

Don Quixote meets Big Brother



Paranoia für Einsteiger



Ich sehe was, was du nicht siehst

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

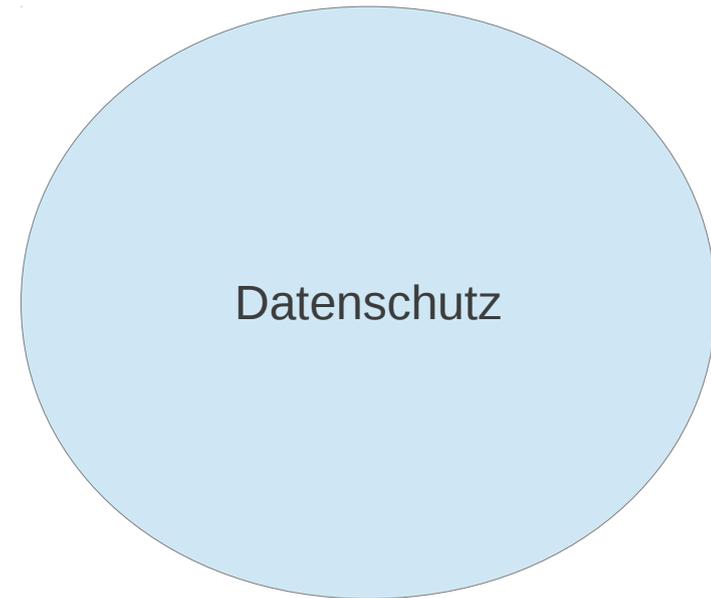
Ich sehe was, was du nicht siehst

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

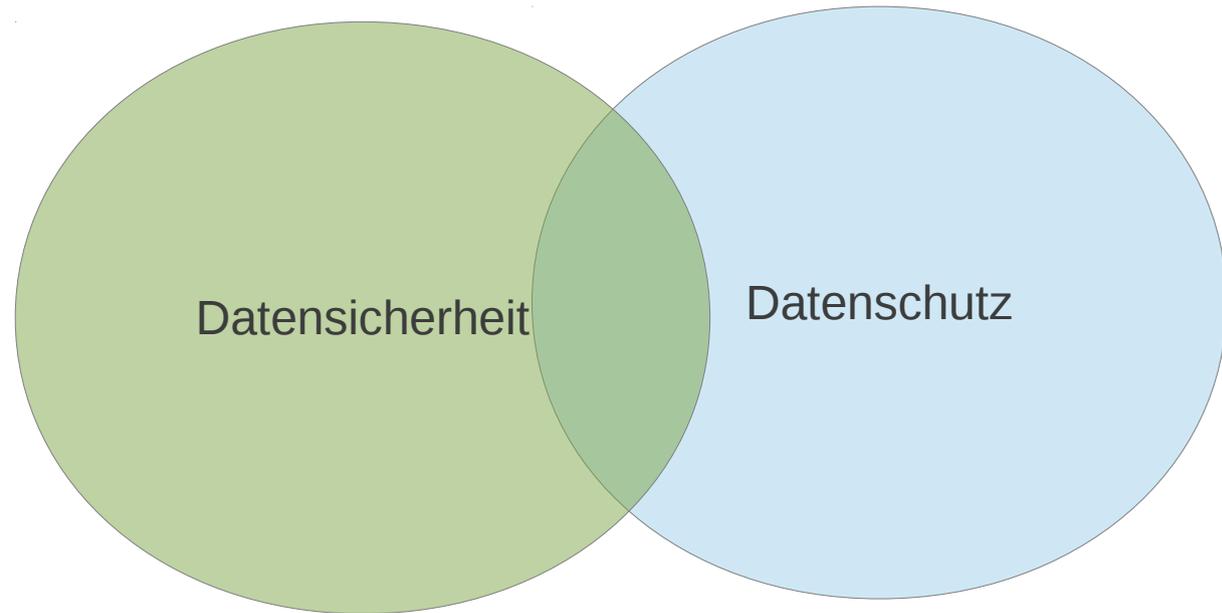
Ich sehe was, was du nicht siehst

- 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

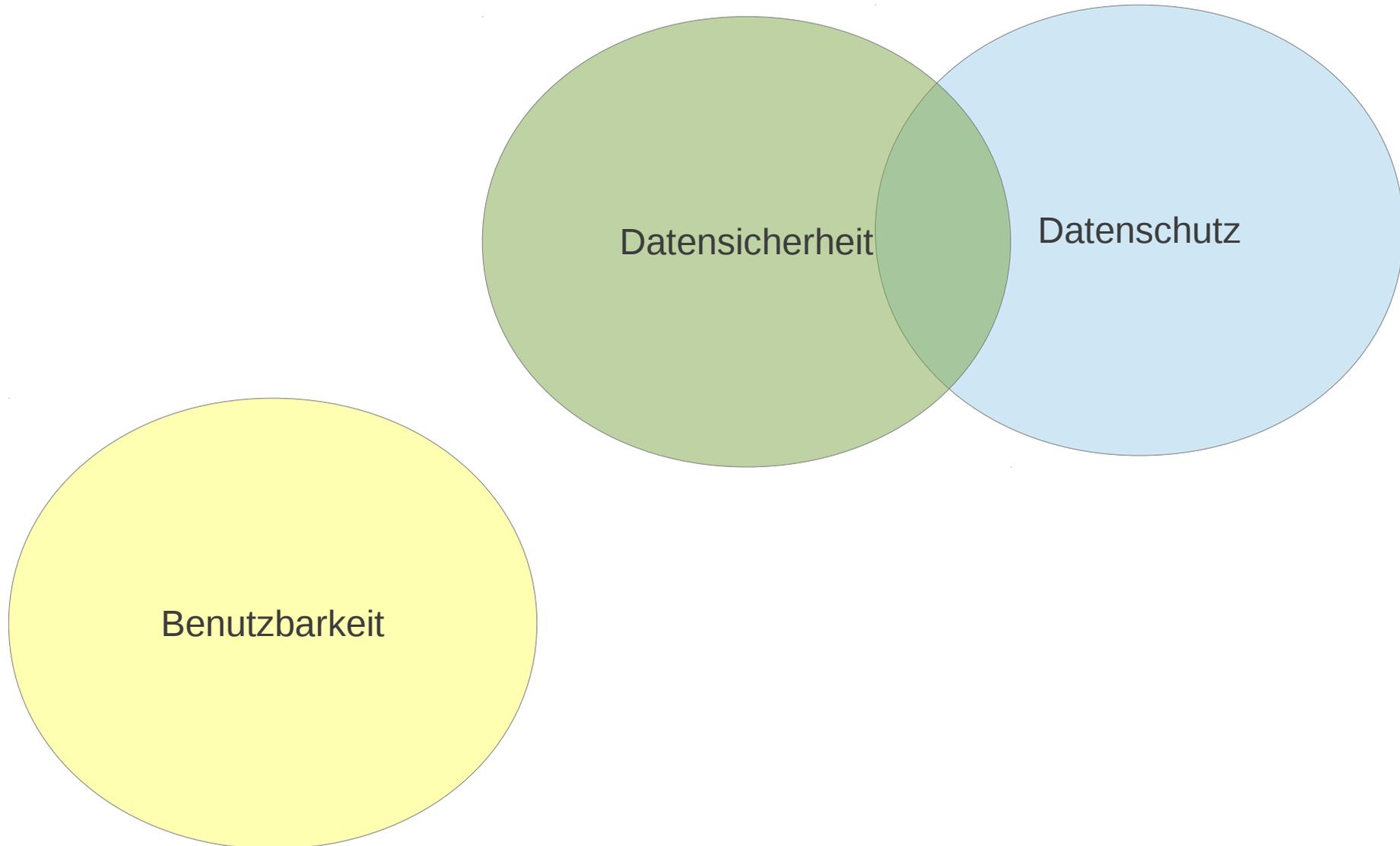
Abgrenzung



Abgrenzung



Abgrenzung



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

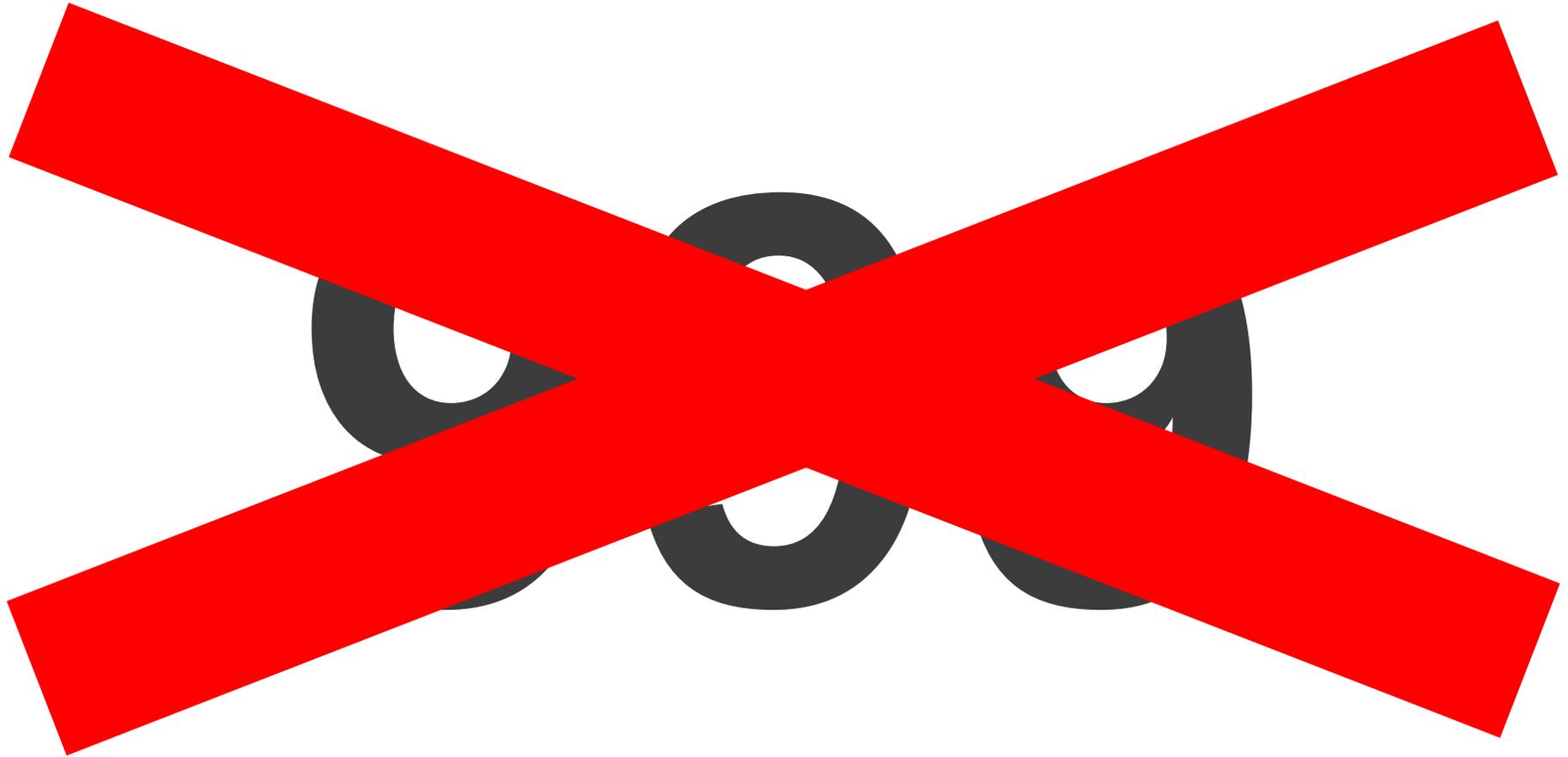
Cool Tools

**Cooler Tools
und
warum sie nicht funktionieren**

“Natürlich funktionieren die.”

999

“Natürlich funktionieren die.”



“Natürlich funktionieren die.”

0118999881999

1197253

“Natürlich funktionieren die.”

0118999881999

1197253

That's easy to remember.

Truecrypt



TrueCrypt

Free open-source disk encryption software for Windows 7/Vista/XP, Mac OS X, and Linux

News

• 2012-02-07
TrueCrypt 7.1a
Released

• 2011-09-01
TrueCrypt 7.1
Released

• 2010-09-06
TrueCrypt 7.0a
Released

• 2010-07-19
TrueCrypt 7.0
Released

• 2009-11-23
TrueCrypt 6.3a
Released

[[News Archive](#)]



Main Features:

- Creates a **virtual encrypted disk** within a file and mounts it as a real disk.
- Encrypts an **entire partition or storage device** such as USB flash drive or hard drive.
- Encrypts a **partition or drive where Windows is installed** (*pre-boot authentication*).
- Encryption is **automatic, real-time** (*on-the-fly*) and **transparent**.
- [Parallelization](#) and [pipelining](#) allow data to be read and written as fast as if the drive was not encrypted.

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

Truecrypt



TrueCrypt

Free open-source disk encryption software for Windows 7/Vista/XP, Mac OS X, and Linux

News

• 2012-02-07
TrueCrypt 7.1a
Released

• 2011-09-01
TrueCrypt 7.1
Released

• 2010-09-06
TrueCrypt 7.0a
Released

• 2010-07-19
TrueCrypt 7.0
Released

• 2009-11-23
TrueCrypt 6.3a
Released

[\[News Archive\]](#)



Main Features:

- Creates a **virtual encrypted disk** within a file and mounts it as a real disk.
- Encrypts an **entire partition or storage device** such as USB flash drive or hard drive.
- Encrypts a **partition or drive where Windows is installed** (*pre-boot authentication*).
- Encryption is **automatic, real-time** (*on-the-fly*) and **transparent**.
- [Parallelization](#) and [pipelining](#) allow data to be read and written as fast as if the drive was not encrypted.

- 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

home
catalog
contacts

Inform Open Source Software
Action

what is it? features changelog screenshots forum faq get it!

NoScript is **Free Software**: if you like it, you can support its progress!
[Donate](#)
VISA VISA
[Flatir this!](#)

INSTALL

proudly sponsored by **nlnet** FOUNDATION

The **NoScript Firefox extension** provides extra protection for Firefox, Seamonkey and other mozilla-based browsers: this free, open source add-on allows **JavaScript, Java, Flash and other plugins** to be executed only by **trusted web sites of your choice** (e.g. your online bank).

NoScript also provides the **most powerful anti-XSS and anti-Clickjacking** protection ever available in a browser.

NoScript's unique **whitelist based pre-emptive script blocking** approach prevents exploitation of **security vulnerabilities** (known and **even not known yet!**) with no loss of functionality...

You can enable JavaScript, Java and plugin execution for sites you trust with a simple left-click on the **NoScript status bar icon** (look at the picture), or using the contextual menu, for easier operation in popup statusbar-less windows.
[Watch the "Block scripts in Firefox" video](#) by cnet.

Staying safe has never been so easy!
Experts will agree: **Firefox is really safer with NoScript!**

Experts do agree...

08/06/2008, "I'd love to see it in there." ([Window Snyder](#), "Chief Security Something-or-Other" at Mozilla Corp., interviewed by [ZDNet](#) about "adding NoScript functionality into the core browser").

03/18/2008, "Consider switching to the Firefox Web browser with the NoScript plug-in. NoScript selectively, and non-intrusively, blocks all scripts, plug-ins, and other code on Web pages that could be used to attack your system during visits" (Rich Mogull on [TidBITS](#), [Should Mac Users Run Antivirus Software?](#)).

11/06/2007, [Douglas Crockford](#), world-famous JavaScript advocate and developer of JSON (one of the building blocks of Web 2.0), [recommends using NoScript](#).

03/16/2007, [SANS Internet Storm Center](#), the authoritative source of computer security related wisdom, runs a front-page [Ongoing interest in Javascript issues](#) diary entry by [William Stearns](#) just to say "Please, use NoScript".) Actually, NoScript has been recommended several times by SANS, but it's nice to see it mentioned in a dedicated issue, rather than as a work-around for specific exploits in the wild. Many thanks, SANS!

05/31/2006, [PC World's The 100 Best Products of the Year](#) list features NoScript at #52!
Many thanks to PC World, of course, for grokking NoScript so much, and to IceDogg who kindly [reported](#) these news...

Mozilla Firefox Multiple Vulnerabilities

SA39240
2010-03-31
2010-04-05

About NoScript...
Options...

1,251 view
[0 comments](#)

Allow Scripts Globally (dangerous)
 Allow all this page
 Temporarily allow all this page

Highly critical Untrusted

Security Byp: Allow secunia.com
System acce: Temporarily allow secunia.com
From remote

NoScript is **Free Software**: if you like it, you can support its progress :)
[Donate](#)
VISA VISA
[Flatir this!](#)

PC WORLD
WORLD CLASS 2006

- + Blockiert Javascript
- + Blockiert gefährliche Konstrukte
- Umständliches Freischalten

Ghostery

Ghostery™

[DOWNLOAD NOW](#) [ABOUT GHOSTERY](#) [PRIVACY POLICY](#) [SUPPORT](#) [GHOSTERY BLOG](#)

Detect

Ghostery™ sees the invisible web - tags, web bugs, pixels and beacons. Ghostery tracks the trackers and gives you a roll-call of the ad networks, behavioral data providers, web publishers, and other companies interested in your activity.

Learn

After showing you who's tracking you, Ghostery™ also gives you a chance to learn more about each company it identifies. How they describe themselves, a link to their privacy policies, and a sampling of pages where we've found them are just a click away.

Control

Ghostery™ allows you to block scripts from companies that you don't trust, delete local shared objects, and even block images and iframes. Ghostery puts your web privacy back in your hands.

[CONNECT WITH GHOSTERY](#)

[Follow Us On Twitter](#)

[Friend Us on Facebook](#)

[FEATURED ON](#)

The New York Times

THE GLOBE AND MAIL

The Washington Post

[OUR PROMISE](#)

NO ADWARE, SPYWARE OR MALWARE...EVER.

Ghostery is free to download and use - plus you have our promise that Ghostery will never be used for advertising. In fact, Ghostery is now part of Evidon, whose mission is to enable

[DOWNLOAD GHOSTERY FOR FREE](#)

- + Blockiert Usertracking
- Blockiert nur bekannte Tracker

Cookie-Blocker

The screenshot shows the Mozilla Add-ons website interface. At the top, there are navigation links for "Register or Log in", "Other Applications", and the Mozilla logo. A search bar is present with the text "search for add-ons". Below the navigation, the breadcrumb "Extensions » Cookie Monster" is visible. The main content area features the "Cookie Monster 1.1.0" add-on by "s1tony". It includes a star rating of 4.5, "161 user reviews", and "55,287 users". A green "+ Add to Firefox" button is prominently displayed. Below the main description, three screenshots illustrate the add-on's functionality: a cookie list, a settings dialog, and a cookie notification. At the bottom, there are links for "About this Add-on" and "Support site".

- + Blockiert Cookies
- Manuelles Freischalten sinnvoller Cookies

Better Privacy

Register or Log in Other Applications mozilla

ADD-ONS
EXTENSIONS | PERSONAS | THEMES | COLLECTIONS | MORE...

search for add-ons

Extensions » BetterPrivacy



BetterPrivacy 1.68
by NC

Remove or manage a new and uncommon kind of cookies, better known as LSO's. The BetterPrivacy safeguard offers various ways to handle Flash-cookies set by Google, YouTube, Ebay and others...

Latest updates: See bottom link 'version history'!

[+ Add to Firefox](#)

FEATURED

★★★★★
336 user reviews
699,218 users

[Add to collection](#)
[Share this Add-on](#)



HTTPS everywhere



HTTPS Everywhere

HTTPS Everywhere is a Firefox and Chrome extension that encrypts your communications with many major websites, making your browsing more secure.
Encrypt the web: Install HTTPS Everywhere today.

[HTTPS Everywhere](#)

[FAQ](#)

[Creating HTTPS Everywhere Rulesets](#)

[Hack On The Code](#)

[How to Deploy HTTPS Correctly](#)



Install in Firefox
Version 2.2 Stable



Install in Chrome
Alpha Version

HTTPS Everywhere is produced as a collaboration between [The Tor Project](#) and the [Electronic Frontier Foundation](#). Many sites on the web offer some limited support for encryption over [HTTPS](#), but

[Donate to EFF](#) 

[Join EFF](#) 

Stay in Touch

Email Address

[SIGN UP NOW](#)

Follow EFF

President of #Taiwan vows to work on expediting entry into the #TPP agreement
[#https://eff.org/r.a8ju](https://eff.org/r.a8ju) #ACTA
AUG 21 @ 10:52AM

Green Parties release a joint statement against #TPP and

Tor

The screenshot shows the Tor Project website homepage. At the top left is the Tor logo, a purple onion. To its right is a navigation menu with links for Home, About Tor, Documentation, Projects, Press, Blog, and Store. Below the navigation are three buttons: Download, Volunteer, and Donate. The main content area is divided into several sections. On the left, there's a green box titled 'Anonymity Online' with the text 'Protect your privacy. Defend yourself against network surveillance and traffic analysis.' and a 'Download Tor' button. To the right of this box are three bullet points describing Tor's benefits. Below this is a 'What is Tor?' section with a brief description and a link to 'Learn more about Tor'. To the right of that is a 'Why Anonymity Matters' section with a detailed explanation and a link to 'Get involved with Tor'. On the far right, there's a 'Who Uses Tor?' section with five categories: Family & Friends, Businesses, Activists, Media, and Military & Law Enforcement, each with a small image and a brief description.

Tor

Home About Tor Documentation Projects Press Blog Store

Download Volunteer Donate

Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.

Download Tor

- Tor prevents anyone from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, remote logins, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android

What is Tor?

Tor is free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as [traffic analysis](#)

[Learn more about Tor »](#)

Why Anonymity Matters

Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location. Tor works with many of your existing applications, including web browsers, instant messaging clients, remote login, and other applications based on the TCP protocol.

[Get involved with Tor »](#)

Who Uses Tor?

Family & Friends

People like you and your family use Tor to protect themselves, their children, and their dignity while using the Internet.

Businesses

Businesses use Tor to research competition, keep business strategies confidential, and facilitate internal accountability.

Activists

Activists use Tor to anonymously report abuses from danger zones. Whistleblowers use Tor to safely report on corruption.

Media

Journalists and the media use Tor to protect their research and sources online.

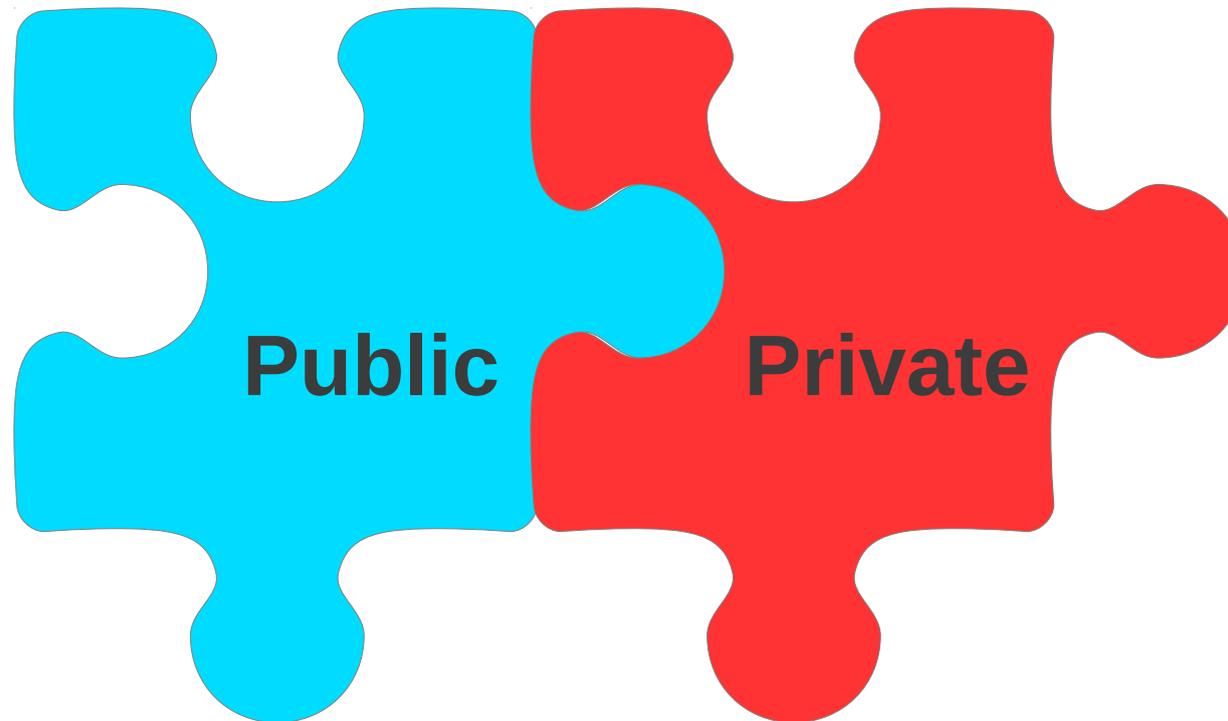
Military & Law Enforcement

Militaries and law enforcement use Tor to protect their communications, investigations, and intelligence gathering online.

Our Projects

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

Asymmetrische Verschlüsselung

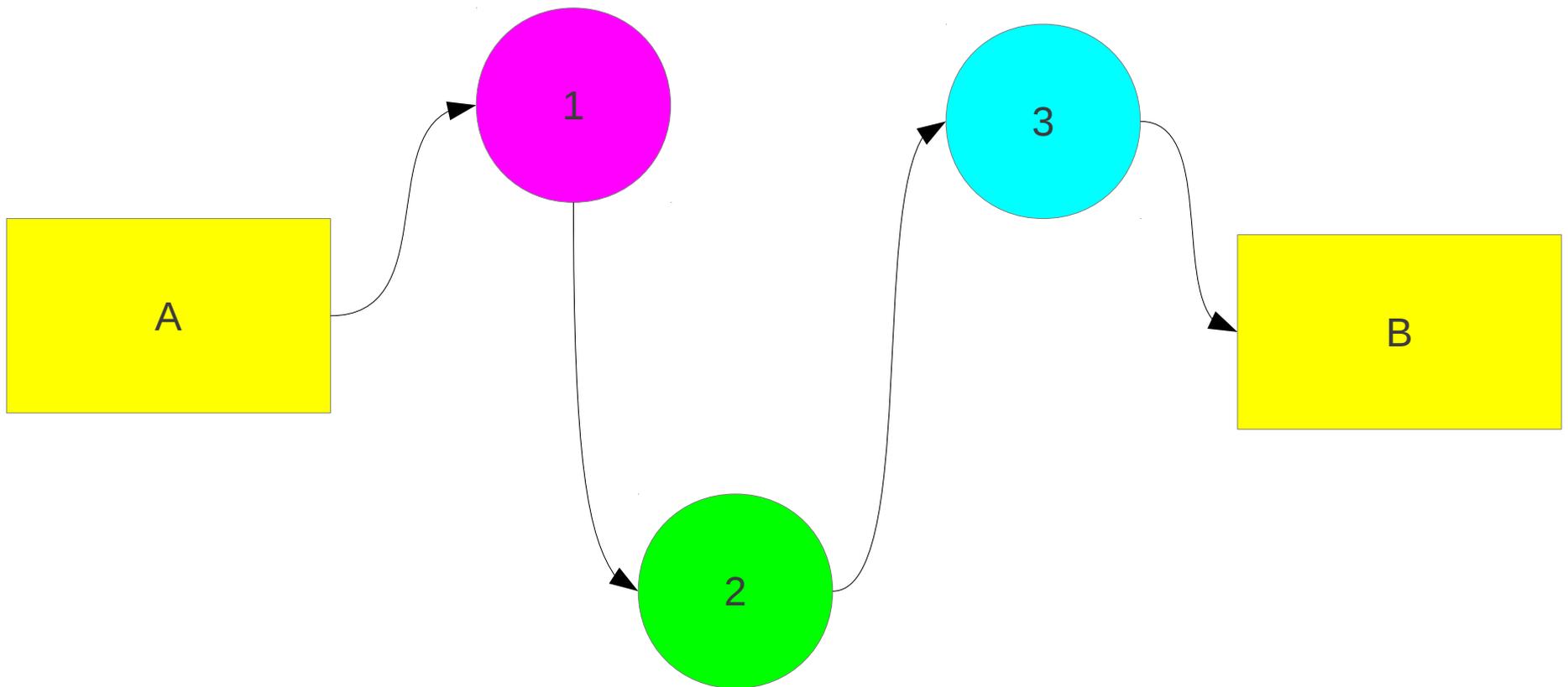


- Kann und soll veröffentlicht werden
- Kann nur verschlüsseln
- Kann Signaturen prüfen

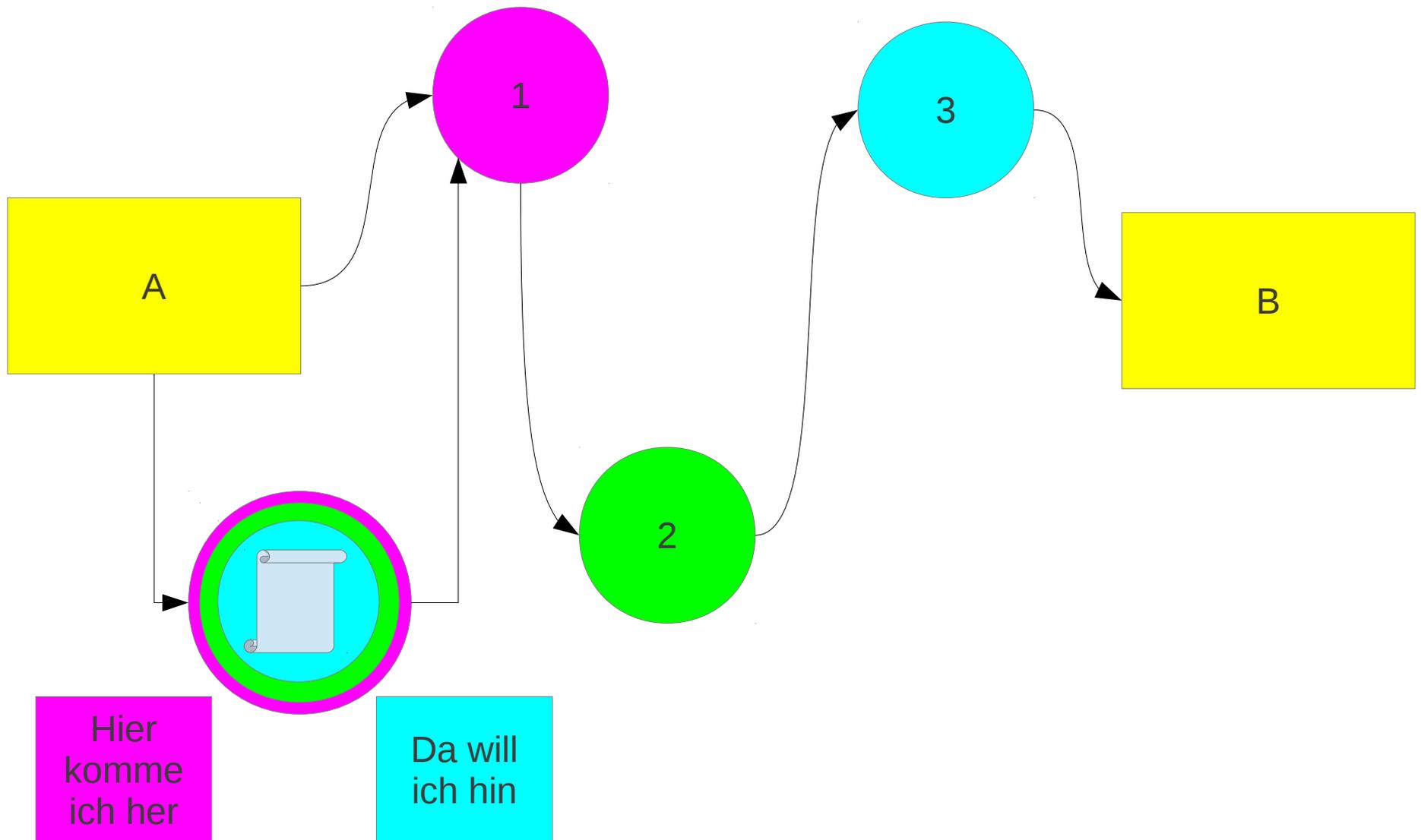
- Muss geheim bleiben
- Kann entschlüsseln
- Kann Signaturen erzeugen



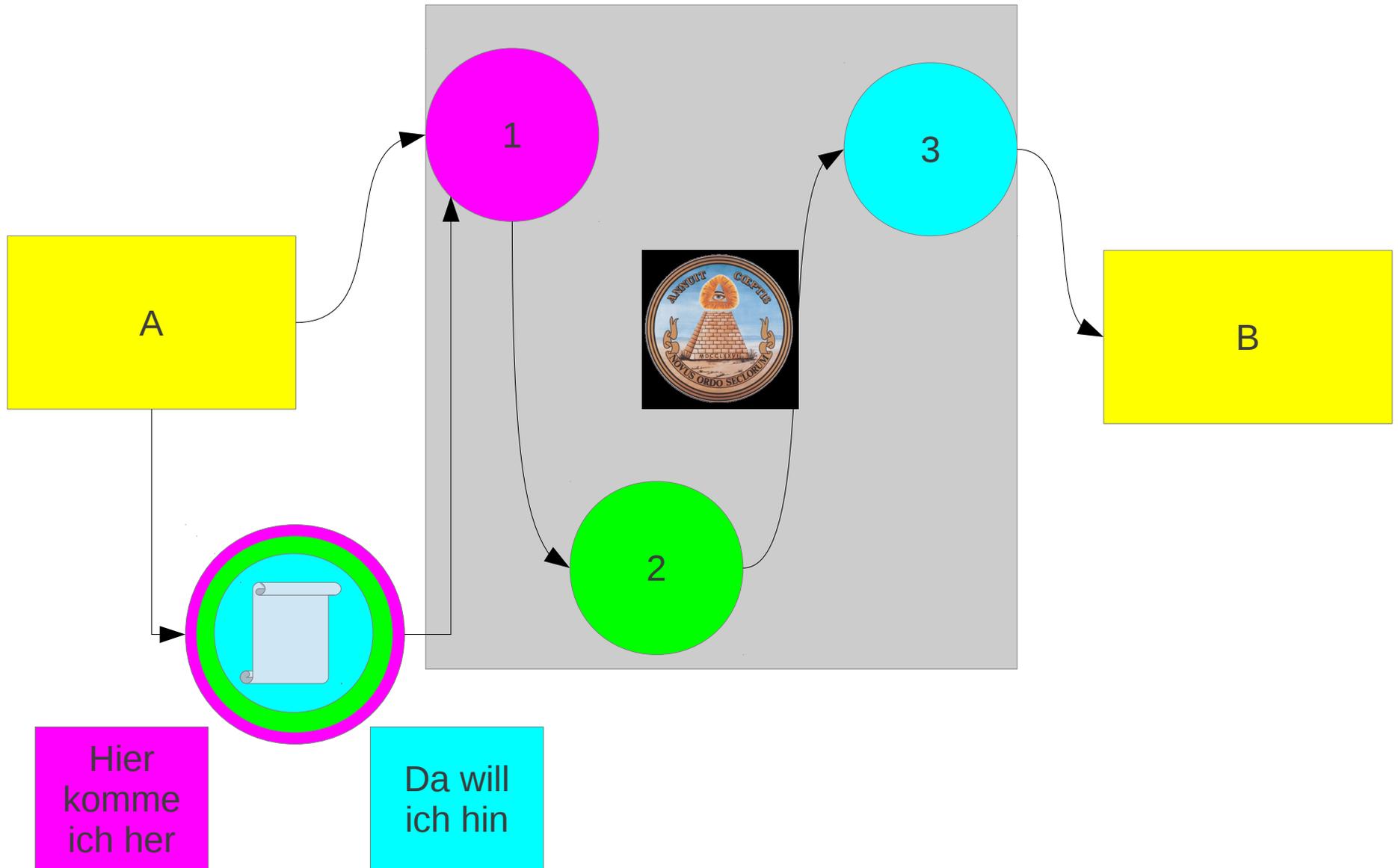
Proxykaskaden



Proxykaskaden



Proxykaskaden



Vidalia

The screenshot shows the Vidalia project page on the Tor Project website. At the top left is the Tor logo. The navigation menu includes Home, About Tor, Documentation, Projects (highlighted), Press, Blog, and Store. Below the navigation are buttons for Download, Volunteer, and Donate. A breadcrumb trail reads HOME » PROJECTS » VIDALIA ». A sidebar on the left lists various software and services, with Vidalia highlighted in green. The main content area features a screenshot of the Vidalia graphical interface, which shows a status window with a green onion icon and the text 'Connected to the Tor network!'. Below the status window are several shortcuts: Stop Tor, Setup Relaying, View the Network, Use a New Identity, Bandwidth Graph, Help, About, Message Log, Settings, and Exit. There is also a checkbox for 'Show this window on startup' and a 'Hide' button. Below the screenshot, there is a paragraph describing Vidalia as a cross-platform graphical controller for the Tor software, built using the Qt framework. It mentions that Vidalia runs on most platforms supported by Qt 4.3 or later, including Microsoft Windows, Apple OS X, and Linux or other Unix variants using the X11 window system. It was originally written by Matt Edman and is currently maintained by Tomás Touceda. Another paragraph explains that Vidalia lets users start and stop Tor, view bandwidth usage, see active circuits on a global map, view messages from Tor, and configure the Tor client, bridge, or relay with a simple interface. It also mentions an extensive help system. Below this is a 'Downloads' section with a 'Tor Tip' icon and text advising users to download Vidalia as part of a Tor software bundle and to use the Tor Browser Bundle instead of installing Vidalia themselves. At the bottom left, there is a URL: https://www.torproject.org/torbutton/index.html.en

HOME » PROJECTS » VIDALIA »

▼ Software & Services

- TorButton
- Tor Browser Bundle
- Vidalia**
- Arm
- Orbot
- Tails
- Onionoo
- Metrics Portal
- Tor Cloud
- Obsfproxy
- Shadow
- Tor2Web

Vidalia

Status
Connected to the Tor network!

Vidalia Shortcuts

- Stop Tor
- Setup Relaying
- View the Network
- Use a New Identity
- Bandwidth Graph
- Help
- About
- Message Log
- Settings
- Exit

Show this window on startup

Vidalia is a cross-platform graphical controller for the [Tor](#) software, built using the [Qt](#) framework. Vidalia runs on most platforms supported by Qt 4.3 or later, including Microsoft Windows, Apple OS X, and Linux or other Unix variants using the X11 window system. It was originally written by Matt Edman, and is currently maintained by Tomás Touceda.

Vidalia lets you start and stop Tor, see how much bandwidth you are consuming, see how many circuits you currently have active, see where these circuits are connected on a global map, view messages from Tor about its progress and current state, and let you configure your Tor client, bridge, or relay with a simple interface. Included in Vidalia is an extensive help system which helps you understand all of the options available to you. All of these features are translated into a large number of languages.

Downloads

You should simply download Vidalia as part of a [Tor software bundle](#). **Users should be using Tor Browser Bundle, not installing Vidalia themselves.**

Tor Tip

<https://www.torproject.org/torbutton/index.html.en>

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](#)

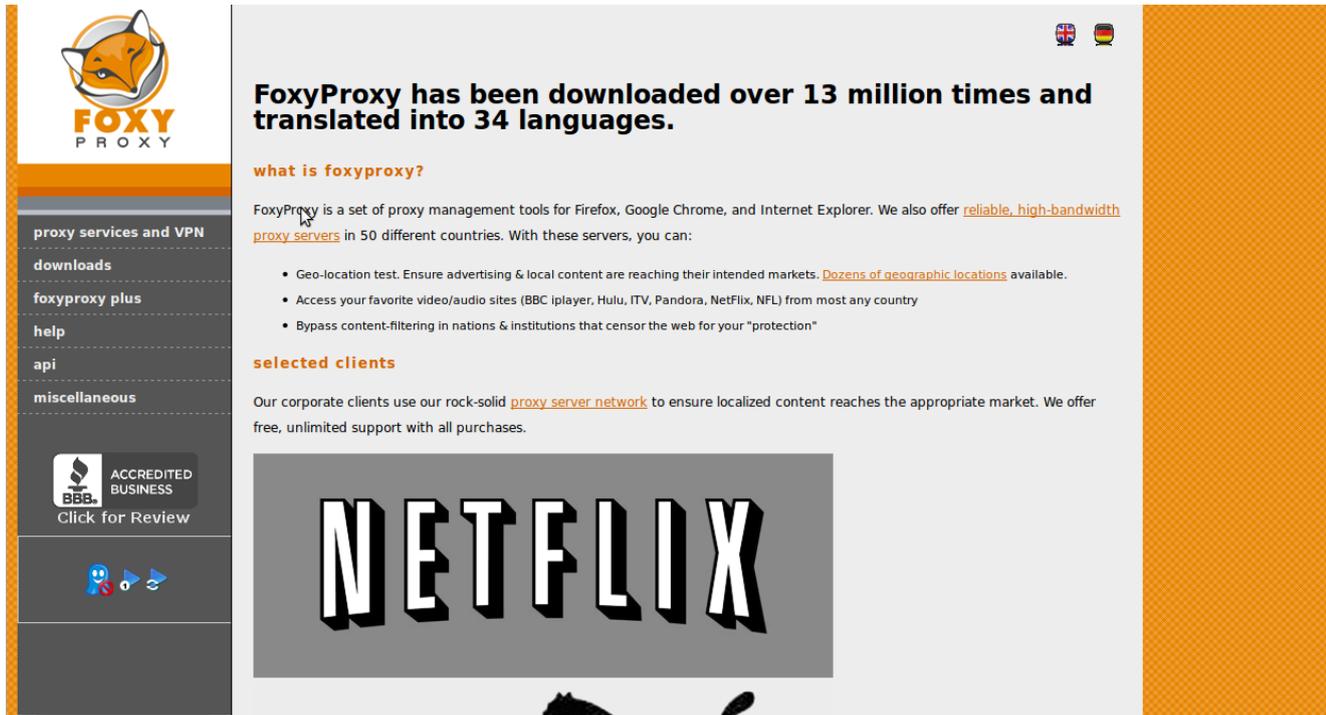
- Zusatzwerkzeug für Tor
- Kann bei Bedarf Headerdaten manipulieren
- Kann Zugriff auf gefährliche Inhalte sperren
- Headerdatenmanipulation funktioniert nicht richtig

User Agent Switch

The screenshot shows the Mozilla Add-ons page for the 'User Agent Switcher' extension. The page header includes the Mozilla logo, a search bar, and navigation links. The extension details section shows the name 'User Agent Switcher' by 'chrispederick', version '0.7.3', and a description: 'The User Agent Switcher extension adds a menu and a toolbar button to switch the user agent of a browser.' It has a 4.5-star rating, 239 user reviews, and 574,538 users. A green '+ Add to Firefox' button is prominent. Below this, there is a 'Contribute' section with a 'Contribute' button and a suggested amount of '\$1.99'. At the bottom, a screenshot of the extension's menu is shown, with 'iPhone 3.0' selected. The menu options are: Default User Agent, Internet Explorer, Search Robots, iPhone 3.0 (checked), Edit User Agents..., and User Agent Switcher.

Fälscht Browserkennung

Foxyproxy



The image shows a screenshot of the FoxyProxy website. On the left is a dark sidebar with navigation links: 'proxy services and VPN', 'downloads', 'foxyproxy plus', 'help', 'api', and 'miscellaneous'. Below these links is a BBB Accredited Business badge with the text 'Click for Review' and social media icons for Facebook, Twitter, and YouTube. The main content area has a light gray background. At the top right of the main area are flags for the UK and Germany. The main heading reads 'FoxyProxy has been downloaded over 13 million times and translated into 34 languages.' Below this is a section titled 'what is foxyproxy?' which describes the tool as a set of proxy management tools for Firefox, Google Chrome, and Internet Explorer. It lists features such as geo-location testing, access to video/audio sites like BBC iPlayer, Hulu, ITV, Pandora, Netflix, and NFL, and the ability to bypass content filtering. A 'selected clients' section mentions that corporate clients use the proxy server network for localized content. At the bottom of the main content area is a large, stylized 'NETFLIX' logo.



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.



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/repoFolder1856
92807/strategie_eng_265-150.jpg HTTP/1.1" 304 -
"http://myhost/wcms/logistics/folder100577464/folder156818914/folder1572
31140/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/folder1572311
40/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
%2FCAs0wvd0id3Lv4ZPKHfdE%2Fq49VIZ5kiQYMM0zIEsVaKzvgfawZHR%2Bo
%3D&lang&spa&time&1345584656&ip&23.42.47.11&user&myuser&expires&1440"
"resp:65822" "pid:18041"
```

Anonym durch Proxy-IPs?

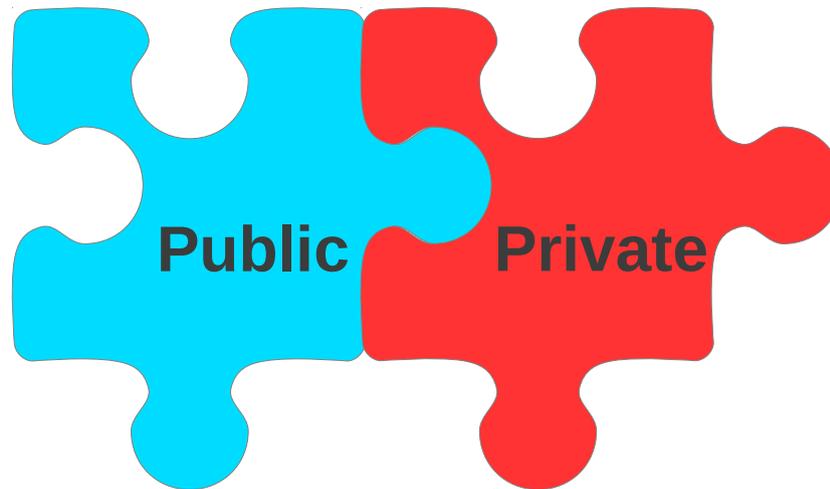
- Unternehmensweit gibt es zwei verschiedene Standardinstallationen: XP und Win 7
- User IDs im Log: **23632**
- Verschiedene User Agent Strings: **3710**
- Chance, einen User allein anhand seines Agent-Strings zu identifizieren: **1:6**

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?

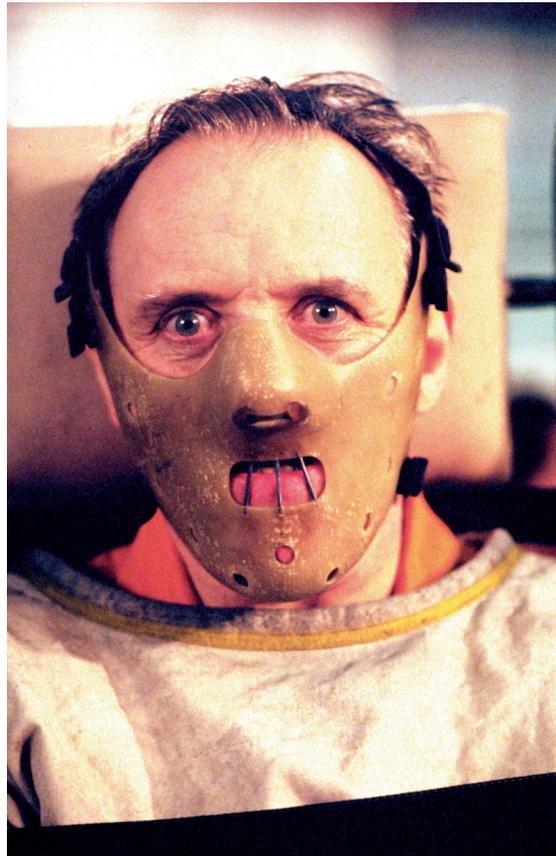
Schlüsselverteilung

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

Antwort:

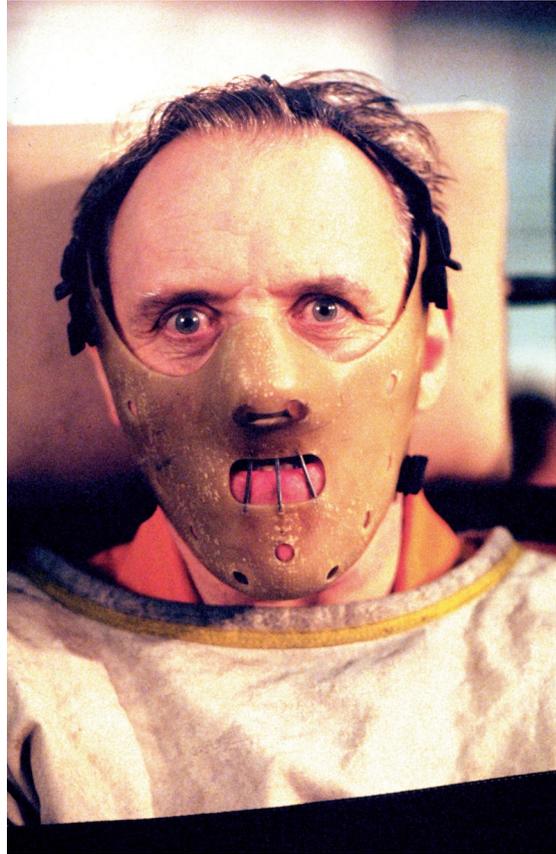
- Direkte Aushändigung
- Zentrale CA (Verisign, Signtrust, DigiNotar)
- Web of Trust

Web of Trust



vertraut

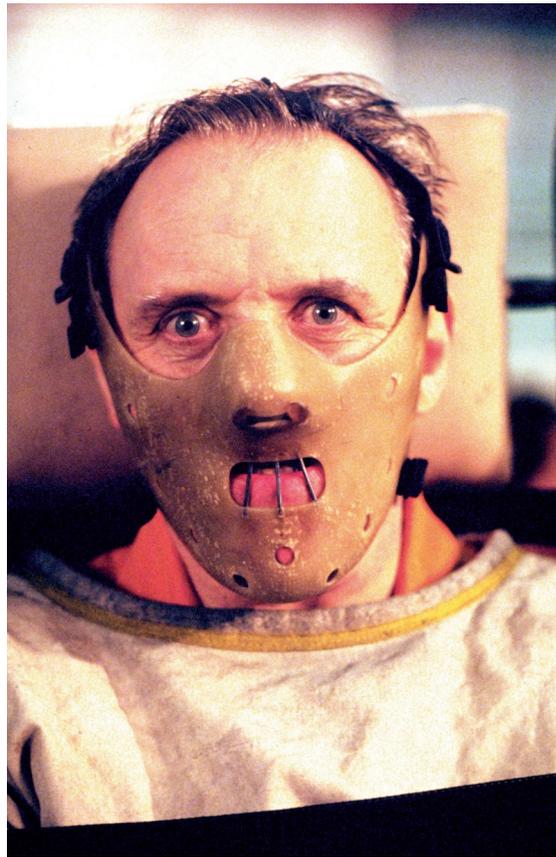
Web of Trust



vertraut

Web of Trust

vertraut



vertraut

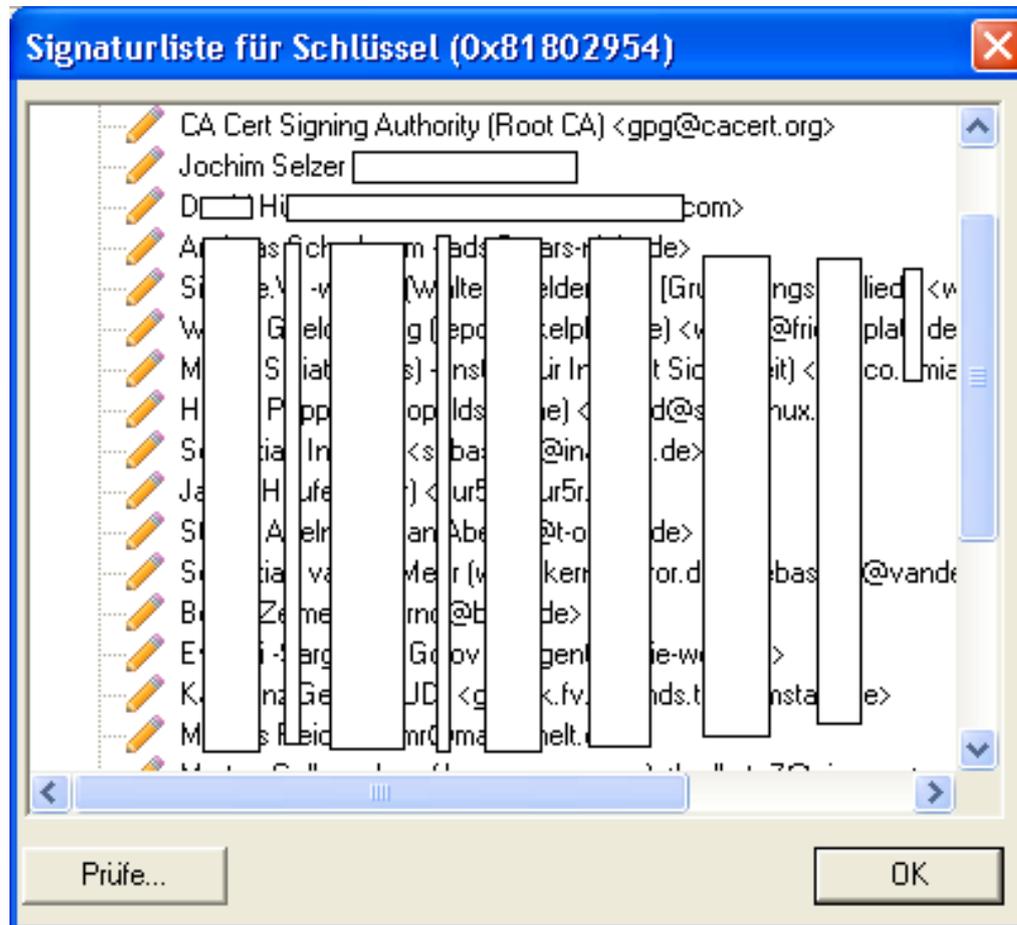
vertraut

PKP-Schlüsselring

| Benutzerkennung | SchlüsselID | Typ | Größe | Cipher | Gültigkeit | Vertrauen | Erstellung |
|-----------------|-------------|--------|-----------|----------|------------|-----------|------------|
| .de> | 0x | 05 pub | 2048/2048 | RSA/R... | Keine | Keine | 18.04.2005 |
| ail robot) <... | 0x | 7 pub | 1024/1024 | DSA/ELG | Keine | Keine | 06.03.2002 |
| | 0x | 3 pub | 1024/1024 | DSA/ELG | Keine | Keine | 21.02.2008 |
| | 0x | 5 pub | 1024/2048 | DSA/ELG | Keine | Keine | 18.04.2009 |
| | 0x | 13 pub | 2048/2048 | RSA/R... | Keine | Keine | 24.06.2010 |
| > | 0x | 9F pub | 1024/2048 | DSA/ELG | Keine | Keine | 18.04.2009 |
| pi i net> | 0x | E pub | 1024/2048 | DSA/ELG | Keine | Keine | 22.12.2000 |
| @re... | 0x | 16 pub | 1024/1024 | DSA/ELG | Keine | Keine | 28.09.2002 |
| nar@debi... | 0x | 2 pub | 4096/4096 | RSA/R... | Keine | Keine | 16.06.2010 |
| .org> | 0x | 0A pub | 1024/2048 | DSA/R... | Keine | Keine | 14.08.2000 |
| .org> | 0x | AC pub | 1024/4096 | DSA/ELG | Keine | Keine | 19.05.2001 |
| .com> | 0x | 51 pub | 1024/2048 | DSA/ELG | Keine | Keine | 19.09.2000 |
| post) <ahu... | 0x | 06 pub | 1024/4096 | DSA/ELG | Keine | Keine | 05.02.2010 |
| p-il : 'b... | 0x | 86 pub | 1024/2048 | DSA/ELG | Keine | Keine | 15.01.2007 |
| en@gmx.d... | 0x | 6C pub | 1024/4096 | DSA/ELG | Keine | Keine | 07.03.2005 |
| nicht.de> | 0x | E pub | 1024/4096 | DSA/ELG | Keine | Keine | 29.09.2000 |

Standardschlüssel: 0x 3 geheime(r) Schlüssel 298 Schlüssel

PGP-Signaturen



Enigmail

THE ENIGMAIL PROJECT
OPENPGP EMAIL SECURITY FOR MOZILLA APPLICATIONS

Home Download Documentation Support News Links

A simple interface for OpenPGP email security

Download

v1.4.4 for Linux (3kbit) 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.

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?

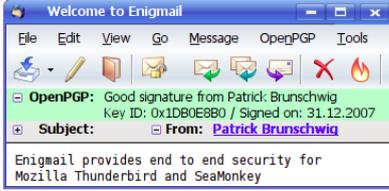
We'd love it if you did! Telling other people about Enigmail, helping out in the [forums](#) and on [mailing lists](#), giving feedback on [the manual](#), translating Enigmail into another language, [reporting](#) and [fixing](#) bugs, or helping out

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



Are you new to CAcert?

If you want to have free certificates issued to you, join the [CAcert Community](#) .

If you want to use certificates issued by CAcert, read the CAcert [Root Distribution License](#) .This license applies to using the CAcert root keys .

LATEST NEWS

Bug fixing

The software developing team released recently some bug fixes that affect the users.Firstly, the software now is able to give the correct assurer status. This has the effect that all assurers that have given assurances in the past but have not passed the CATS test will now no longer be ...

[[Full Story](#)]

FrOSCon 2012 in St. Augustin 25./26. August 2012

For the English version see below.Auch in diesem Jahr wird CAcert wieder auf der FrOSCon am 25. und 26. August in St. Augustin mit einem Stand vertreten sein.Des Weiteren wird es im Entwicklerraum "Freie Software für Betrieb und Verwaltung" einen Vortrag zum Thema "Zertifikate im betrieblichen Alltag" von CAcert geben.Sprecht ...

[[Full Story](#)]

PING e.V. Sommerfest, 18.8.2012, Dortmund

Die Westfälische Rundschau und der PING e.V. laden am 18. August 2012 ab 15:30 Uhr zu „Abenteuer Ferien“ ein.Besucher haben an diesem Tag die Möglichkeit, hinter die Kulissen unseres Vereins zu schauen und die aktiven Mitglieder kennenzulernen.Für diesen Tag haben die aktiven Mitglieder des PING e.V. ein vielseitiges Kurzvortragsprogramm vorbereitet. ...

[[Full Story](#)]

[[More News Items](#)]

Join CAcert.org

[Join](#)
[Community Agreement](#)
[Root Certificate](#)

My Account

[Password Login](#)
[Lost Password](#)
[Net Cafe Login](#)
[Certificate Login](#)

+ About CAcert.org

[CAcert News](#)
[Wiki Documentation](#)
[Policies](#)
[Point System](#)
[Bug Database](#)
[CAcert Statistics](#)
[RSS News Feed](#)
[CAcert Board](#)
[Mailing Lists](#)
[Sourcecode](#)

+ Translations

[العربية](#)
[Български](#)
[Čeština](#)
[Dansk](#)
[Deutsch](#)
[Ελληνικά](#)
[English](#)
[Español](#)
[Français](#)

- SSL und S/MIME
- PGP

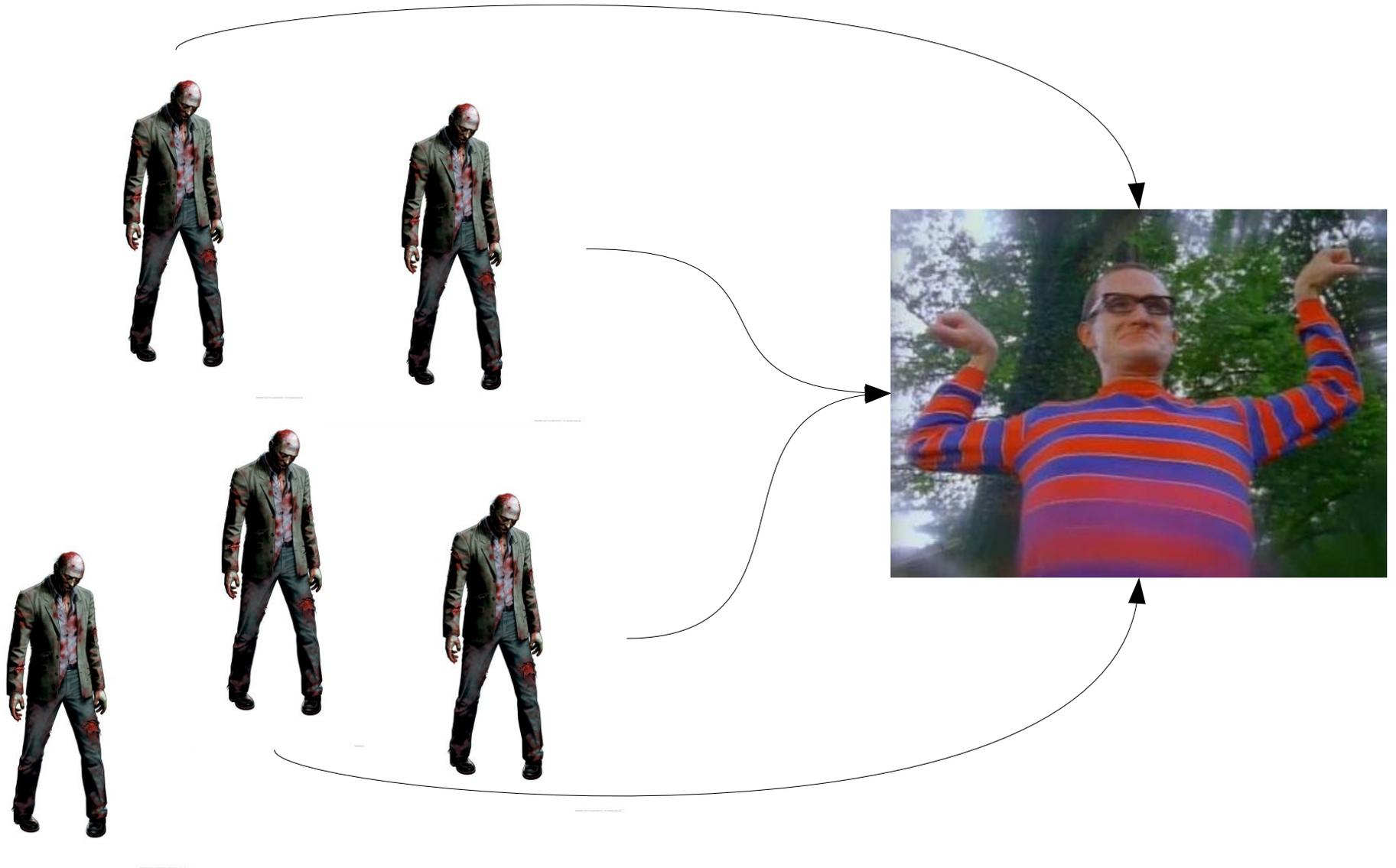
Web of Trust



Web of Trust



Web of Trust



Web of Trust



Schwachstellen

- Phantome
- Ungeklärte Datenschutzfragen
 - Konflikte mit europäischem Datenschutzrecht
 - Assurancebögen
 - Mailserver
- Komplizierte und ausbaufähig sortierte Dokumentation
- Selbst erfahrene Mitglieder sind sich über Grundlagen uneins (z.B. Punktesystem).

Woran die Nutzer scheitern

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

Sichere Passwörter?

- Mindestens 8 Zeichen

Sichere Passwörter?

- Mindestens 8 Zeichen

password

Sichere Passwörter?

- Mindestens 8 Zeichen
- Groß- und Kleinschreibung

`password`

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 Vormonatpasswort

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 Vormonatsspasswort

\$epTemBer_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 **'lll!100'** merken?

Size Matters

Zeichenvorrat 100

8 Stellen, **10^{16}** Kombinationen

12 Stellen, **10^{24}** Kombinationen

14 Stellen, 10^{28} Kombinationen

16 Stellen, 10^{32} Kombinationen

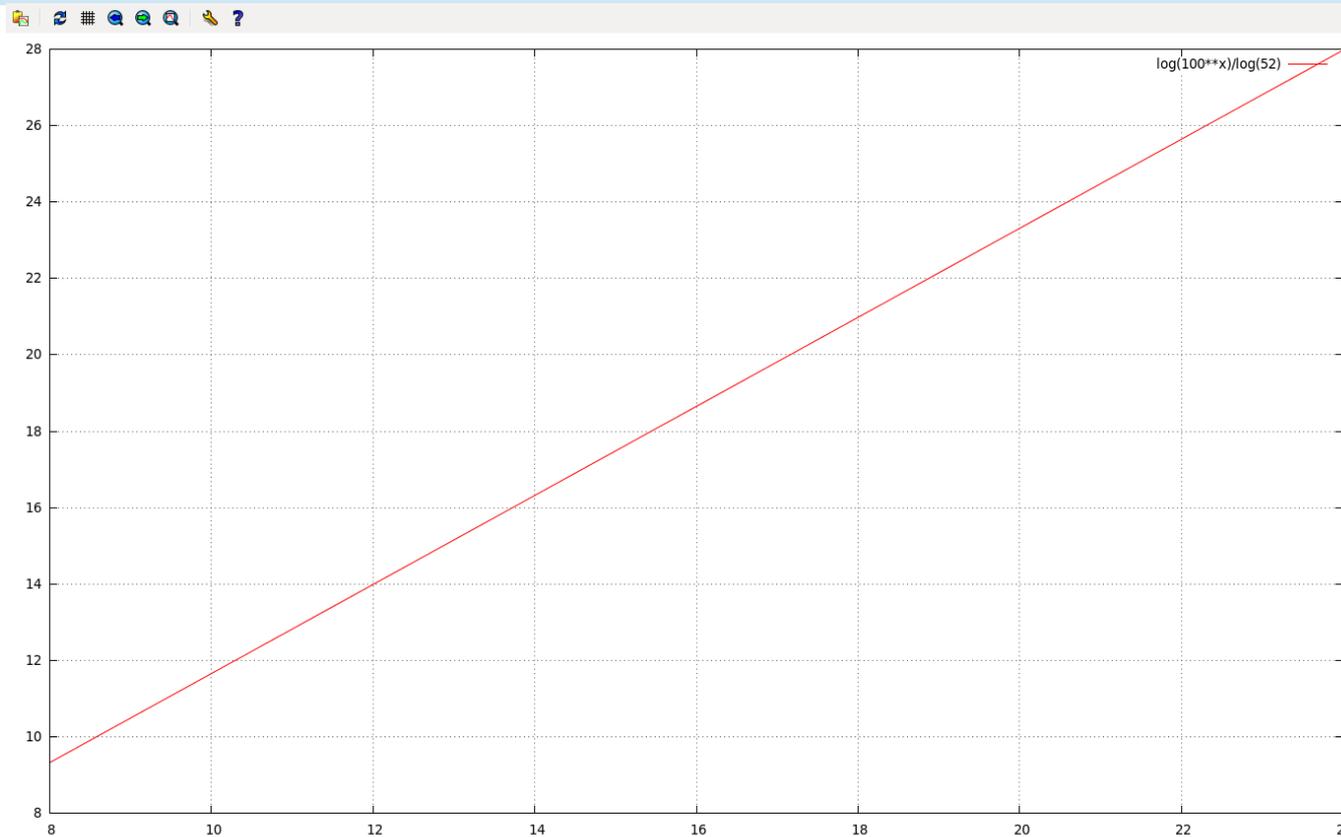
Groß- und Kleinschreibung

10 Stellen, $1,4 * 10^{17}$ Kombinationen

14 Stellen, **10^{24}** Kombinationen

17 Stellen, **$1,5 * 10^{29}$** 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} Komb | 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

| | |
|----------------------------------|-----------------|
| <code>^cec7FIX{^6L1Q_HB</code> | Homebanking |
| <code>^cec7FIX{^6L1Q_mail</code> | Mail |
| <code>^cec7FIX{^6L1Q_ebay</code> | Versteigerungen |

KeePass



KeePass Password Safe

This is the official website of KeePass, the free, open source, light-weight and easy-to-use password manager.

[\[Awards\]](#) [\[RSS Feed\]](#)

Home

- Home & News
- Forums
- Feature List
- Screenshots

Getting KeePass

- Downloads
- Translations
- Plugins / Ext.

Information / WWW

- Help
- FAQ
- Security
- Awards
- Links
- Search

Latest News

- KeePass 1.23 released**
2012-07-01 13:39. [Read More >](#)
- KeePass 2.19 released**
2012-05-01 13:44. [Read More >](#)
- KeePass 1.22 released**
2012-04-20 11:36. [Read More >](#)
- KeePass 2.18 released**
2012-01-05 13:52. [Read More >](#)

[\[News Archive\]](#)

What is KeePass?

Today you need to remember many passwords. You need a password for the Windows network logon, your e-mail account, your website's FTP password, online passwords (like website member account), etc. etc. etc. The list is endless. Also, you should use different passwords for each account. Because if you use only one password everywhere and someone gets this password you have a problem... A serious problem. The thief would have access to your e-mail account, website, etc. Unimaginable.

Support this project [Donate](#)

KeePass is a free open source password manager, which helps you to manage your passwords in a secure way. You can put all your passwords in one database, which is locked with one master key or a key file. So you only have to remember one single master password or select the key file to unlock the whole database. The databases are encrypted using the best and most secure encryption algorithms currently known (AES and Twofish). For more information, see the [features page](#).

MyDatabase.kdb - KeePass Password Safe

| File | User Name | Password | URL | Notes |
|-------------|-----------|----------|-----|-----------------------------|
| Example #1 | Anonymous | | | Copy User Name to Clipboard |
| Example #2 | Anonymous | | | Copy Password to Clipboard |
| Example #3 | Anonymous | | | Open URL |
| Example #4 | Anonymous | | | Copy Password to... |
| Example #5 | Anonymous | | | Print Auto Type |
| Example #6 | Anonymous | | | Auto Type |
| Example #7 | Anonymous | | | Edit/View Entry |
| Example #8 | Anonymous | | | Duplicate Entry |
| Example #9 | Anonymous | | | Delete Entry |
| Example #10 | Anonymous | | | Open Website (if Selected) |
| Example #11 | Anonymous | | | Select All |
| Example #12 | Anonymous | | | End in Database... |
| Example #13 | Anonymous | | | Find in Group... |
| Example #14 | Anonymous | | | Delete |

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

KeePass



KeePass Password Safe

This is the official website of KeePass, the free, open source, light-weight and easy-to-use password manager.

[\[Awards\]](#) [\[RSS Feed\]](#)

Latest News

- KeePass 1.23 released**
2012-07-01 13:39. [Read More >](#)
- KeePass 2.19 released**
2012-05-01 13:44. [Read More >](#)
- KeePass 1.22 released**
2012-04-20 11:36. [Read More >](#)
- KeePass 2.18 released**
2012-01-05 13:52. [Read More >](#)

[\[News Archive\]](#)

What is KeePass?

Today you need to remember many passwords. You need a password for the Windows network logon, your e-mail account, your website's FTP password, online passwords (like website member account), etc. etc. etc. The list is endless. Also, you should use different passwords for each account. Because if you use only one password everywhere and someone gets this password you have a problem... A serious problem. The thief would have access to your e-mail account, website, etc. Unimaginable.

KeePass is a free open source password manager, which helps you to manage your passwords in a secure way. You can put all your passwords in one database, which is locked with one master key or a key file. So you only have to remember one single master password or select the key file to unlock the whole database. The databases are encrypted using the best and most secure encryption algorithms currently known (AES and Twofish). For more information, see the [features page](#).

Support this project [Donate](#)

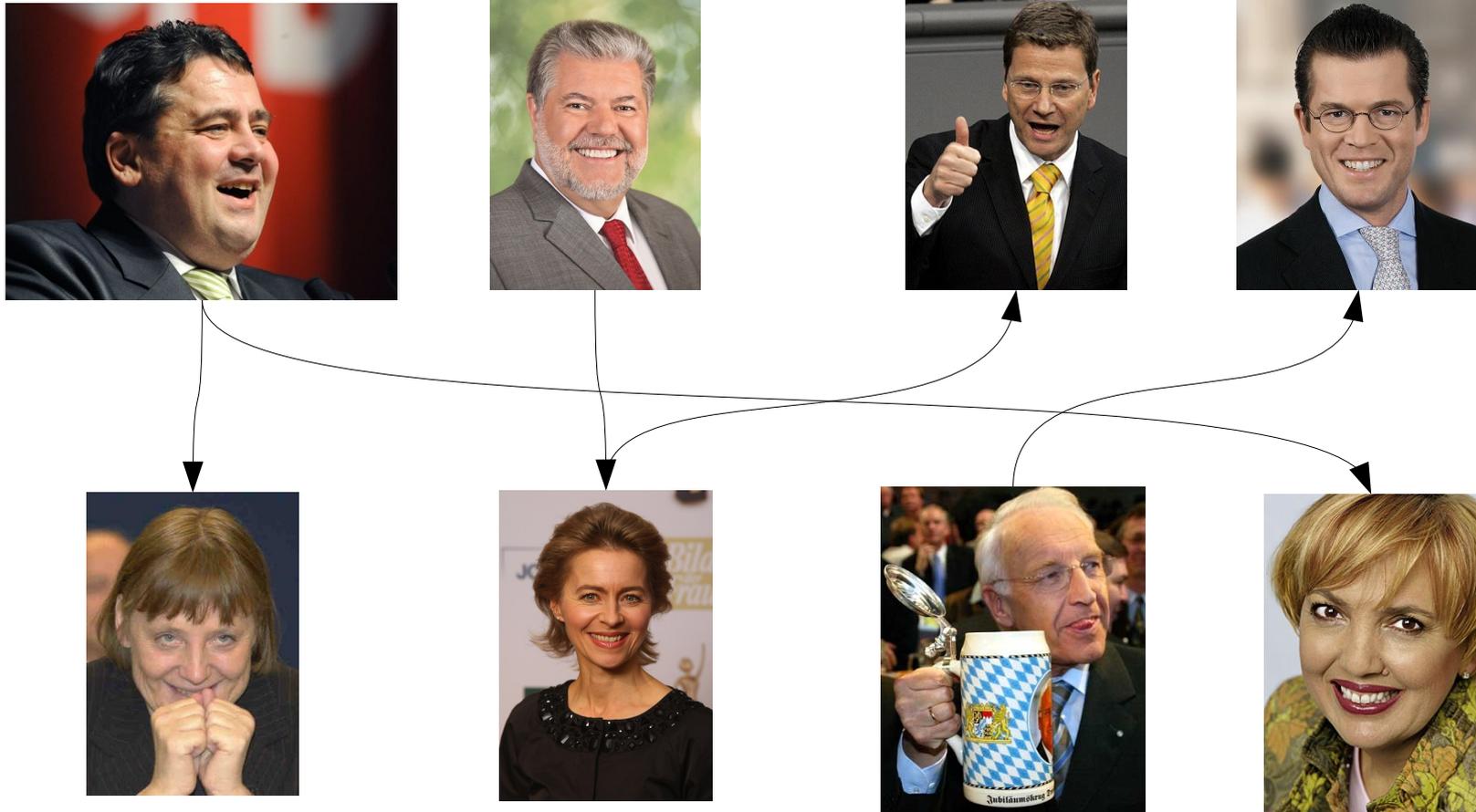
- + Erleichtert die Verwaltung umfangreicher Passwortsammlungen
- + Komplexe und häufig wechselnde Passwörter werden handhabbar
- Keystore-Passwort SPOF
- Funktioniert nicht (Zwischenablage != Zwischenablage)

Fazit

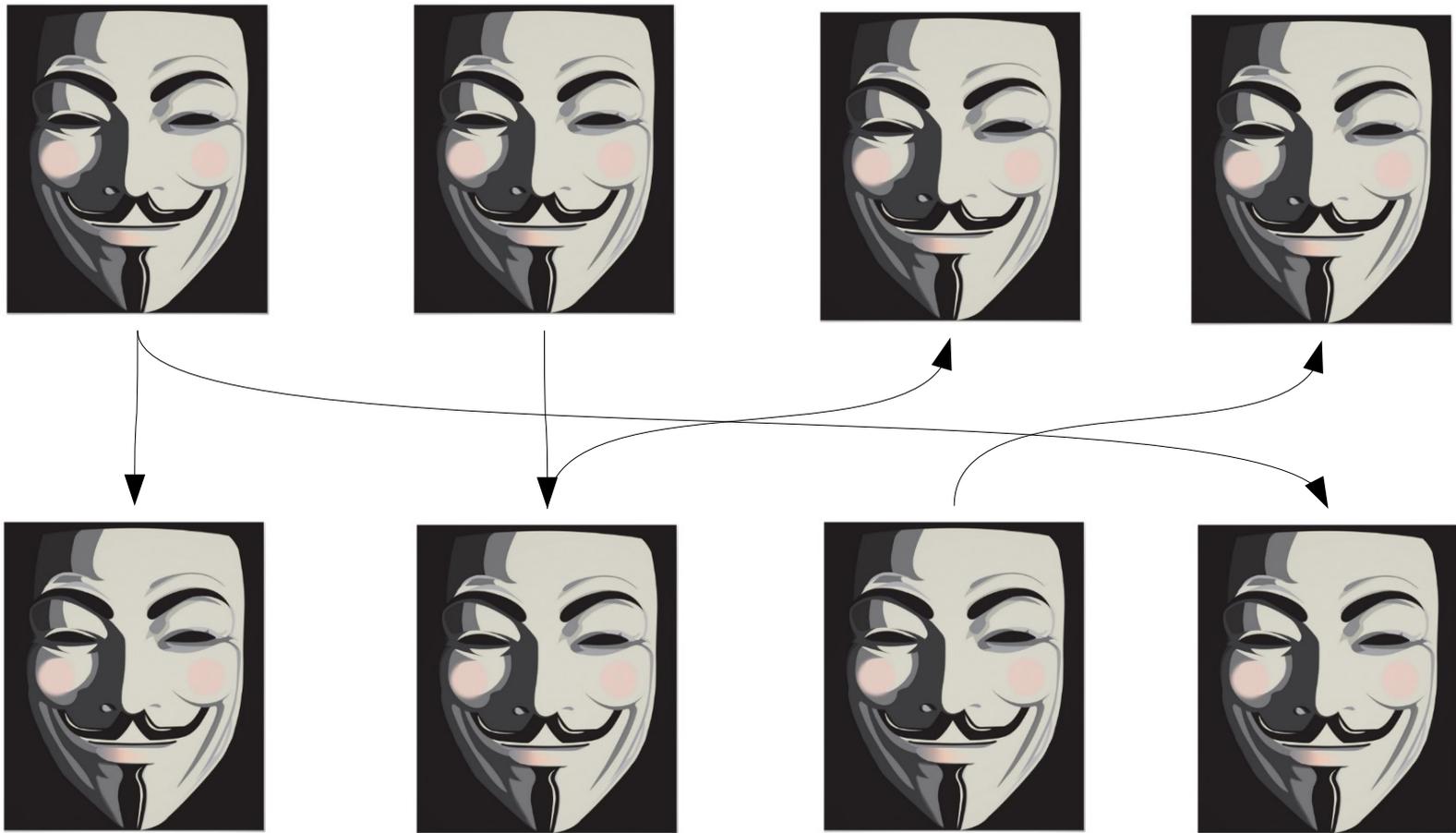
- Passworte sind Mist
- Die Alternativen (Biometrie, Gesten) ebenfalls
 - teure Zusatzhardware
 - geringe Verbreitung
 - Erkennungsfehler
 - angreifbar



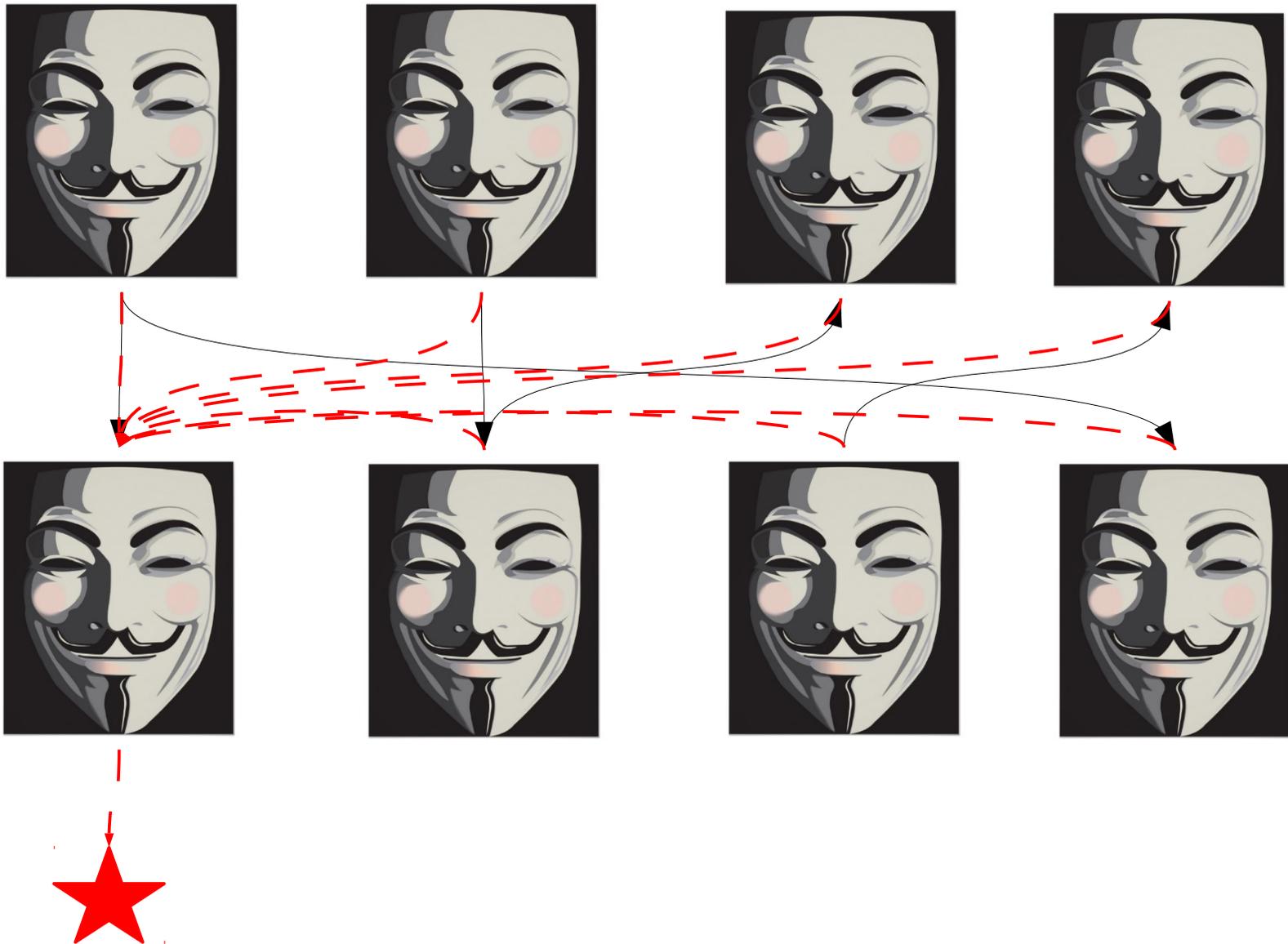
Verschlüsselung allein schützt nicht



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.

