Orte (auch aus Romanen) sind ebenfalls frei verfügbar.
  - „John the Ripper“ bringt Wortlisten für 20 Sprachen mit 4 Millionen Einträgen mit,
  - eine Wortliste mit praktisch allen Sprachen und 40 Millionen Einträgen kostet 27,95 $.
- Ein Angriff ist mit handelsüblichen PCs in Sekunden oder Minuten möglich.

Brute-Force-Angriffe

- Es werden sämtliche Zeichenkombinationen durchprobiert.
- Sicherheit hängt somit allein von der Qualität des Passwortes ab.
  - 5 Zeichen Kleinschreibung → $26^5 = 11.881.376$.
  - BSI-Empfehlung: 12 Zeichen Groß-, Kleinschreibung, Zahlen und Sonderzeichen → $96^{12} =$ 612.709.757.329.767.363.772.416 (entspricht in etwa der Zahl der Sandkörner auf der Erde).

Passwörter

- Schlechte Passwörter:
  - Passwort, qwertz, Susanne, Harry Potter — aber auch wz>59C.
- Gute Passwörter:
  - %34Pb+m8M*x0<h, !Ui9x"X?Is:+PX
  - Ega1eT,l&gmP7e.Dbm71M0mM.

Merkbare und sichere Passwörter

Es gibt allerdings einen einfachen Trick, lange und gut merkbare Passwörter zu erstellen. Dazu bildet man zunächst einen Merksatz oder mehrere Merksätze.

Merkbare und sichere Passwörter

E**s **g**ibt **a**llerdings **e**inen **e**infachen **T**rick**, l**ange **u**nd **g**ut **m**erkbare **P**asswörter **z**u **e**rstellen**. D**azu **b**ildet **m**an **z**unächst **e**inen **M**erksatz **o**der **m**ehrere **M**erksätze**.

EgaeeT,lugmPze.DbmzeMomM.

E**s **g**ibt **a**llerdings **einen e**infachen **T**rick**, l**ange **und g**ut **m**erkbare **P**asswörter **zu e**rstellen**. D**azu **b**ildet **m**an **z**unächst **einen M**erksatz **o**der **m**ehrere **M**erksätze**.

Ega*1*eT,l*&*gmP*7*e.Dbm*71*M*0*mM.

Zugangsschutz ./. Verschlüsselung

- Zugangsschutz:
  - Nur der Zugang zum Gerät ist gesperrt.
  - Wer die Festplatte (oder den Speicher im Handy) ausbaut, hat Zugriff auf die Daten.
- Verschlüsselung:
  - Alle Daten sind verschlüsselt.
  - Wer Zugang zur Festplatte (oder den Speicher im Handy) hat, sieht nur Zeichensalat.

Schutz mobiler Geräte

Siegener Anwaltverein, 28. November 2014

Koch & Neumann
RECHTSANWÄLTE

iPhone/iPad

- Die Geräte sind von Hause aus vollverschlüsselt.
- Einfacher Code und „Code anfordern“: „Sofort“ oder langes PWD und „Code anfordern“: „Nach 1 Stunde“.
  - Einstellungen → (Touch ID &) Code → Code anfordern / Einfacher Code
- Daten löschen nach zehn Anmeldeversuchen aktivieren.
  - Einstellungen → (Touch ID &) Code → Daten löschen
- Fernlöschen aktivieren.
  - Einstellungen → iCloud → Mein iPhone suchen → Ein → Mein iPhone suchen / Letzten Standort senden.
  - Zugriff über <https://icloud.com>.

Android

- Die (meisten) älteren Geräte sind nicht vollverschlüsselt.
  - Verschlüsselung kann teilweise manuell eingerichtet werden, das ist im Alltag aber äußerst hinderlich …
- Seit Android 5 (Lollipop) ist eine Vollverschlüsselung Standard.
  - Bei einem Update muss sie allerdings über Einstellungen → Sicherheit → Verschlüsselung manuell aktiviert werden.
- Fernlöschen aktivieren.
  - Google Einstellungen (eigene App, nicht zu zu verwechseln mit Einstellungen) → Android Geräte-Manager → Remote-Ortung für dieses Gerät durchführen / Remote-Sperre und Löschen zulassen.
  - Zugriff über <https://www.google.com/android/devicemanager>.

USB-Sticks/Laptops

- Alle Daten, die man verlieren kann, ~~sollten~~ müssen verschlüsselt sein!
- Also: Keine ungesicherten Daten auf Laptops oder USB-Sticks transportieren!

TrueCrypt

- TrueCrypt kann:
  - Verschlüsselte Container erstellen,
  - Festplatten verschlüsseln,
  - das gesamte System verschlüsseln.
- ***TrueCrypt wird nicht weiterentwickelt.***
- ***Die letzte Version gilt als sicher und kann weiterverwendet werden.***

TrueCrypt-Container

- TrueCrypt-Container lassen sich wie externe Festplatten/USB-Sticks nutzen.
- Container können auch auf USB-Sticks gespeichert werden.
- … selbst ein Abgleich über die DropBox ist möglich.

TrueCrypt-Container erstellen

Create Volume → Create an encrypted file container → Next → Standard TrueCrypt volume → Next → Select file… → Speicherort auswählen und Dateinamen eingeben (.tc als Endung verwenden) → Next → AES und RIPEMD-160 belassen → Next → Größe eingeben, z. B. 150 MB → Next → Passwort zweimal eingeben → Next → Maus über dem Fenster bewegen → Format → Exit.

TrueCrypt-Container nutzen

- Einbinden:
  - Doppelklick auf .tc-Datei (oder Select file → Datei auswählen) → Mount → Passwort eingeben.
  - Container kann wie ein normales Laufwerk genutzt werden.
- Auswerfen:
  - Dismount oder Dismount all.

AES

- Advanced Encryption Standard.
- Wurde in Belgien entwickelt.
- Sehr einfach (500 Zeilen Programmcode).
- Sehr gut erforscht.
- AES-192 und AES-256 sind in den USA für Dokumente mit der höchsten Geheimhaltungsstufe „TOP SECRET“ zugelassen.
- 2^{256}=115.792.089.237.316.195.423.570.985.008.687.907.853. 269.984.665.640.564.039.457.584.007.913.129.639.936 (115 Dodezilliarden)

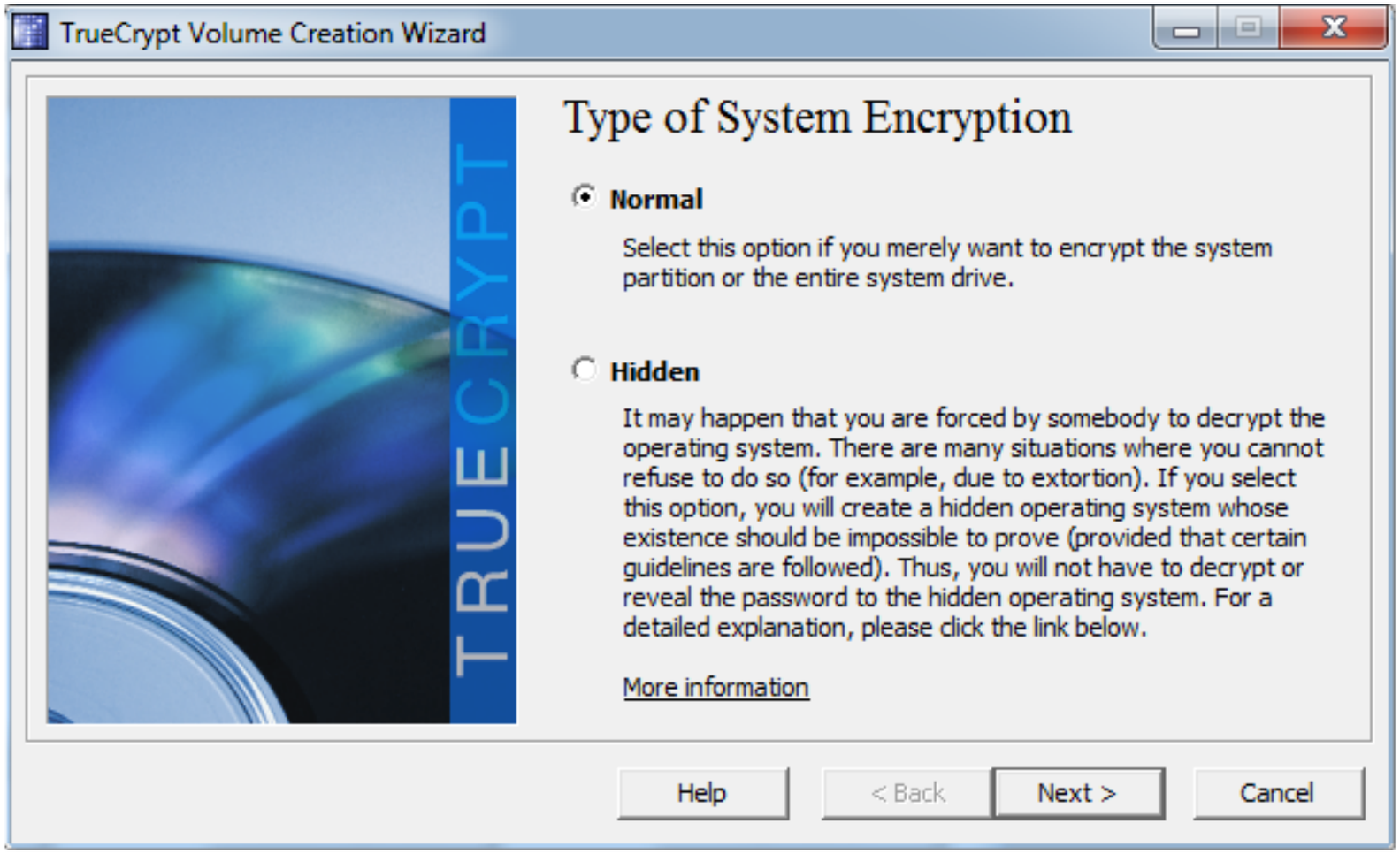
Vollverschlüsselung

- VORHER ein Backup machen!
- ***VORHER ein Backup machen!!***
- ***VORHER ein Backup machen!!!***

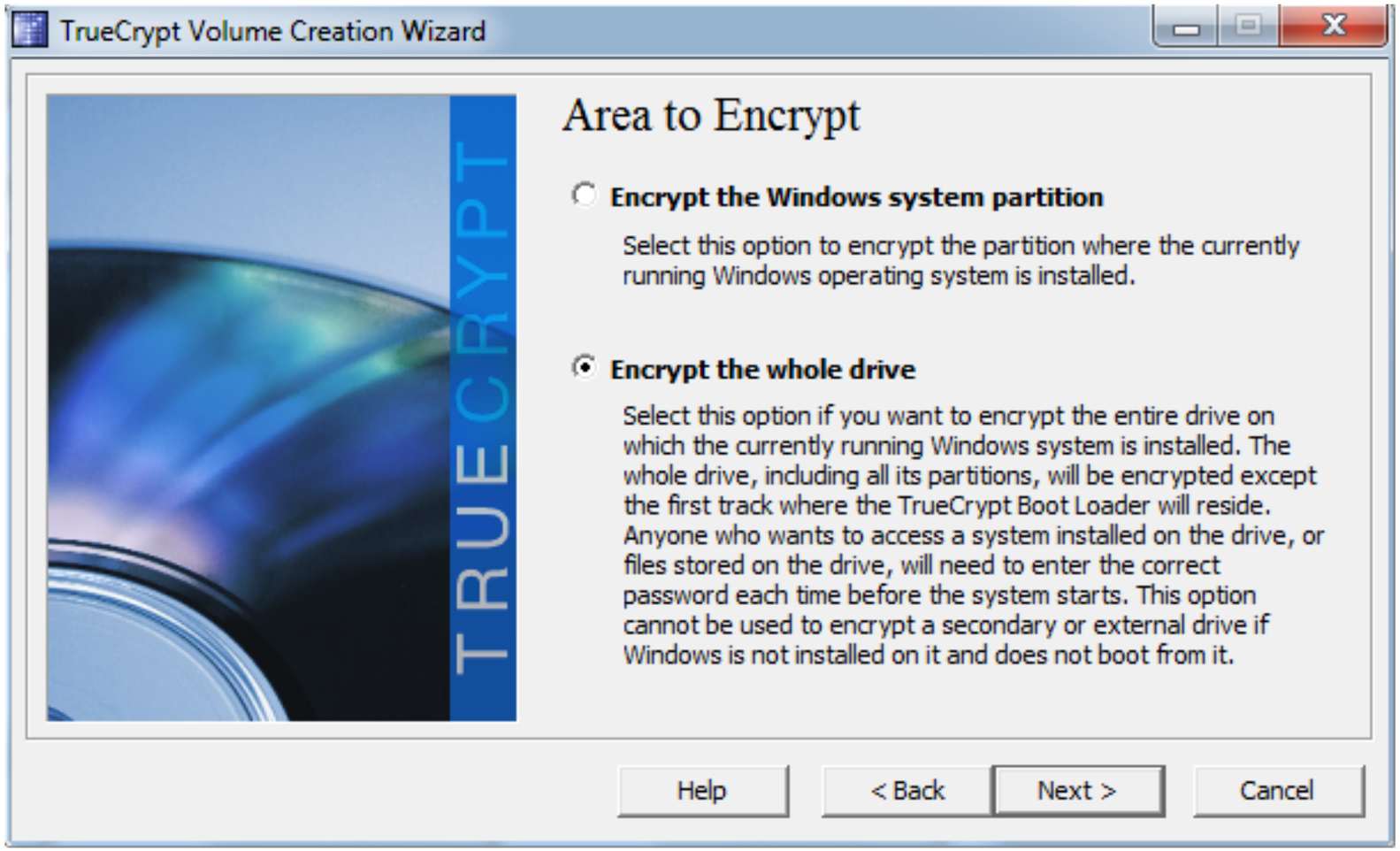
- Das System ist nur gesichert, wenn es ordentlich heruntergefahren wurde.
  - Es gibt Programme für Ermittlungsbehörden, die aus laufenden Systemen das Passwort auslesen können!
- Gegen Diebe und unehrliche Finder sollte auch ein Bildschirmschoner mit Passwortschutz reichen.

Vollverschlüsselung

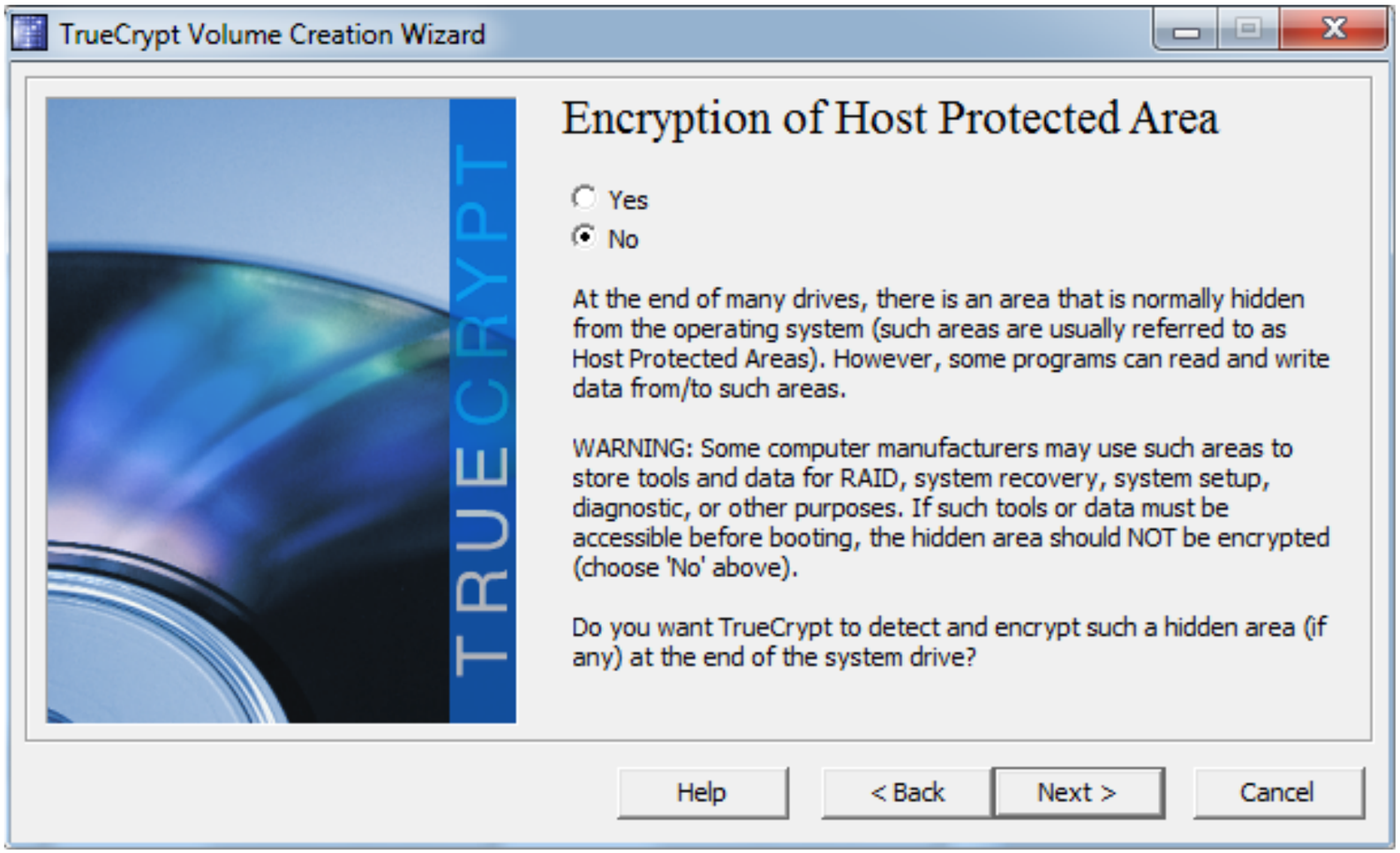
- MacOS: FileVault.
  - Über die Systemeinstellungen (Sicherheit → FileVault) aktivieren und vergessen. (Arbeitet bei mir seit Jahren ohne Probleme!)
- Windows:
  - BitLocker:
    - Setzt Windows 7 Ultimate oder Enterprise, Windows 8 Pro voraus; PC sollte außerdem über ein Trusted Platform Module verfügen.
    - Aktiveren über Systemsteuerung → System → Sicherheit → BitLocker aktivieren.
  - TrueCrypt oder DiskCrypter: Gehen immer ...



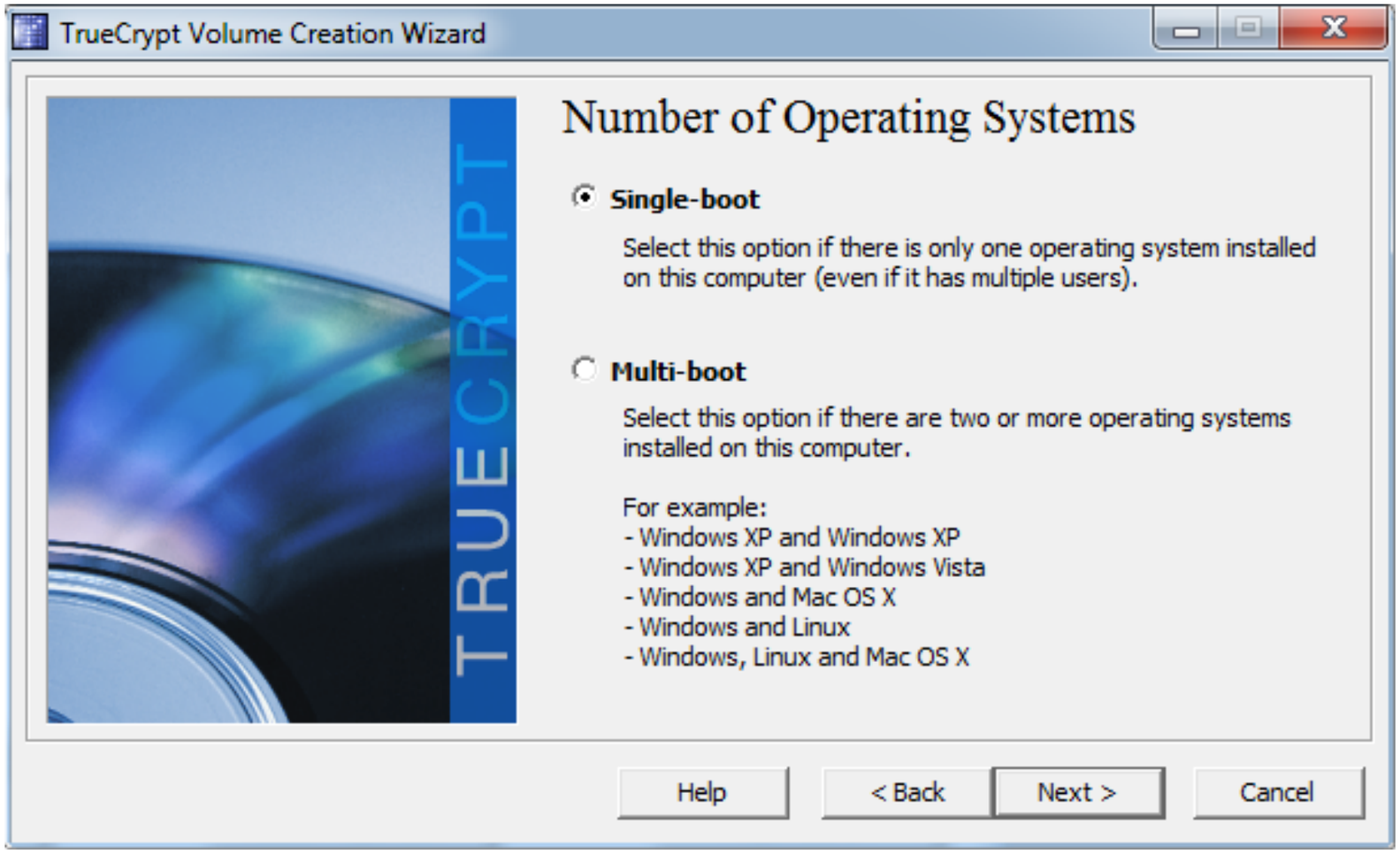
Um die Vollverschlüsselung zu starten, ruft man TrueCrypt auf und wählt im Menü „System“ – „Encrypt System Partition/Drive...“. Es startet dann ein Assistent, der durch die notwendigen Schritte führt.



TrueCrypt kann entweder nur die Windows-Systempartition verschlüsseln oder die gesamte Festplatte. Sinnvoll dürfte es hier sein, die gesamte Festplatte zu verschlüsseln.



TrueCrypt kann außerdem die „Host Protected Area“ der Festplatte verschlüsseln. TrueCrypt empfiehlt, hier „No“ zu wählen, was man im Zweifel befolgen sollte.

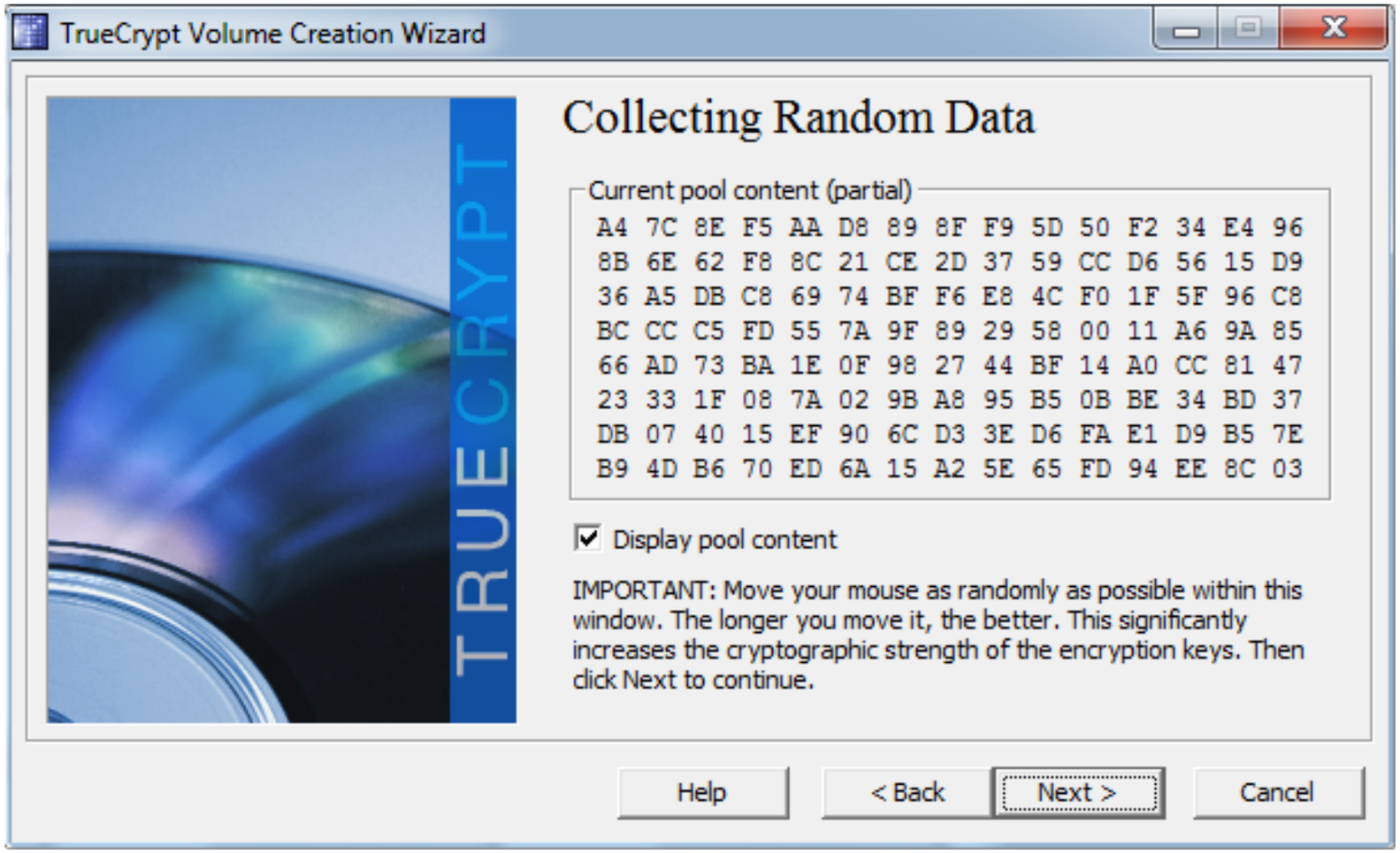


Im nächsten Schritt fragt TrueCrypt, ob neben Windows noch ein weiteres Betriebssystem installiert ist. Hier liegt man im Zweifel mit „Single-boot“ richtig.

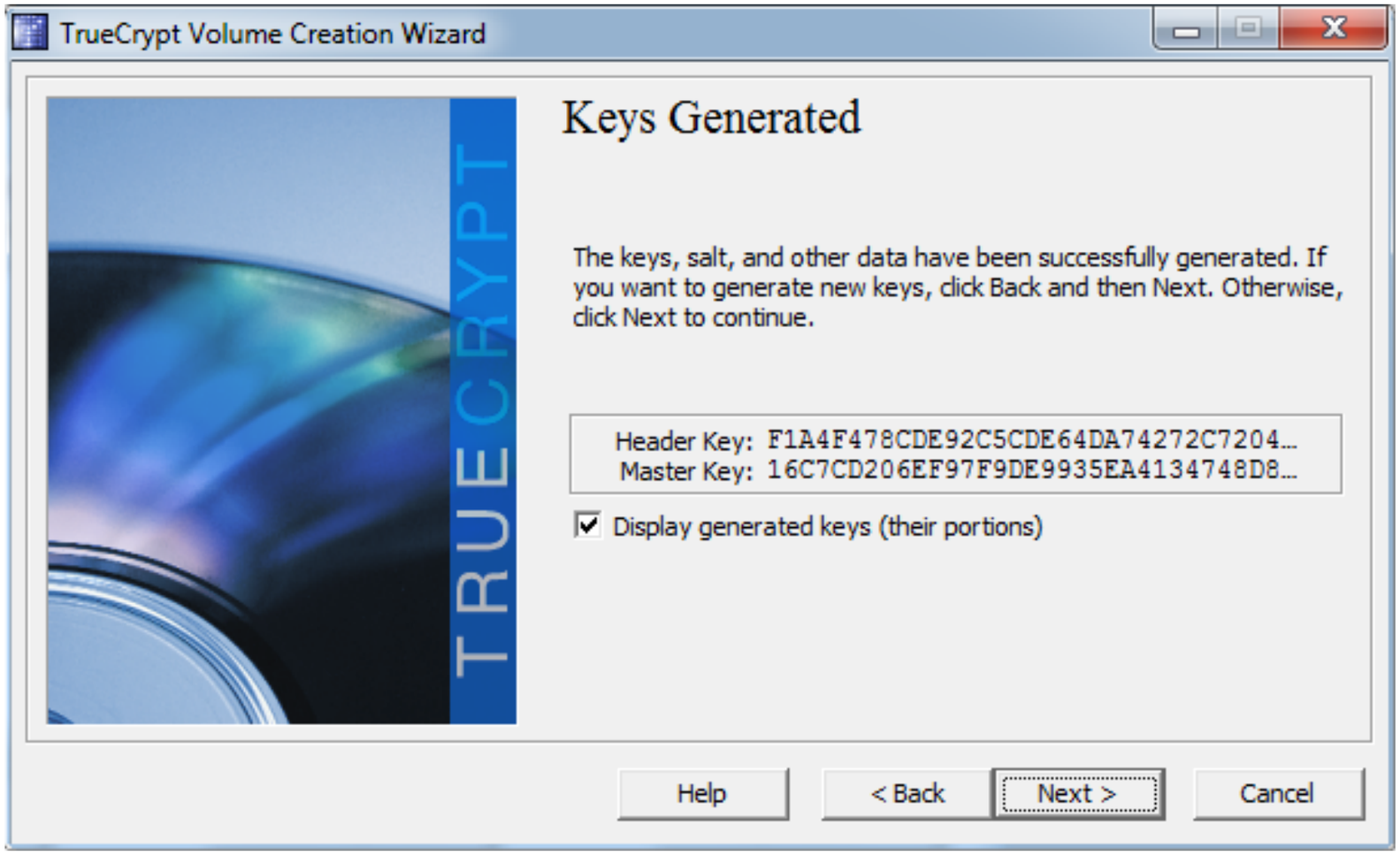
In der nächsten Dialogbox muss man einen Verschlüsselungs-algorithmus und einen Hashalgorithmus auswählen.

AES und RIPEMD-160 können belassen werden.

Nun muss ein Passwort (doppelt) eingegeben werden ...



… und Zufallszahlen müssen erzeugt werden.



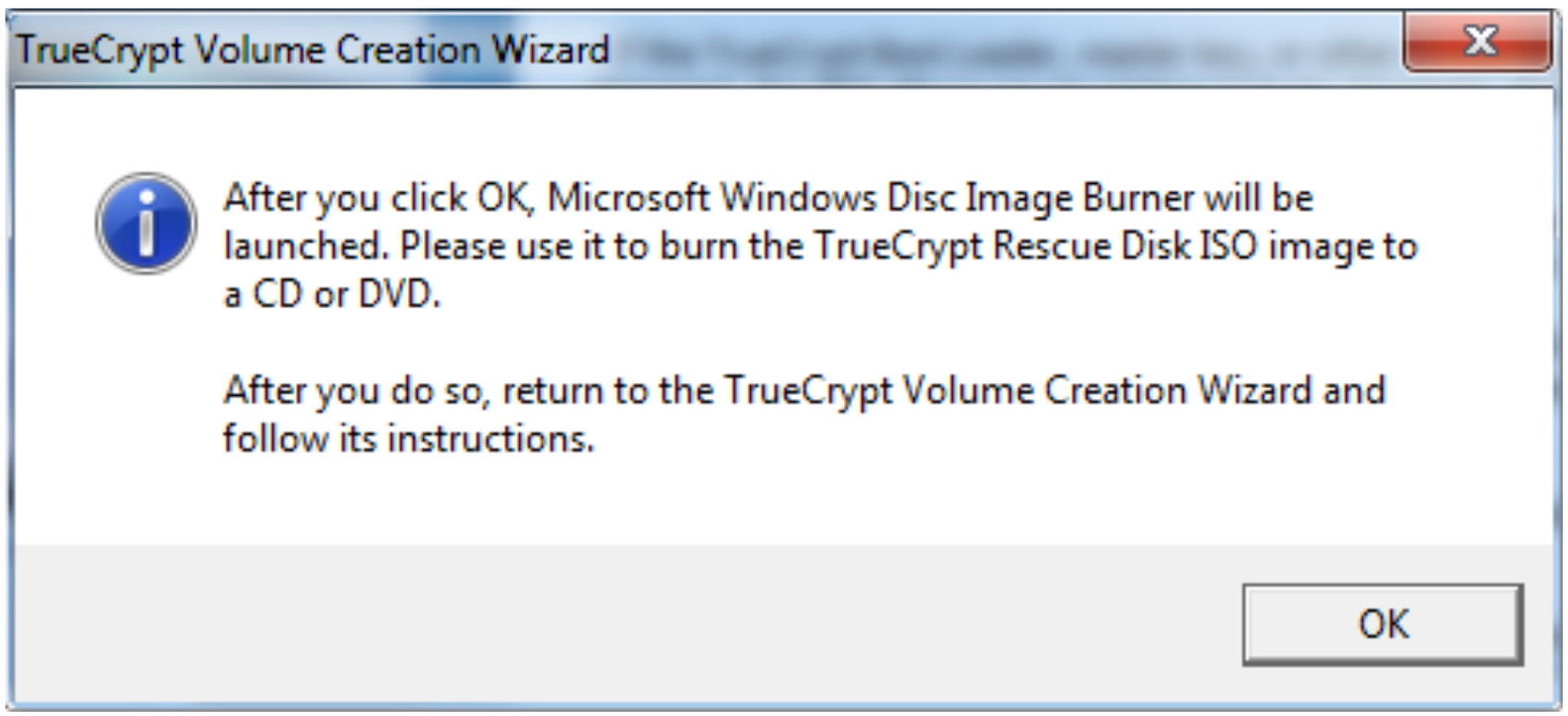
Danach werden die erzeugten Schlüssel angezeigt – man kann hier gleich mit „Next“ weitermachen.

TrueCrypt muss sehr tiefgreifende Veränderungen an der Festplatte vornehmen. Um die Daten später wieder entschlüsseln zu können, müssen bestimmte Bereiche der Festplatte lesbar sein.

Kommt es in diesen Bereichen zu Fehlern, können die restlichen Daten nicht mehr entschlüsselt werden.

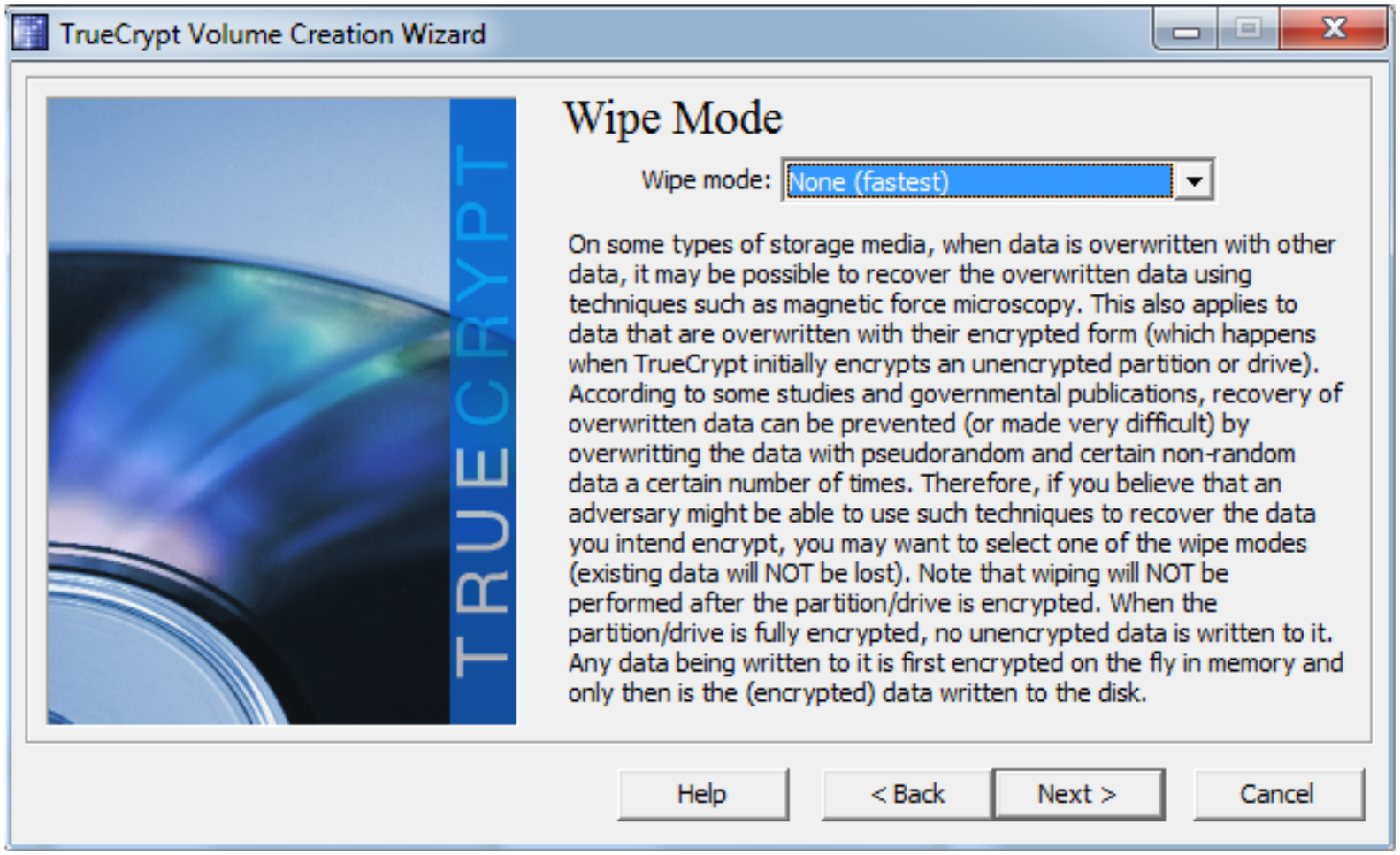
Deshalb bietet TrueCrypt an, ein Backup dieser Daten auf CD/DVD anzufertigen. Die entsprechende CD sollte man sicher aufbewahren.

Dieser Schritt kann – aus sehr guten Gründen – nicht einfach übersprungen werden.



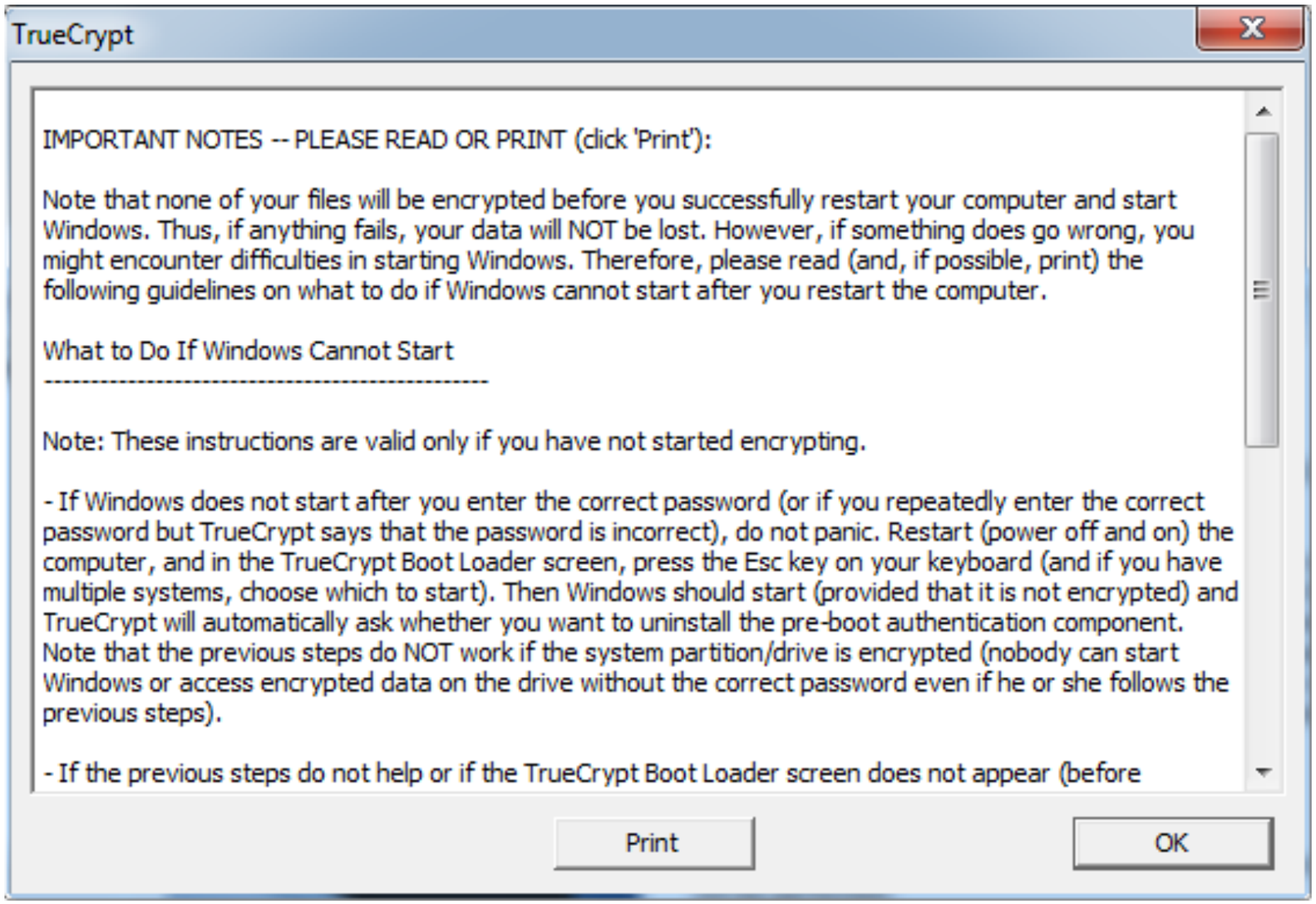
TrueCrypt nutzt nun die Systemfunktion von Windows, um die Sicherheits-CD zu brennen.

Nachdem die Sicherheits-CD erstellt wurde, wird diese von TrueCrypt überprüft.

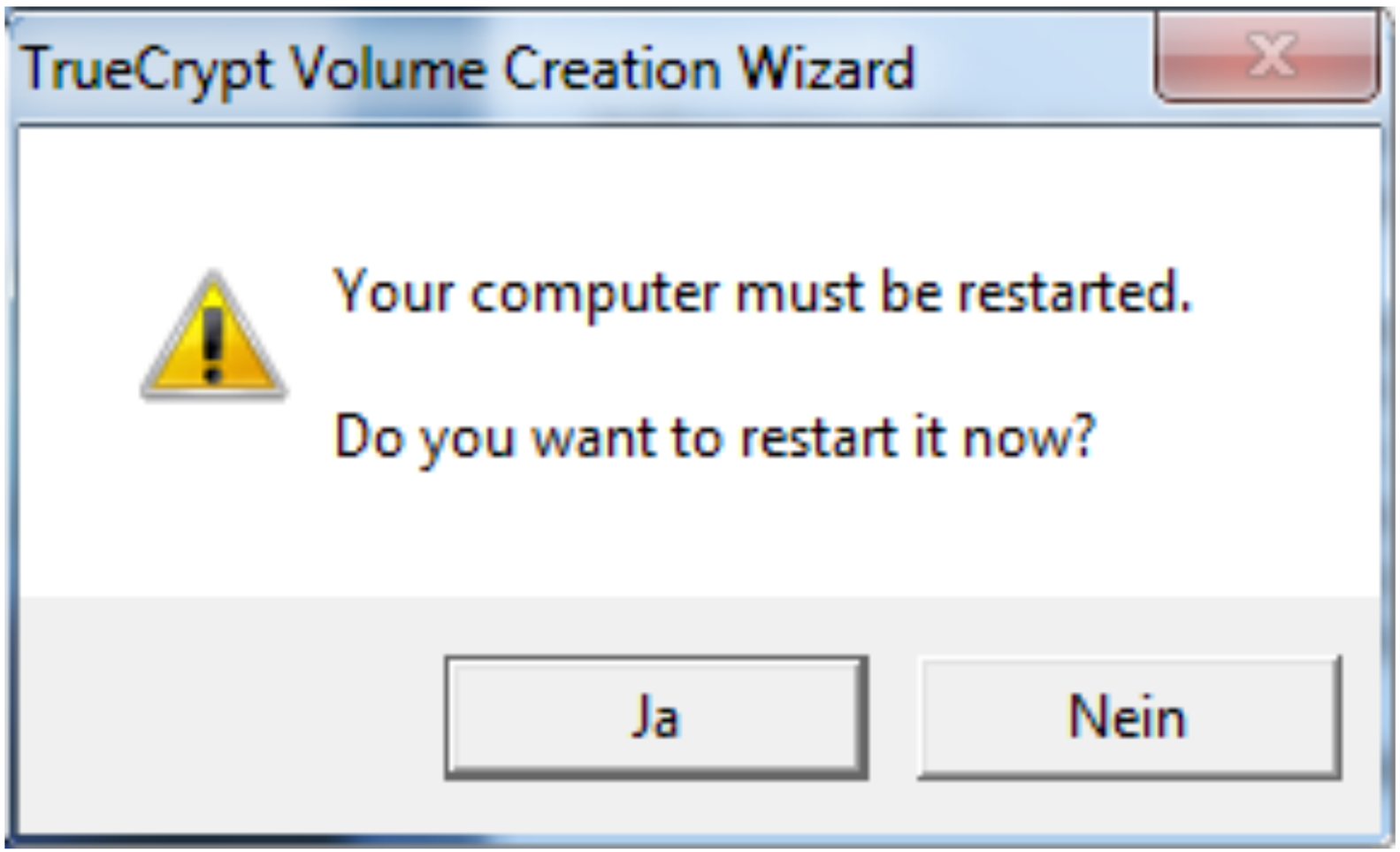


Beim Verschlüsseln wird die bislang unverschlüsselte Festplatte mit den verschlüsselten Daten überschrieben. Theoretisch könnte ein Angreifer versuchen, aus der „Restmagnetisierung“ die überschriebenen (unverschlüsselten) Daten wiederherzustellen. Soll die Verschlüsselung primär als Schutz gegen Diebstahl dienen, kann hier „None fastest“ belassen werden. Wer Sorge hat, dass die fähigsten Geheimdienste alle ihre Ressourcen auf die Entschlüsselung der eigenen Festplatte konzentrieren könnten, sollte hier zu einer paranoideren Einstellung greifen.

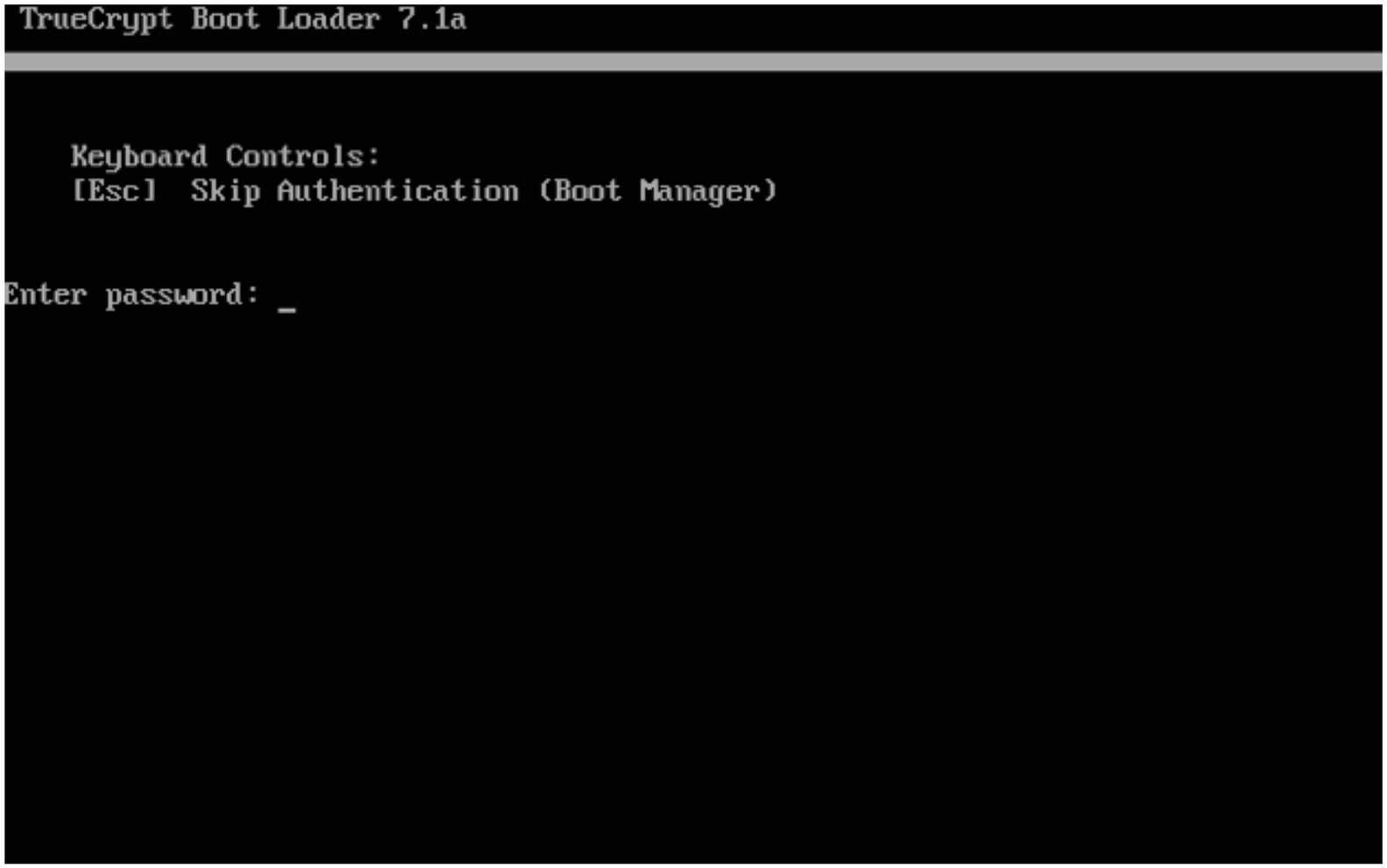
TrueCrypt wird nun einen Test durchführen, bei dem noch keine Daten verschlüsselt werden.



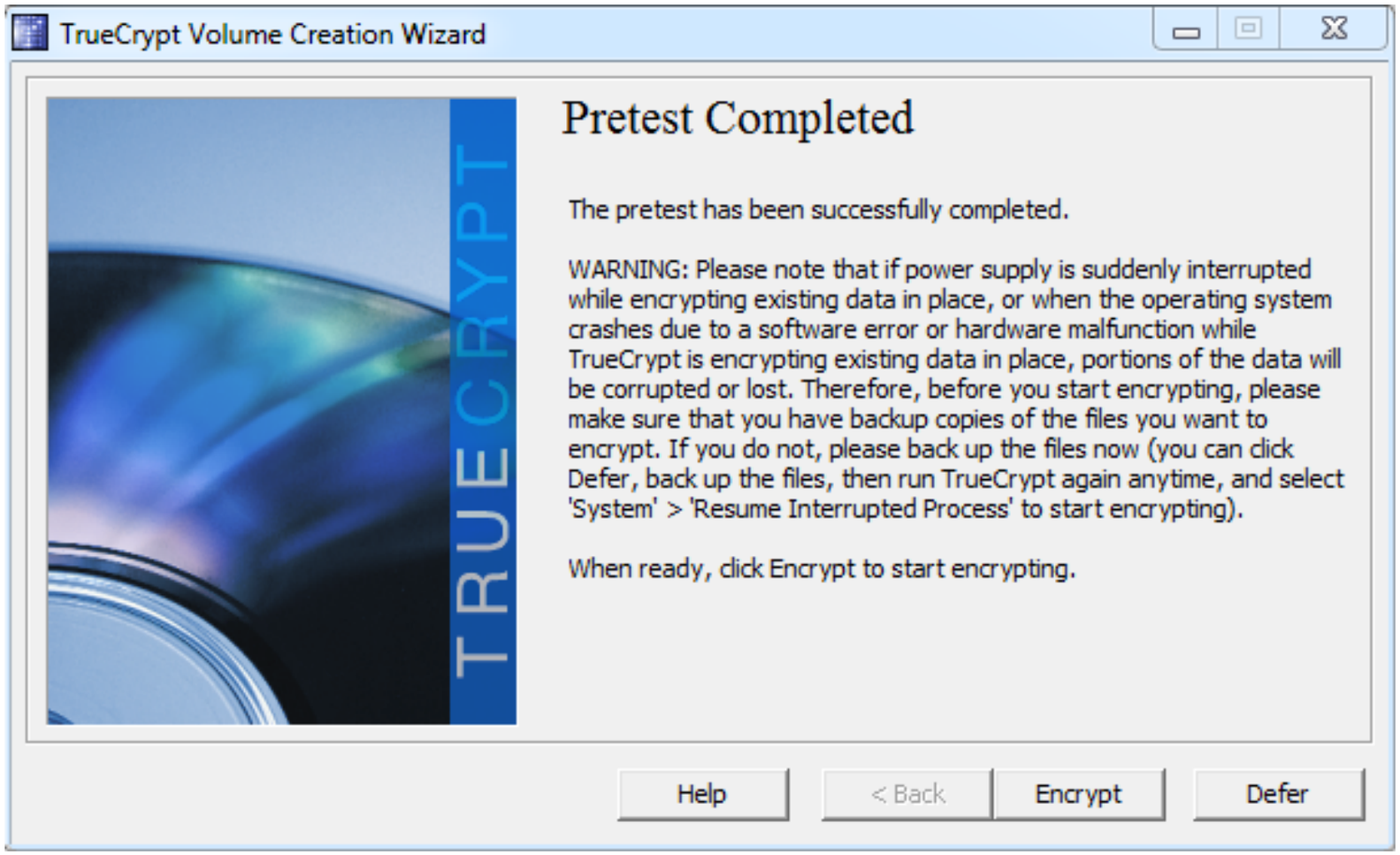
Für den Fall, dass etwas schiefgeht, gibt TrueCrypt vorab noch einige Hinweise, wie man ggf. verfahren kann. Diese Hinweise sollte man sich sinnvollerweise ausdrucken.



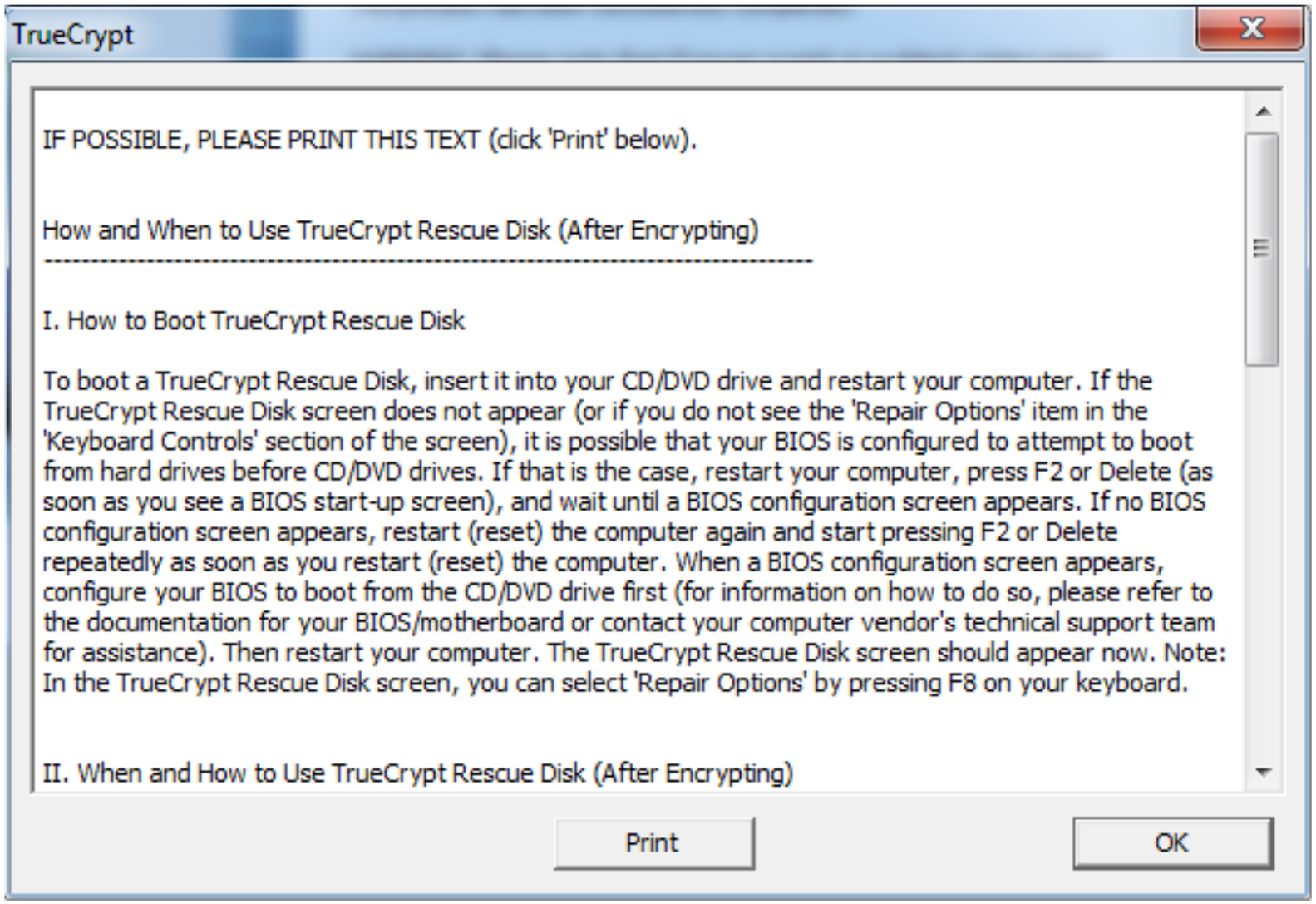
Es folgt eine letzte Abfrage, ob der Computer neu gestartet werden soll.



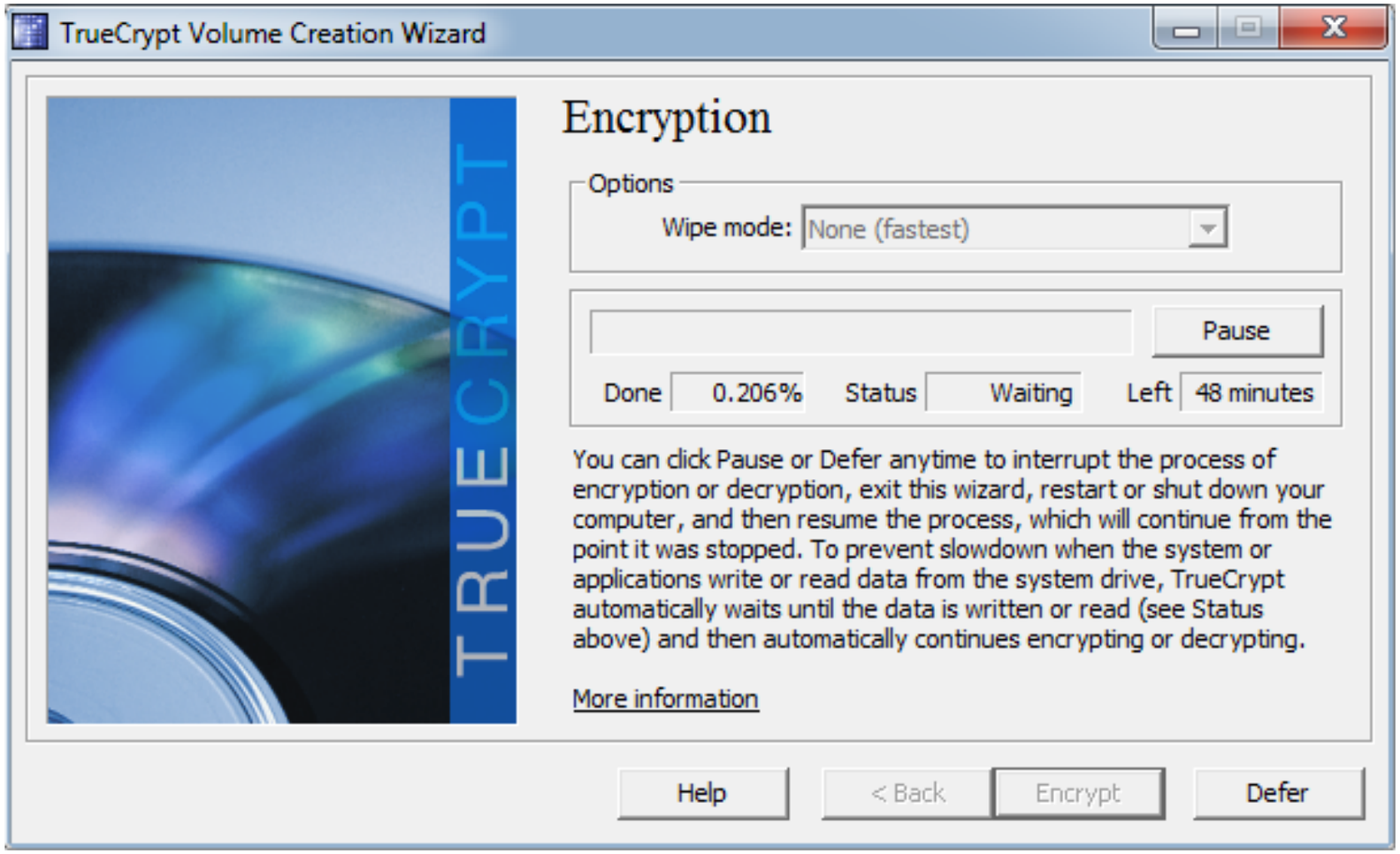
Beim Neustart fragt TrueCrypt nach dem Passwort.



Hat der Test funktioniert, bietet TrueCrypt an, mit der Verschlüsselung zu beginnen.

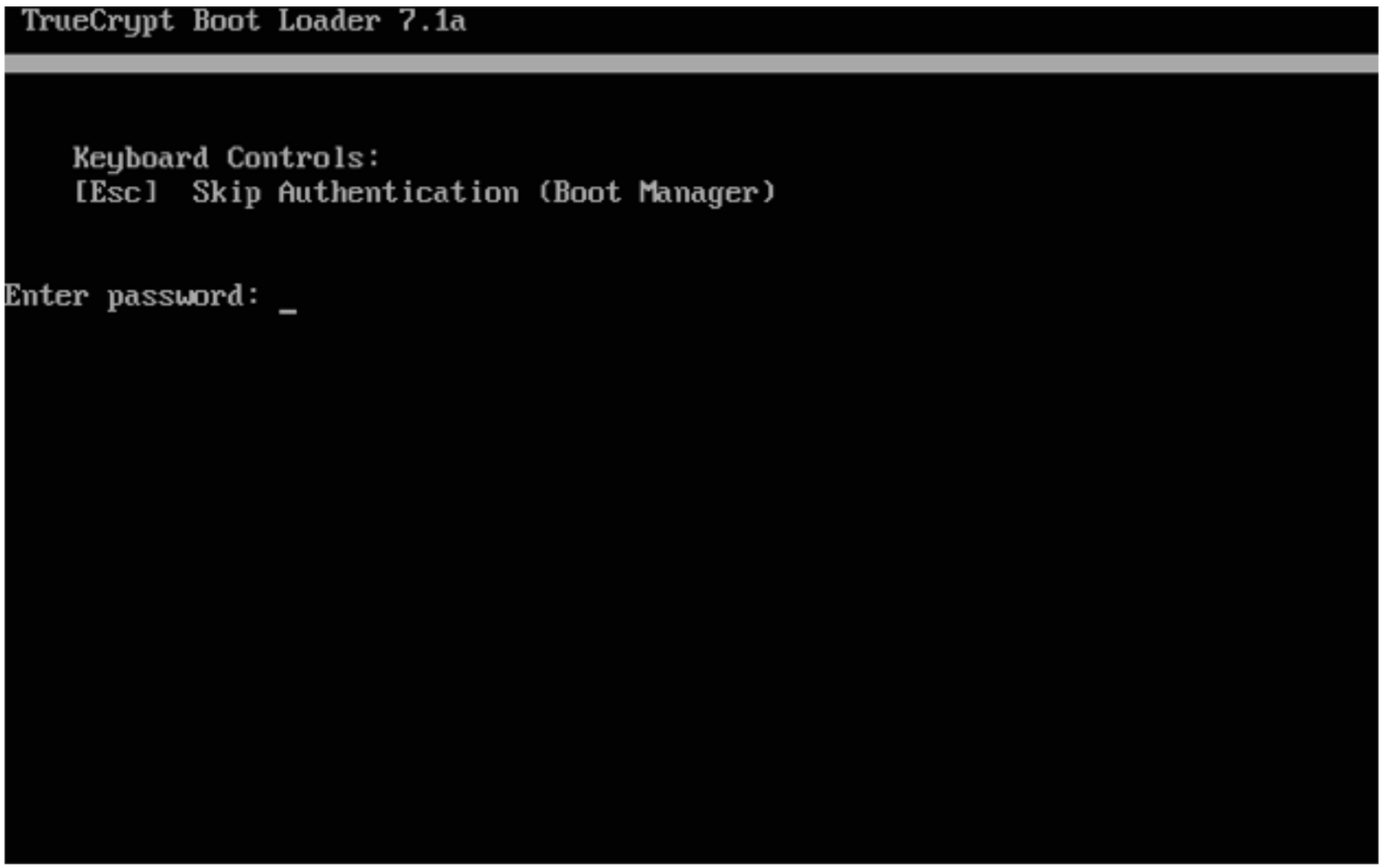


Zuvor gibt es allerdings noch einmal Hinweise, was man unternehmen muss, sollte es zu Schwierigkeiten kommen. Diese sollte man erneut ausdrucken.



Jetzt beginnt die Verschlüsselung. Das wird eine ganze Weile dauern. Während dieser Zeit sollte man den Rechner in Ruhe lassen!

Nachdem die Verschlüsselung durchgelaufen ist ...

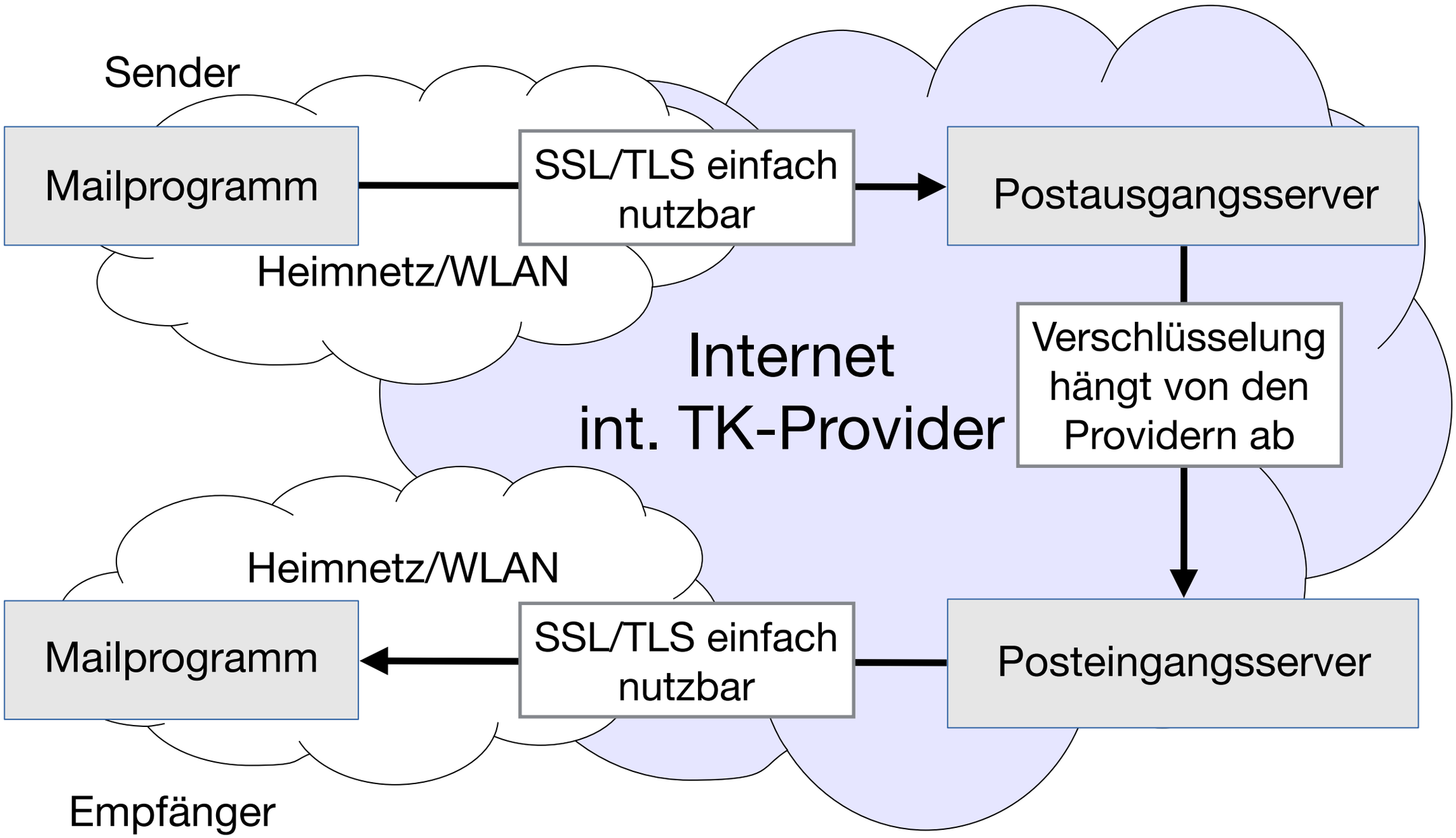


… kann Windows neu gestartet werden. Direkt nach dem Einschalten erscheint nun eine Passwortabfrage, bei der man das TrueCrypt-Passwort eingeben muss.

E-Mail

Koch & Neumann
RECHTSANWÄLTE

E-Mail


Sender
Mailprogramm
SSL/TLS einfach nutzbar
Postausgangsserver
Heimnetz/WLAN
Internet
int. TK-Provider
Verschlüsselung hängt von den Providern ab
Heimnetz/WLAN
Mailprogramm
SSL/TLS einfach nutzbar
Posteingangsserver
Empfänger

E-Mail

- Es kann nur der Weg zum und vom eigenen E-Mailserver kontrolliert werden.
- Es muss davon ausgegangen werden, dass (staatliche) Angreifer Zugriff auf die Metadaten (Sender, Empfänger, Betreff) nehmen können.
- **IMMER, IMMER, IMMER SSL/TLS** verwenden …
  - Muss für Postausgangs- (SMTP) und Posteingangsserver (POP/IMAP) (ggf. separat) eingeschaltet werden.
- … sonst kann jeder im lokalen Netz (dazu zählt auch das WLAN im Hotel/Café) mitlesen!

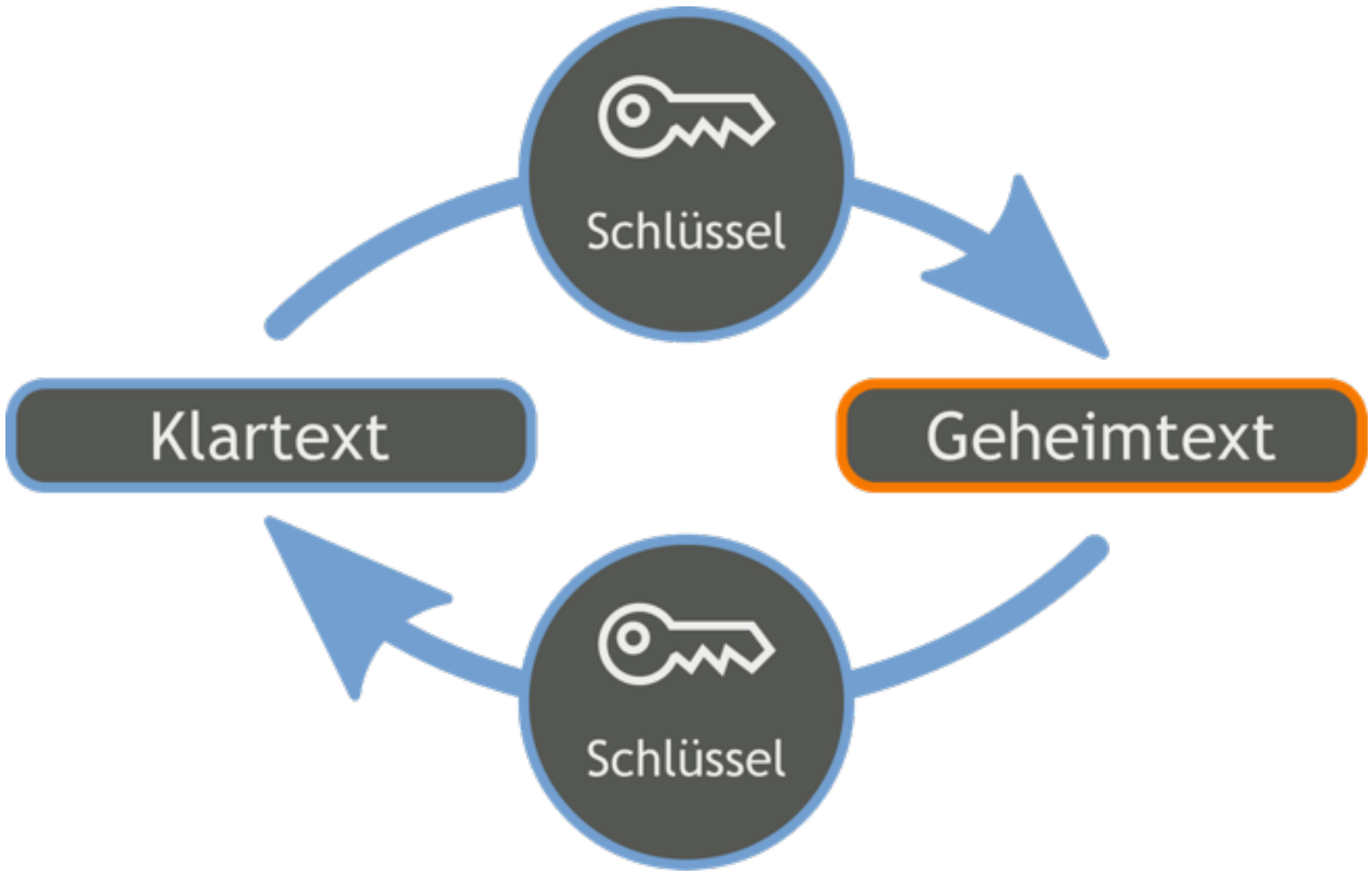
SSL/TLS

- Mail.app:
  - Mail → Einstellungen … → Accounts → Konto auswählen:
    - Eingang: Erweitert.
    - Ausgang: SMTP-Server → Serverliste bearbeiten → Erweitert.
- iPhone/iPad:
  - Einstellungen → Mail, Kontakte, Kalender → Konto auswählen → Account:
    - Eingang: Erweitert.
    - Ausgang: SMTP → Server auswählen.

SSL/TLS

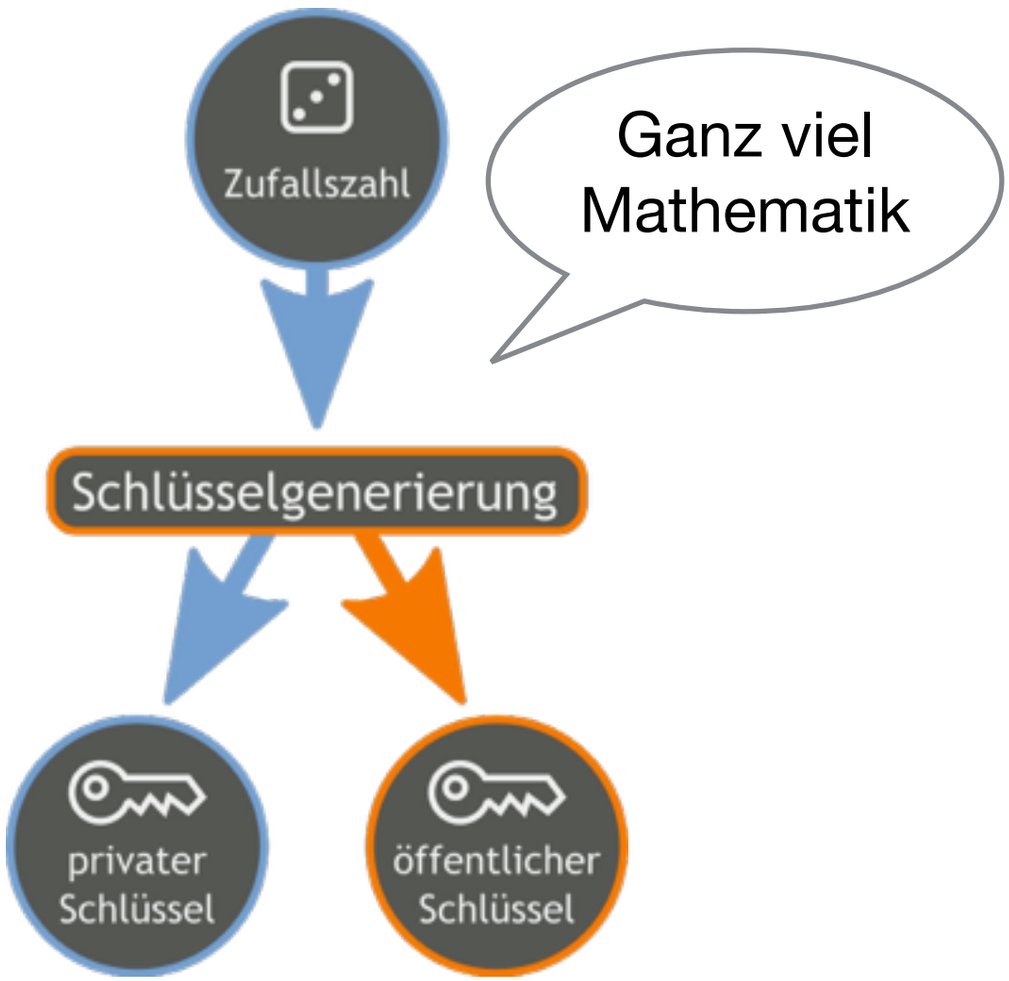
- Outlook:
  - Datei → Informationen → Konto auswählen → Kontoeinstellungen → Kontoeinstellungen → E-Mail → Doppelklick auf Konto → Weitere Einstellungen → Erweitert (für Posteingangsserver und Postausgangsserver jeweils einstellen).
- Thunderbird:
  - Konto auswählen → Konten-Einstellungen bearbeiten:
    - Eingang: Server-Einstellungen.
    - Ausgang: Postausgang-Server (SMTP) → Bearbeiten…

Symmetrische Verschlüsselung



https://de.wikipedia.org/wiki/Datei:Orange_blue_symmetric_cryptography_de.svg

Asymmetrische Verschlüsselung

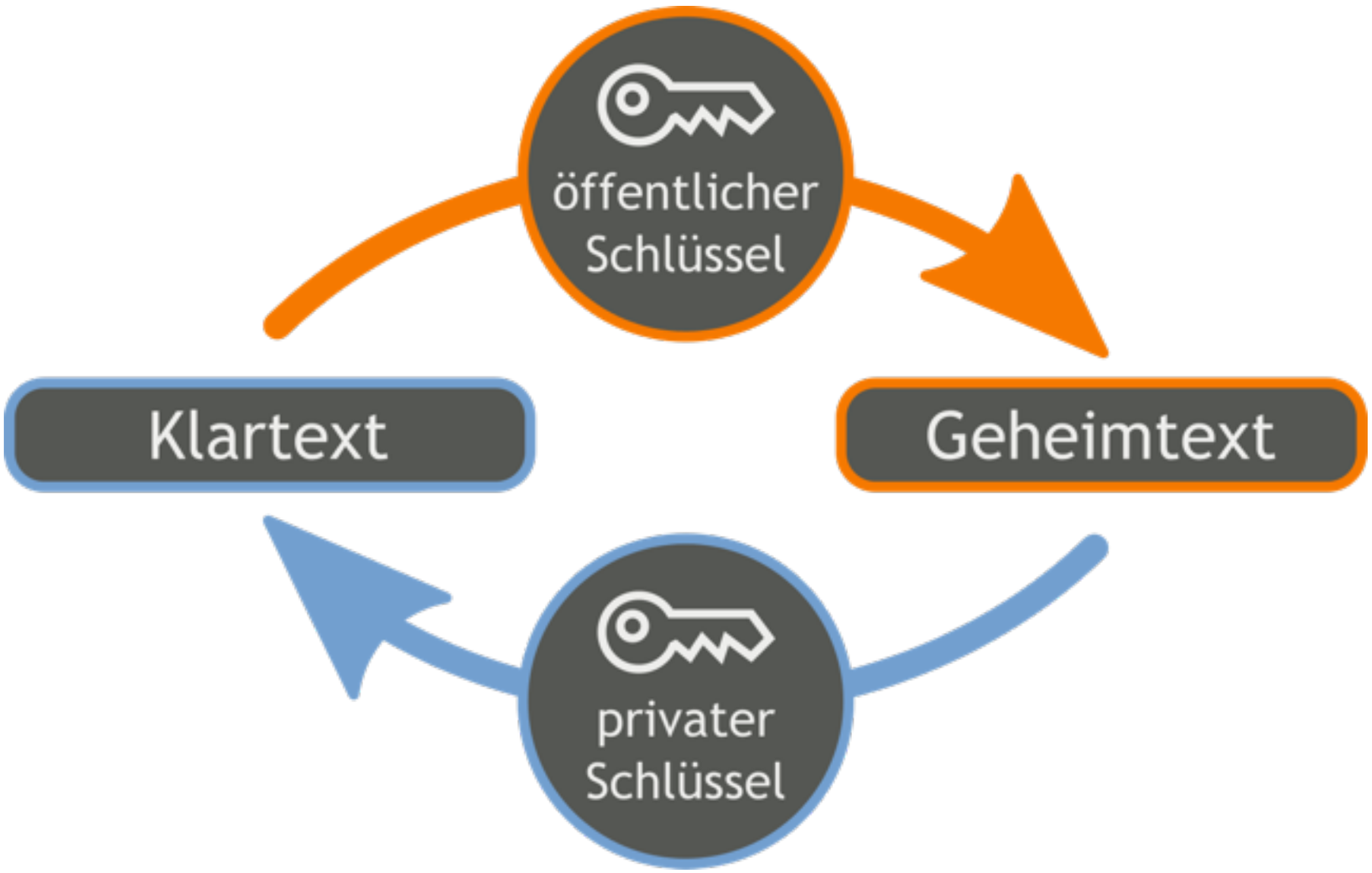


https://de.wikipedia.org/wiki/Datei:Orange_blue_public_private_keygeneration_de.svg

Mathematik

- Was ist 76.333 x 80.149?
  - 6.118.013.617.
  - Multiplikation ist sogar per Hand ohne weiteres möglich.
- Was sind die Primfaktoren von 4.634.629.529?
  - 58.417 und 79.337.
  - Primfaktorenzerlegung ist äußerst aufwändig!
- Asymmetrische Verschlüsselung ist sicher, solange die mathematischen Probleme nicht gelöst sind (wofür derzeit nichts spricht).

Asymmetrische Verschlüsselung



https://de.wikipedia.org/wiki/Datei:Orange_blue_public_key_cryptography_de.svg

PGP/GnuPG

- PGP wurde Anfang der 1990er-Jahre von Phil Zimmermann entwickelt.
- GnuPG ist eine quelloffene Umsetzung von PGP.
- PGP/GnuPG arbeiten mit öffentlichen und privaten Schlüsseln.
- Umsetzungen sind für alle Betriebssysteme (einschließlich Smartphones) verfügbar.

Programm

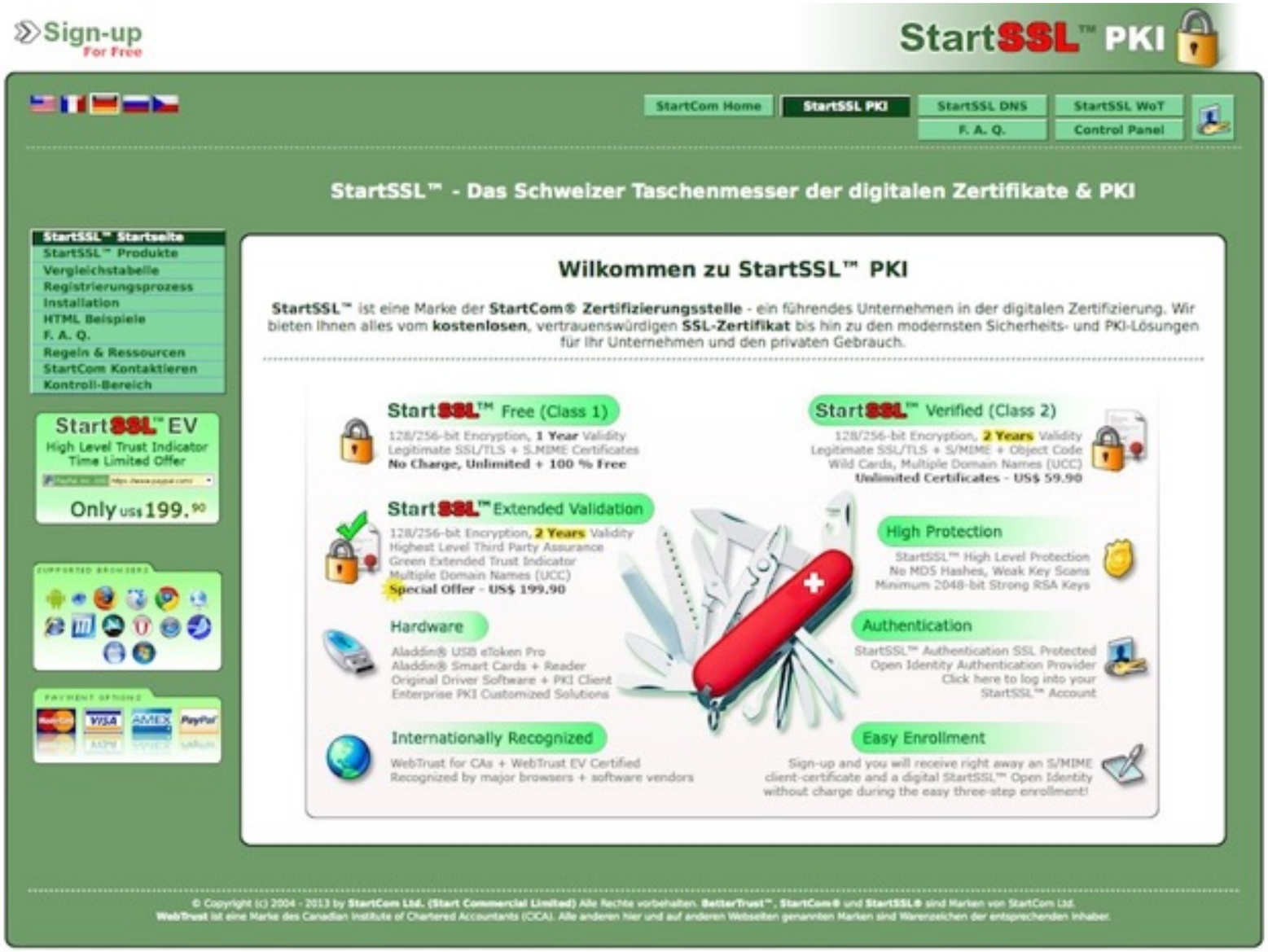
- Schlüsselpaar erstellen.
- Schlüssel exportieren und importieren.
- Verschlüsseln und Entschlüsseln von E-Mail.
  - Mail.app, Thunderbird und Outlook.

Schlüssellänge

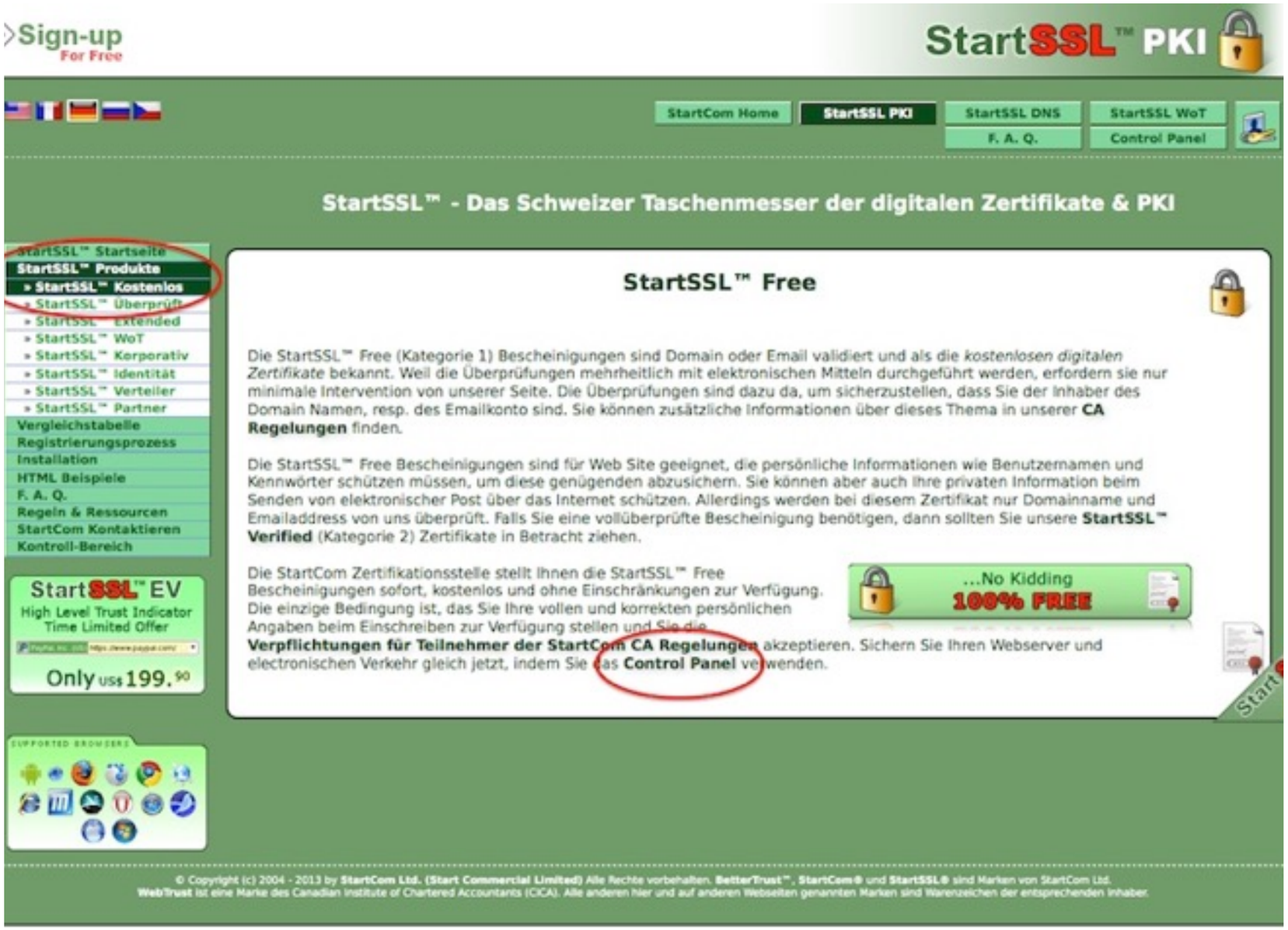
- 48 Bit Schlüssellänge → 2^{48} Schlüsselkombinationen.
- 2048 Bit RSA-Schlüssel ≈ 112 Bit konventionelle Schlüssellänge.
- 2^{112} = 5.192.296.858.534.827.628.530.496.329.220.096 (5 Quintilliarden).
- Der derzeit schnellste Rechner würde für den gesamten Schlüsselraum (mindestens) so lange benötigen, wie die Erde existiert …

S/MIME

- System zum Verschlüsseln und Signieren von E-Mails.
- Nichtkompatibel zu PGP/GnuPG.
- Zentrale Verwaltung der Zertifikate.
- Zertifikat muss (sinnvollerweise) von einer anerkannten Zertifizierungsstelle erzeugt werden – z. B. <https://startssl.com>.
- S/MIME funktioniert meist ohne weitere Konfiguration!

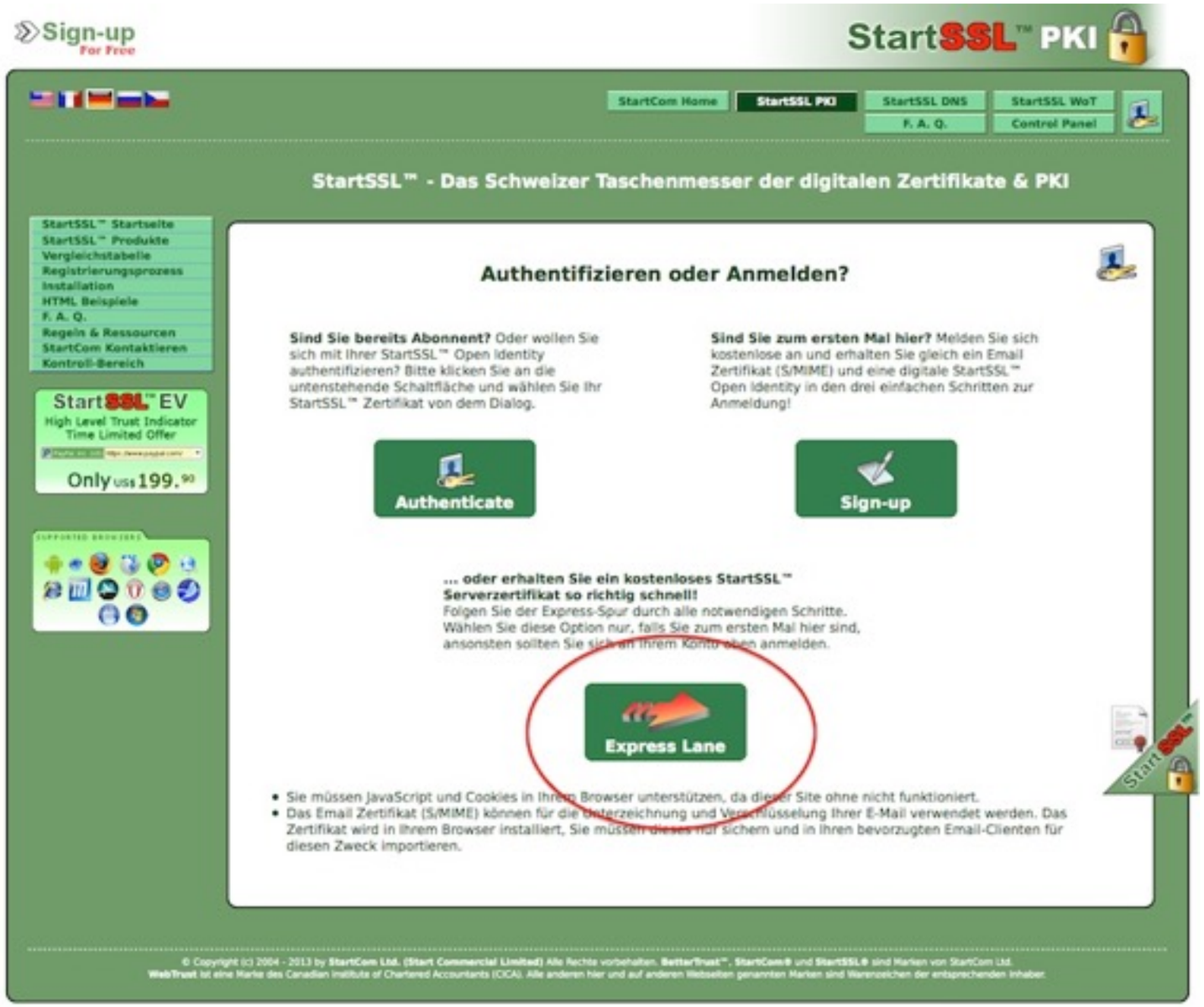


Zunächst muss man die WWW-Seite von StartSSL aufrufen: <https://www.startssl.com>.

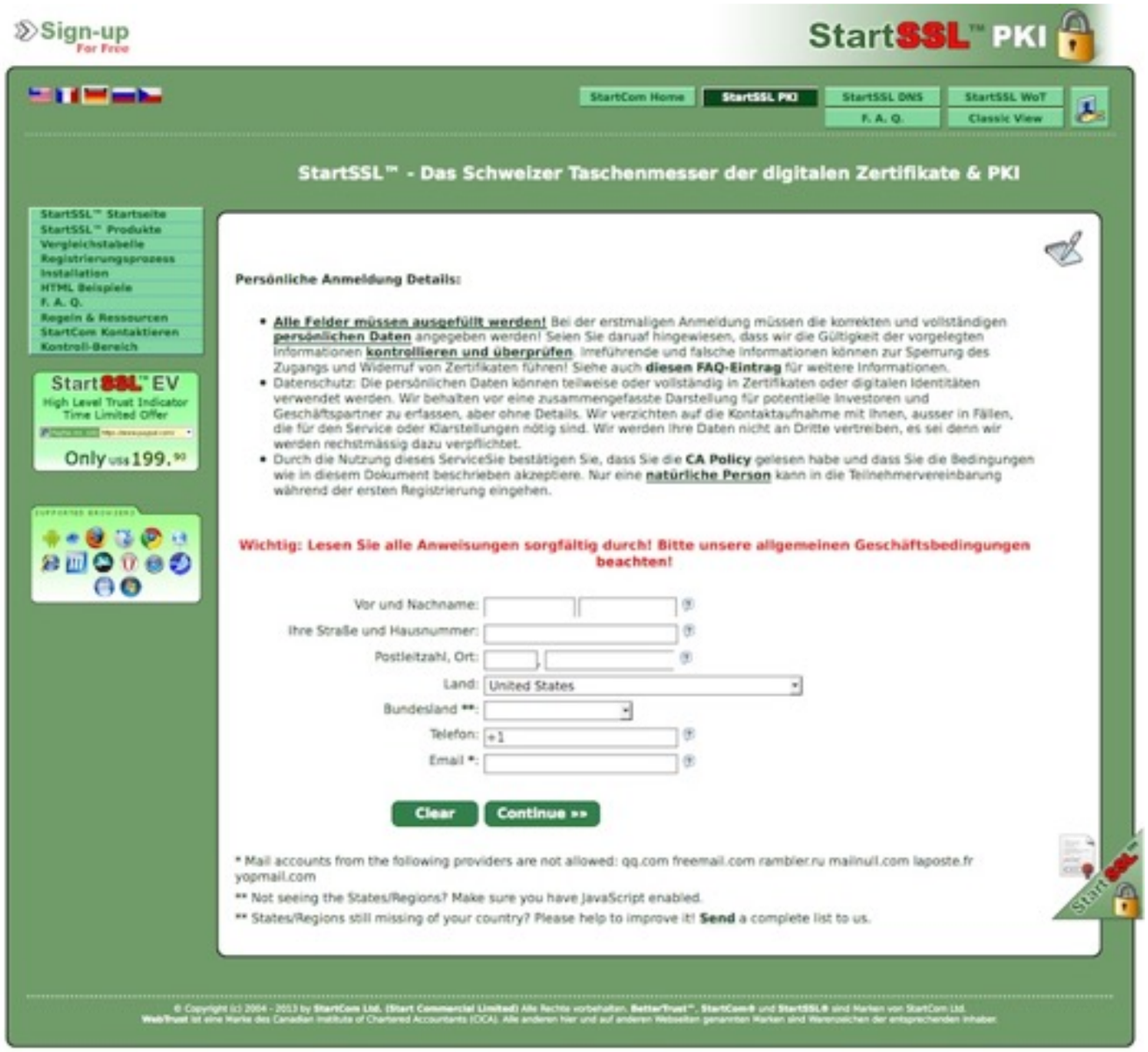


Nun im Menü auf der linken Seite „StartSSL™ Produkte“ und „StartSSL™ Kostenlos“ auswählen.

Nun weiter zum „Control Panel“ (den entsprechenden Link anklicken).

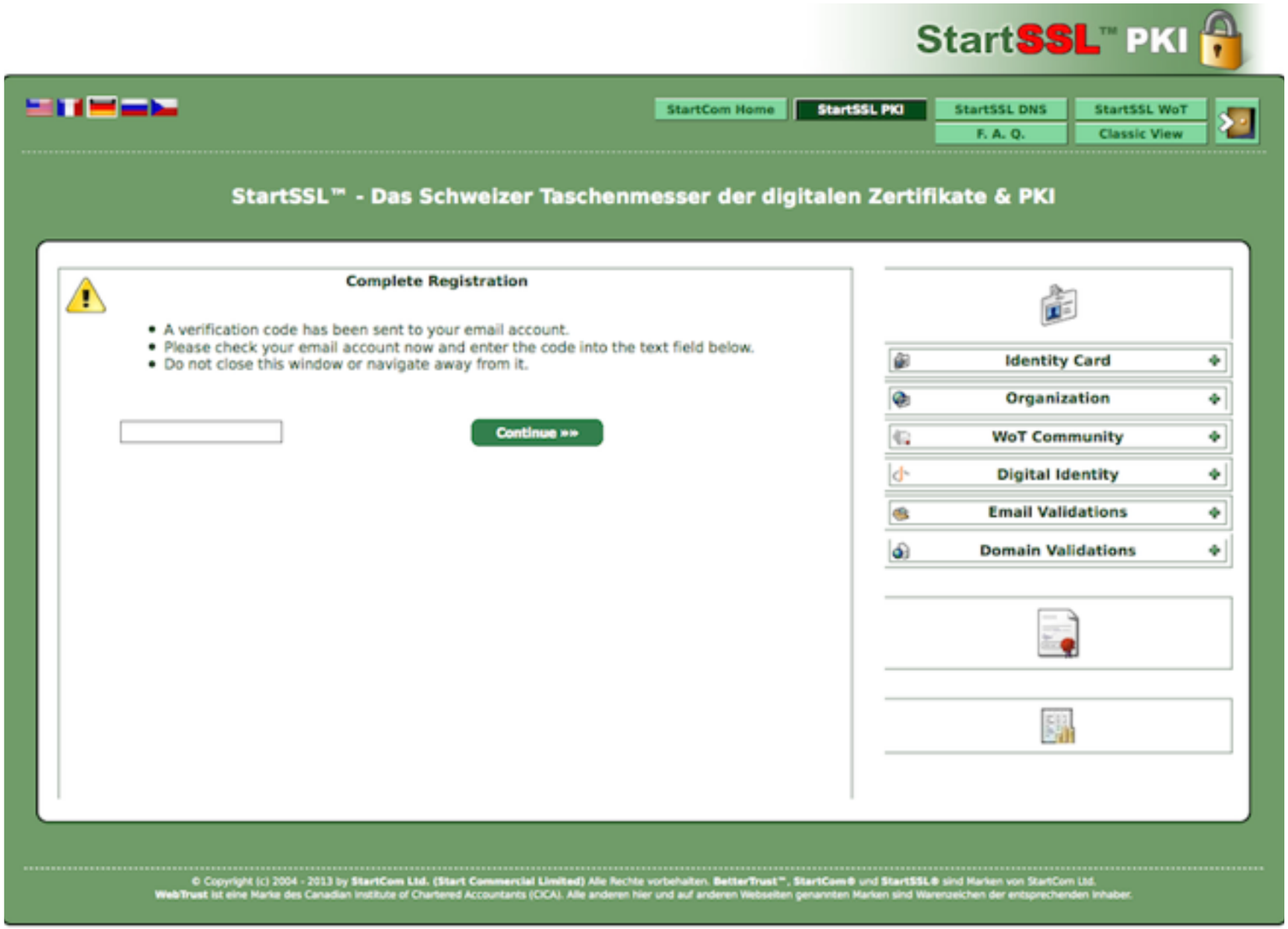


… und weiter über die „Express Lane“.

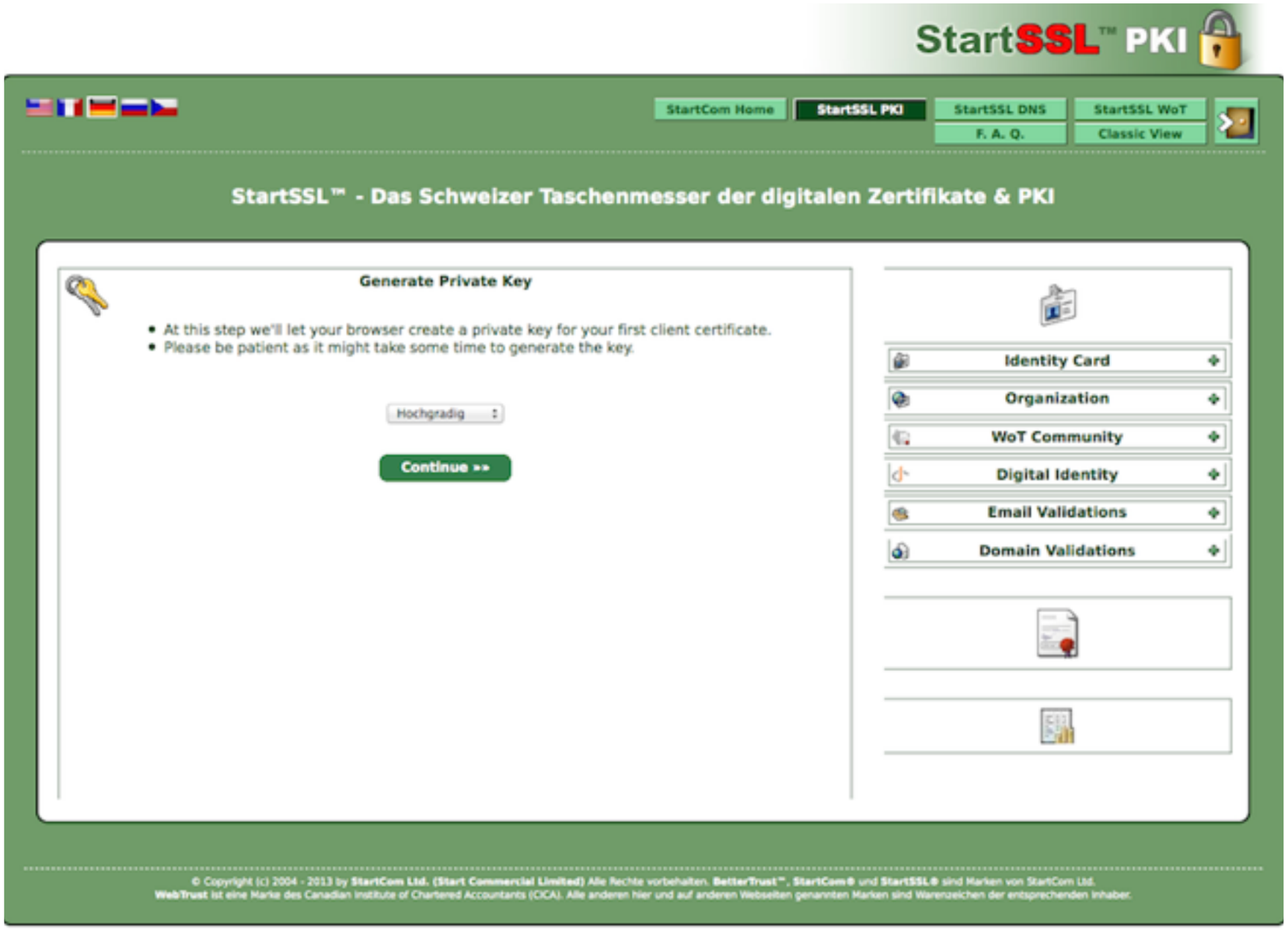


Die folgenden Angaben sollte man sich durchlesen und die entsprechenden Felder ausfüllen.

StartSSL verschickt jetzt eine E-Mail mit einem Verifizierungscode. Diese Mail muss also abgewartet werden.



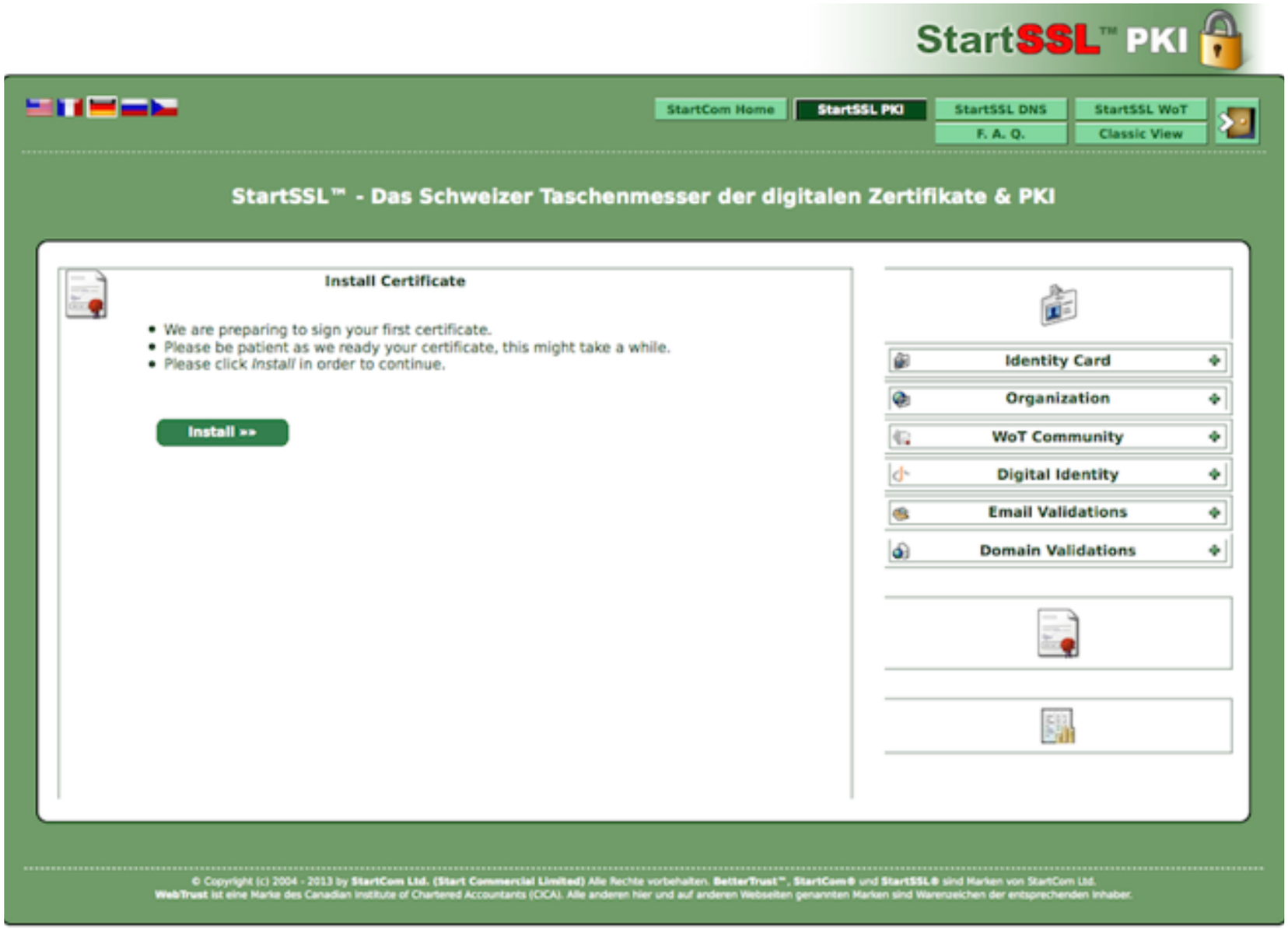
Wenn der Verifizierungscode per E-Mail eingetroffen ist, diesen in das entsprechende Feld eintragen und fortfahren.



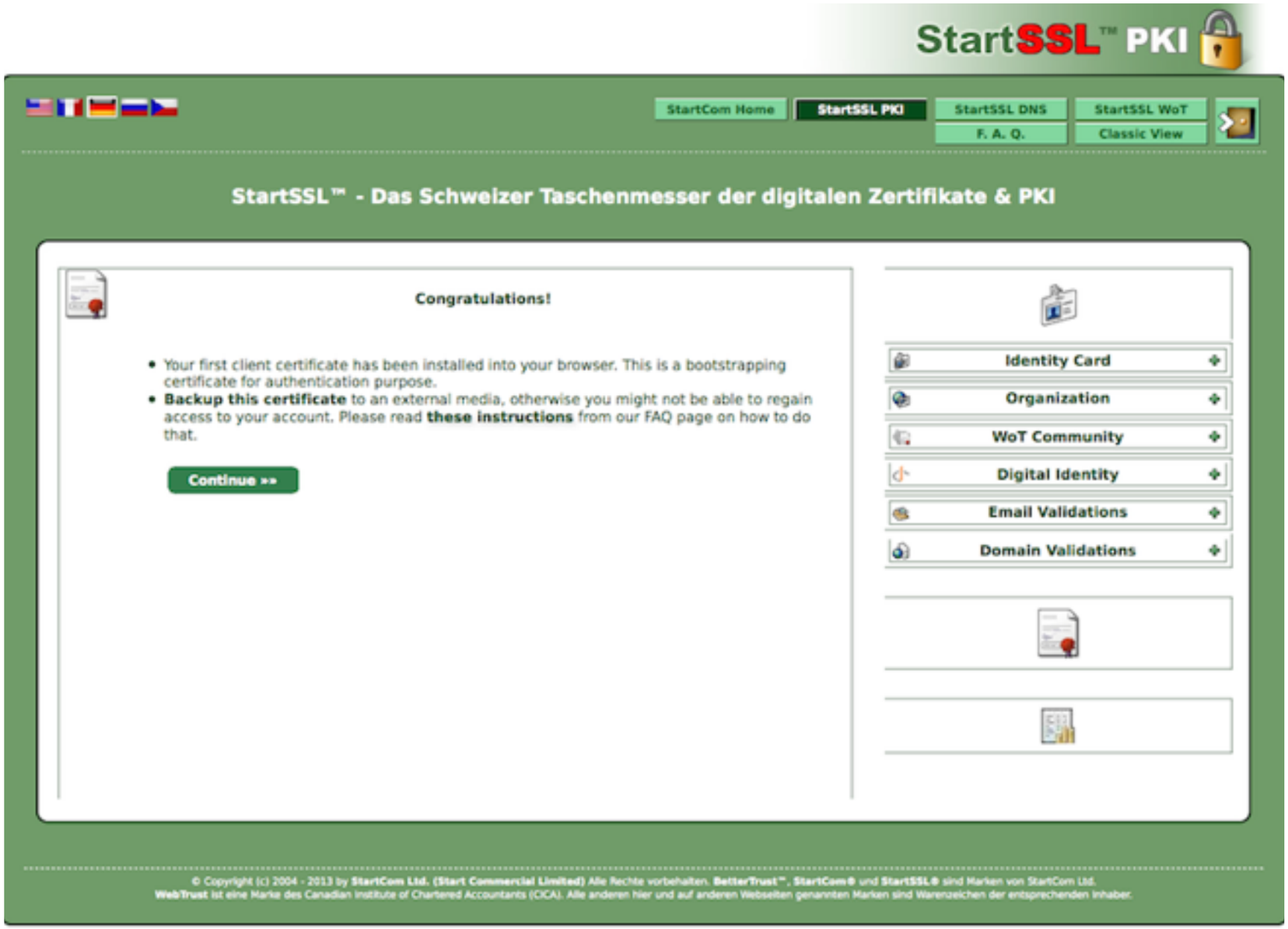
Nun wird der private Schlüssel erzeugt. Dieser Vorgang kann eine Weile dauern.

Die Erzeugung des Schlüssels erfolgt im Browser – der geheime Schlüssel sollte also nicht an StartSSL übertragen werden.

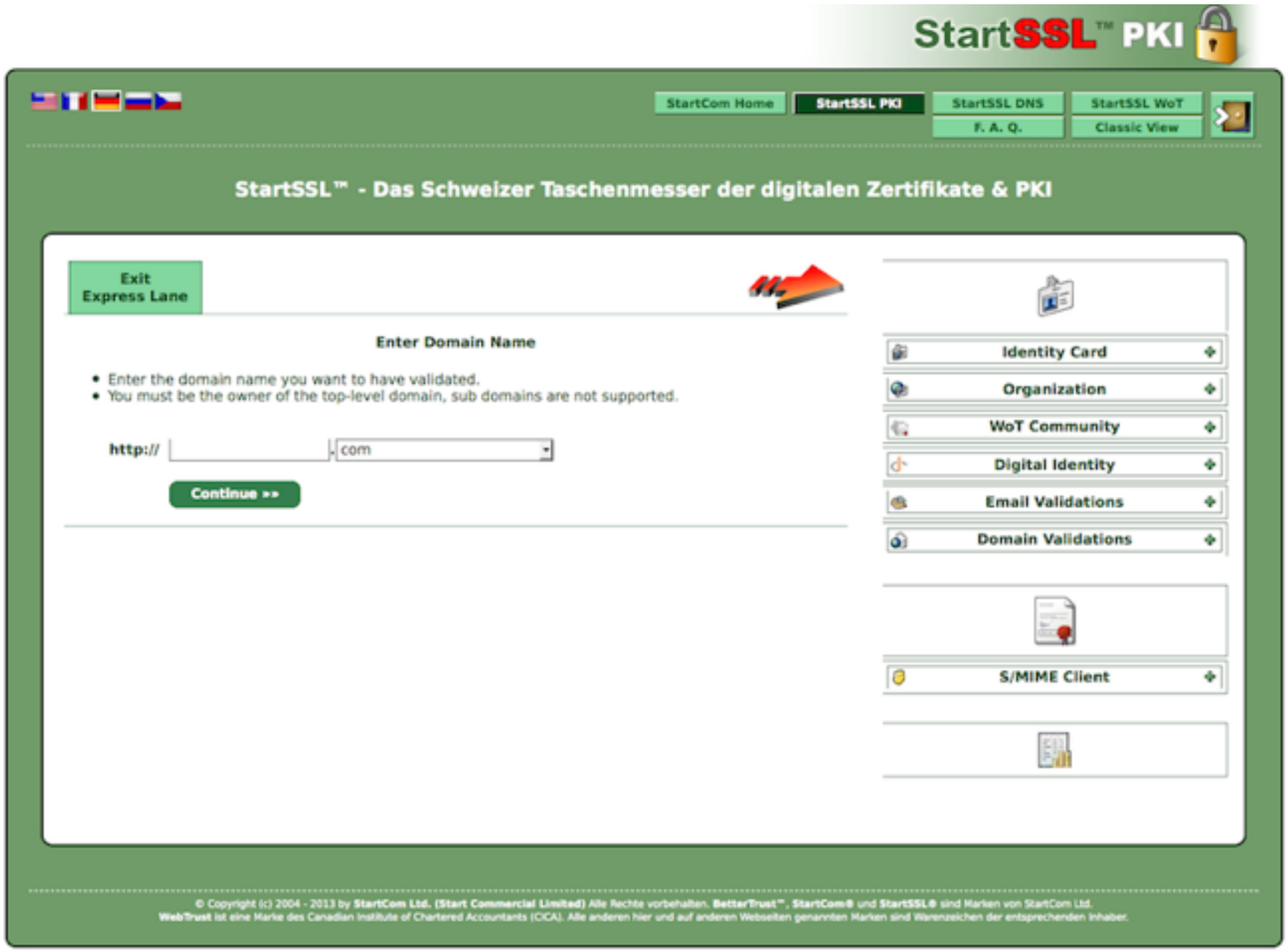
Ist das Zertifikat fertig erzeugt, wird man aufgefordert, mit der Installation fortzufahren.



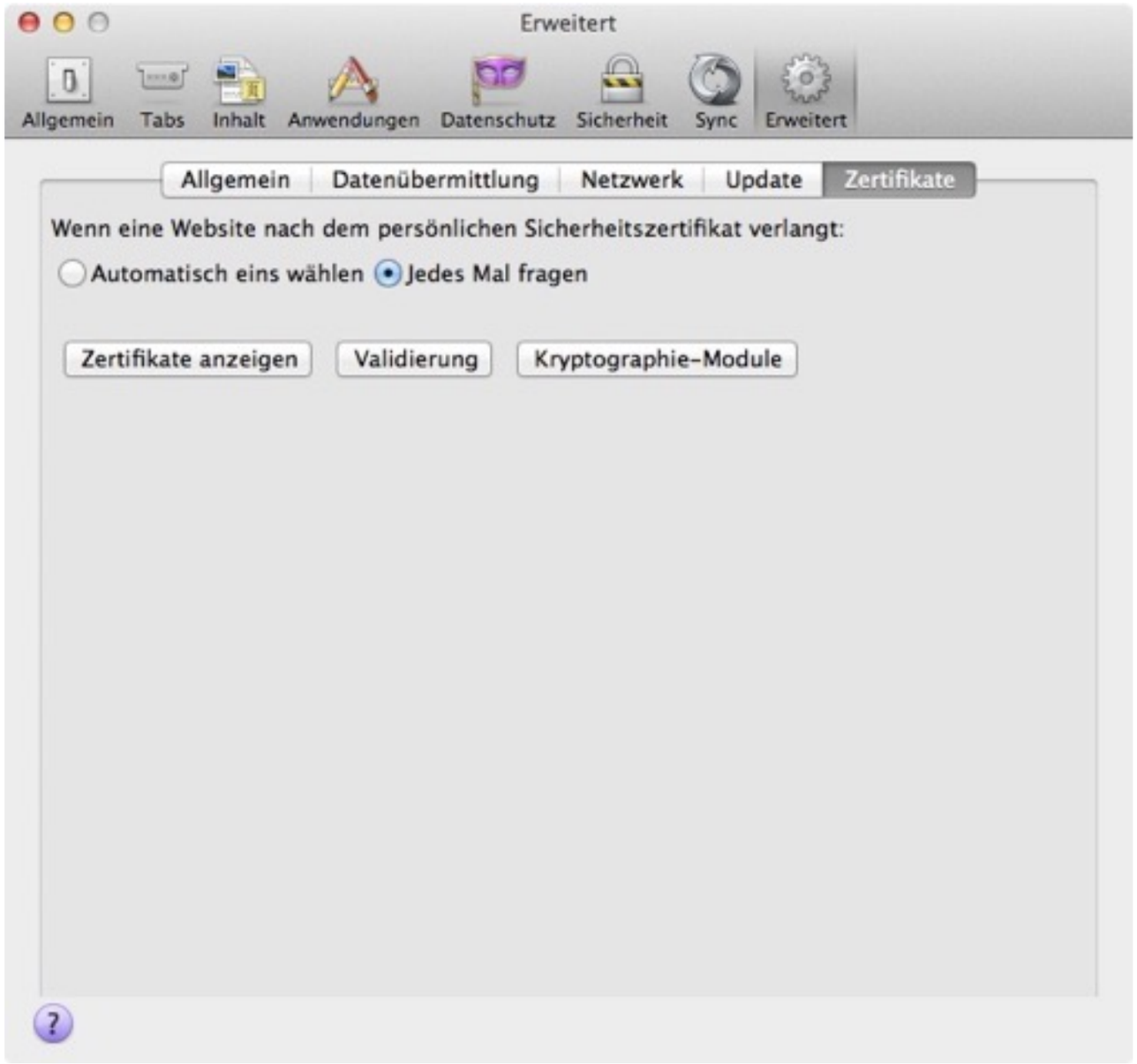
Das Zertifikat wird nun im Browser installiert …



… und StartSSL rät ein Backup des gerade erzeugten Zertifikats anzulegen.



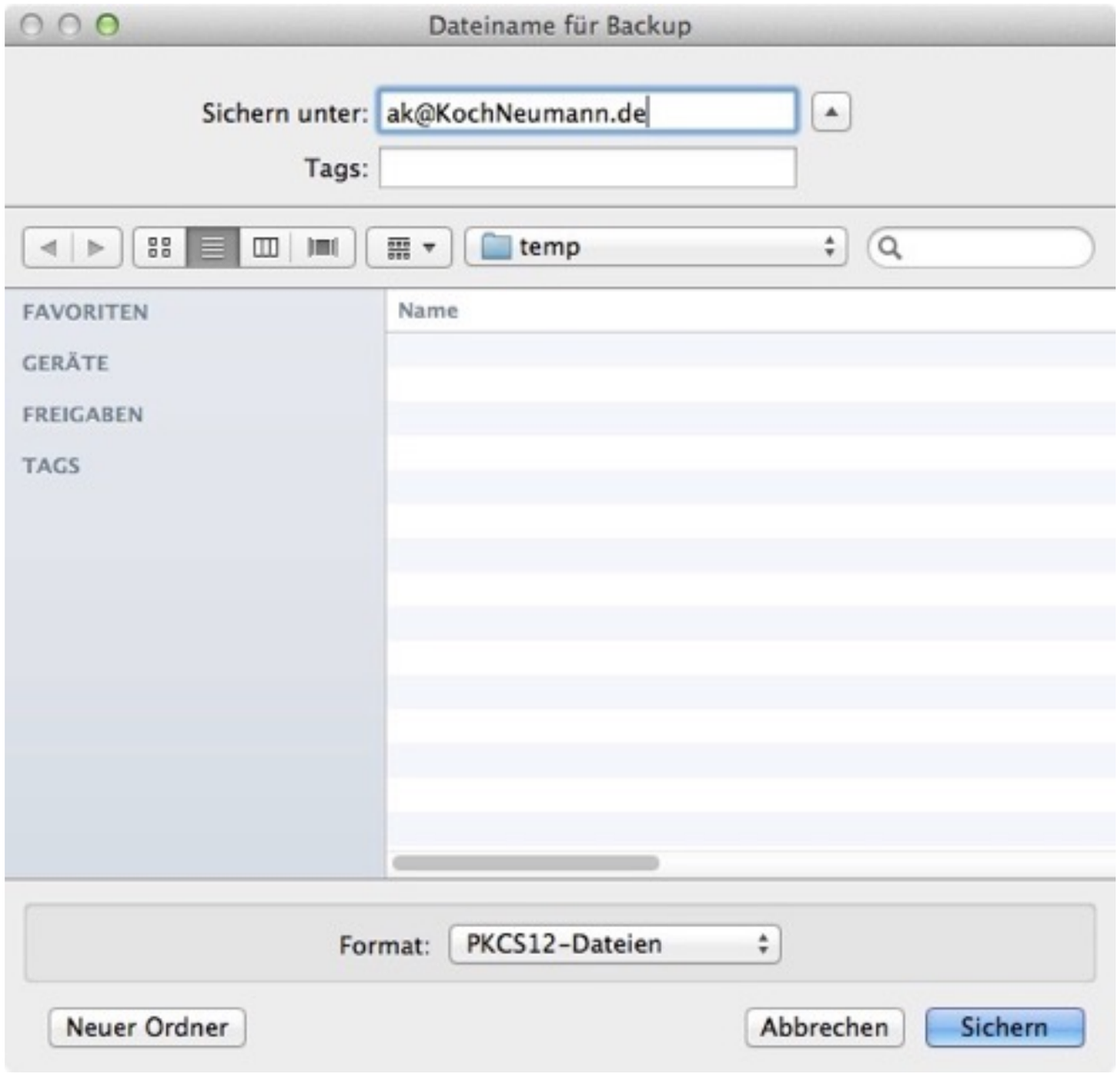
StartSSL fordert nun dazu auf, einen Domänennamen einzugeben. Man könnte hierdurch gleich noch ein SSL-Zertifikat erzeugen. Benötigt man nur ein S/MIME-Zertifikat, kann man an dieser Stelle abbrechen.



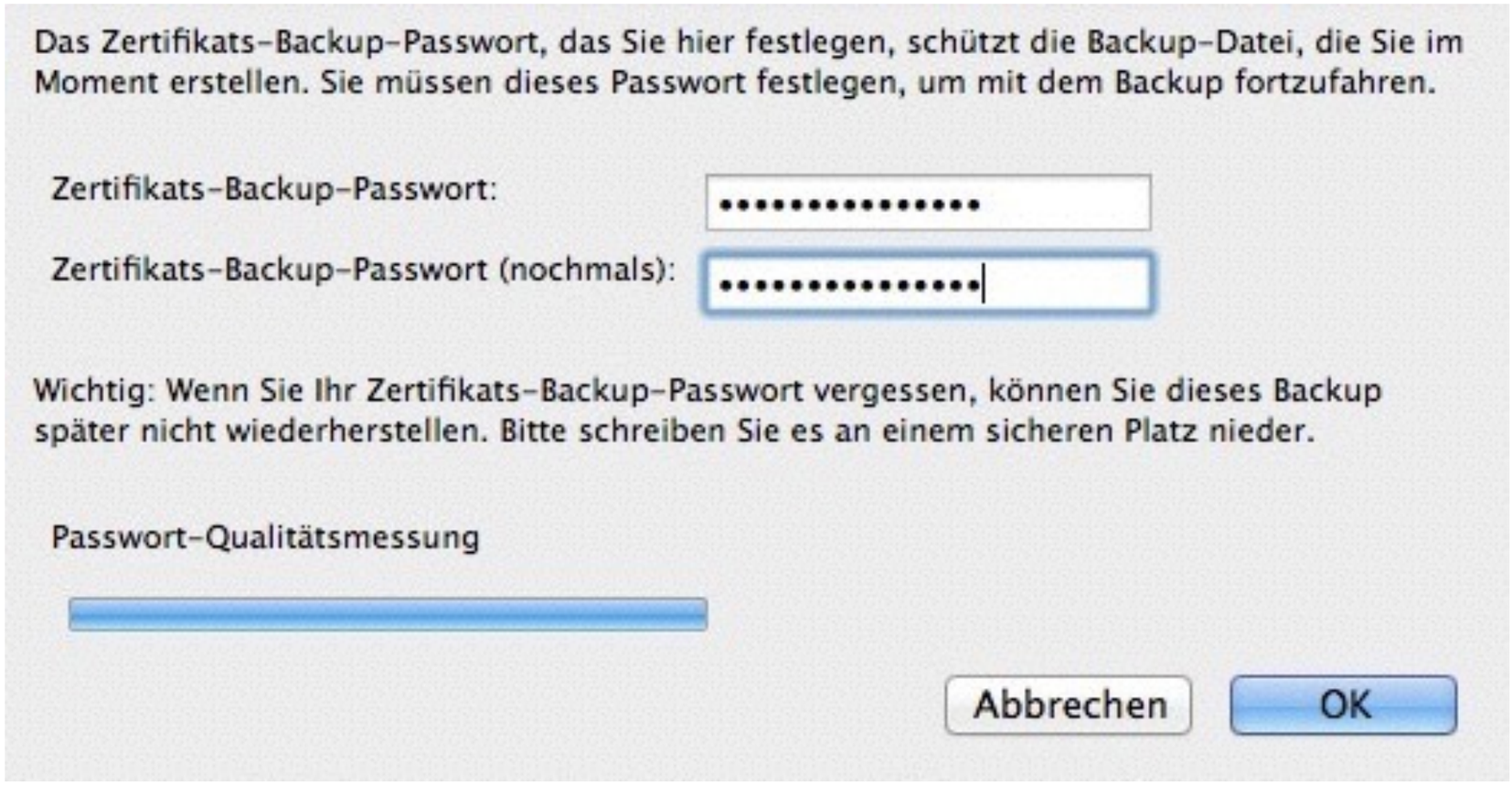
Das Zertifikat wurde im Firefox gespeichert und muss zunächst exportiert werden. Hierzu muss die Zertifikateverwaltung von Firefox über „Firefox“ – „Einstellungen ...“ – „Erweitert“ – „Zertifikate“ aufgerufen werden. Dort muss man „Zertifikate anzeigen“ anklicken.

Im ersten Reiter werden die eigenen Zertifikate angezeigt.

Hier muss man das gerade erzeugte Zertifikat anklicken und über „Sichern ...“ speichern.



Im Speicher-Dialog muss zunächst ein beliebiger Name für das Zertifikat vergeben werden. Sinnvoll ist es, die verwendete E-Mailadresse zu nutzen.



Das Zertifikat muss schließlich noch mit einem Passwort gesichert werden.

Das Zertifikat sollte nun als erstes auf einem sicheren Datenträger gesichert werden. Geht es verloren, kann es nicht neu erstellt werden.

ZIP

- … wenn PGP/GnuPG oder S/MIME zu kompliziert sind …
- Es können nur Anhänge verschlüsselt werden.
- Die Dateinamen werden nicht verschlüsselt.
- Es muss zunächst ein Passwort sicher ausgetauscht werden.
- Mac und Windows können von Hause aus nicht mit (sicher) verschlüsselten ZIP-Dateien umgehen.
- Darauf achten, dass das ZIP-Programm die AES-256-Verschlüsselung beherrscht.

Was nun?

	PGP/GnuPG	S/MIME	ZIP
Verbreitung	- -	-	++
Einrichtung	- -	- -	+
Nutzung	O	++	+
E-Mail-Integration	++ (Outlook -)	++	- -
Schlüsseltausch	+	+ +	- -
Sicherheit	+ +	+ +	- - / AES ++

Die schlechteste Verschlüsselung ist immer noch besser als überhaupt keine Verschlüsselung!

Datensicherheit

Koch & Neumann
RECHTSANWÄLTE

Datensicherheit

- Festplatten sind Verschleißteile!
  - Fraglich ist nicht, ***ob*** eine Festplatte ausfällt, sondern nur, ***wann*** sie ausfällt!
- Wichtige Daten möglichst auf einem RAID-System sichern.
  - Daten werden parallel auf zwei (oder mehr) Festplatten gespeichert.
  - Fällt eine Festplatte aus, kann diese (im Betrieb) ohne Datenverlust gegen eine neue ersetzt werden.
- RAID-Systeme ersetzen kein Backup!

Backup

- Backup sollte automatisiert erfolgen.
- Generationenbackup erzeugen:
  - Stündlich, täglich, wöchentlich, monatlich.
- Backup sollte an einem anderen Ort aufbewahrt werden …
- … oder besser gleich (verschlüsselt) über das Internet dort erzeugt werden.
- Ein Backup ist gut. Zwei Backups sind besser!

Material und weitere Hinweise

http://kochneumann.de/index.php5?direktmodus=vortrag-datensicherung-siegen-2014

Vielen Dank für die Aufmerksamkeit!

Dr. Alexander Koch
Koch & Neumann
Rheinweg 67
53129 Bonn
Tel: 0228/8 50 86 63
E-Mail: ak@KochNeumann.de
http://KochNeumann.de

PGP/GnuPG: C68842E5
(Fingerabdruck: 88B5 21CC FBBD 8EE5 7F0F 0EB9 ADAA 780B C688 42E5)