In god we trust
the rest we monitor

Anonyme (und private) Kommunikation

Leitfaden für TOR, OpenPGP und weitere zur Anonymität und Privatsphäre

Inhaltsverzeichnis

0 Vorwort

Dieses Dokument wurde geschrieben, um allen Interessierten eine Anleitung zu geben, mit der sie ihre Privatsphäre und Anonymität bequem wahren können. Das können Journalisten sein, sowie auch Unternehmen (Firmengeheimnisse) oder der Otto-Normalverbraucher. Der Inhalt des Dokuments basiert auf eigenen Erfahrungen und am besten bewerteten Lösungswegen und dient dem Einblick und Einstieg zu den am wichtigsten empfundenen Methoden.

Viele Menschen sind dem noch zu fremd und scheuen, aufgrund des komplexen Eindrucks, sich mit den Themen auseinanderzusetzen. Hier sind keine neuartigen Wundermittel aufgeführt, sondern nur Vorgänge, die in weniger als eine Stunde zu einer völlig anonymen Identität im Internet verhelfen und dazu gebraucht werden können, private und anonyme Kommunkations-Infrastrukturen aufzubauen, wie sie z.B. von Firmen verwendet werden.

Man braucht auch kein Informatik-Studium absolviert zu haben um diesen Text zu verstehen. Man sollte aber auch kein Laie sein. Hier finden Verweise auf Dokumentationen und Seiten statt, wenn ich der Meinung bin, dass diese sich besser ausdrücken, als ich es je könnte. Man sollte sich möglichst alle anschauen oder sich dessen Inhalt bewusst sein, damit keine Fragen offen bleiben.

1 TOR

https://www.torproject.org/

TOR ist ein Anonymisierungsdienst zur Verschleierung der Netzwerkverbindungen. Alle ausgehenden Verbindungen können von TOR gehandhabt werden. Zumeist wird es in Kombination eines HTTP-Proxys (http://www.privoxy.org/) zum Surfen verwendet, aber man kann auch IM-Dienste oder den E-Mail-Verkehr darüber leiten, worauf wir hier tiefer eingehen werden. Es wird empfohlen sich mit TOR vertraut zu machen, denn es ist unser fundamentales Werkzeug, um volle Anonymität und Privatsphäre zu sichern.

Jedoch muss man sich aber auch der Gefahr bewusst sein, dass ausgehender Verkehr beim TOR-Exit-Node unverschlüsselt durchläuft und deshalb abgehört werden kann. Dies lässt aber nicht auf den Nutzer schließen (außer man überträgt sensible Daten, die einem verraten) und die Daten können wir anhand von nochmals verschlüsselten Verbindungen (SSL, TLS) verunkenntlichen, was wir auch machen werden.

1.1 Warum TOR und nicht I2P, JAP o.ä.?

http://www.i2p2.de/

http://anon.inf.tu-dresden.de/

TOR ist von allem am meisten auf unsere Bedürfnisse zugeschnitten. I2P wurde mit der Intention entwickelt, ein internes Netzwerk im Internet zu bauen, das vollkommen anonym ist. Das ist auch eine sehr gute Idee, jedoch ist die Bindung zum "normalen" Internet (worauf wir hier eigentlich aus sind) bei diesem Dienst ungeeignet. Außerdem beinhaltet TOR auch ein solches internes Netzwerk (Hidden-Services), auch wenn dieses nicht so schnell ist wie von I2P.

JAP ist sehr hinterfragt, daher auch hier als ungeeignet betrachtet.

1.2 Informationen

Es gibt sehr viele Seiten, die ausführliche Informationen über TOR bereithalten. Dazu zählen Dokumentationen zur Bedienung von TOR (einfach per Suchmaschine auffindbar) bis hin zu Statusinformationen über das Netzwerk, wie z.B.

```
https://torstat.xenobite.eu/
http://torstatus.blutmagie.de/index.php
```

Dort sind IP's, Nicknamen, Kontaktinformationen, Fingerprints, Schlüssel und weitere Informationen von allen TOR-Servern hinterlegt, was uns bei einem späterigem Problem weiterhelfen wird.

1.3 Download & Installation

http://www.torproject.org/download.html.de

Es wird empfohlen das Paket zu installieren. Hier sind bereits die wichtigsten Konfigurationen vorgenommen und man erspart sich eine Menge Arbeit. Zur Installation, Grund-Konfiguration und Funktionsweise gibt es bereits ausführliche Dokumentationen, bei der ich auf eine verweisen möchte:

```
http://www.torproject.org/docs/tor-doc-windows.html.de
```

Es ist empfehlenswert vorher wenigstens grob zu verstehen, wie das TOR-Netzwerk funktioniert. Es ist nicht kompliziert und es ist besser ein Bild vor dem geistigen Auge zu haben, bevor man mit diesem Dokument fortfährt. Ich erwarte, dass die meisten Nutzer darüber eh schon informiert sind, weswegen ich hier keine ausführliche Erklärung gebe.

1.4 Konfiguration

Viele empfinden TOR im Rohzustand als sehr langsam. Das auch zurecht, hat aber auch seine Gründe. Es gibt einzelne Nutzer, die das Netzwerk schnell überladen (Filesharing, übertriebene Downloads) was sich unmittelbar auf die anderen Nutzer auswirkt, weswegen wir ein wenig an den Einstellungen rumschrauben. Zunächst ist aber zu bemerken, dass die Geschwindigkeit des Netzwerks schneller ist, wenn man als Server mitmacht. Am sichersten ist es, wenn man sich nur für das interne Netzwerk anbietet und keinen Ausgang zum Internet erlaubt (in der torrc: "ExitPolicy reject *:*") was Mißbrauchsvorwürfe fernhält.

1.5 torrc

http://keksa.de/?q=pimpmytor

Es gibt für TOR viele Konfigurationen, die vieles beeinflussen. Diese Konfigurationen sind in der "torrc"-Datei einsehbar und veränderbar. Eine komplette Dokumentation der Optionen gibt es hier:

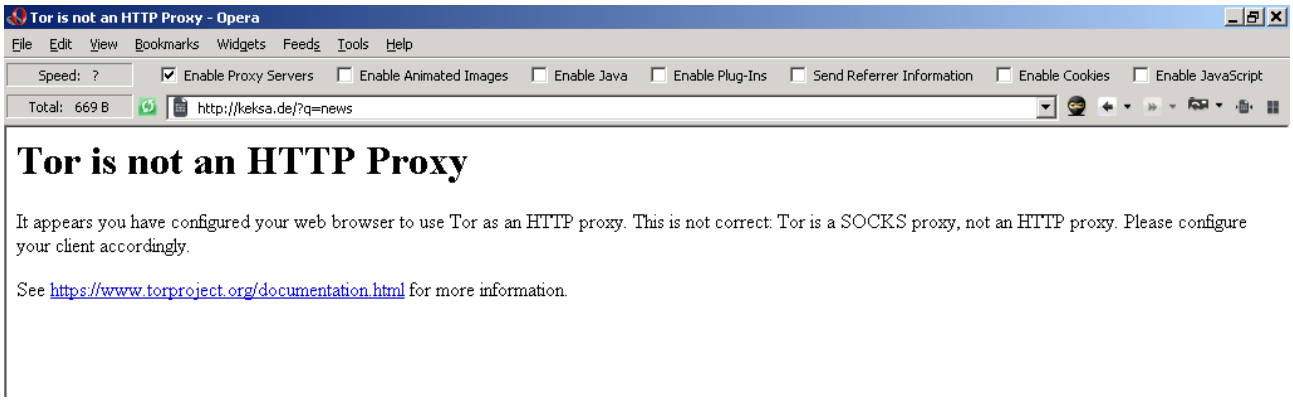
```
http://www.torproject.org/tor-manual.html.en
```

Die wichtigste Option, die unsere Schnelligkeit beeinflusst, ist "NumEntryGuards". Als Standardwert ist 3 vorkonfiguriert, jedoch reagiert das Netzwerk viel schneller, wenn wir dieses auf 16 einstellen. Es bewirkt, dass mehr "Eingänge" zum Netzwerk gehalten werden. Also hängen wir unserer torrc folgendes an:

```
NumEntryGuards 16
```

2 Surfen über TOR

TOR selber bietet nur einen SOCKS-Proxy. Diese Art von Proxy kann keine HTTP-Anfragen handhaben. Deshalb benötigen wir zwischen unserem Browser und TOR noch einen HTTP-Proxy. Wir verwenden hier Privoxy, da sich dieser in unseren Kreisen am meisten etabliert hat.



2.1 Privoxy

http://www.privoxy.org/

Privoxy bietet sehr viele Möglichkeiten der Veränderung. Es filtert automatisch ungewollte Scripts und Bilder (Werbung) aus und ist klein sowie auch schnell. Diese Eigenschaften machen wir uns zunutze; wir werden bei TOR noch Fähigkeiten ausnutzen, die sich mit Privoxy gut verbinden lassen. Dazu öffnen wir die "user.action"-Konfigurationsdatei von Privoxy und fügen am Ende folgendes ein:

```
{ +client-header-filter{hide-tor-exit-notation} }
.exit
```

Dies führt dazu, dass Anfragen vom Browser mit speziellen Hostnamen (z.B. http://aboutyou.keksa.de.$7f6a632b86036964b7e364e78453def982eaee4f.exit/) in dem HTTP-Header modifiziert werden. Es ermöglicht uns dann für einzelne Netzwerkverbindungen ausgesuchte Exit-Nodes auszuwählen, was von strategischem Vorteil ist. Aber dazu später mehr.

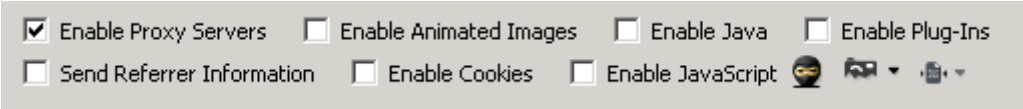
2.2 Browser

http://www.mozilla-europe.org/de/firefox/

http://de.opera.com/

Empfohlene Browser sind der Firefox und Opera. Dieses Tutorial basiert auf Beispielen des Opera-Browsers, da der schon ohne Erweiterungen alle Funktionen bringt, die wir benötigen. Und zwar setzen wir auf die schnelle und unkomplizierte Konfigurationsmöglichkeiten des Browsers. Hierzu können wir uns über die Anpassung der Opera-Oberfläche folgende Einstellungs-Knöpfe direkt auf die Oberfläche ziehen:

```
"Javascript aktivieren"
"Cookies aktivieren"
"Herkunfts-Informationen senden"
"Plug-Ins aktivieren"
"Java aktivieren"
"Proxy Server aktivieren"
"Bilder aktivieren/deaktivieren" (Browser-Ansicht)
```



2.3 Browser-Einstellungen

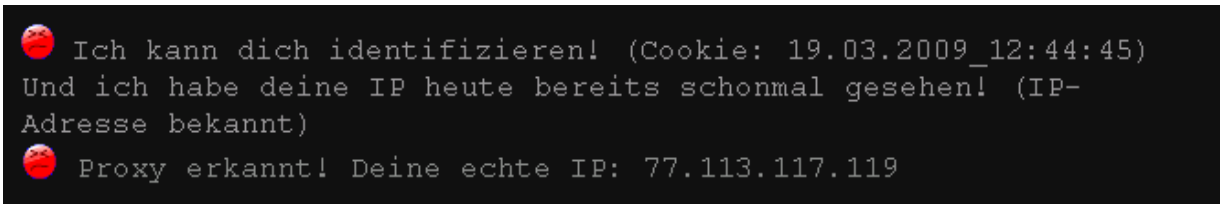
Die richtige Konfiguration des Browsers ist auch ein sehr wichtiger Punkt. Eine falsche Konfiguration kann unsere Anonymität aufdecken oder sogar zum Ausnutzen von Sicherheitslücken führen, womit wir womöglich sogar den ganzen Inhalt des Computers preisgeben. Außerdem haben viele Seiten Scripte und Plug-Ins implementiert, die das Surfen um einiges langsamer und unerträglicher machen.

2.3.1 Javascript

Standardmäßig deaktivieren. Javascript ist auf fast jeder Seite eingebunden und lahmt den Browser (meist ohne für den Otto-Normalverbraucher erkennbare Funktion) ab und sendet oftmals zusätzliche Anfragen. Google hat auf wahnsinnig vielen Webseiten Javascripte eingebunden, um Nutzerverhalten zu tracken. Fast alle Sicherheitslücken machen sich Javascript zunutze. Also nochmals: Deaktivieren!

2.3.2 Cookies

Standardmäßig deaktivieren. Cookies sind auch heute noch sehr umfragene Gestalten. Deren Intention ist es eigentlich nur, den Nutzer zu identifizieren. Dies ist bei Authentifizierungen auch manchmal sehr hilfreich und nützlich, aber leider wird diese Technologie fast immer übertrieben ausgenutzt und dient ebenfalls nur zum Tracken von Nutzerverhalten.



2.3.3 Herkunfts-Informationen

Das sogenannte Referrer-Feld im HTTP-Header dient dazu um der besuchten Seite zu sagen, von welcher Seite man kommt. Dies hat zwar keine großen Negativen auswirkungen, aber trotzdem würde ich dies ebenfalls standardmäßig deaktivieren.

2.3.4 Plug-Ins

Als Plug-Ins sind hier Browserimplementionen wie Flash, Quicktime, Adobe Reader und Windows-Mediaplayer gemeint. Diese werden oftmals auch als Sicherheitslücke ausgenutzt und könnten die eigene Identität verraten. Deshalb deaktivieren.

2.3.5 Java

Deaktivieren. Ein Java-Aplett, das im Browser ausgeführt wird, ist ein (zwar eingeschränktes, aber dennoch) selbstständiges Programm. Es verfolgt seine eigenen Regeln und übernimmt z.B. nicht die Proxy-Einstellungen des Browsers. Dies können Internet-Seiten ausnutzen um ein Aplett zu starten, das sich selbst mit der Seite verbindet und somit die wahre IP und Identität des Besuchers aufdeckt. Beispiel eines solchen Java-Apletts finden Sie auf:

```
http://aboutyou.keksa.de/
```

Dieses Beispiel ist sehr einfach selbstprogrammiert und Open Source (http://keksa.de/?q=proxychecker).

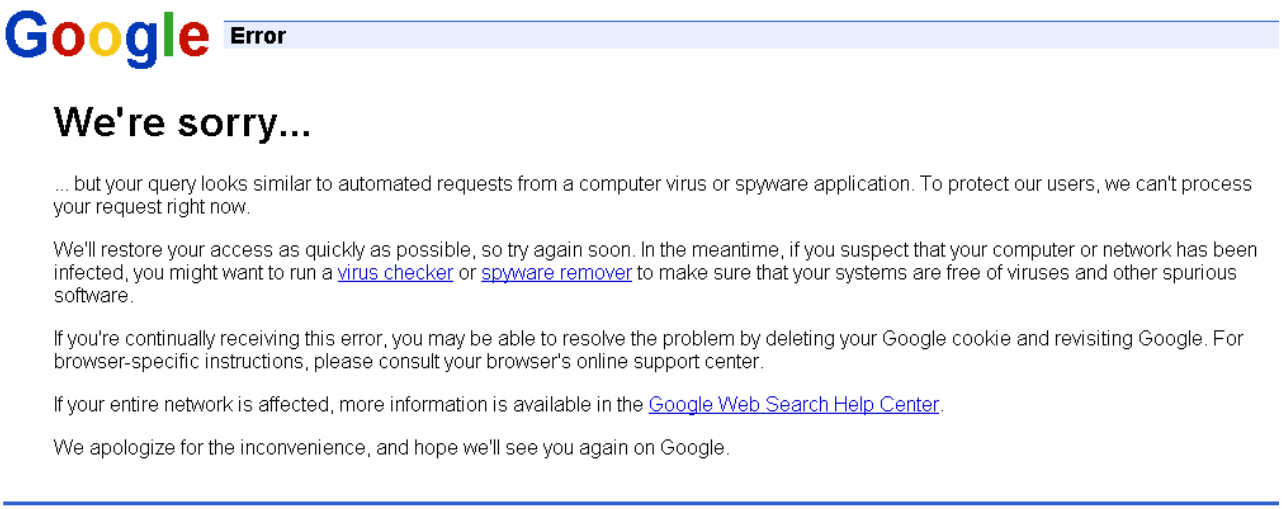
2.3.6 Bilder

Es wird empfohlen Bilder im Browser zu deaktivieren. Beim Surfen wird für jedes Bild eine eigene Anfrage gesendet, was sich bei TOR als sehr große Surf-Bremse herausstellt. Auch beim normalen Surfen führt das Deaktivieren der Bilder zu einem unfassbar schnellen Surferlebnis.

Die meisten Bilder im Web sind eh nur verwirrende Dekoration. Falls aber dennoch Bilder gebraucht werden (z.B. Captcha's oder Internet-Seiten, die nur aus Bildern bestehen) kann man dies schnell mit einem Klick in der angepassten Browser-Oberfläche aktivieren.

2.4 Google und TOR

Wenn man länger über TOR surft, bemerkt man, dass man öfters auf einer Sorry-Seite von Google landet, wenn man dort Suchanfragen tätigt. Es wird in Frage gestellt, ob man Spyware auf dem Rechner hat. Keine Sorge, dies sollte nicht der Fall sein. Es liegt daran, dass von dem TOR-Server, von dem unsere Suchanfrage ausgeht, in kurzer Zeit sehr viele Suchanfragen ausgegangen sind, was Google mit dieser Seite blockt. Das ist nervig, aber es gibt auch da eine Lösung.



Dazu muss jemand Adsense-Verträge mit Google (Irland) abschließen und kriegt dann die Möglichkeit mit Google seine eigene Seite durchsuchen zu lassen. Aber auch das ganze Web kann durchsucht werden, und dies ohne, dass jemals eine "Sorry"-Seite auftaucht. Dabei muss bei der Google-Homepage der Partner-Code angegeben werden. Ich selber habe eine Homepage, habe diese Verträge abgeschlossen und bin Partner. Ich nutze "meine" Suchmaschine andauernd ohne gestört zu werden, die URL dazu ist:

```
http://www.google.com/custom?
hl=de&client=pub-1276475330944308&channel=7715305802&cof=FORI
D%3A1%3BAH%3Aleft%3BS%3Ahttp%3A%2F%2Fkeksa.de%3BCX%3Akeksa
%252Ede-Suche%2520%2528v%252E13%252E37%2529%3BL%3Ahttp%3A%2F
%2Fkeksa.de%2FBilder%2FWlogo.jpg%3BLH%3A50%3BBGC%3A
%23111111%3BT%3A%23aaaaaa%3BLC%3A%23cccccc%3BVLC%3A
%23888888%3BGALT%3A%23999999%3BGFNT%3A%23999999%3BGIMP%3A
%23999999%3BDIV%3A%23ffffcc
%3B&adkw=AELymgUlzau3j56ZlO7W5itP0pSB4N8amIFetpXJRpOKjJ89or70
BFkVBcMPzTpG49Li6ptHc86etWIHlXE_VKMIX4CYHRuHLpS4YWZ1aOlKCti5e
G6RQRJ7e6heTxUMmLzCDSLKeAInFSbWXiFM7wRy6rftuLFYoVjSt0xLDfigNC
kPHw2PaDZakL6WfcZT_n9RM09qc9JYA8c_PDaaFY7yVyFBJsryrkAdrimpr1U
pFgmC_afuvRRYp9usi-
HmvmtSt5E9RL2IrIxm9xHnCEliv4KXAnG0FwQ7a6PAe4u_YvPLxy-
kh2R0qyKlyWAvFq7EbFcpiVEJFqE34eZ-
uvbcvoURwVr3YmmDCtQT_BMivIEq8_8AYNjXG4HSs6DeXVddwFaAySIHARB_G
GzS1-8soyVEsC7jc913S16Tpdy-
D0yCa1kjboM&num=100&ie=ISO-8859-1&oe=ISO-8859-1&q=&btnG=Suche
&cx=%21partner-pub-1276475330944308%3A9pgwhy-6zq0
```

So lautet die Original-Adresse. Falls euch die Farben nicht gefallen, kann ich es gerne ändern oder auf Google-Standard setzen, mir sind sie egal. Die Adresse ist etwas lang, deswegen habe ich eine verkürzte Version gemacht, die auch die Original-Google-Farben beinhalten. Ich kann aber nicht versichern, dass diese kurze Adresse immer funktionieren wird, da man sie in dieser Form eigentlich nicht verwenden sollte. Hier die kurze Version:

```
http://www.google.com/custom?hl=de&num=100&cx=
%21partner-pub-1276475330944308%3A9pgwhy-6zq0
```

Ich bin auf der Welt nicht der einzigste Partner von Google, deswegen werden sich sicherlich noch tausend andere solche URL's oder Partner-Codes finden lassen.

3 E-Mail

Das nächst-interessante wäre wohl ein voll-anonymer und privater E-Mail Verkehr. Dazu bedienen wir uns ebenfalls dem TOR-Netzwerk und zusätzlich noch der wunderbaren Fähigkeit der OpenPGP's. Hier als Beispiel verwende ich den E-Mail Clienten „Thunderbird“ von Mozilla (http://www.mozilla-europe.org/de/products/thunderbird/), für diesen gibt es ein sehr bequemes OpenPGP-Plug-In.

3.1 E-Mail-Account registrieren

Doch bevor wir uns dem Thunderbird zuwenden, müssen wir uns einen Account registrieren. Hierbei ist es wichtig, dass wir einen Mailer finden, der verschlüsselte Verbindungen zum Abrufen (POP3) und Senden (SMTP) der E-Mails erlaubt, da ansonsten das Abhören der Zugangsdaten beim TOR-Exit-Node möglich wäre. Als Beispiel nenne ich hier Freemail von web.de (http://web.de/fm/), da dieser unsere Anforderungen erfüllt und dazu auch noch gratis ist. Außerdem gibt es bei Freemail eine interessante Hürde, die wir überwinden müssen und die zum Verständnis von TOR-Netzwerk beitragen kann.

Und zwar besuchen wir die Freemail-Seite natürlich per Browser über das TOR-Netzwerk, damit man keine direkte Verbindung zu uns hat. Wenn wir nun eine kostenlose E-Mail-Adresse einrichten möchten, stoßen wir mit hoher Warscheinlichkeit auf eine Meldung, die besagt, dass wir von einer nicht-erlaubten IP auf die Seite zugreifen. Freemail mag es nämlich nicht, wenn man über das TOR-Netzwerk neue Adressen anlegt, da Freemail großes Interesse daran zeigt, bei Mißbrauch den tatsächlichen Nutzer feststellen zu können. Deswegen ist Anonymität nicht willkommen und die meisten IP's der TOR-Server werden geblockt.

Aber es ist kein Problem dagegen vorzugehen. Die IP-Listen der meisten Block-Einrichtungen sind nämlich nicht aktuell. Es ist schwer die IP-Listen aktuell zu halten, außer man betreibt einen eigenen TOR-Server (was Anbieter wie Freemail nicht tun). Deswegen können wir uns einen ganz neuen Server aus dem TOR-Netzwerk aussuchen, der noch nicht geblockt wird und eine Anfrage über diesen versenden (das setzt aber vorraus, dass Privoxy wie oben genannt konfiguriert ist).

Dazu besuchen wir die TOR-Infoseite von blutmagie.de und lassen uns die Liste nach "Uptime" (Online-Zeit der Server) sortieren:

```
http://torstatus.blutmagie.de/index.php?SR=Uptime&SO=Asc
```

Nun suchen wir uns einen Server heraus, der gerade frisch dem TOR-Netzwerk beigetreten ist und zudem als Exit-Server markiert ist. Diesen inspizieren wir, indem wir auf den Router-Namen klicken und wichtige Details über den Server erhalten. Und zwar benötigen wir die "Exit Policy Information", die uns unten rechts angezeigt wird und den Fingerprint in der "General Information"-Tabelle. Wir schauen zuerst, ob der Server in der Exit Policy einen Ausgang für unsere Dienste erlaubt. Bei Freemail läuft die Registrierung über HTTPS, also Port 443 (normales HTTP ist Port 80). Wenn der Server Port 443 blockt (Exit Policy "reject *:443" o.ä.), dann ist er für uns unbrauchbar und wir müssen in der Liste den nächst-besten heraussuchen. Wenn wir einen Server gefunden haben, der unsere benötigten Ports erlaubt (am besten "accept *:80" und "accept *:443" oder "accept *:*" o.ä.), dann notieren wir uns von diesem den Fingerprint. Anhand des Fingerprints können wir den Server ansprechen und gezielt als Exit-Node verwenden. Wichtig ist nur, wie gesagt, dass man Privoxy dazu konfiguriert hat die hide-tor-exit-notation zu Filtern, sonst kommen die Webserver durcheinander und man bekommt eine Fehlermeldung als Antwort.

Dem Fingerprint entnehmen wir nun alle Leerzeichen und fügen ihn in der URL-Leiste des Browsers hinter dem Hostnamen mit vorgehendem ".$" und danach folgendem ".exit" an. Beispiel:

```
Fingerprint:
     "AAAA AAAA AAAA AAAA AAAA AAAA AAAA AAAA AAAA AAAA"

Leerzeichen entfernen:
     "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"

Hostname "web.de" mit .$<fingerprint>.exit erweitern:
     "web.de.$AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.exit"
```

Mit diesem modifiziertem Hostnamen besuchen wir nun die Freemail-Seite erneut. Da der TOR-Server neu ist, ist er der Freemail-Seite unbekannt; sie wissen also nicht, dass wir einen Anonymisierungsdienst verwenden und die Registrierung der E-Mail-Adresse kann problemlos und anonym fortgeführt werden.

3.2 Thunderbird konfigurieren

http://www.mozilla-europe.org/de/products/thunderbird/

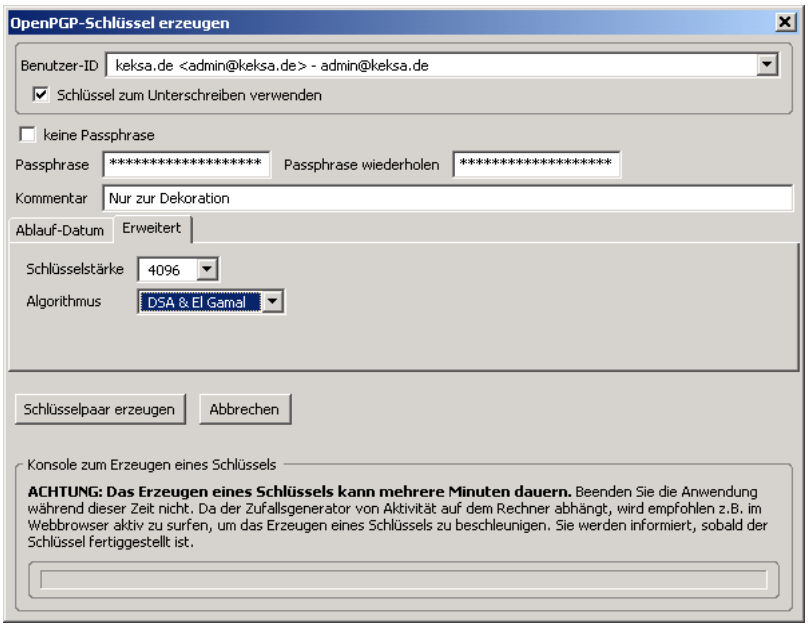
Es dürfte keinerlei Problem sein auch Anleitungen zur Konfiguration anderer üblichen E-Mail-Clients zu finden. Hier gehe ich aber speziell auf Thunderbird ein. Zunächst laden wir uns für Thunderbird das Torbutton Plug-In (https://addons.mozilla.org/en-US/thunderbird/addon/2275) und installieren es. Dieses erlaubt uns immer einen Überblick über die Proxy-Konfiguration zu haben (wie beim Opera-Beispiel) und schnell Änderungen vorzunehmen. Nun konfigurieren wir Thunderbird dazu, TOR zu verwenden. Und zwar verwenden wir für HTTP und SSL den Privoxy-Port (Standard 8118) und für SOCKS den TOR-Port (Standard 9050).

Nun erstellen wir uns ein neues Konto und richten unsere Verbindungen ein. Bei Freemail lautet der POP-Server "pop3.web.de", dabei verwenden wir SSL (Verschlüsselung ist hier dringend zu empfehlen) und den Port 995. Als Ausgangs-Server nutzen wir "smtp.web.de" mit TLS-Verschlüsselung und Port 587 (Freemail hat hier einen speziellen Reserve-Port, den wir verwenden). Wir vergewissern uns, dass unser Torbutton "Tor enabled" anzeigt und rufen zum Testen mit Thunderbird die Mails ab. Nun haben wir eine E-Mail-Adresse bei der wir nicht einmal unsere Identität verraten haben und vollig anonym sind. Als nächstes kommt die Privatsphäre, die wir uns durch OpenPGP holen.

3.2.1 OpenPGP

In diesem Fall dient die PGP-Verschlüsselung einzig und alleine der Geheimhaltung der Nachrichten vor dem E-Mail-Provider oder andere Drittpersonen. Für gewöhnlich bevorzugt man PGP auch, um sich dessen zu vergewissern, dass der Gesprächspartner der ist, für den er sich ausgibt; da wir aber auf anonymer Schiene fahren ergibt sich das. Wir laden uns für Thunderbird das Enigmail OpenPGP Plug-In (https://addons.mozilla.org/thunderbird/addon/71) und installieren dies. Mit diesem Plug-In ist es auch für Laien ein Kinderspiel sich PGP-Schlüssel erzeugen zu lassen. Ist das Plug-In installiert und aktiviert, so können wir über die Schlüssel-Verwaltungsoberfläche alle nötigsten Einstellungen vornehmen.

Bevor wir aber ein Schlüsselpaar erzeugen, müssen wir uns vergewissern, dass wir bereits ein Konto für die gewünschte E-Mail-Adresse in Thunderbird angelegt haben, da dies Voraussetzung ist. Beim Erzeugen gibt es nicht viele Optionen, daher ist es recht simpel. Man sollte aber bemerken, dass es besonders auf die Passpharse ankommt, falls der private Schlüssel mal geklaut oder versehentlich veröffentlicht wird. Viele halten auch bei den Verschlüsselungs-Algorithmen die Luft an, tatsächlich kann man sich informieren und von einem Algorithmus überzeugen lassen. Aber im Grunde genommen ist RSA zum Verschlüsseln und signieren, DSA nur zum signieren und El-Gamal nur zum verschlüsseln da (deswegen sind die letzten beiden auch in eine Gruppe gefasst). Das Ablauf-Datum ist dient dazu, jeden Nutzer in regelmäßigen Zeitabständen die Schlüssel zu erneuern (wie bei einem Passwort, das man regelmäßig ändern sollte, da man nie weiß, ob es nicht mittlerweile geknackt oder geklaut wurde).



Zur Erklärung: Dieser Erstellen generiert zwei Schlüssel (http://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem). Einen privaten Schlüssel und einen öffentlichen Schlüssel.

Den öffentlichen Schlüssel exportiert und veröffentlicht man, dieser beinhaltet die E-Mail-Adresse, das Ablauf-Datum, die Schlüssel-ID und den Schlüssel zum Verschlüsseln. Es reicht also, wenn man einfach nur den öffentlichen Schlüssel als Kontaktmöglichkeit angibt. Alle Nachrichten, die mit dem öffentlichen Schlüssel verschlüsselt werden, können nur mit dem privaten wieder entschlüsselt werden.

Der private Schlüssel ist nur dazu da, um die mit dem öffentlichen Schlüssel verschlüsselte Nachrichten zu entschlüsseln. Man hat die Möglichkeit beim privaten Schlüssel eine "Passpharse" anzugeben. Das ist ein Passwort, das abgefragt wird, wenn man diesen Schlüssel verwenden möchte. Dies ist dazu da, um geklaute private Schlüssel nicht so leicht verwendbar zu machen. Deshalb ist es von großer Bedeutung, dass man sich eine gute Passpharse ausdenkt.

Damit haben wir unsere Privatsphäre sehr weit ausgebaut. Überwacher, sei es nun der Provider oder auch jemand mit höherer Macht, haben es technisch nun sehr schwer Informationen zu lesen oder überhaupt Identitäten feststellen zu können.

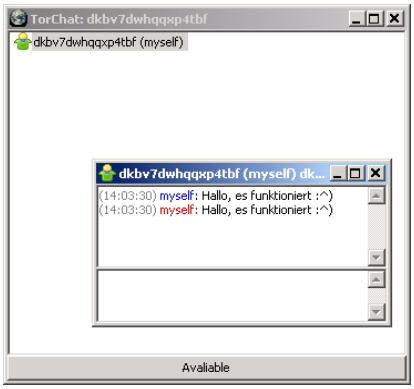
4 Instant Messaging

Es ist auch möglich gängige IM-Netzwerke über TOR zu verwenden. Jedoch ist dies nicht immer zu empfehlen, da die Datenströme vom TOR-Exit-Node abgefangen werden können. Dazu wurde für TOR ein eigener IM-Client namens "TorChat" (http://code.google.com/p/torchat/) geschrieben, der sich den Hidden Services bedient.

4.1 TorChat

http://code.google.com/p/torchat/

TorChat ist der wohl am simpelsten zu bedienende Instant Messenger. Er bedient sich dem internen Netzwerk von TOR, den Hidden Services. Alle Chat-Nachrichten und Dateitransfers sind vollkommen verschlüsselt und anonym. Man braucht nur TorChat zu starten (Registrierung erfolgt voll automatisch) und den gewünschten Gesprächspartner seine ID zu übermitteln.



Nachteil ist die anfängliche Trägheit, da der Client (besonders auf dem Windows-Systemen) fest an einem eigenen TOR-Prozess gebunden ist.

Zusätzlich ist anzumerken, dass man die eigene ID nicht überall publiziert, da es ein Kinderspiel ist fremde ID's zu übernehmen.

5 Kontakt

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.8 (MingW32)

mQGiBEmYWAkRBADAqTnw9Lwr6lma//jCFKsaa86kd1pWYsVh0G+tlZTZo1u9Ku/U
5Z5C5i3zblbFaiXLk1S/+mmdT6JtYy9VEL12dD5xhipTa68car4UkceDiW8KTmnf
2fphl29oRP8aJn0g96cOE6ulwCLlEO07tPwU9j9TXleOlIMEZNvnsFVy/wCg+Mz4
A5zCgMavX/5F7wEXR5R0hZUD/0r0hyuBxZNz2Vm+dgYtPvJdoJhYIosTb6goWtk7
iCJwJkoojISKfIjbxpRk4aLaUy7SXsjQpgmnABYcH/4JPU4pJJno4Adk1tKeVp6R
3fa+0zONiBZ/9bCCr7SmYa2PHk14v3nujMfPiecBaogsK43URauQ3uzCwZWvJncI
SXMiA/9RfCHJ09/TZto/NP5FS99so2nCyDYwpKk5gf63seTj8/seewG1+Ak+I5Bo
A8tBOTu2FOOjysDt0sg9+H8EpSNh+cFpTBRmwYOHL/2Rnwdn79ckeQTqQxHFjCYF
jv3EqBNp4V6jUnYJQZdrC5lMD6uCGPmOvv/5ruH6JuDMle9M9rQZa2Vrc2EuZGUg
PGFkbWluQGtla3NhLmRlPohmBBMRAgAmBQJJmFgJAhsjBQkHPEuABgsJCAcDAgQV
AggDBBYCAwECHgECF4AACgkQOSX6iWGT93cdwwCgrYA6Al28Ty6IGpIgkr88QscS
XYYAoJ5VMdMeluDYW7eufRLppWJysTMCuQINBEmYWAkQCADcLzRv4p/7M1pAqAW1
qvXbIhmfhSMD0CgBkA/UIzpN5/Dw5LbjWFs4H5nnuEVfedNkAP3rKzZUD6gabuNL
h8ppFZmhst/R035wCaDSL9+ZtdGlFX2JT3s8EjyiSCguOlzVICporgWtkcQ3y/VQ
PEU2Mj135nluRloDe9/2rr8lhMi/P0zIxPk2sjSXWg9GMEE0IfW7okl8TUsf0z7R
zEVVYXPMynCbSHW7kCmgQJhg480/y8khrnsa1hbPnJsbSzAWdVMJud8val5+UwII
3nmBM7bKPHM6g6kWBeMGbY2SvvarbFVlsW2G+7fHSysoG40ZezKEoB/xdPshLTHX
4Od3AAMFCACP3S7hFuWKi4z7bBoC4Z+ayGeaO6L/JGj9IzNeEa447aqNQtsm4Bve
iIU39O9z7KG1txR16pFaYnomnKCdmtvcbAKw5peidB763mTNXZkWeezsxdKtZem7
q2CLcPddBoj3cR6BFpPUjAMKXIxKjk+J3p5Kv5a0L6yKEKWKz8/wuSN35EapaIiH
wSt+prq3tk58N99IG9d8Rsq3eOEazNaFQgWOd8DvrBEzsTGbLEj2LVuN3FKVfYrq
jjn0zSRklC7lKtN0fLi9W3CzpbhlBsLYQTkFdk+4ezlutHJDfTlHtSl0x+UYv11e
BBs5njD5Nl2uNCqSVhyI59zUkQi3BOkTiE8EGBECAA8FAkmYWAkCGwwFCQc8S4AA
CgkQOSX6iWGT93e1OwCeNH6nr3W64SEU9I64jNYQ76oY1UoAn3HL36qv03xS6jkV
PL3d+b2FxZLs
=kdwO
-----END PGP PUBLIC KEY BLOCK-----

--

Webpage: http://keksa.de
E-Mail:  Tobias <admin@keksa.de>
Contact: http://keksa.de/?q=respond
PGP-Key: http://keksa.de/keksa.de.asc
Privacy: https://privacybox.de/keksa.msg
TorChat: (by appointment)
```