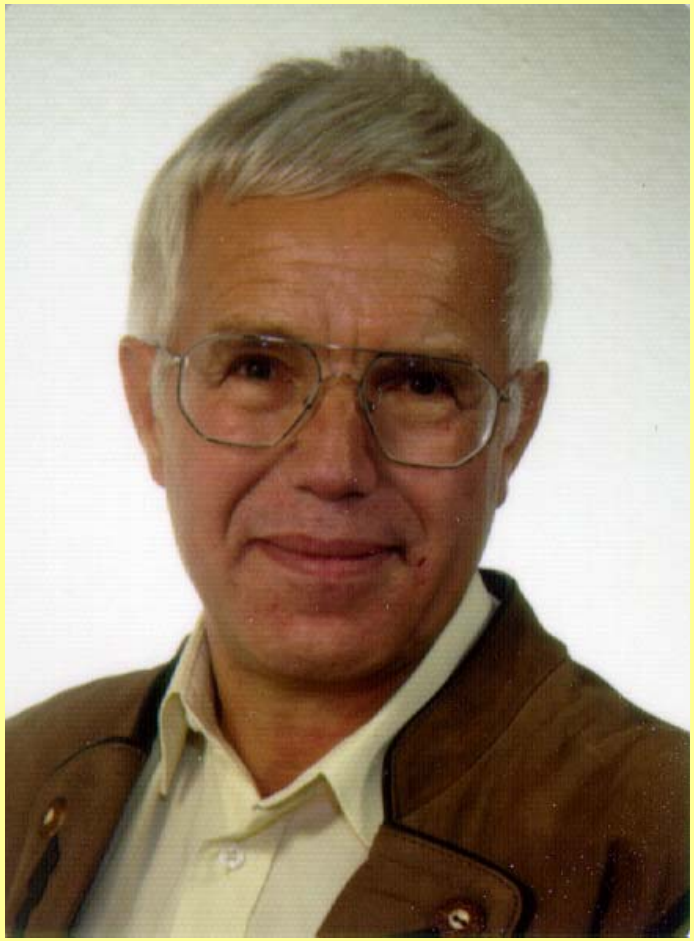
Referent

Reinhard Schmitt

Reinhard@ReinhardSchmitt.De



Adresse http://www.muela.de/stammtische/putzbrunn/favorite.html Wechseln zu

Vorträge

Home
Vorträge
Links

Lageplan
Unsere Adresse in map24

Dienstag 01.02.2005 / 20 Uhr Referent: Reinhard Schmitt. Steganos Security Suite

Die Firma Siemens erlaubt seinen Mitarbeitern für Geschäftliche Arbeiten nur noch Laptops, welche die gespeicherten Daten verschlüsselt. Sollte ein Laptop verloren gehen oder geklaut werden, so können die Geschäftsdaten nicht missbraucht werden.
Gleiches gilt für den Privatmann, wenn er in Urlaub fährt. Es gibt viele private Daten, wenn sie in fremde Hände fallen, kann dies zusätzlichen Schaden verursachen.
Hier hilft die Security Suite der Firma Steganos.

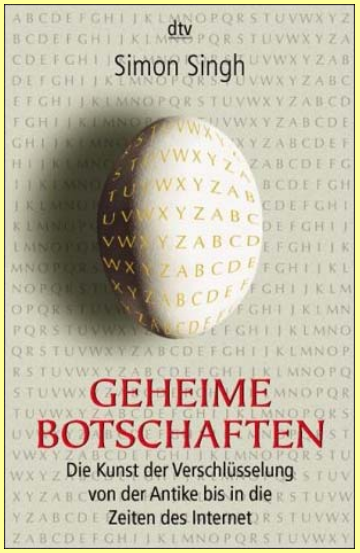
Über meine Erfahrungen möchte ich berichten.

E-Mail Reinhard@ReinhardSchmitt.De
http://www.ReinhardSchmitt.De

Neu überarbeitet!!

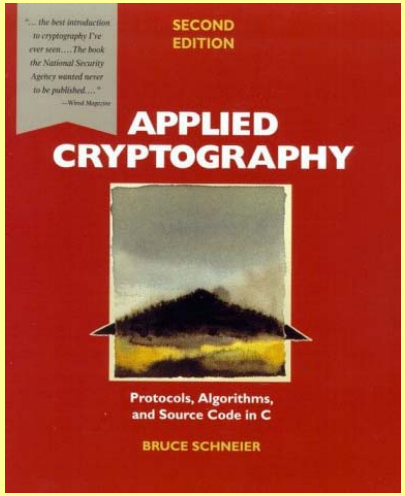
Die Vorträge sind für Vereinsmitglieder kostenlos, Nichtmitglieder zahlen 5 Euro Eintritt.

[Home][Vorträge][Links]



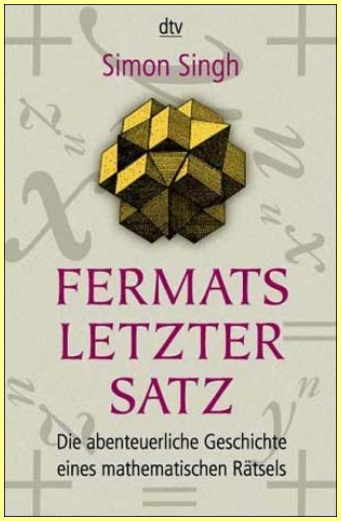
ISBN 3-423-33071-6

Deutsch 12,50 €
Amazon ab 7,99 €



ISBN

Englisch 50,40 €
Amazon ab 38,59 €



ISBN 3-446-19313-8

Deutsch 10,00 €
Amazon ab 7,35 €

ISBN 3-527-50021-9

Deutsch 36,00 €
Amazon ab 24,00 €

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Was möchte man schützen?

Dateiname	Größe	Typ	Geändert am
Adressen		Dateiord...	27.12.03 13:39
Briefe		Dateiord...	27.12.03 13:39
Finanzen		Dateiord...	27.12.03 13:40
Gehalt		Dateiord...	27.12.03 13:47
Gesundheit		Dateiord...	27.12.03 13:47
Haus		Dateiord...	27.12.03 13:57
Jahres_Rückblick		Dateiord...	27.12.03 13:58
Password		Dateiord...	27.12.03 13:58
Recycled		Papierk...	19.01.04 14:27
Rente_CuR		Dateiord...	27.12.03 13:59
Steuern		Dateiord...	27.12.03 13:59
Wohnung		Dateiord...	27.09.04 14:17

Reisedokumente,

Bankdaten,

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

- **Bundesamt für Sicherheit in der Informationstechnik**
  www.bsi.de
  www.bsi.bund.de
- **Sichern aber Wie?**
  www.bsi-fuer-buerger.de/druck/kap_07.pdf
- **Ins Internet - Mit Sicherheit**
  www.bsi-fuer-buerger.de
- **Advanced Encryption Standard (AES)**
  www.korelstar.de/aes.php
  www.computerbase.de/lexikon/Advanced_Encryption_Standard
- **10 Gebote für Passwörter**
  www.hirschbeutel.de/password.html
- **Internet Lexikon (Verschlüsselung)**
  de.wikipedia.org/wiki/Verschlüsselung

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

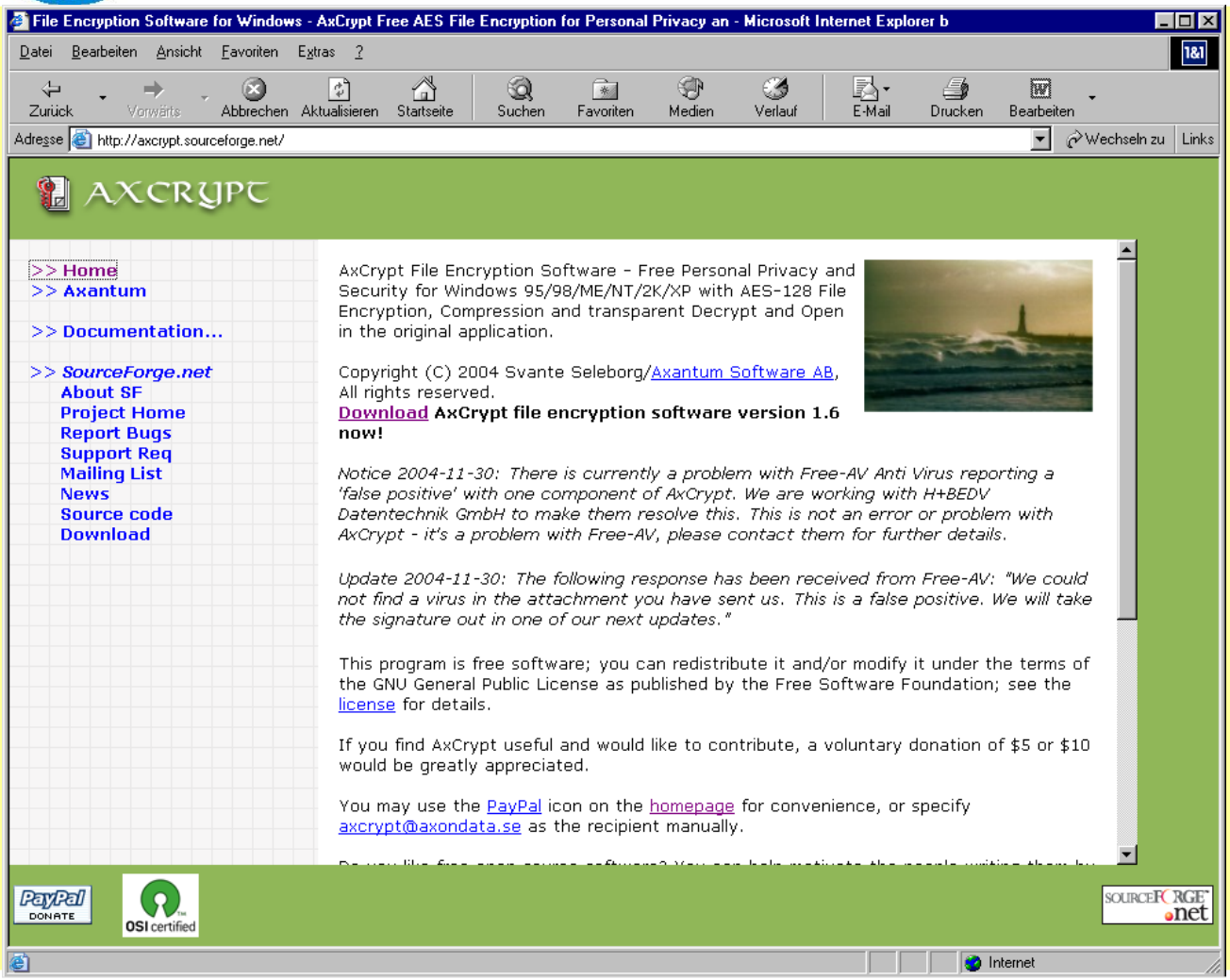
AxCrypt axcrypt.sourceforge.net	**Freeware**
ArchiCrypt Live www.archicrypt.com	**35,00 €**
Steganos www.steganos.com	**24,95 € bzw. (Suite) 39,95 €**

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Was Verschlüsseln?

	AxCrypt	ArchiCrypt	Steganos
1 Datei	X	X	X
Viele Dateien, 1 Ordner	-	X	X
Viele Ordner, 1 Laufwerk	-	X	X
1 Platte	-	X	X
1 Platte mit System	-	?	-
Mit USB-Token, Smart-Card	-	X	-
Dateien verstecken	-	X	X
Selbst entschlüsselnde Dateien	-	X	X

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De



- **AXCrypt Freeware**

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

- Steganos Security Suite 7 39,95 €
- Steganos Safe 7 24,95 €
- Steganos Secure File Sharing 24,95 €

- Steganos Internet Security Suite 39,95 €
- Steganos AntiVirus 29,95 €

- Internet Anonym Pro 7 39,95 €
- Internet Spuren Vernichter 7 24,95 €
- Internet Anonym 7 24,95 €
- Anti Spyware 7 24,95 €

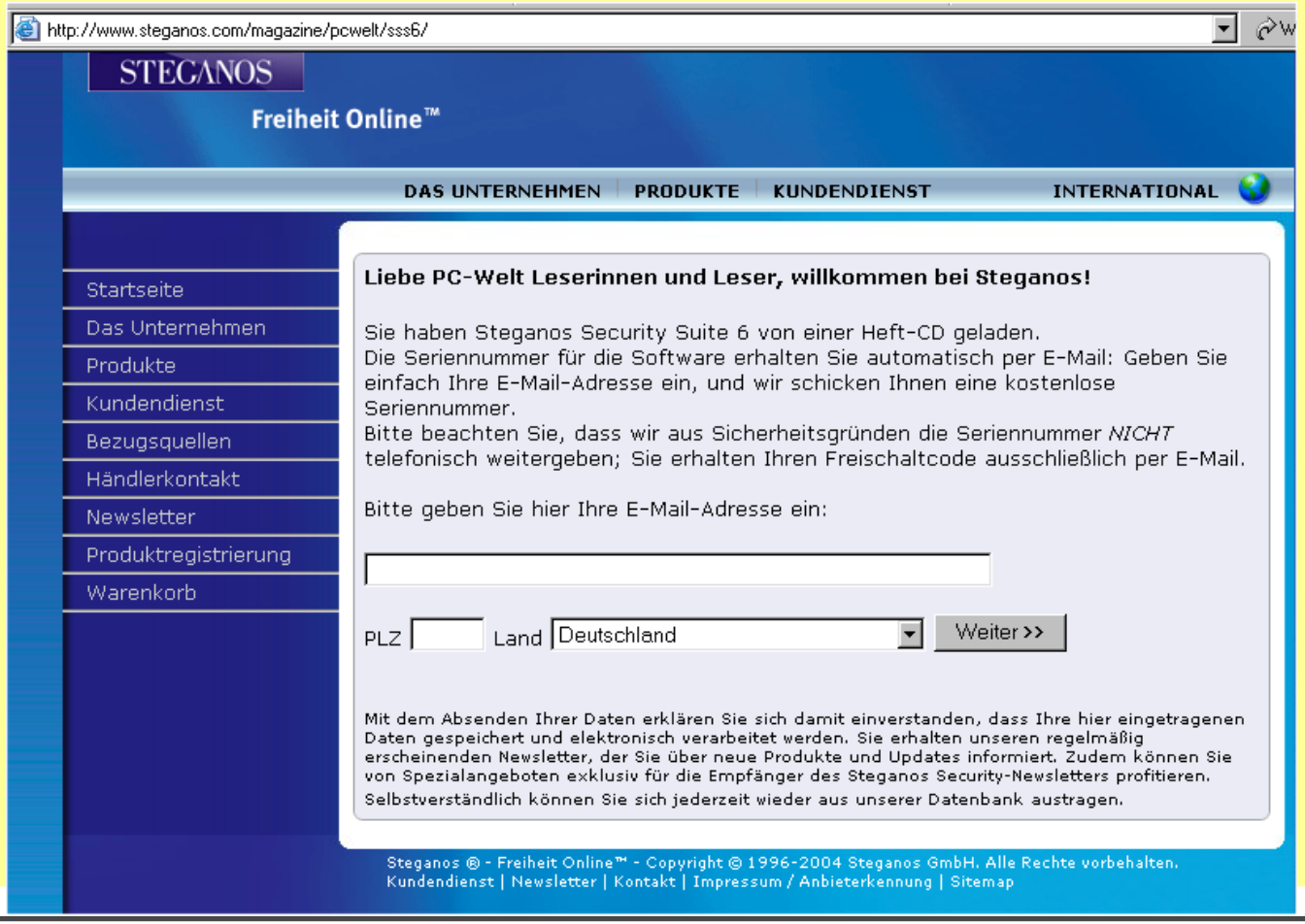
- Hacker Tools 29,95 €

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

ArchiCrypt Safe	
ArchiCrypt Pro	29,-- €
ArchiCrypt Live	35,-- €
ArchiCrypt Live Net	75,-- €
ArchiCrypt Stega	19,95 €
ArchiCrypt Passwort Safe	15,-- €
ArchiCryptX Change (port.safe)	24,95 €
ArchiCrypt Bubble(Card)	11,-- €
ArchiCrypt Live Engine SDK	Anfrage
ArchiCrypt Shredder	19,95 €
ArchiCrypt No Spam	24,95 €
ArchiCrypt Proxy-Collector	15,-- €
ArchiCrypt Stealth (Tarnk. Int.)	25,-- €

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

- **http://www.steganos.com/magazine/pcwelt/sss6/**

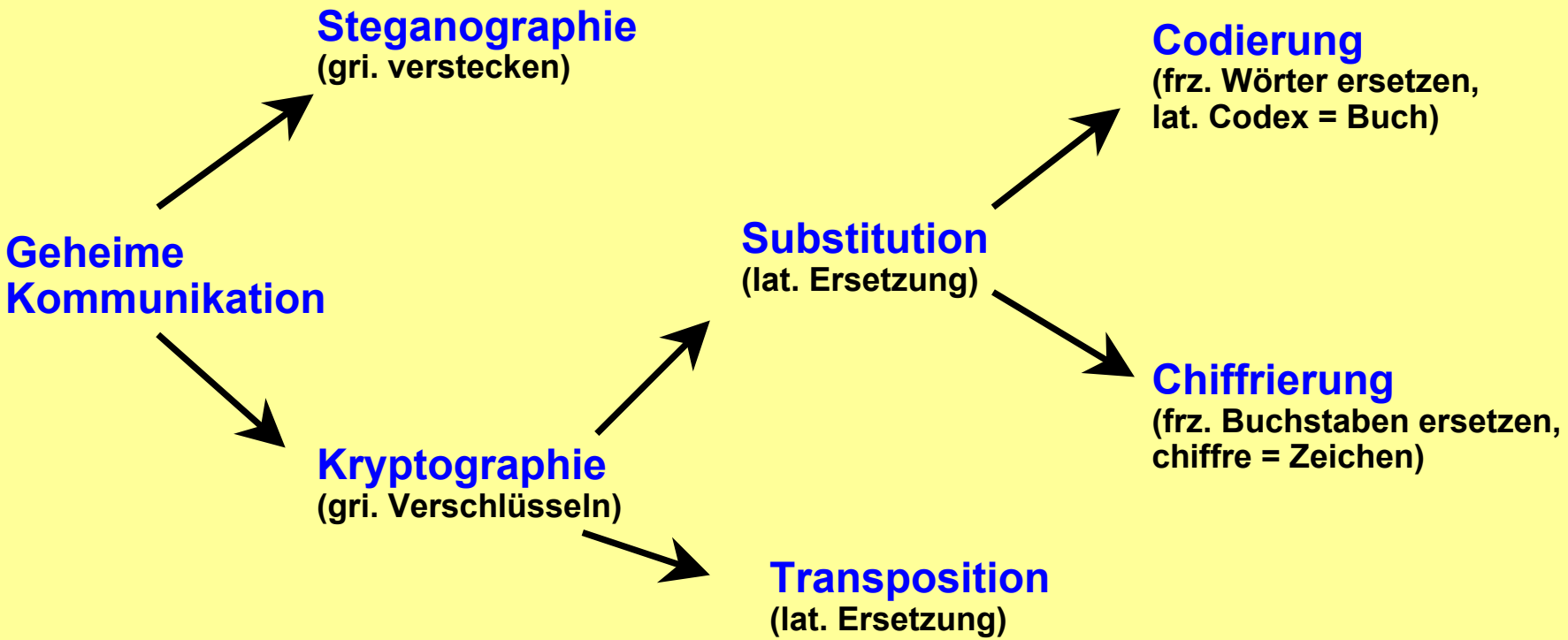


Sicherheit (Security)

- **Safe**
  (Dateiverschlüsselung)
- **Potable Safe**
  (Dateiverschlüsselung auf CD-ROM)
- **E-Mail Verschlüsselung**
  (E-Mail Verschlüsselung als exe / cab)
- **Datei-Manager**
  (Dateien verstecken in Ton- / Bild-Dateien)
- **Passwort-Manager**
  (Speicher für Passwörter)
- **Spuren-Vernichter**
  (Löschen von Fussabdrücken)
- **Shredder**
  (Dateien löschen durch Musterüberschreiben)

Steganos Security Suite 6

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De



Entnommen dem Buch „Geheime Botschaften“ Simon Singh

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Steganografie [aus dem Griechischen]: geschützt schreiben; verdeckt schreiben

Steganografie ist die Kunst, Informationen zu verstecken.

Die wohl bekannteste Form der Steganografie ist die unsichtbare Tinte. Das Informationszeitalter hat neue Methoden und sehr mächtige Techniken hervorgebracht.

Verstecken von Daten in Bild- und Tondateien

Eine moderne Variante der Steganografie ist das Verstecken von Daten in Bild- und Tondateien. Hier lässt sich beispielsweise das am wenigsten signifikante Bit eines Datenelementes nutzen, um Daten darin zu verstecken. Ein Element sind 8 Bit (1 Byte) in einer 8-Bit-Datei und 16 Bit (2 Byte) in einer 16-Bit-Datei. Auf diese Weise lassen sich etwa die niederwertigsten Bits der Bytes in einer 8-Bit-Wave-Klangdatei benutzen, um Daten in ihr zu verstecken. Da diese Veränderungen vom menschlichen Ohr nicht hörbar sind (z.B. wegen des Grundrauschens), sind diese Daten tatsächlich versteckt. Bei Bildern werden die Farben so geringfügig verändert, dass man die Veränderung nicht sehen kann.

Warum Steganografie mit Kryptografie kombinieren?

Beim ausschließlichen Einsatz von Kryptografie sind Daten für Dritte nicht mehr lesbar. Allerdings ist offensichtlich, dass ein geheimer Datenaustausch stattfindet.

Wenn nur Steganografie benutzt wird, sind die versteckten Daten zwar unsichtbar. Allerdings ist es durch simples Überprüfen aller verdächtigen Trägerdateien möglich, geheime Daten wiederherzustellen.

Hochsicher ist eine Kombination beider Technologien. Daten, die sowohl versteckt als auch verschlüsselt worden sind, können weder leicht gefunden noch entschlüsselt werden.

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Kryptografie bedeutet, Informationen so zu schreiben, dass sie für Dritte unlesbar sind.

Bereits seit Tausenden von Jahren werden Verschlüsselungssysteme eingesetzt, um Geheimnisse zu bewahren. Zu keiner Zeit waren die Systeme so zuverlässig, wie sie es heute sind. Dazu hat die moderne Computertechnik genauso beigetragen wie die durch Militär und E-Commerce vorangetriebene Forschung auf diesem Gebiet: Algorithmen sind gut dokumentiert und frei zugänglich. Das Buch *Applied Cryptography* von Bruce Schneier gilt als Standardwerk zum Thema.

In der modernen Kryptografie unterscheidet man Verschlüsselungsmethoden nach mehreren Kriterien - diese sagen jedoch nichts über ihre Sicherheit aus. Das wichtigste Kriterium ist, ob es sich um ein symmetrisches (mit geheimen Schlüsseln) oder asymmetrisches System (mit öffentlichen Schlüsseln) handelt.

Verwendet man ein System mit geheimem Schlüssel, so muss man mit dem Kommunikationspartner ein Passwort vereinbaren. Programme, die auf asymmetrischer Verschlüsselung basieren, funktionieren anders. Ihre Funktionsweise kann man sich wie einen Briefkasten vorstellen: Jeder kann etwas einwerfen (verschlüsseln), aber nur der Besitzer des privaten Schlüssels kann es lesen (entschlüsseln).

Es folgt eine Auflistung der wichtigsten Verschlüsselungs-Algorithmen:

Algorithmus	Erfinder	Typ
Blowfish	Schneier	Symmetrisch
DES	IBM	Symmetrisch
Diffie-Hellman	Diffie, Hellman	Schlüsselaustausch
IDEA	Lai, Messey	Symmetrisch
AES	Daemen, Rijmen	Symmetrisch
RSA	RSA	Asymmetrisch
Skipjack	NSA	Symmetrisch

Bis heute geht man davon aus, dass es nur ein System gibt, das absolute Sicherheit bietet: Das sogenannte *one time pad* (nach seinem Erfinder auch Vernam-Verschlüsselung genannt). Bereits 1917 hat Gilbert S. Vernam, der zu diesem Zeitpunkt für AT&T arbeitete, dieses System entwickelt, um die Kommunikation von Fernschreibern zu sichern. Leider ist das Verfahren nicht praktikabel, da es voraussetzt, dass der Schlüssel mindestens so lang ist wie die geheimen Daten. Angeblich ist das berüchtigte 'rote Telefon' zwischen Washington und Moskau mit dem *one time pad* gesichert.

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Verwendete Algorithmen

Wir verwechseln Sicherheit nicht mit Geheimniskrämerei. Erfahren Sie, welche Algorithmen in der Steganos Security Suite 6 zum Einsatz kommen.

Verschlüsselung

Zur Verschlüsselung werden zwei Algorithmen eingesetzt.

1. Advanced Encryption Standard (AES)

Der AES-Algorithmus wurde im Oktober 2000 vom US-amerikanischen *National Institute of Standards and Technology* (NIST) zum Nachfolger des von IBM entwickelten *Data Encryption Standard* (DES) ernannt. Der DES gilt heute als veraltet – er war fast 30 Jahre lang der Standard für verschlüsselte Informationen. Der AES gilt als absolut sicher und arbeitet mit einer Schlüssellänge von 128 Bit. Er wird im Safe, bei der E-Mail- und Datei-Verschlüsselung und im Passwort-Manager verwendet.

2. Blowfish

Der Algorithmus wurde von dem renommierten Unternehmen *Counterpane Internet Security* entwickelt. Auch Blowfish gilt als absolut sicher. Auch er arbeitet mit einer Schlüssellänge von 128 Bit. Der Blowfish-Algorithmus kommt beim Verstecken von Daten in Bildern und Tondateien zum Einsatz.

Kryptografische Hashvalues

Zur Generierung von Hashvalues (kryptografischen Prüfsummen) kommt der SHA-1-Algorithmus zum Einsatz.

Steganografie

Durch die sogenannte Matrixkodierung müssen besonders wenige Bits in den Trägerdateien verändert werden. Dadurch sind die versteckten Informationen besonders unauffällig. Steganografie wird in der Steganos Security Suite immer zusammen mit Kryptografie verwendet.

Datenvernichtung

Entspricht der Norm des US-Militärs DOD 5220.22-M/NISPOM 8-306 und geht darüber hinaus. Nicht nur Dateiinhalt, sondern auch Dateiname, Grösse, Datum und Attribute werden vernichtet.Wahlweise können Sie auch die Gutmann-Methode nutzen: Sie entspricht den Sicherheitsanforderungen des BSI und der NSA. Der Speicherplatz wird hier nach einem bestimmten Verfahren 35 mal überschrieben.

Green	Green/Yellow	Yellow	Yellow/Red	Red	Unknown
Anguilla Antigua and Barbuda Aruba Belize Campione d'Italia *Canada* Chile Crotia *Cyprus* Dominica Estonia Falkland Islands Germany Gibralter Iceland *Indonesia* *Ireland* Kuwait *etc.*	*Argentina* *Armenia* Australia *Austria* Belgium Brazil Bulgaria Czech Republic Denmark Finland *France* Greece Hungary Italy *Japan* Kenya *South Korea* Luxembourg etc.	Hong Kong Malaysia Slovakia Spain United Kingdom *United States*	India *Israel* Saudi Arabia	Belarus China Kazakhstan Mogolia Pakistan Russia Singapore Tunisia Venezuala Vietnam	Angola Bahrain Cambodia Iran Myanmar Nicaragua Palestine Tatarstan

- http://lawww.de/Library/Krypto/index.shtml#FN(5)
- http://www.fgsec.ch/publ/2/ckrv1.html
- http://www.securius.com/newsletters/Strong_Country_Strong_Crypto.html
- http://rechten.uvt.nl/koops/cryptolaw/cls2.htm
- http://lawww.de/Library/Krypto/index.shtml
- http://www.gilc.org/crypto/crypto-results.html
- http://www.gilc.org/crypto/crypto-survey.html
- http://rechten.uvt.nl/koops/cryptolaw/#C
- http://www2.epic.org/reports/crypto1999.html
- http://www.boran.com/security/sp/int_crypto.html
- http://www.kryptel.com/links/legal.php
- http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/queensland.pdf#search='crypto%20countries,

- `Peter Kapfer Empfehlung: Yahoo.com, Suchwort: Crypto and countries

Dateien oder Verzeichnisse verschlüsseln

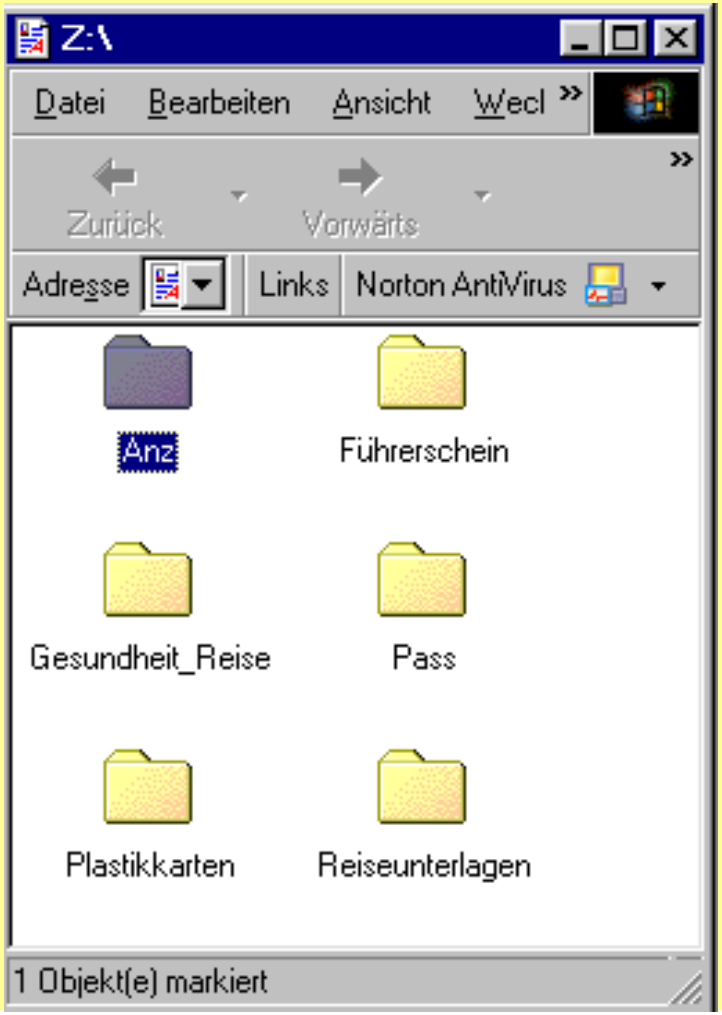
- Bis 4 Safes anlegen
- Safe öffnen und mit Daten füllen
- Safe schliessen

Ein geöffneter Safe wird wie ein neues Laufwerk mit allen Odnern im Explorer angezeigt

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Ein Portabler Safe ist wie ein normaler Safe, nur dass zusätzlich die Software hinzugepackt wird, um den Safe mit Passwort wieder lesen zu können!

Ein Portabler Safe kann auf eine CD oder anderen Datenträger kopiert werden und auf einem fremden PC ohne spezielle Software gelesen und ausgedruckt werden.
Ideal für Reisedokumente!

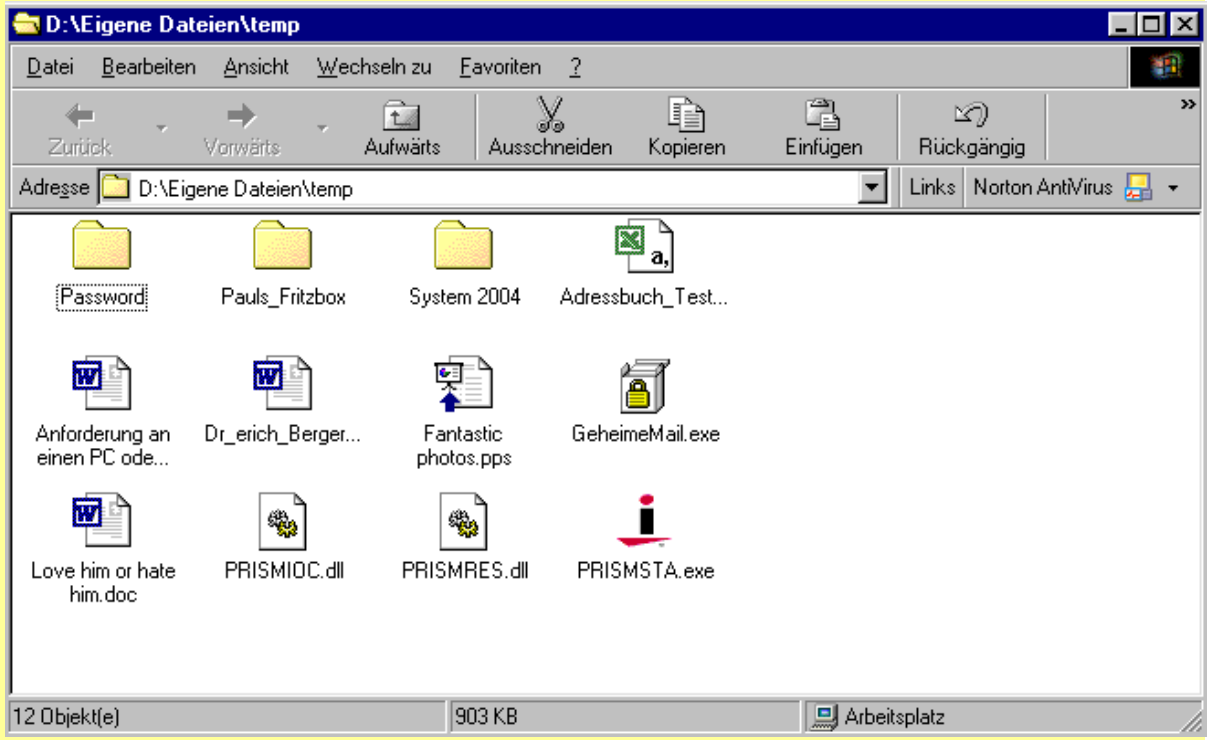


01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Wird ein kleiner Portabler Safe als .exe oder .cab Datei umgewandelt, dann kann er per E-Mail versendet werden.

Der Empfänger kann, dann per Eingabe des Passwortes, den Inhalt wieder lesen.

Steganos kann diese Email auch direkt über das Mail-Programm versenden.



01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Steganografie [aus dem Griechischen]: geschützt schreiben; verdeckt schreiben

Dateien in Ton-Dateien oder Bild-Dateien verstecken

Dateimanager = Steganografie

Steganos Security Suite 6

1. Ihr sollt als Paßwort weder den Namen Eurer Frau, Eures Mannes, Eures Hundes oder Eures Goldfischs verwenden.
2. Ihr sollt nicht das Datum Eurer Geburt oder den Ort Eurer Heims als Paßwort benutzen.
3. Ihr sollt nicht überall das gleiche Paßwort benutzen.
4. Ihr sollt uns spätestens nach einem Zeitraum von drei Monaten ändern.
5. Ihr sollt nicht hochkomplizierte Buchstaben- und Zahlenkombinationen wie "123", "ABC", oder "007" verwenden.
6. Ihr sollt uns nicht "CODE", "GEHEIM" und schon gar nicht "PASSWORT" taufen.
7. Ihr sollt uns nicht in einer Datei mit dem Namen PASSWORT.COD speichern.
8. Ihr sollt uns nicht dann eingeben, wenn Euch gerade 27 Kollegen über die Schulter blicken.
9. Ihr sollt uns nicht auf einen Post-it-Zettel schreiben und diesen auf Euren Monitor, Euren Rechner oder unter Eure Tastatur kleben.
10. Ihr sollt, wenn Ihr uns schon aufschreiben müßt, diese Notiz an einem wirklich sicheren Ort aufheben.

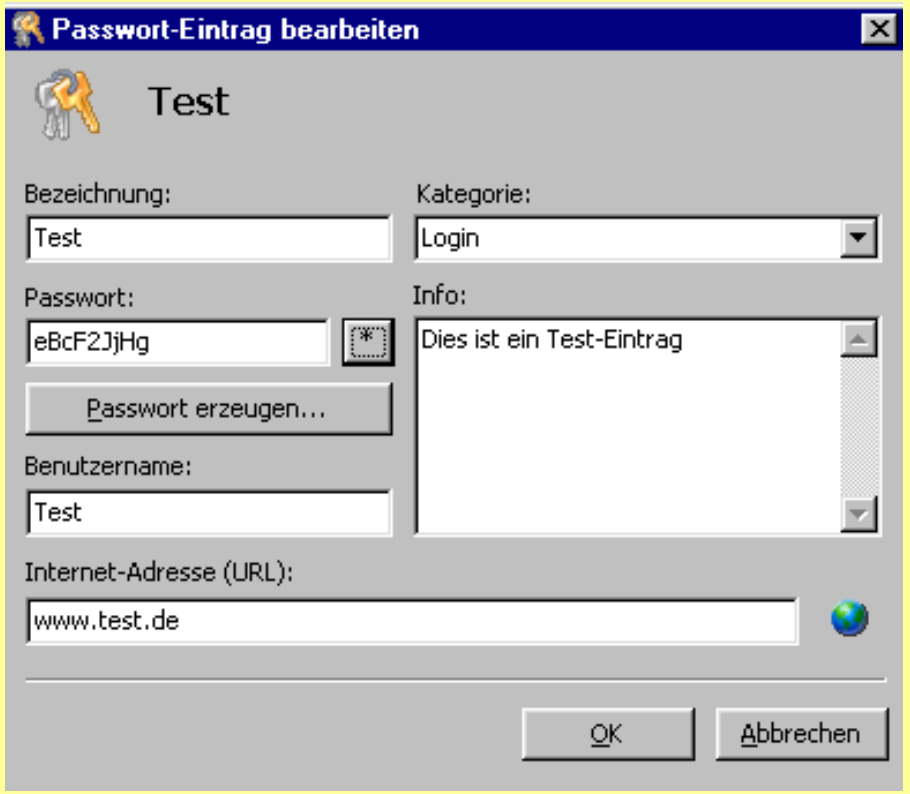
http://www.hirschbeutel.de/password.html

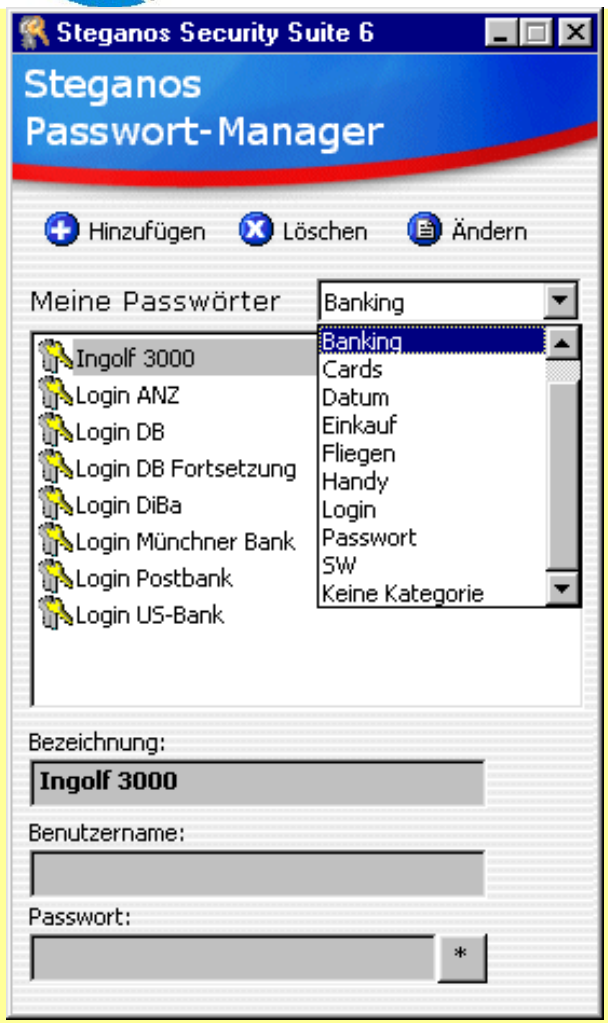
01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Passwörter für Bankverkehr, eBay, Logins, Pins etc. kann man in einem Passwortsafe speichern. Dieser kann nur über ein Masterpasswort geöffnet werden.

Ein Masterpasswort kann auf einem USB-Token oder einer Smart-Card gespeichert werden.

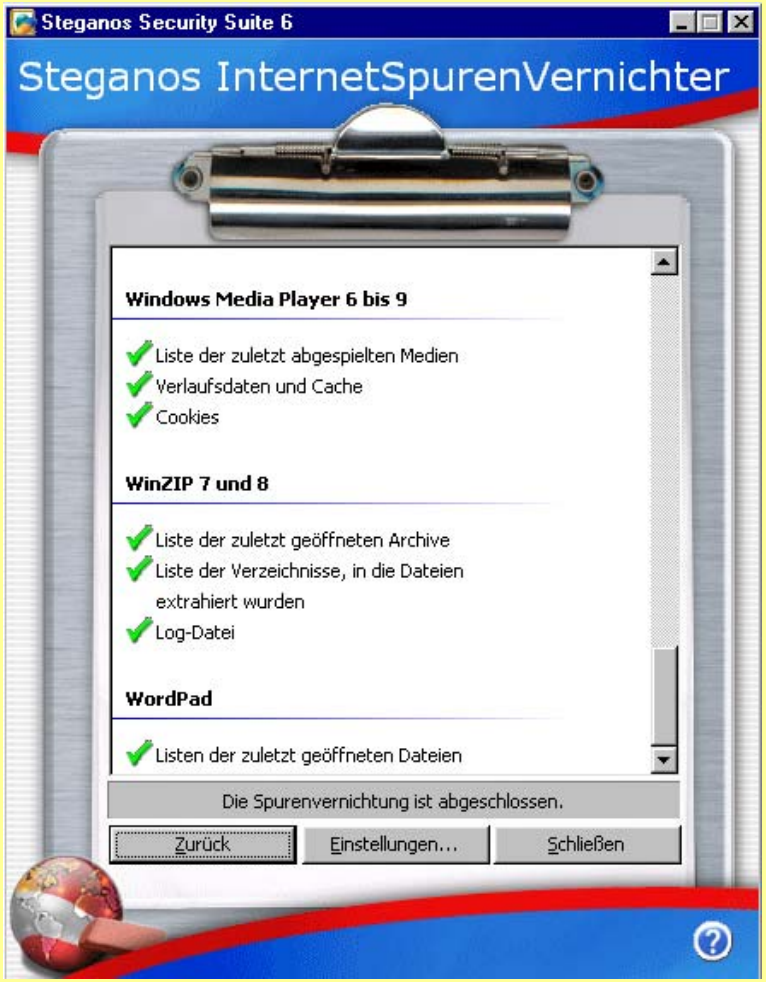
Der Passwortsafe, kann als Ganzes auf einem USB-Stick gespeichert werden





- **Datum =** aktueller Stand
- **Banking** Bank Logins
- **Cards** ADAC, TKK, EC, etc.
- **Einkauf** Amazon, eBay, etc.
- **Fliegen** LH Miles&More, BA, etc.
- **Handy** Pins
- **Login** Provider, ADAC, Mucl, etc.
- **Passwort** PC-/ Laptop-Logins
- **SW** Seriennr., etc.
- **Keine Kategorie** leer

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

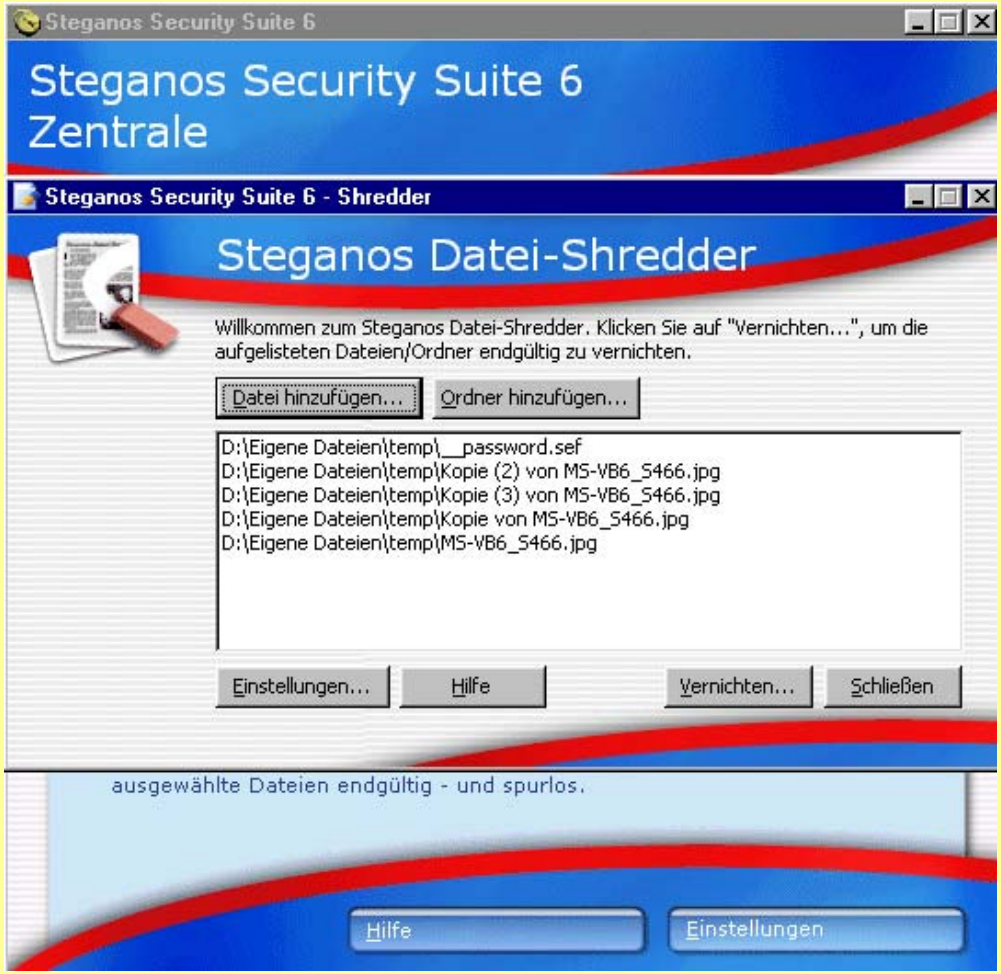


Viele Programme hinterlassen Spuren, Caches, Verlaufslisten, Cookies usw. .

Andere können herauslesen was man besucht oder getan hat.

Diese Spuren kann ich löschen lassen.

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

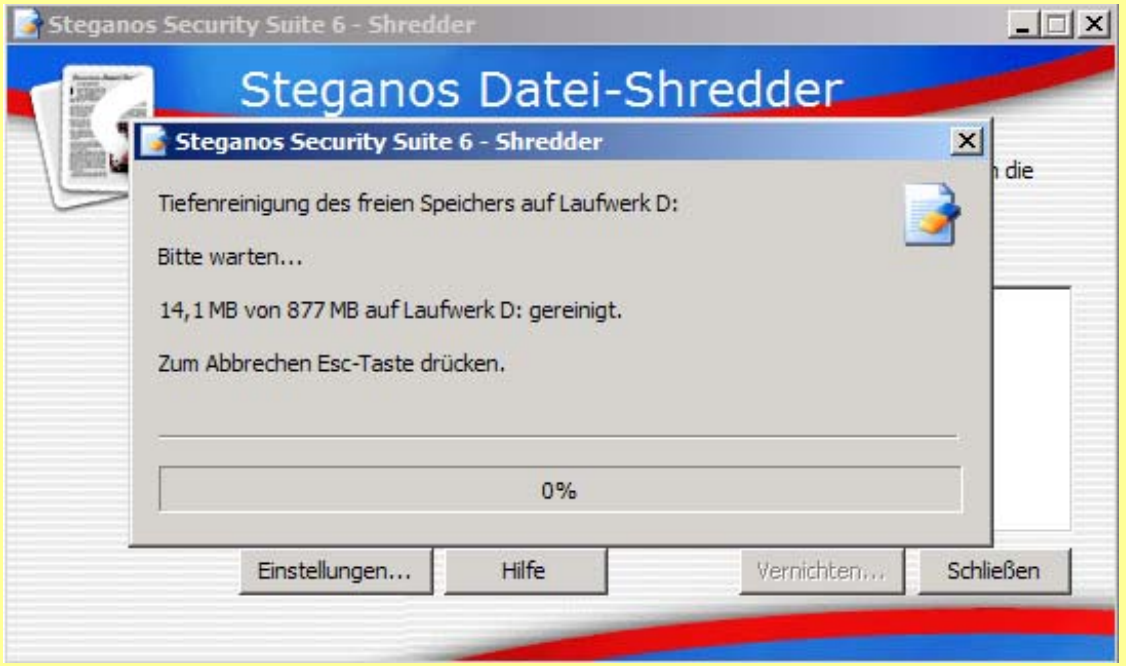


Der Shredder löscht Dateien nicht nur aus dem Dateiverzeichnis, sondern überschreibt den Dateibereich mehrfach.

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Überschreiben des freien Bereiches

So etwas ähnliches muss Max Strauss mit seiner Festplatte gemacht haben!



- Passwort-Manager -> Ton-/Bild-Datei verstecken
  -> als E-Mail exe verstecken
  ->-> auf CD / DVD
  -> USB-Stick
  -> Smart-Card
- Safe oder Portable Safe
  -> als E-Mail exe verstecken
  ->-> auf CD / DVD
  -> USB-Stick
  -> Smart-Card

https - Aufbau einer sicheren Verbindung über das Internet

- https - Verbindung beim Banking
- Protokolle SSL2; SSL3; TSL
- HBCI - Verbindung beim Banking
- Wozu benötigt https Zertifikate
- Was sind digitale Signaturen
- Was sollte ich als Anwender beachten um die Sicherheit nicht zu gefährden

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Sicherheit

SSL 2.0 benutzen

Gibt an, ob Sie verschlüsselte Informationen über SSL2 (Secure Sockets Layer Level 2) senden und empfangen möchten. Dies ist das Standard-Protokoll für sichere Übertragungen und wird von allen sicheren Websites unterstützt.

SSL 3.0 benutzen

Gibt an, ob Sie verschlüsselte Informationen über SSL3 (Secure Sockets Layer Level 3) senden und empfangen möchten; ein Protokoll, das noch sicherer ist als SSL2, aber von einigen Websites nicht unterstützt wird.

TLS 1.0 benutzen

Gibt an, ob Sie verschlüsselte Informationen über TLS (Transport Layer Security) senden und empfangen möchten; ein offener Sicherheitsstandard ähnlich SSL3, der aber von einigen Websites nicht unterstützt wird.

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Zertifikate

Zertifikate helfen dabei, Verschlüsselung und Entschlüsselung von Verbindungen zu sicheren Websites aufzubauen.

Client-Zertifikatswahl

Wenn eine Website eine sichere Verbindung herstellen möchte, wird Firefox standardmäßig automatisch ein geeignetes Zertifikat benutzen. Falls Sie lieber ein Zertifikat manuell auswählen möchten (falls Sie z. B. eine bestimmte Verschlüsselungsart anstelle der automatisch ausgewählten benutzen möchten), markieren Sie die Einstellung *Jedes Mal fragen*. Dadurch haben Sie die komplette Kontrolle darüber, welche Zertifikate während des Browsens benutzt werden.

Zertifikate verwalten

Klicken Sie auf *Zertifikate verwalten...* um die gespeicherten Zertifikate einzusehen, neue Zertifikate zu importieren, oder um alte Zertifikate zu sichern oder zu löschen.

Kryptographie-Module verwalten

Kryptographie-Module können Verbindungen verschlüsseln und entschlüsseln sowie Zertifikate und Passwörter speichern. Falls Sie ein anderes Kryptographie-Modul als das in Firefox benutzen müssen oder um Ihr Master-Passwort zu ändern, klicken Sie auf *Kryptographie-Module verwalten...*

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Validierung

Validierung stellt sicher, dass Zertifikate in Firefox nicht veraltet sind.

CRL

Firefox kann CRLs (Certificate Revocation Lists) benutzen, um sicherzustellen, dass Ihre Zertifikate nicht ungültig sind. Falls Sie ein CRL hinzufügen möchten oder Ihre bereits installierten CRLs einsehen möchten, klicken Sie auf *CRLs verwalten*.

OSCP

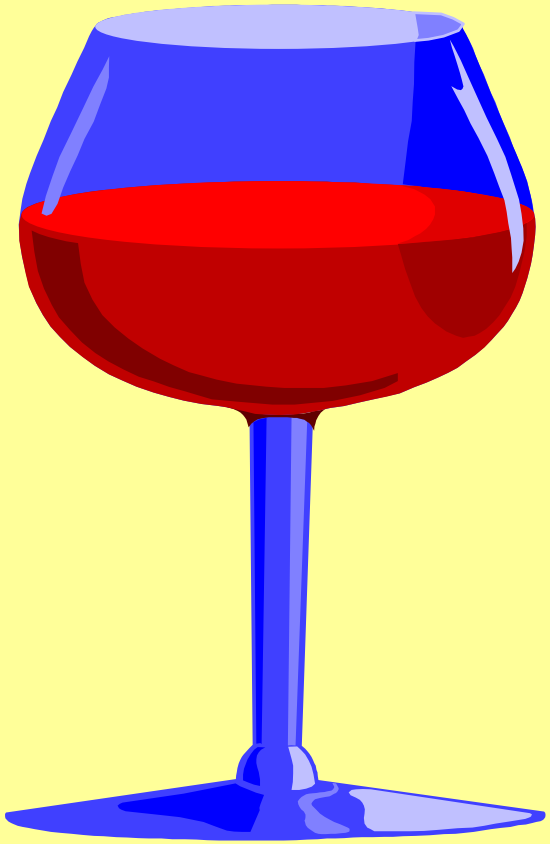
OCSP (Online Certificate Status Protocol) ermöglicht es, daß Zertifikate jedes Mal, wenn Sie betrachtet oder benutzt werden, validieren werden. Firefox verwendet OSCP standardmäßig nicht. Aber wenn Sie es aktivieren möchten, können Sie das hier tun. Sie werden dies wohl nur ändern müssen, falls Ihre Internet-Umgebung das verlangt.

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Weitere mögliche Vortragsthemen (bei Interesse).

- https (SSL, Zertifikate, digitale Signaturen)
- WLAN (Hacking, Hotspots, etc.)
- Registry – das Gehirn von Windows
- IT-Security: Wie schütze ich meinen PC?
- Digitale Bilder fürs Web-Album aufbereiten
- CD & DVD-Authoring (Diashows, Filme, Aufbau)

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De



Fragen und Diskussion

01.02.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De