Don Quixote meets Big Brother

Jochim Selzer, j.selzer@bonn-evangelisch.de

Ich sehe was, was du nicht siehst

- Warum wir Geheimnisse haben
- Warum wir sie haben dürfen
- Wie wir sie bewahren

Ich sehe was, was du nicht siehst

- Warum wir Geheimnisse haben
- Warum wir sie haben dürfen
- Wie wir sie bewahren
- Warum das alles nicht so recht funktioniert

Ich sehe was, was du nicht siehst

- Warum wir Geheimnisse haben
- Warum wir sie haben dürfen
- Wie wir sie bewahren
- Warum das alles nicht so recht funktioniert
- Warum wir es dennoch versuchen sollten

Warum wir Geheimnisse haben

Warum wir Geheimnisse haben

- Weil wir es dürfen

Warum wir Geheimnisse haben

- Weil wir es dürfen
  - GG Art 1 und 2
  - BDSG
  - Volkszählungsurteil
  - Trojanerurteil

Warum wir Geheimnisse haben

- Weil wir es dürfen
  - GG Art 1 und 2
  - BDSG
  - Volkszählungsurteil
  - Trojanerurteil
- Weil wir es sollten
  - PINs, private Telefonnummern etc.
  - Beeinflussbarkeit, Berechenbarkeit

Grundlagen der Datenerhebung

- Datenvermeidung und -sparsamkeit (§ 3a)
- Wer erhebt was warum (§ 4)
- Freiwilligkeit (§ 4a)
- Auskunftspflicht (§ 19)
- Benachrichtigungspflicht (§ 19a)
- Berichtigung, Löschung, Sperrung, Widerspruch (§ 20)

Maßnahmen

1) Zutrittskontrolle
2) Zugangskontrolle
3) Zugriffskontrolle
4) Weitergabekontrolle
5) Eingabekontrolle
6) Auftragskontrolle
7) Verfügbarkeitskontrolle
8) Trennung

Grundsätzliche Strategien

- Nur das Nötigste angeben
- Wegwerfadressen
- Phantasie beim Ausfüllen von Formularen
- Viele verschiedene Nutzernamen und Passwörter

Sicherheit und Open Source

Sicherheit und Open Source

- Sicherheit ohne offene Quellen ist russisches Roulette

- Kerckhoffs’ Prinzip
  http://de.wikipedia.org/wiki/Kerckhoffs%E2%80%99_Prinzip

Truecrypt

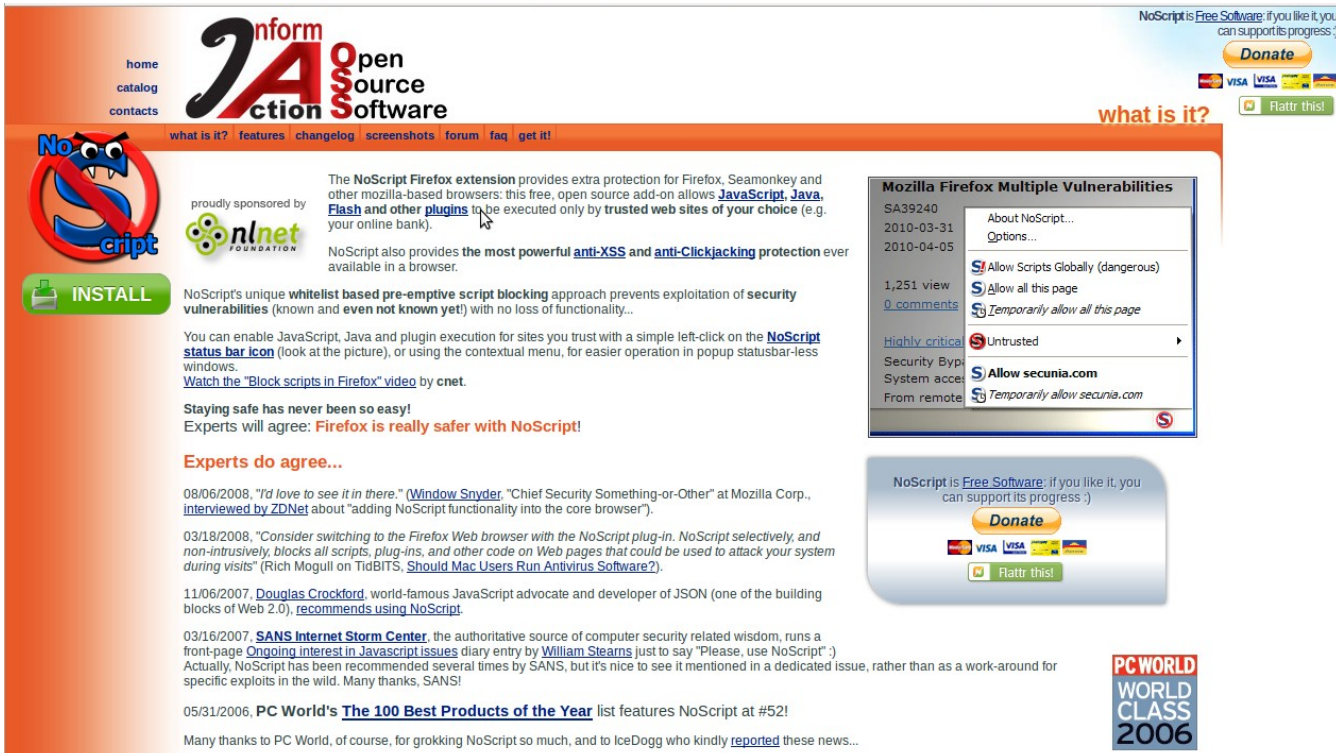
- Festplattenverschlüsselung
- Cryptocontainer
- Hidden volumes
- Plausible deniability
- Kein aufwendiges Löschen der Daten beim Abgeben des Datenträgers nötig

Truecrypt

- Festplattenverschlüsselung
- Cryptocontainer
- Hidden volumes
- Plausible denyability
- Kein aufwendiges Löschen der Daten beim Abgeben des Datenträgers nötig

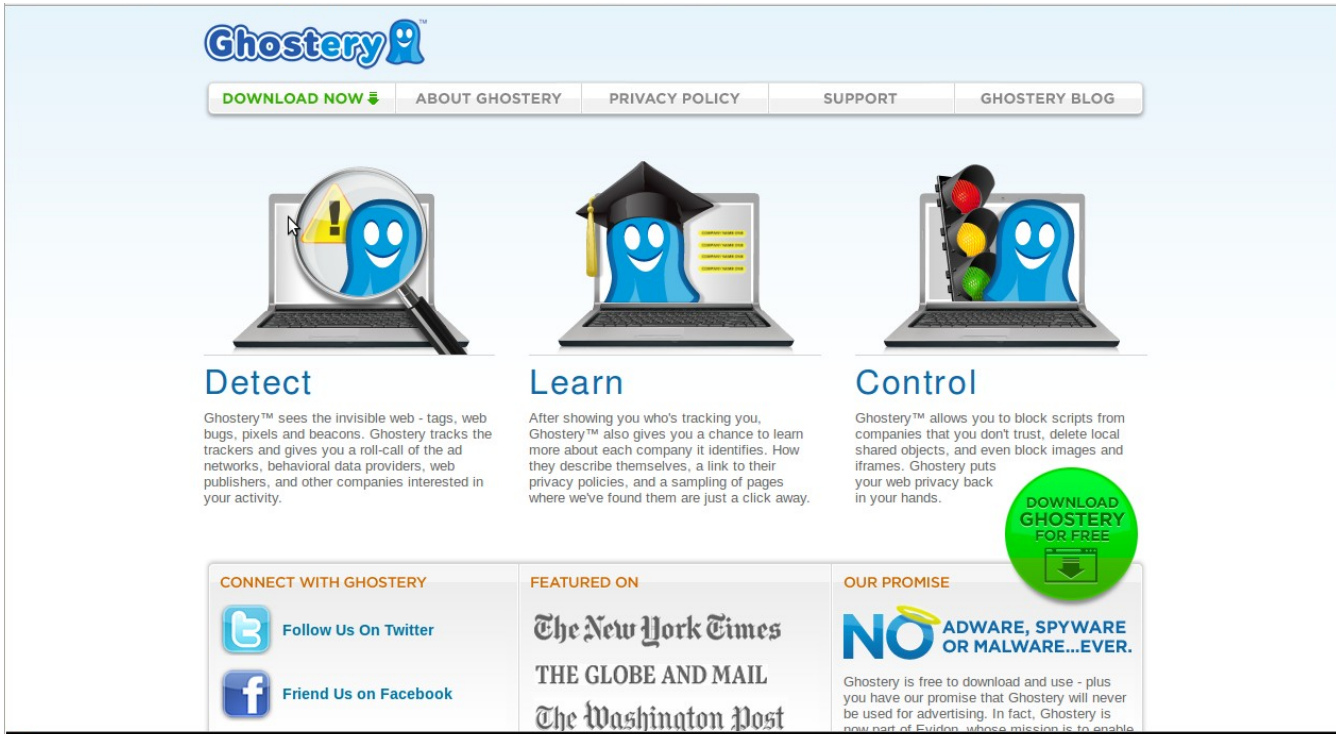
- Sicherheit hängt von der Güte des Passworts ab

NoScript



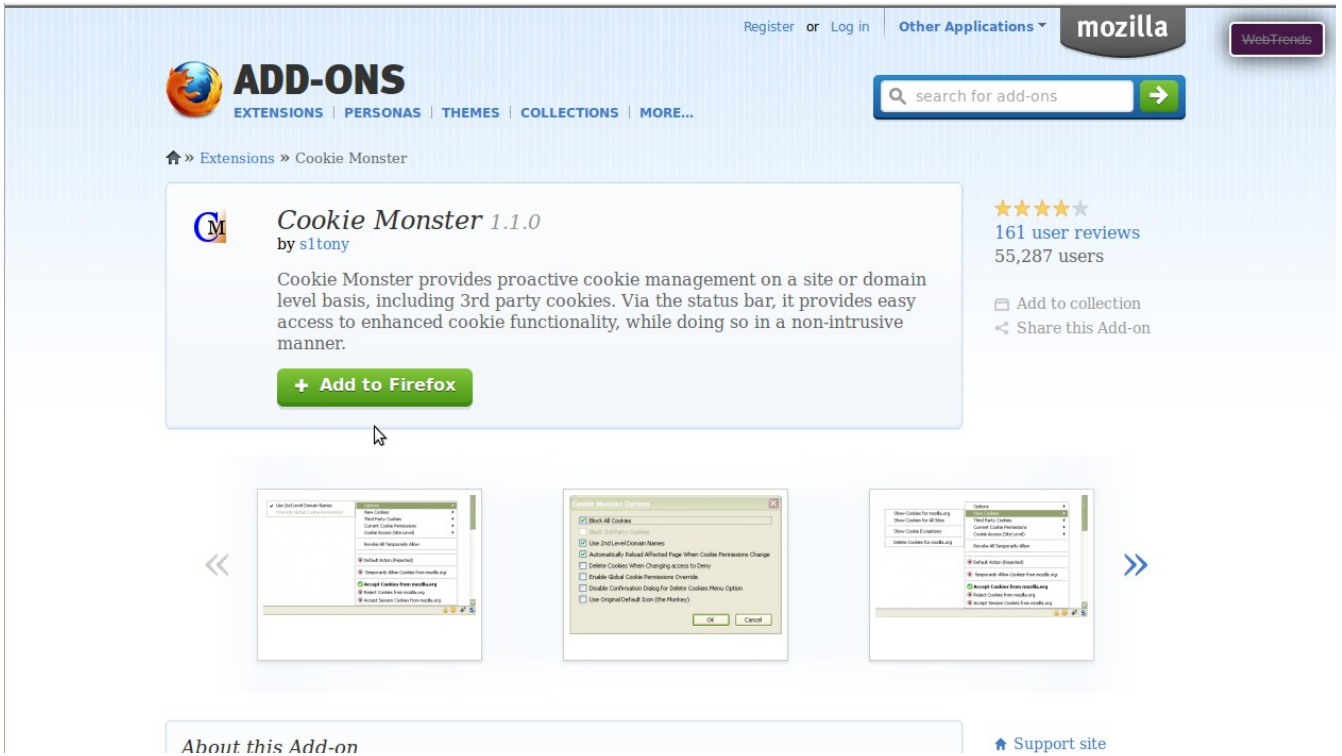
+ Blockiert Javascript
+ Blockiert gefährliche Konstrukte
- Umständliches Freischalten

Ghostery



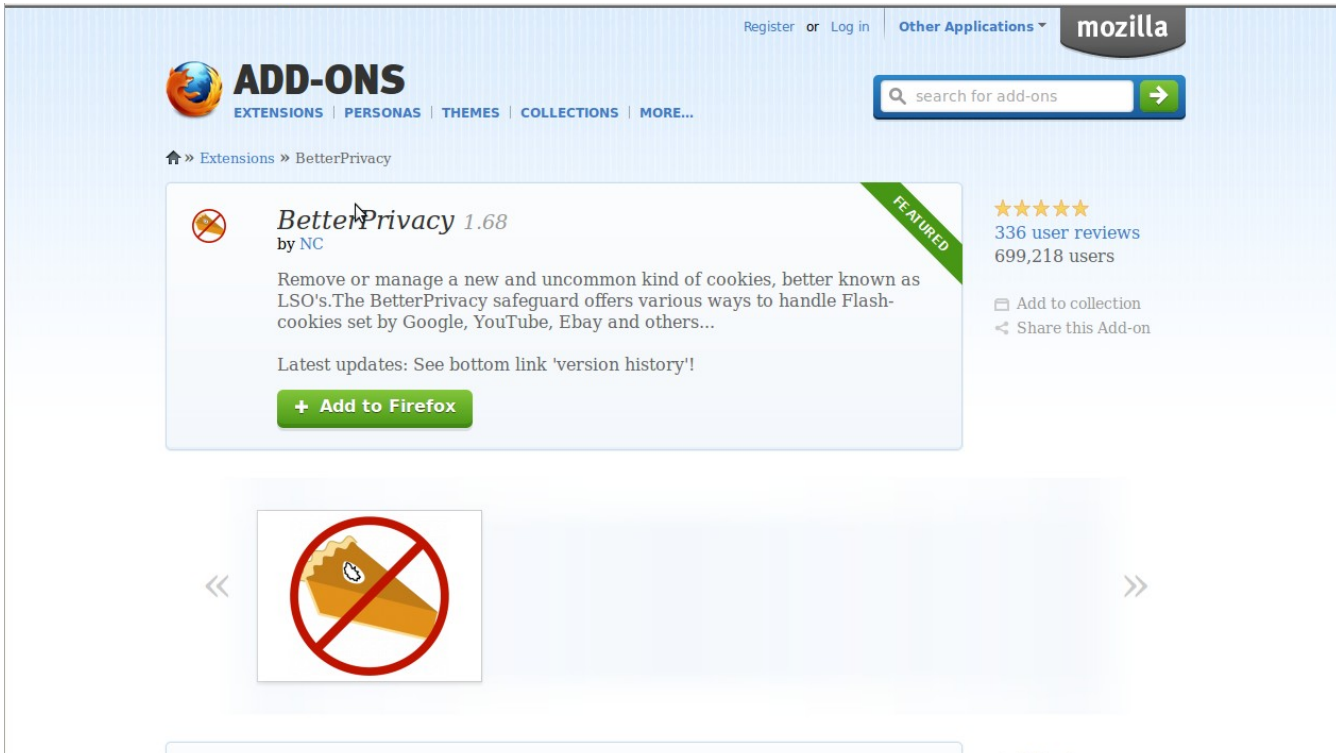
+ Blockiert Usertracking
- Blockiert nur bekannte Tracker

Cookie-Blocker

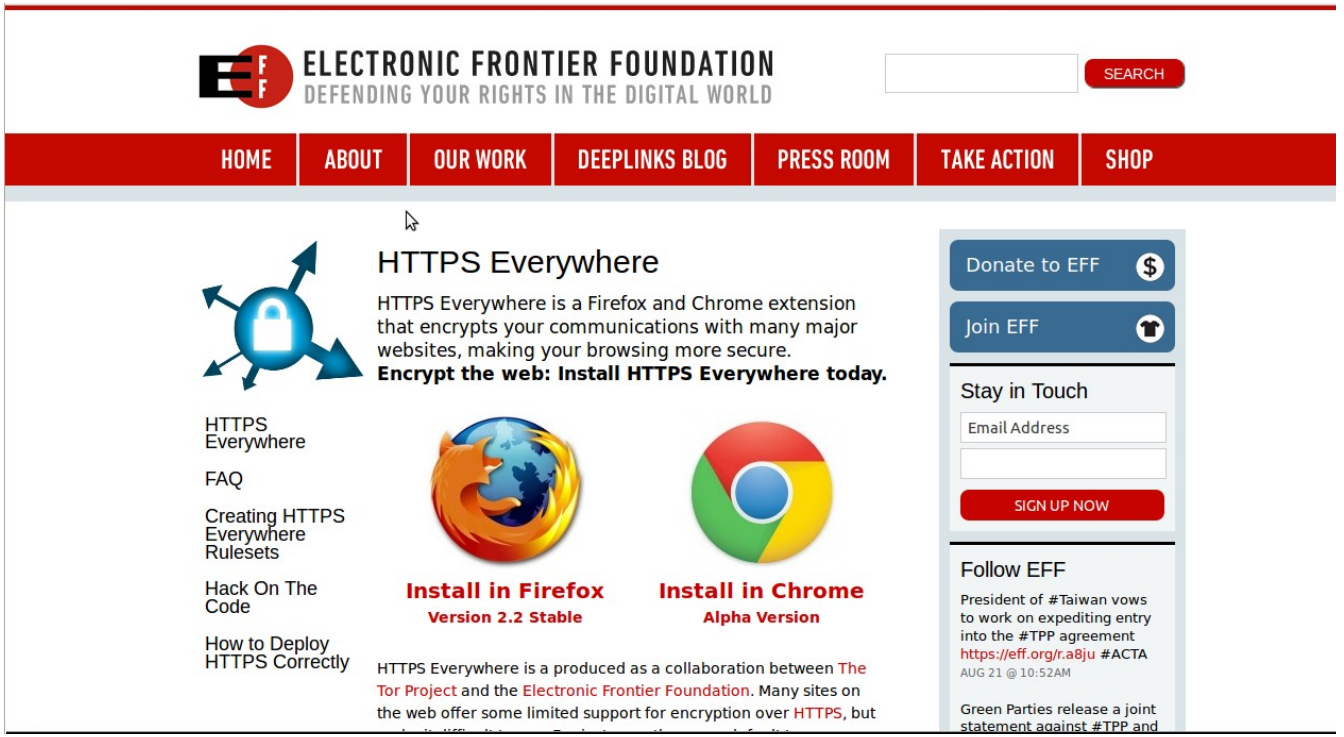


+ Blockiert Cookies
- Manuelles Freischalten sinnvoller Cookies

Better Privacy



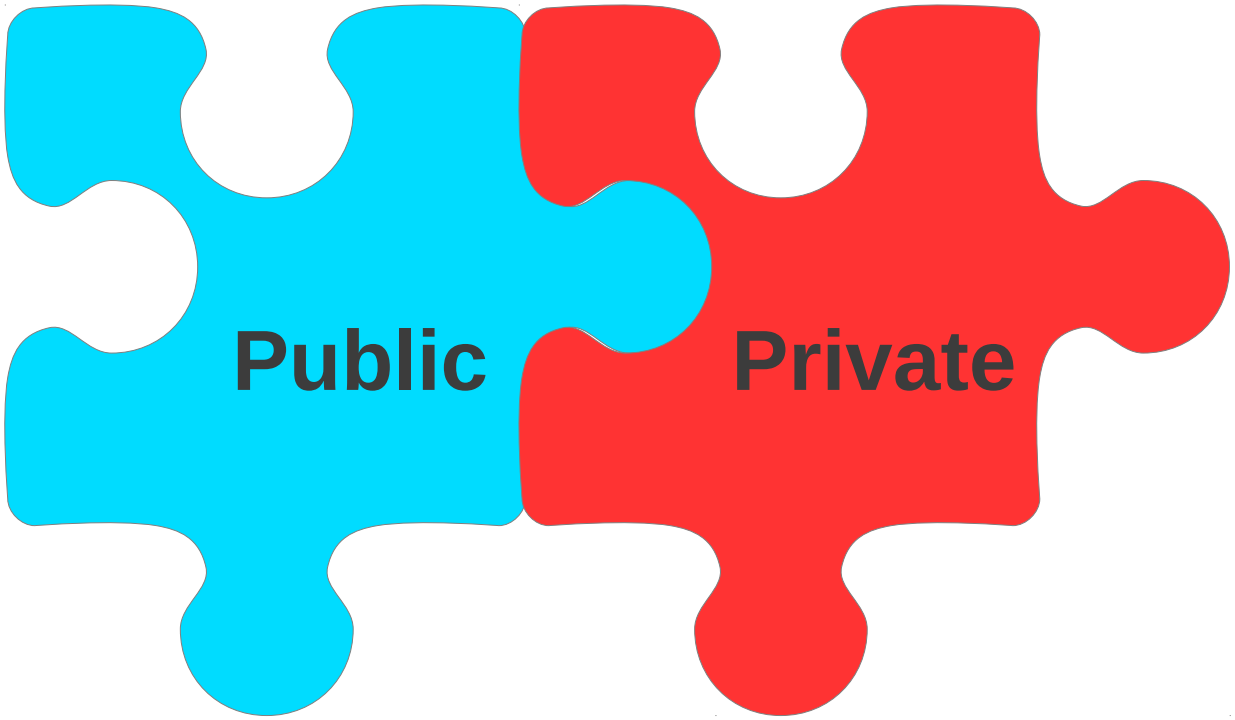
HTTPS everywhere



Tor

- Anonymisiert
- Anti-Zensur-Werkzeug (u.a. durch hidden Network)
- Anonymität natürlich nur bis zum ersten Login auf einer Seite

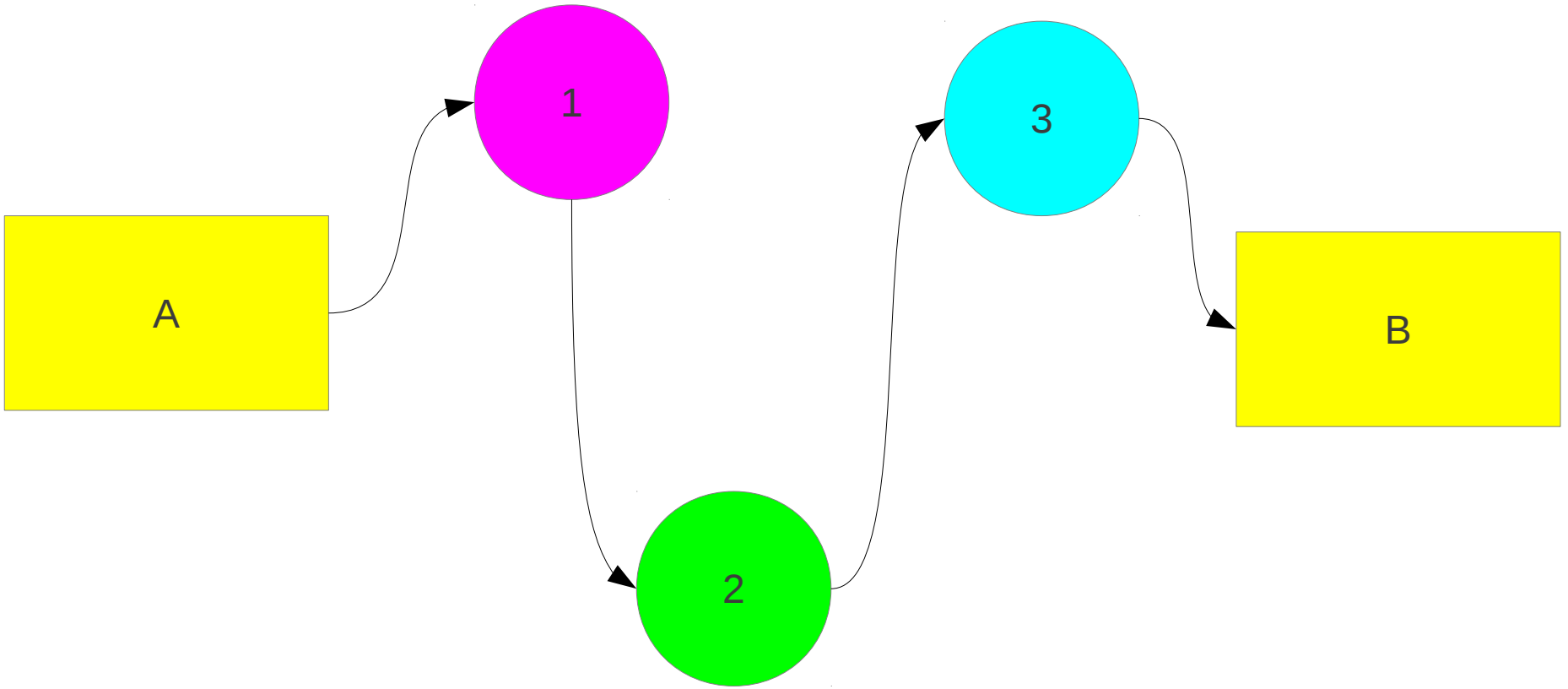
Asymmetrische Verschlüsselung



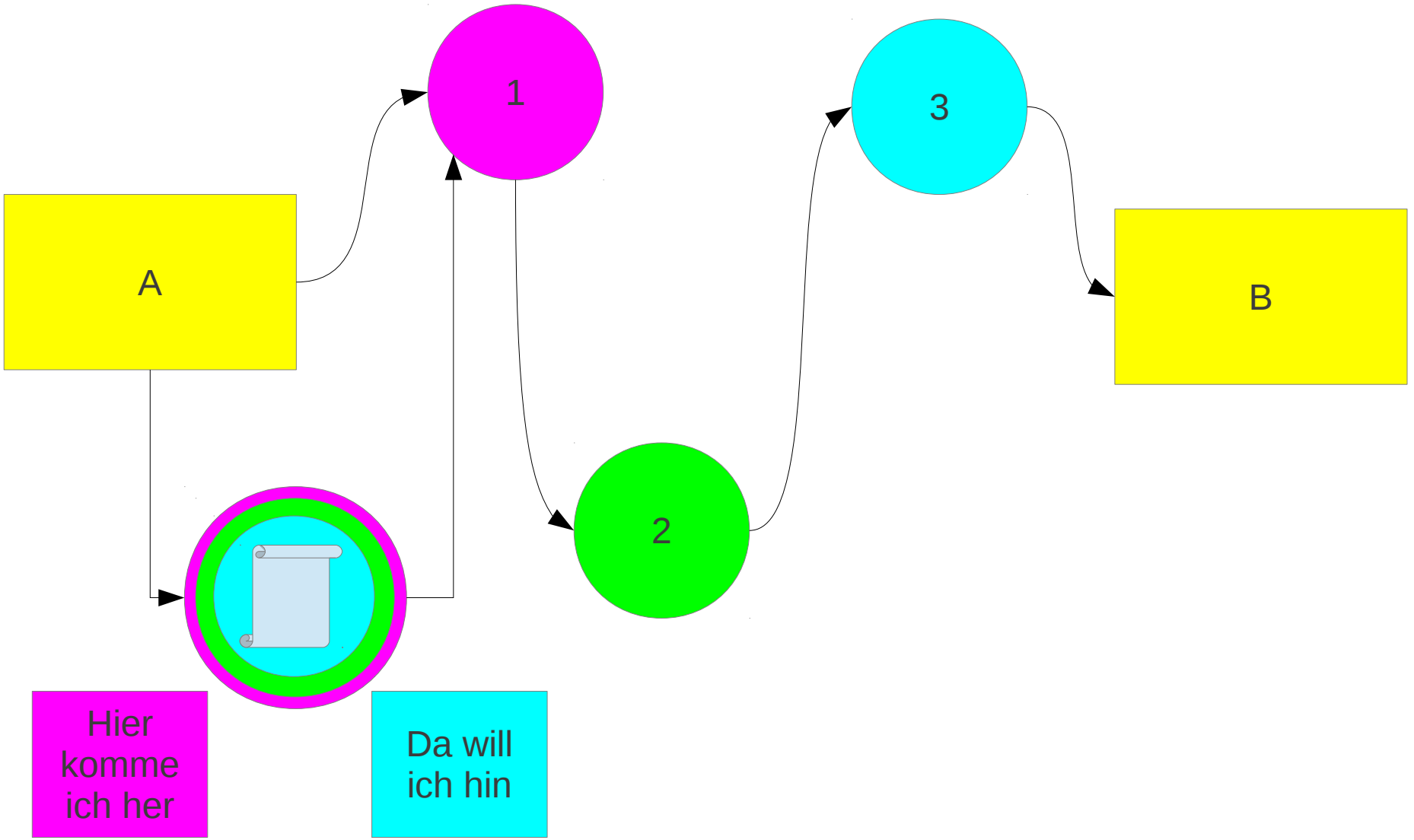
- Kann und soll veröffentlicht werden
- Kann nur verschlüsseln
- Kann Signaturen prüfen

- Muss geheim bleiben
- Kann entschlüsseln
- Kann Signaturen erzeugen

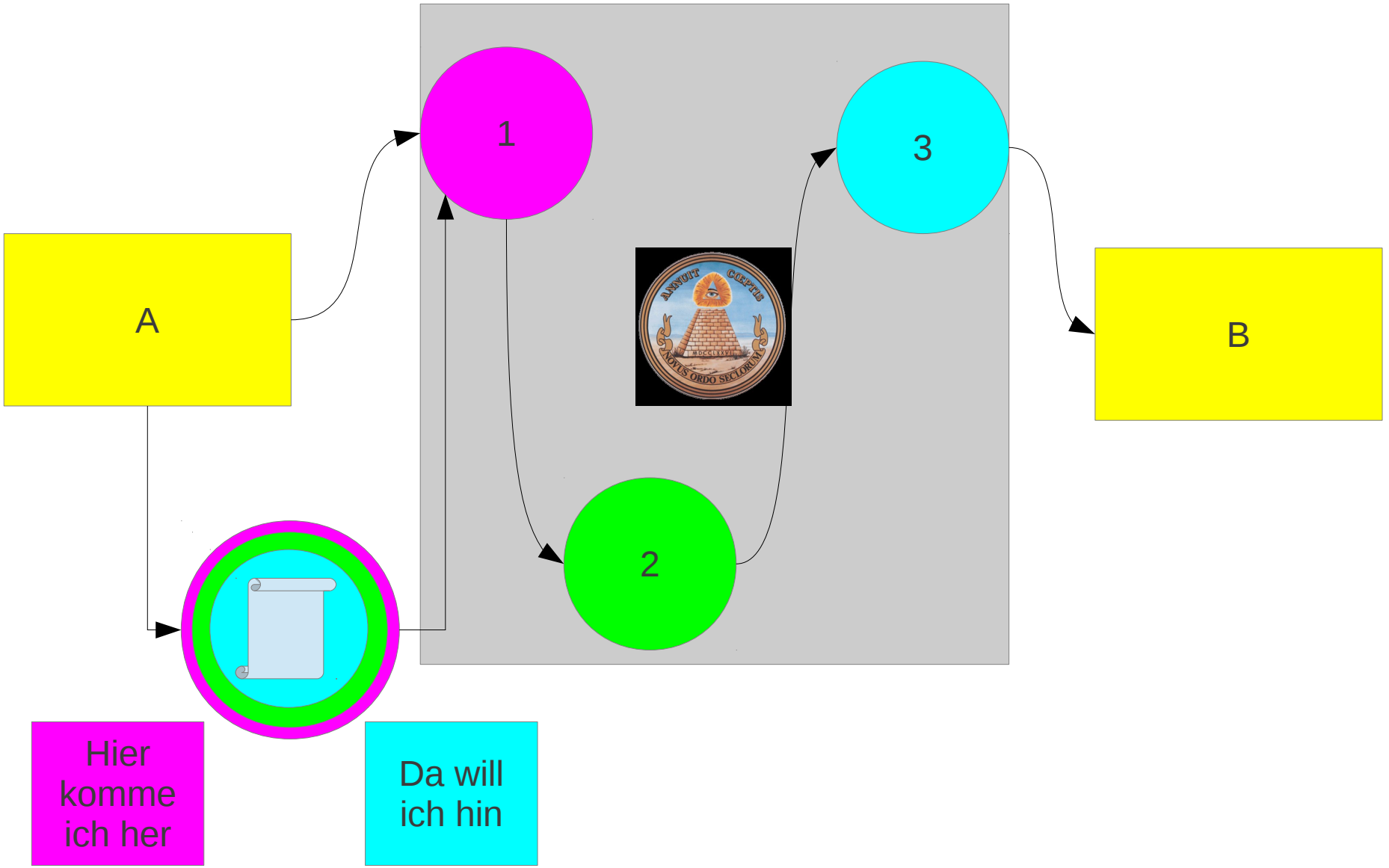
Proxykaskaden



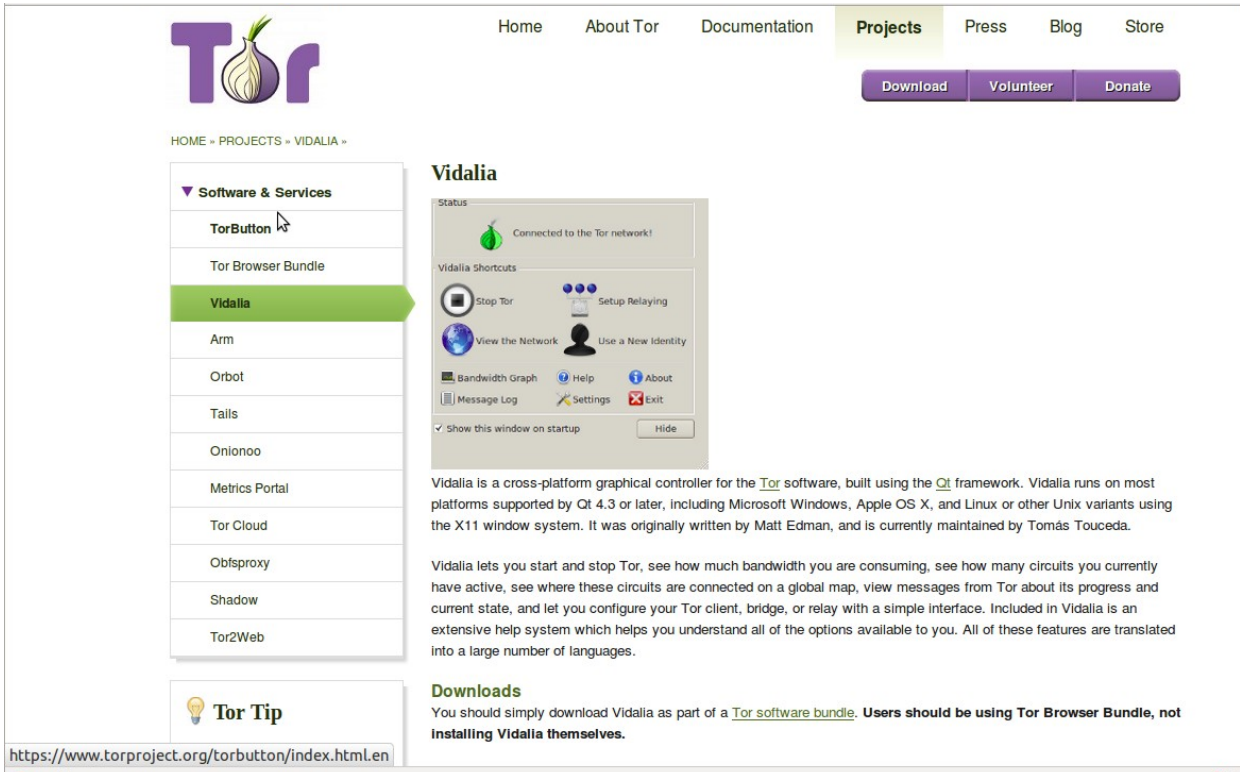
Proxykaskaden



Proxykaskaden



Vidalia



Grafische Oberfläche für Tor

Privoxy

Privoxy - Home Page

Privoxy is a non-caching web proxy with advanced filtering capabilities for enhancing privacy, modifying web page data and HTTP headers, controlling access, and removing ads and other obnoxious Internet junk. Privoxy has a flexible configuration and can be customized to suit individual needs and tastes. It has application for both stand-alone systems and multi-user networks.

Privoxy is Free Software and licensed under the GNU GPLv2.

Privoxy is an associated project of Software in the Public Interest (SPI).

Helping hands and donations are welcome:

- http://www.privoxy.org/faq/general.html#PARTICIPATE
- http://www.privoxy.org/faq/general.html#DONATE

The most recent release is 3.0.19 (stable).

Download

- Download recent releases
- Quickstart after installation

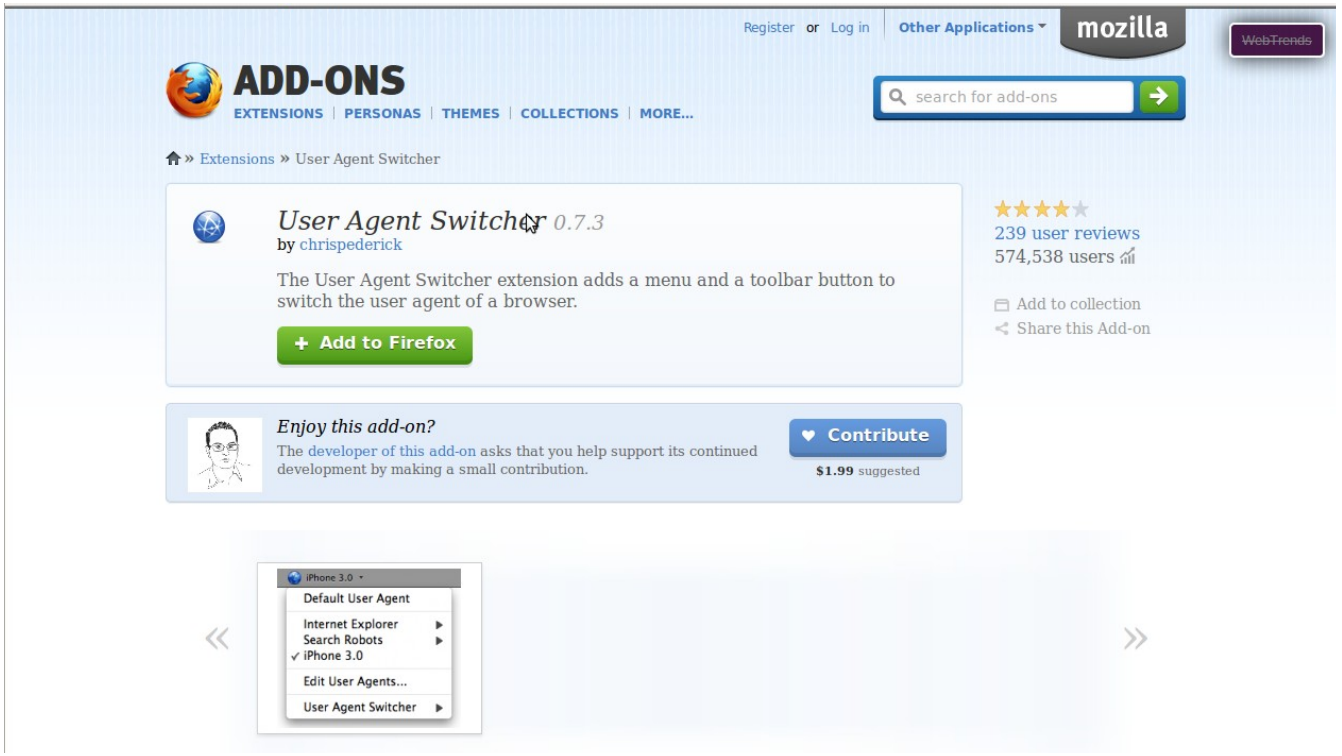
Documentation

- User manual
- Frequently Asked Questions
- Developer Manual

- Zusatzwerkzeug für Tor
- Kann bei Bedarf Headerdaten manipulieren
- Kann Zugriff auf gefährliche Inhalte sperren

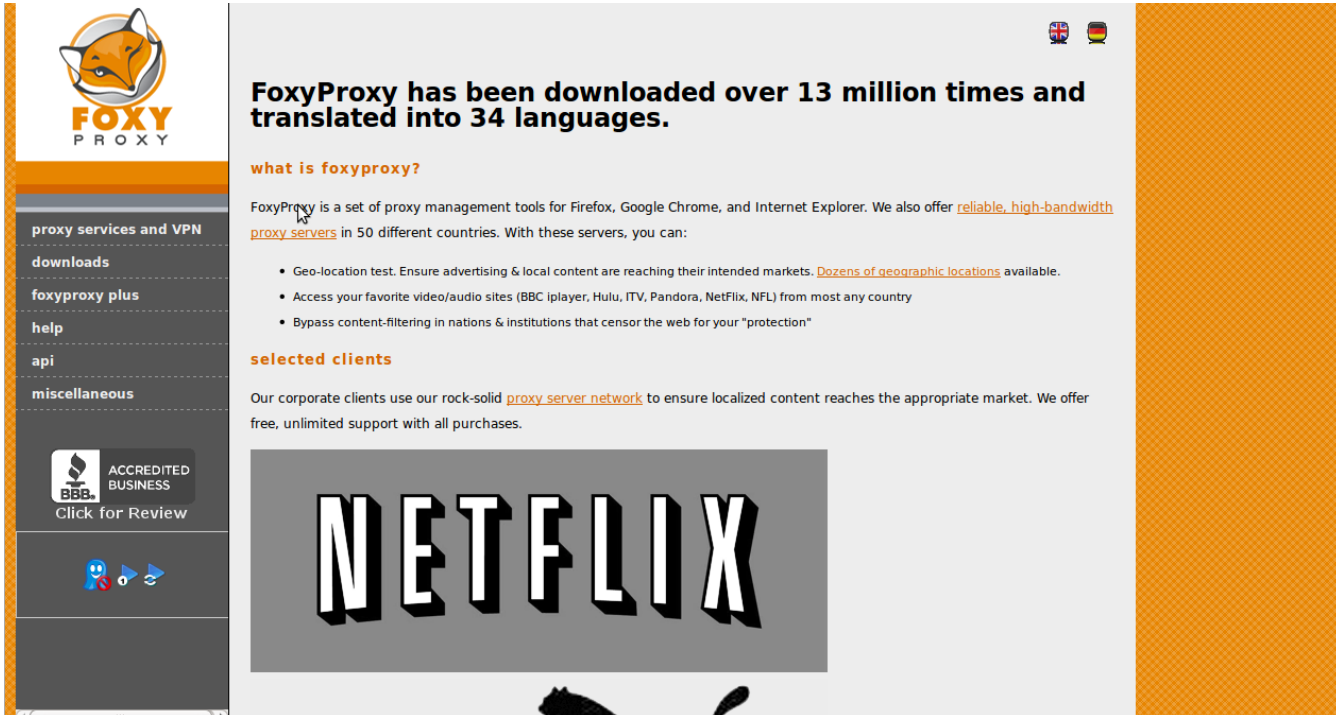
- Headerdatenmanipulation funktioniert nicht richtig

User Agent Switch



Fälscht Browserkennung

Foxyproxy


FOXY
PROXY
proxy services and VPN
downloads
foxyproxy plus
help
api
miscellaneous
ACCREDITED BUSINESS
Click for Review
FoxyProxy has been downloaded over 13 million times and translated into 34 languages.
what is foxyproxy?
FoxyProxy is a set of proxy management tools for Firefox, Google Chrome, and Internet Explorer. We also offer reliable, high-bandwidth proxy servers in 50 different countries. With these servers, you can:
Geo-location test. Ensure advertising & local content are reaching their intended markets. Dozens of geographic locations available.
Access your favorite video/audio sites (BBC iplayer, Hulu, ITV, Pandora, NetFlix, NFL) from most any country
Bypass content-filtering in nations & institutions that censor the web for your "protection"
selected clients
Our corporate clients use our rock-solid proxy server network to ensure localized content reaches the appropriate market. We offer free, unlimited support with all purchases.
NETFLIX

Die Kehrseite

- Wir bekämpfen ein politisches Problem (mangelnder Datenschutz, Zensur) mit technischen Mitteln
- Proxykaskaden sind langsam
- Das hidden Network arbeitet unzuverlässig
- I2p kann es auch nicht besser
- Anonymisierung auf Netzwerkebene reicht nicht

Anonym durch Proxy-IPs?

23.42.47.11 - **myuser** [22/Aug/2012:00:01:46 +0200] "GET /wcmsrepo/repo182460902/repo185314901/repoFolder177189079/repoFolder185692807/strategie_eng_265-150.jpg HTTP/1.1" 304 - "http://myhost/wcms/logistics/folder100577464/folder156818914/folder157231140/index" **"Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.1)"** myhost "BIGipServerpl_1.4.7.1-8080=2270644389.36895.0000; JSESSIONID=DZ152HN1XAI2DJKIK4GB5VQ; informationPersURL=http%3A//myhost/wcms/logistics/folder100577464/folder156818914/folder157231140/index; searchPersURL=http%3A//myhost/coin/templates/page/html/search_page.jsp%3Fcategory%3Dcontent%26q%3Dannouncement; networkPersURL=/coin/templates/page/html/network_page.jsp; helpPersURL=/coin/templates/page/html/help_page.jsp; request_uri=http%3A%2F%2Fmyhost%2F; Ticket=hash&j4RGhwB6x%2Ft5fJrEvKdmcwIWiSquxHDo5vK4g2o4IrXsVI9lBrN23SqGJ8Az4edNEArTHA%2BJ3JUE2B%2F3QORLwc4xtLD5ddya%2FHpAsVSUqhQpx1HVjEaJ%2FCAsOwvd0id3Lv4ZPKHfdE%2Fq49VIZ5kIQYMM0zIEsVaKzvgfawZHr%2Bo%3D&lang&spa&time&1345584656&ip&**23.42.47.11**&user&**myuser**&expires&1440" "resp:65822" "pid:18041"

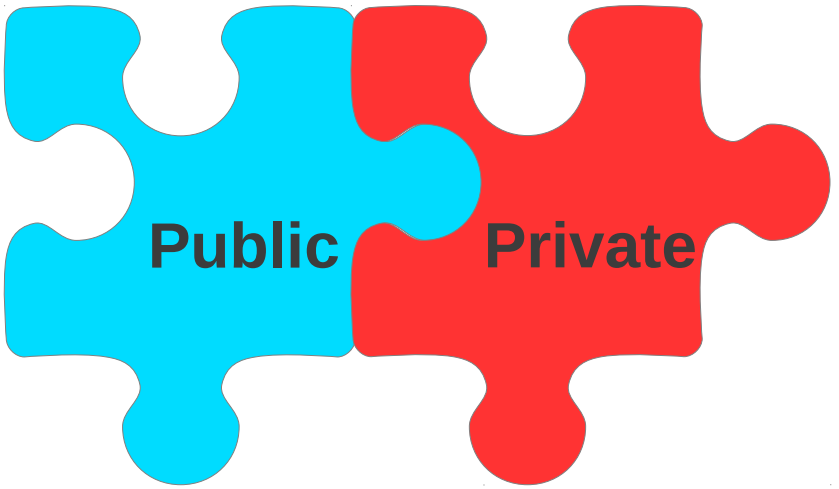
Anonym durch Proxy-IPs?

- Unternehmensweit gibt es zwei verschiedene Standardinstallationen: XP und Win 7
- User IDs im Log: **23632**
- Verschiedene User Agent Strings: **3710**
- Chance, einen User allein anhand seines Agent-Strings zu identifizieren: **1:6**

PGP

Public

Private



Schwachstellen

- Eigentlich müssten alle alles verschlüsseln

Schwachstellen

- Eigentlich müssten alle alles verschlüsseln
  - Private Key geht verloren
  - Passphrase geht verloren

Schwachstellen

- Eigentlich müssten alle alles verschlüsseln
  - Private Key geht verloren
  - Passphrase geht verloren
- Vertrauenswürdigkeit des Schlüssels schwer sicher zu stellen

Schlüsselverteilung

Wie kann ich sicher sein, dass ein öffentlicher Schlüssel wirklich der angeblichen Besitzerin gehört?

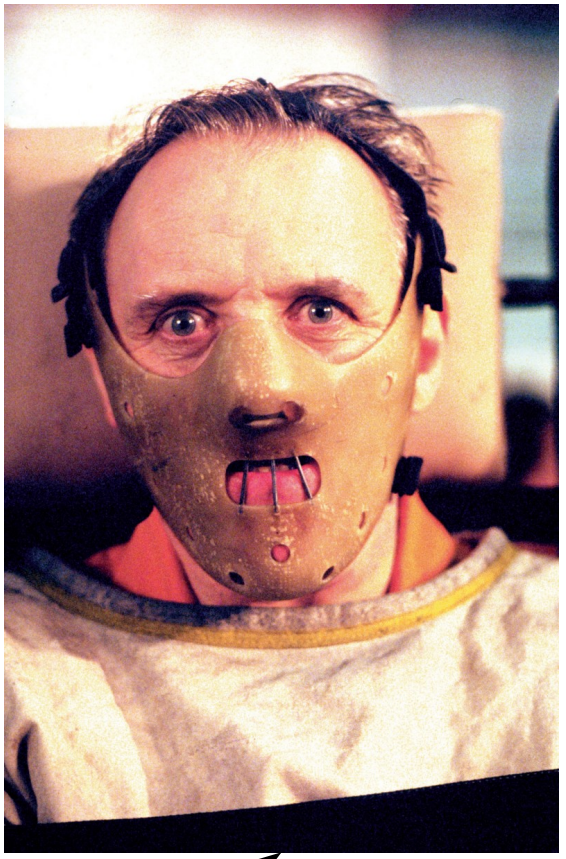
Schlüsselverteilung

Wie kann ich sicher sein, dass ein öffentlicher Schlüssel wirklich der angeblichen Besitzerin gehört?

Antwort:

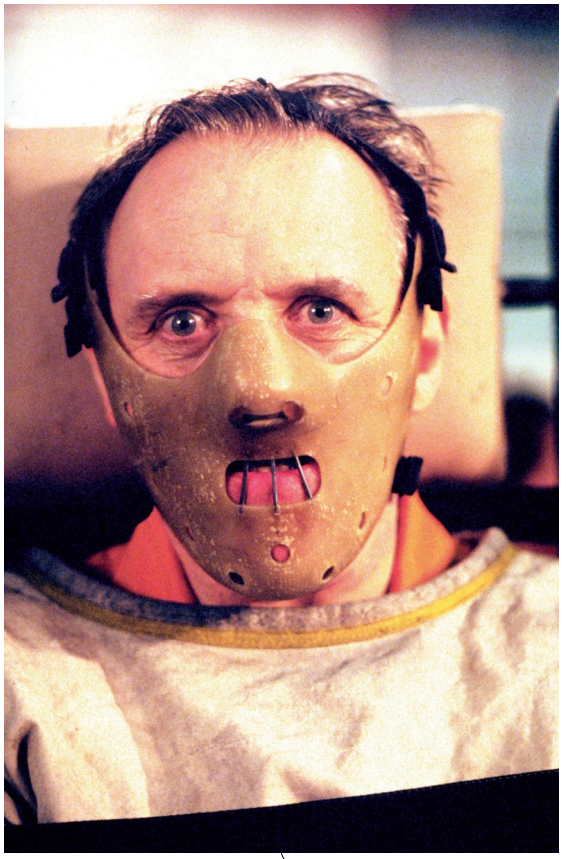
- Zentrale CA
- Web of Trust

Web of Trust



vertraut

Web of Trust



vertraut

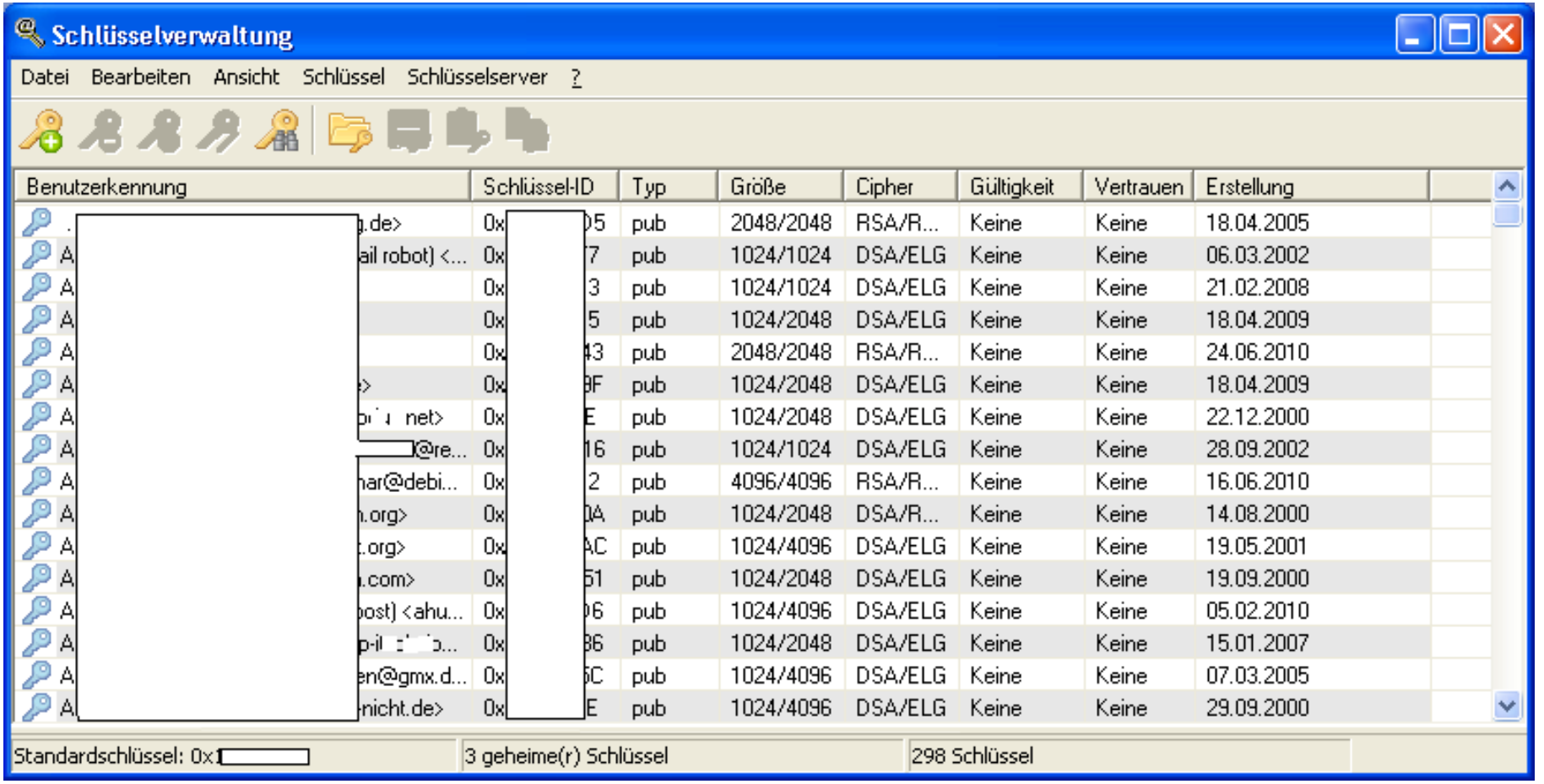
Web of Trust

vertraut

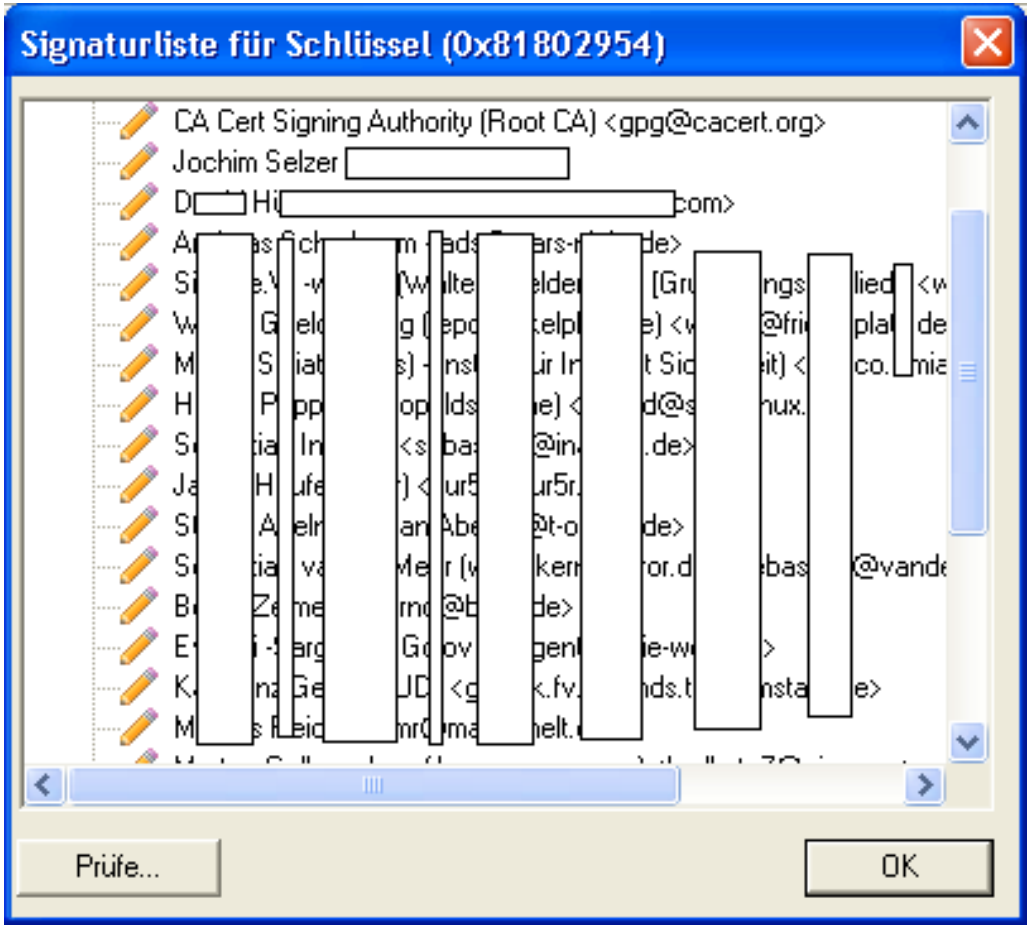
vertraut

vertraut

PKP-Schlüsselring



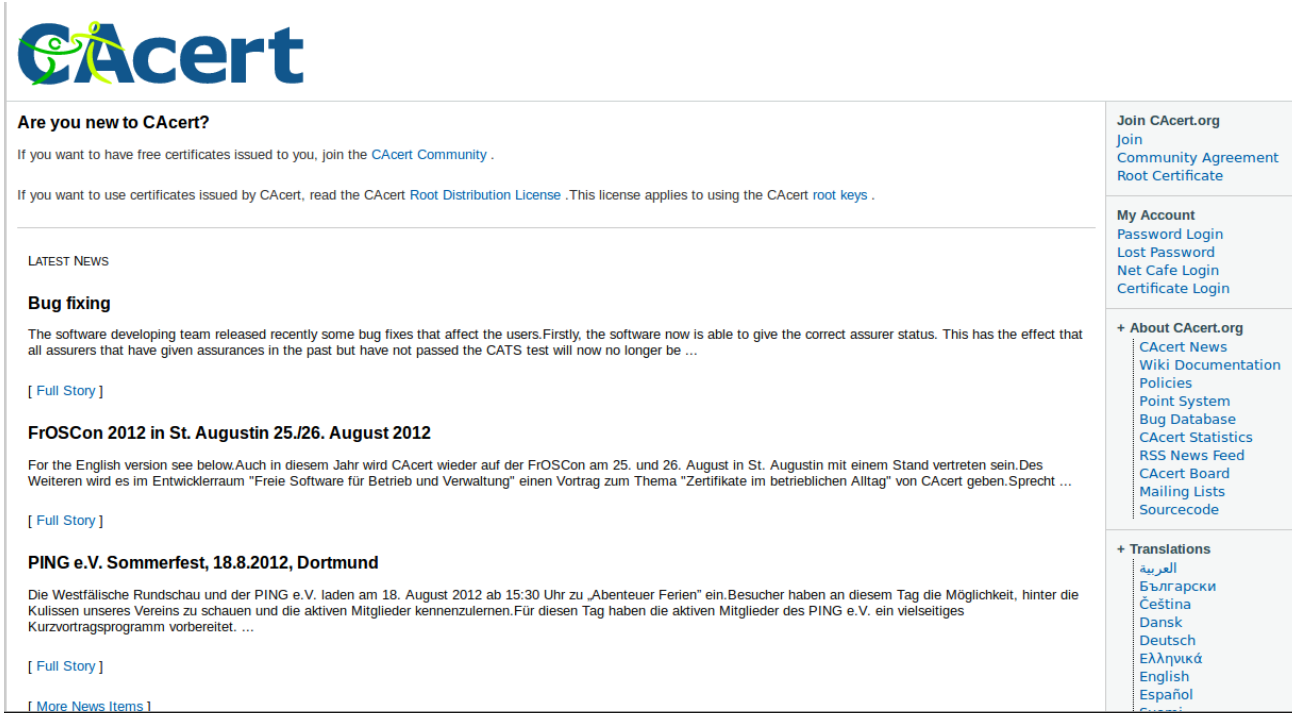
PGP-Signaturen



Enigmail

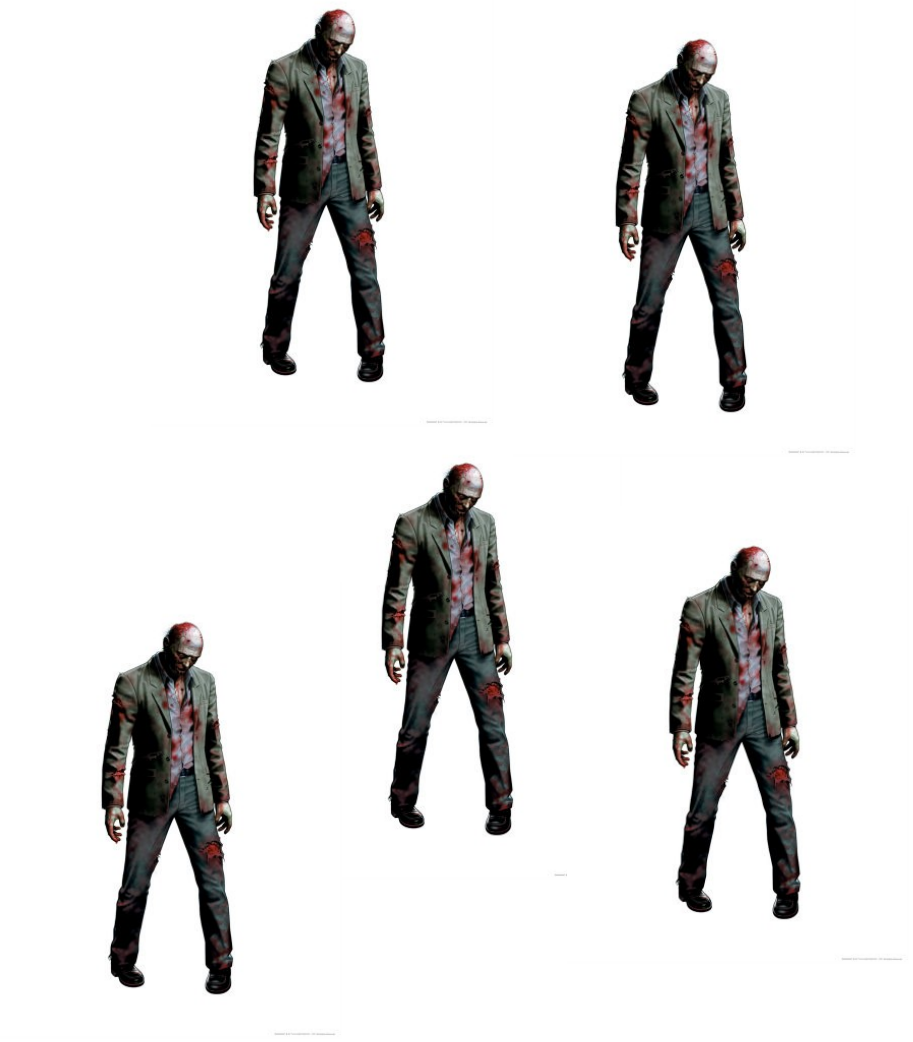

THE ENIGMAIL PROJECT
OPENPGP EMAIL SECURITY FOR MOZILLA APPLICATIONS
Home
Download
Documentation
Support
News
Links
search
A simple interface for OpenPGP email security
Download
v1.4.4 for Linux (32bit) on Thunderbird 14.0
Announcements
Enigmail has a new home
About Enigmail
Features
Screenshots
FAQ
Quick start guide
Handbook
Configuration
Community
Subscribe to the mailing list
Browse the list archives
Join the forums
Contact the dev team
What is this all about?
Enigmail is a security extension to Mozilla Thunderbird and Seamonkey. It enables you to write and receive email messages signed and/or encrypted with the OpenPGP standard.
Sending and receiving encrypted and digitally signed email is simple using Enigmail.
When starting it for the first time, you are guided through the basic setup. We also prepared a new users' guide that explains how to use OpenPGP.
Welcome to Enigmail
File Edit View Go Message OpenPGP Tools
OpenPGP: Good signature from Patrick Brunschwig
Key ID: 0x1DB0E8B0 / Signed on: 31.12.2007
Subject:
From: Patrick Brunschwig
Enigmail provides end to end security for Mozilla Thunderbird and SeaMonkey
Enigmail automatically decrypts and verifies your Email
How should I start?
New users should look at our Quick start guide.
Then install GnuPG and the right Enigmail package for your system.
Is there a manual?
Of course there is. To find out all about configuration options, or in case you encounter problems, please first have a look into our user manual
Where can I get help?
The best place to get help is our mailing list. User forums are also available.
How can I contribute?
We'd love it if you did! Telling other people about Enigmail, helping out in the forums and on mailing lists, giving feedback on the manual, translating Enigmail into another language, reporting and fixing bugs, or helping out
What do I need?
Enigmail is an email plugin. It cannot be run by itself.
You need a supported email client, the GNU Privacy Guard (GnuPG), and a little patience. You may also need to install the proper Enigmail language pack.
Complete installation instructions can be found in the Quick start guide.

CAcert

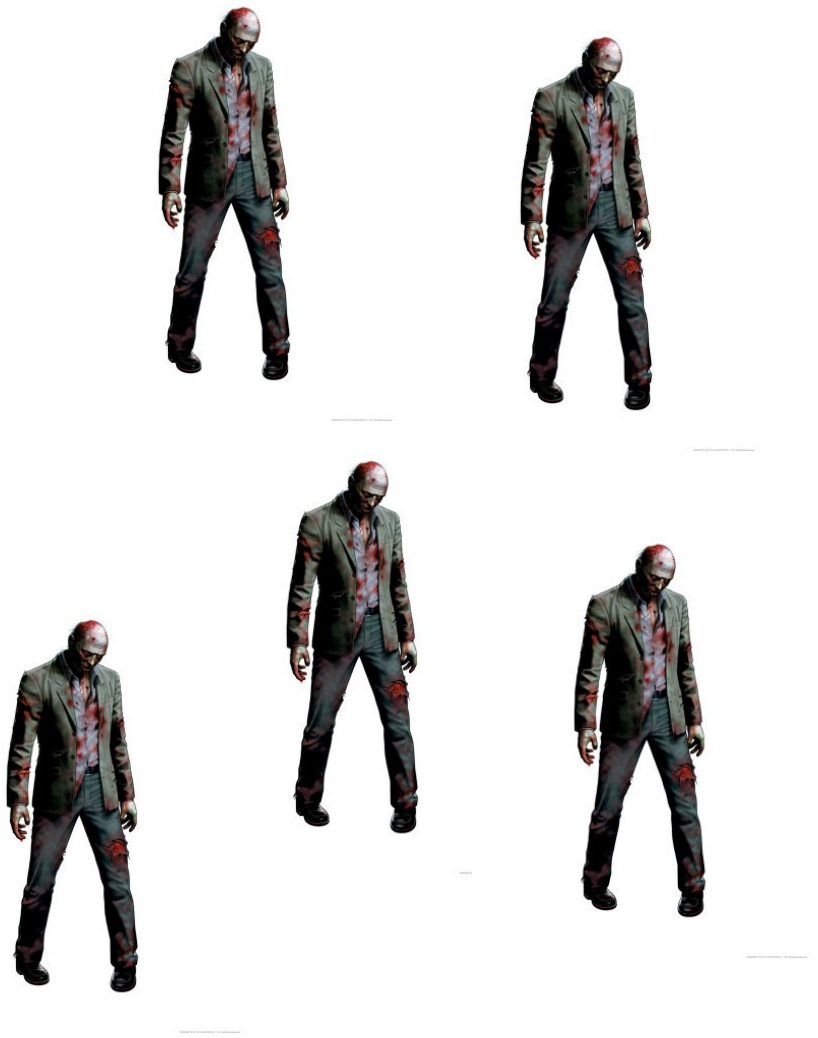


- SSL und S/MIME
- PGP

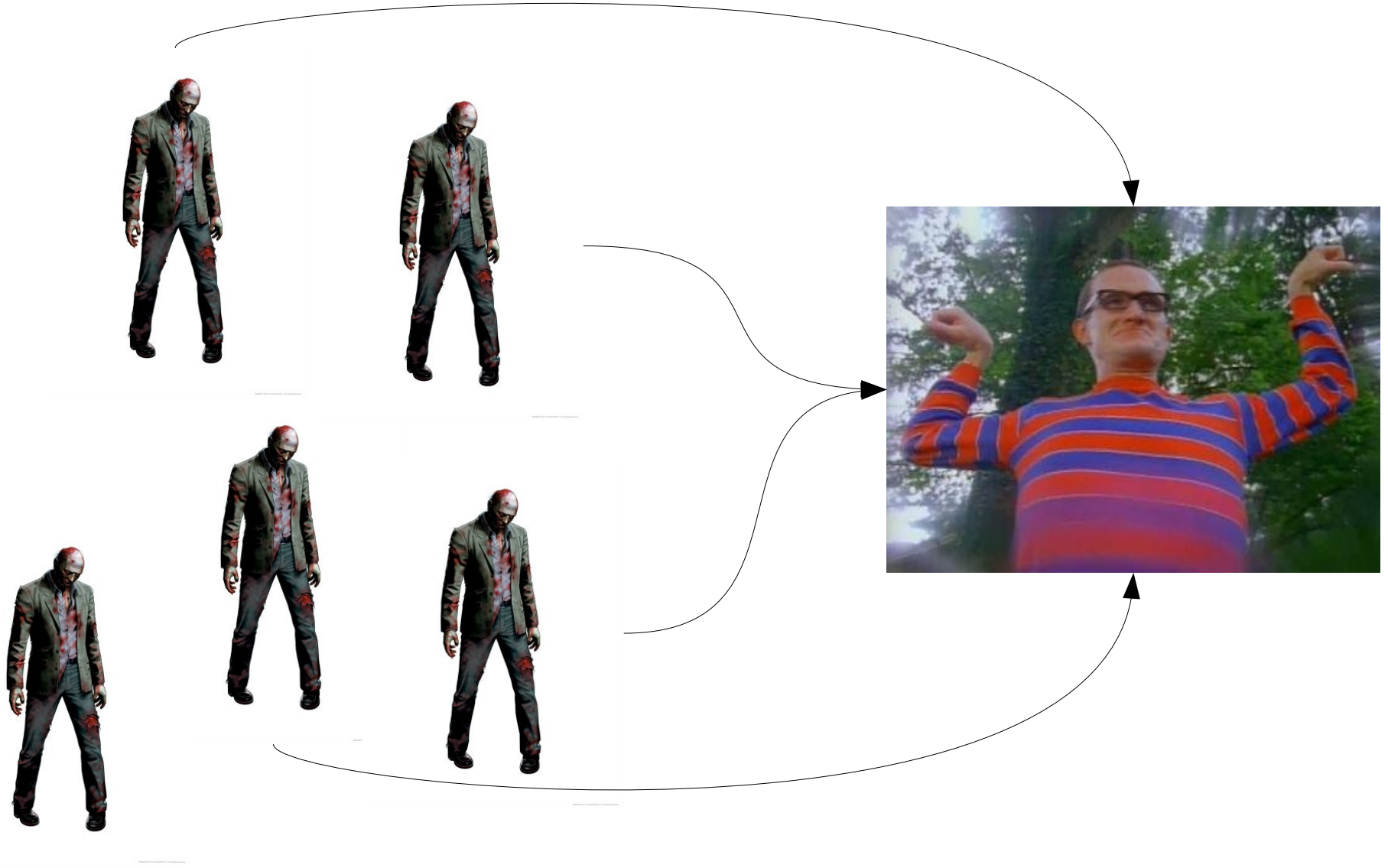
Web of Trust



Web of Trust



Web of Trust



Web of Trust

Schwachstellen

- Phantome
- Ungeklärte Datenschutzfragen
  - Konflikte mit europäischem Datenschutzrecht
  - Assurancebögen
  - Mailserver

Woran die Nutzer scheitern

- Installation der Root-CA
- Erzeugen von Serverzertifikaten
- Passwort verloren

Sichere Passwörter?

- Mindestens 8 Zeichen

Sichere Passwörter?

- Mindestens 8 Zeichen

`passwort`

Sichere Passwörter?

- Mindestens 8 Zeichen
- Groß- und Kleinschreibung

`passwort`

Sichere Passwörter?

- Mindestens 8 Zeichen
- Groß- und Kleinschreibung

`Passwort`

Sichere Passwörter?

- Mindestens 8 Zeichen
- Groß- und Kleinschreibung
- Mindestens zwei Zeichen aus jeder Klasse

`Passwort`

Sichere Passwörter?

- Mindestens 8 Zeichen
- Groß- und Kleinschreibung
- Mindestens zwei Zeichen aus jeder Klasse

`PassWort`

Sichere Passwörter?

- Mindestens 8 Zeichen
- Groß- und Kleinschreibung
- Mindestens zwei Zeichen aus jeder Klasse
- Zahlen

`PassWort`

Sichere Passwörter?

- Mindestens 8 Zeichen
- Groß- und Kleinschreibung
- Mindestens zwei Zeichen aus jeder Klasse
- Zahlen

`Pas5W0rt`

Sichere Passwörter?

- Mindestens 8 Zeichen
- Groß- und Kleinschreibung
- Mindestens zwei Zeichen aus jeder Klasse
- Zahlen
- Sonderzeichen

`Pas5W0rt`

Sichere Passwörter?

- Mindestens 8 Zeichen
- Groß- und Kleinschreibung
- Mindestens zwei Zeichen aus jeder Klasse
- Zahlen
- Sonderzeichen

`Pa$5_W0rt`

Sichere Passwörter?

- Mindestens 8 Zeichen
- Groß- und Kleinschreibung
- Mindestens zwei Zeichen aus jeder Klasse
- Zahlen
- Sonderzeichen
- Monatlicher Wechsel, mindestens 3 Zeichen Abweichung vom Vormonatspasswort

`Pa$5_W0rt`

Sichere Passwörter?

- Mindestens 8 Zeichen
- Groß- und Kleinschreibung
- Mindestens zwei Zeichen aus jeder Klasse
- Zahlen
- Sonderzeichen
- Monatlicher Wechsel, mindestens 3 Zeichen Abweichung vom Vormonatspasswort

`AuGu$t_12`

Sichere Passwörter?

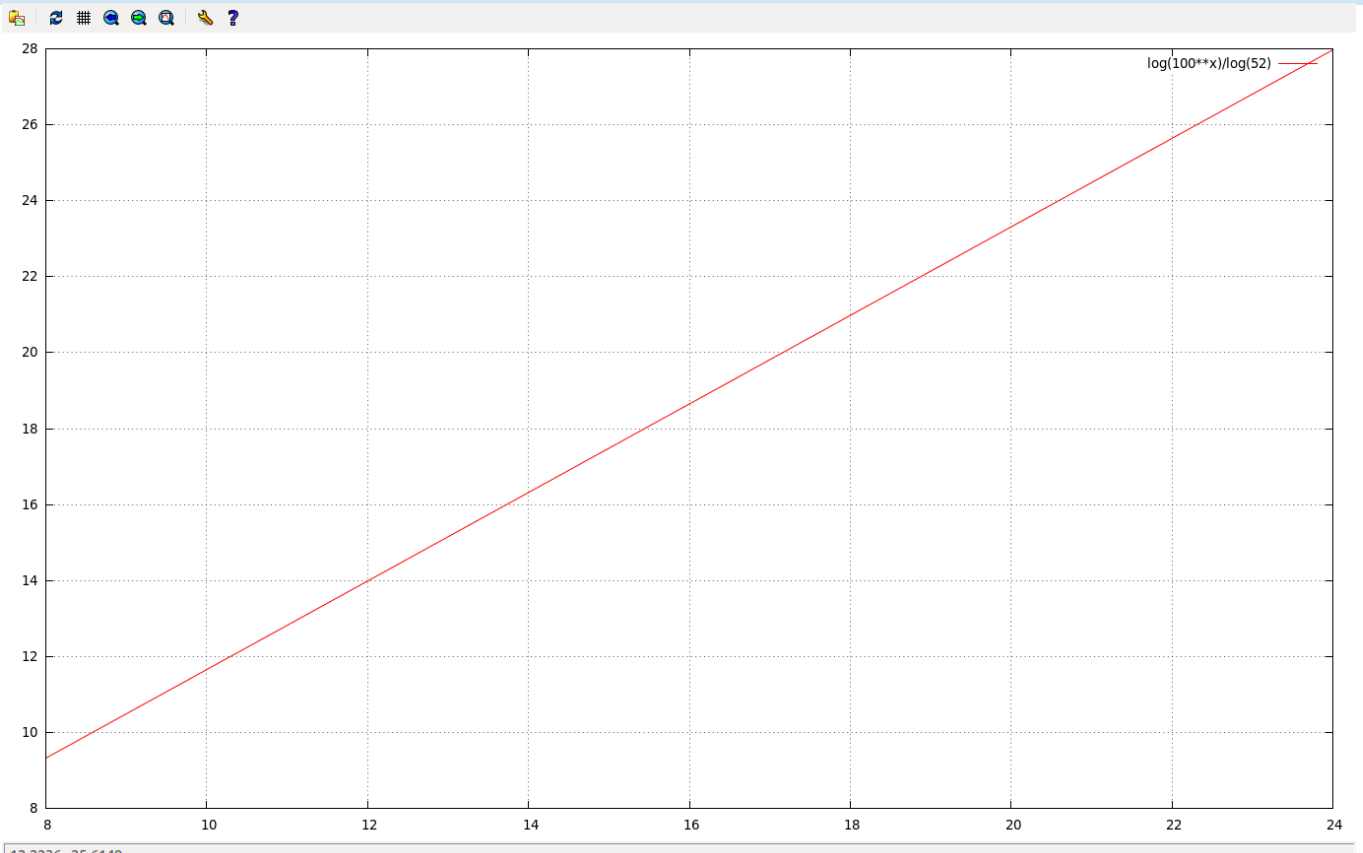
- Groß- und Kleinbuchstaben: **52 Zeichen**
- Zahlen: **10 Zeichen**
- Sonderzeichen: `!”§$%&/()=?`´\{[]}*+~<>|,;.:-_#'°^` **- 34 Zeichen**
- Insgesamt: **96 Zeichen**
- Bei achtstelligen Passwörtern: 96^8 < 100^8 = 10^16 = 10 Billiarden Kombinationen
- Bei zwölfstelligen Passwörtern: 100^12 = 10^24 = 1 Quadrillionen Kombinationen

Sichere Passwörter?

- Groß- und Kleinbuchstaben: 52 Zeichen
- Zahlen: 10 Zeichen
- Sonderzeichen: 34 Zeichen
- Insgesamt: 96 Zeichen
- Bei achtstelligen Passwörtern: 96^8 < 100^8 = 10^16 = 10 Billiarden Kombinationen
- Bei zwölfstelligen Passwörtern: 100^12 = 10^24 = 1 Quadrillionen Kombinationen
- Wer kann sich **'lli|!10O´** merken?

Size Matters

Zeichenvorrat 100	Groß- und Kleinschreibung
8 Stellen, **10^16** Kombinationen	10 Stellen, 1,4 * 10^17 Kombinationen
12 Stellen, **10^24** Kombinationen	14 Stellen, **10^24** Kombinationen
14 Stellen, 10^28 Kombinationen	17 Stellen, **1,5 * 10^29** Kombinationen
16 Stellen, 10^32 Kombinationen	19 Stellen, **4 * 10^32** Kombinationen



Size Matters

Zeichenvorrat 100	Groß- und Kleinschreibung	Deutsche Worte (135.000)
8 Stellen, **10^16** Komb	10 Stellen, 1,4 * 10^17 Komb	2 Wörter, 1,8 * 10^10 Komb
12 Stellen, **10^24** Kom	14 Stellen, **10^24** Komb	3 Wörter, 2,5 * 10^15 Komb
14 Stellen, 10^28 Komb	17 Stellen, **1,5 * 10^29** Komb	4 Wörter, **3,3 * 10^20** Komb
16 Stellen, 10^32 Komb	19 Stellen, **4 * 10^32** Komb	5 Wörter, **4,5 * 10^25** Komb

Erweiterungen

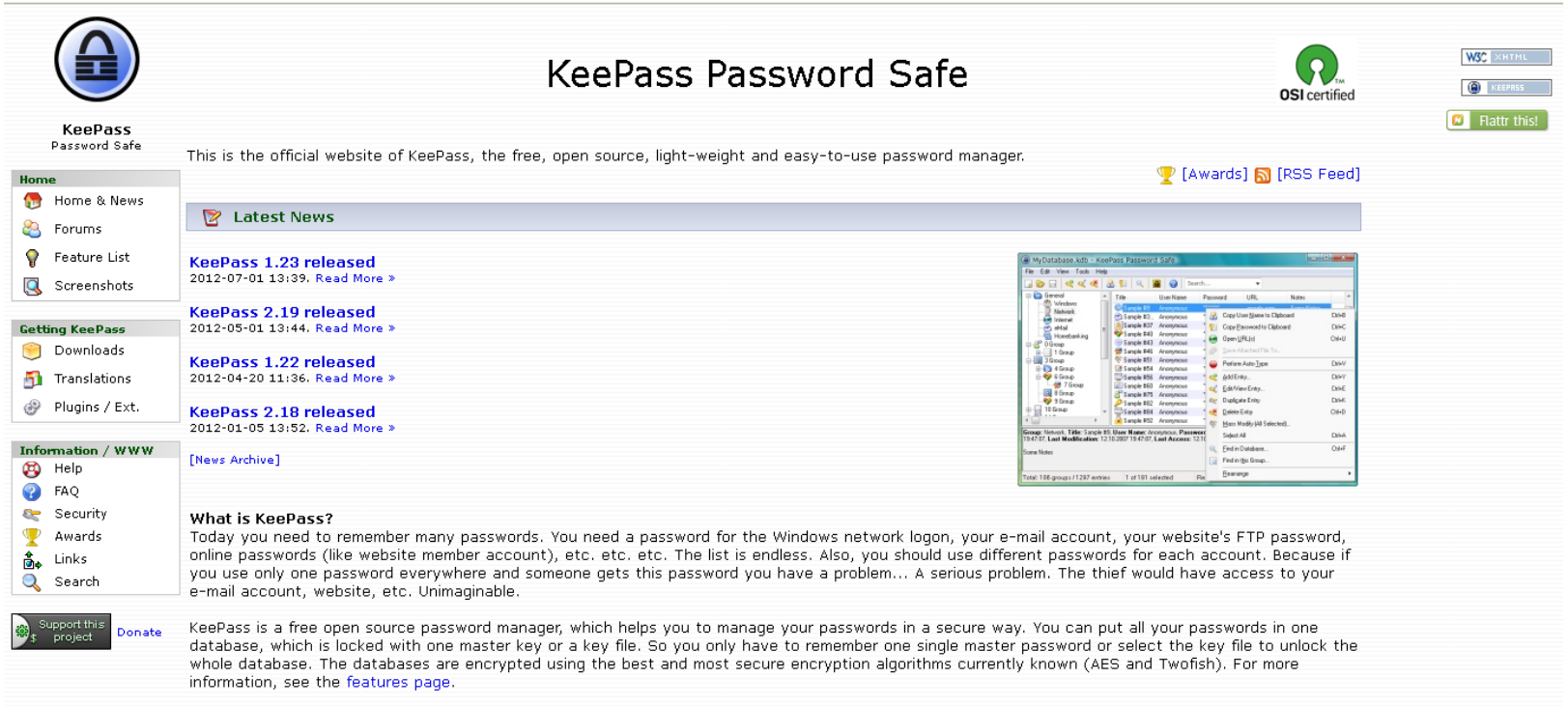
Ein starkes Passwort plus fallbezogene Erweiterung

`^cec7FIX{^6LlQ_HB`	Homebanking
`^cec7FIX{^6LlQ_mail`	Mail
`^cec7FIX{^6LlQ_ebay`	Versteigerungen

KeePass

+ Erleichtert die Verwaltung umfangreicher Passwortsammlungen
+ Komplexe und häufig wechselnde Passwörter werden handhabbar
- Keystore-Passwort SPOF

KeePass

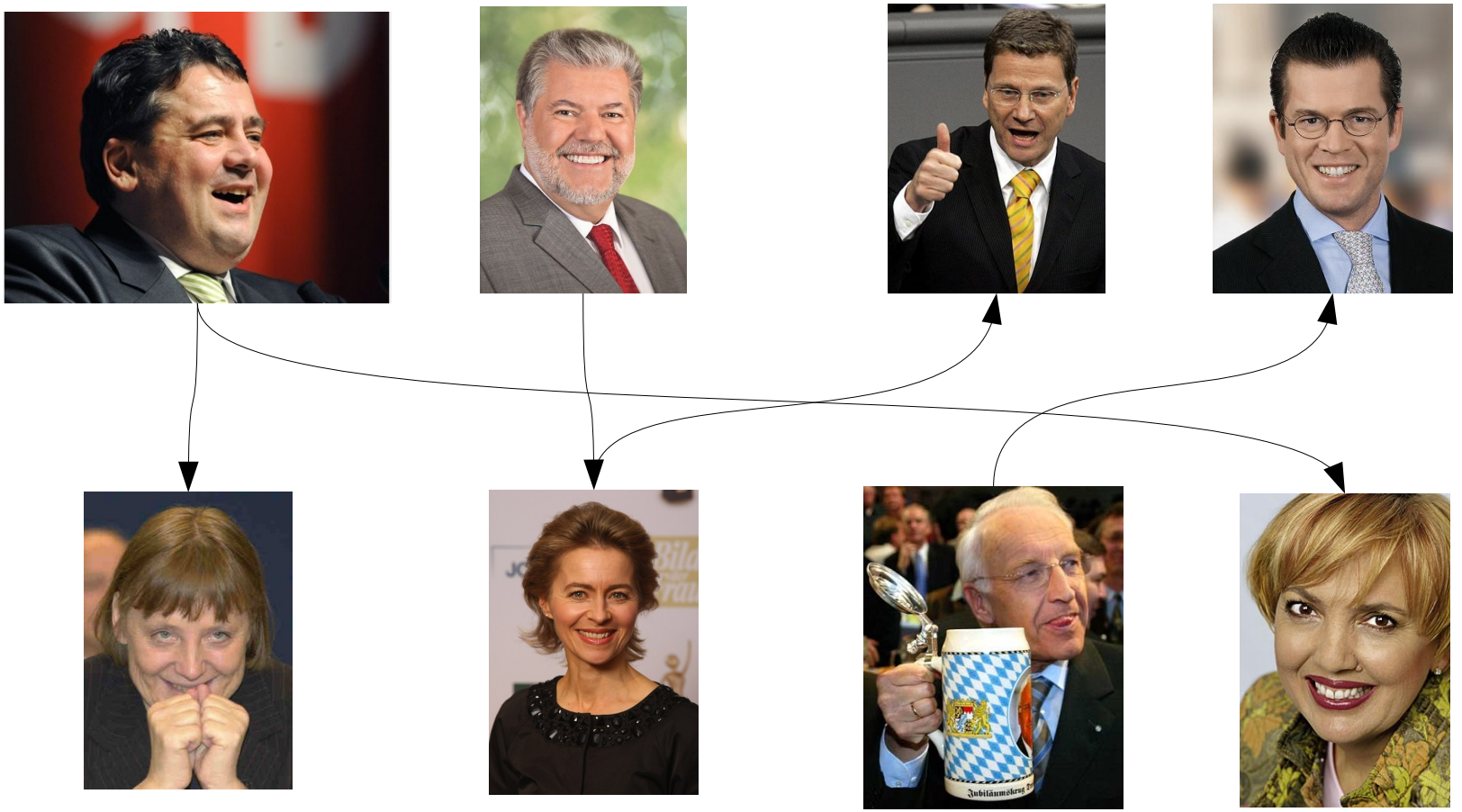


+ Erleichtert die Verwaltung umfangreicher Passwortsammlungen
+ Komplexe und häufig wechselnde Passwörter werden handhabbar
- Keystore-Passwort SPOF
- Funktioniert nicht (Zwischenablage != Zwischenablage)

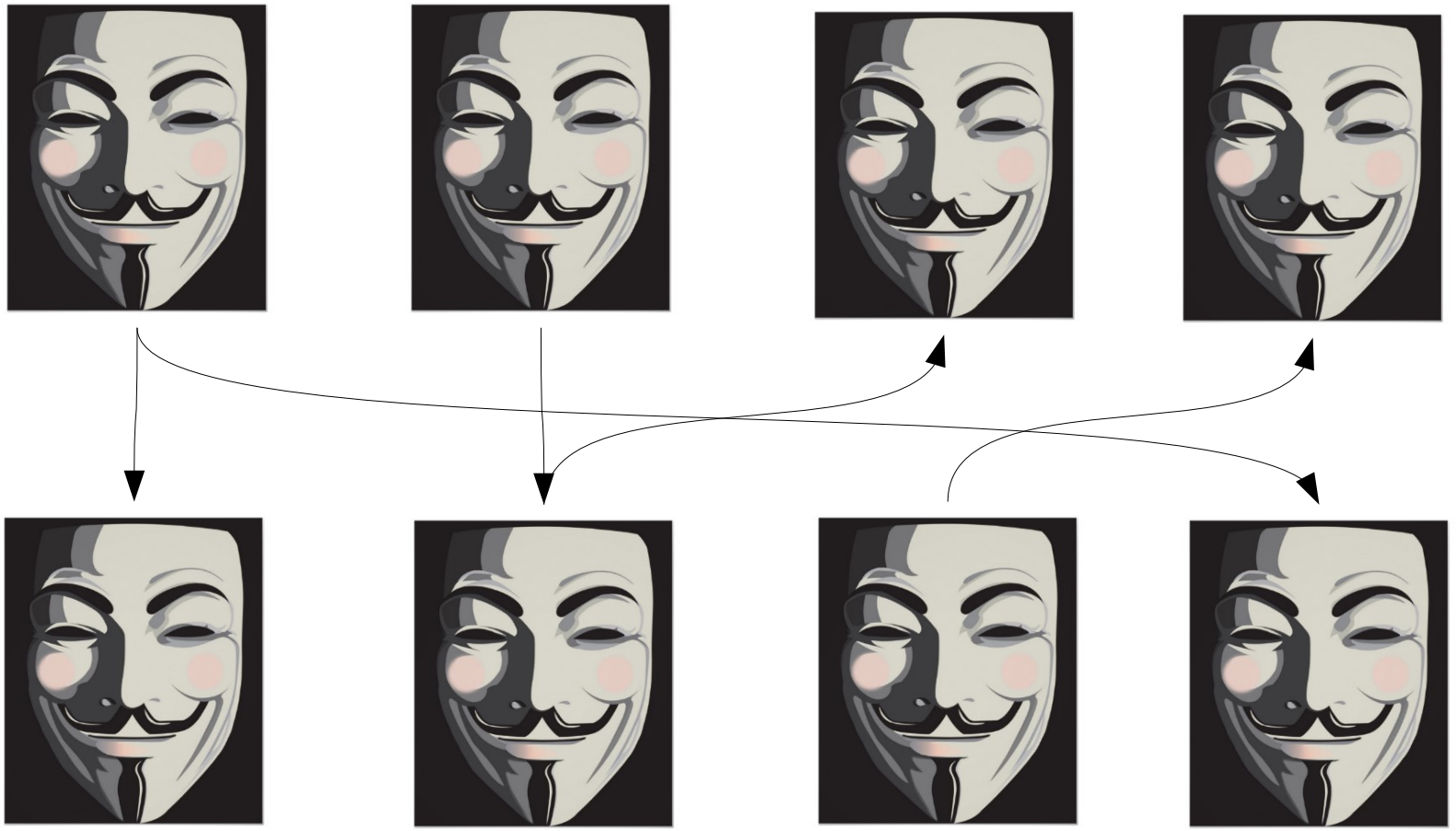
Fazit

- Passworte sind Mist
- Die Alternativen (Biometrie, Gesten) ebenfalls
  - teure Zusatzhardware
  - geringe Verbreitung
  - Erkennungsfehler
  - angreifbar

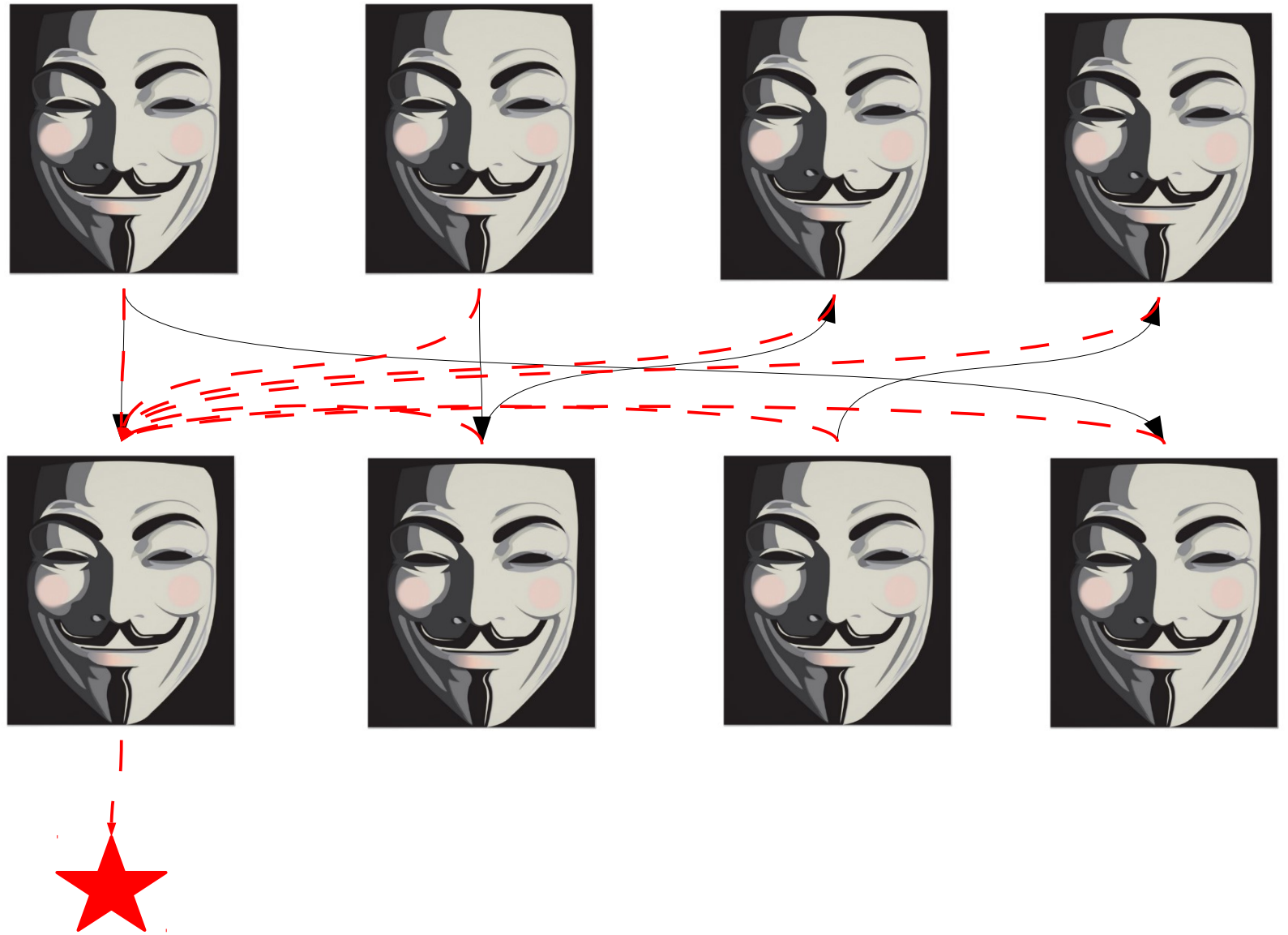
Verschlüsselung allein schützt nicht



Verschlüsselung allein schützt nicht



Verschlüsselung allein schützt nicht



Wir werden alle sterben!

Wir werden alle sterben!

- Perfekte Sicherheit kann es nicht geben.

Wir werden alle sterben!

- Perfekte Sicherheit kann es nicht geben.
- Das heißt nicht, dass man es nicht versuchen sollte.
- Be a moving target.