

E-Mail jenseits der Überwachung

WINDOWS

21. Dezember 2011

Zusammenfassung

Auch bei der Nutzung von GnuPG oder S/MIME für die Verschlüsselung von E-Mails ist es mitlesenden Dritten möglich, Absender und Empfänger zu protokollieren und anhand der erfassten Daten Kommunikationsprofile zu erstellen. Insbesondere die Vorratsdatenspeicherung und die darauf aufbauenden internationalen ESTI-Standards für Geheimdienste und Strafverfolger zeigen, dass diese nicht verschlüsselbaren Informationen für die Überwachung bedeutsam sind.

Es gibt mehrere Projekte, die einen überwachungsfreien Austausch von Nachrichten ermöglichen und somit beispielsweise für investigative Journalisten und deren Informanten den nötigen Schutz bieten und die Erstellung von Kommunikationsprofilen für E-Mails behindern.

1 Anonyme E-Mail Accounts

Im Kapitel Anonymisierungsdienste gibt es Anleitungen, wie man mit JonDo & Thunderbird oder mit Tor & Thunderbird einen anonymen E-Mail Account nutzen könnte. Als E-Mail Provider kann man einen zuverlässigen Anbieter im Web nehmen. Außerdem bieten I2P und Tor spezielle Lösungen:

- Das Invisible Internet Project (I2P) bietet mit Susimail einen anonymen Mailservice inklusive SMTP- und POP3-Zugang und Gateway ins Web oder mit I2P Bote einen serverlosen, verschlüsselten Mailedienst.
- TorMail gibt es als Hidden Service unter <http://jhiwjllqpyawmpjx.onion> mit POP3 und SMTP Service und ist auch aus dem Web unter xxx@tormail.net erreichbar.
- Tor Privat Messaging unter <http://4eiruntyxxbgfv7o.onion/pm/> ist ein Tor Hidden Service im Onionland, um Textnachrichten unbeobachtet auszutauschen. Der Dienst kann nur im Webinterface genutzt werden.

Hinweis: Informationen über Langzeitkommunikation können ihr Pseudonym deanonymisieren. Anhand der Freunde in der E-Mail Kommunikation sind Schlussfolgerungen auf ihre reale Identität möglich. Wenn sie einen wirklich anonymen E-Mail Account für eine bestimmte Aufgabe benötigen - z.B. für Whistleblowing - dann müssen sie einen neuen Account erstellen. Löschen sie den Account, sobald sie ihn nicht mehr brauchen.

2 alt.anonymous.messages

Um die Zuordnung von Absender und Empfänger zu erschweren, kann man das Usenet nutzen. In der Newsgruppe *alt.anonymous.messages* werden ständig viele Nachrichten gepostet und sie hat tausende Leser. Jeder Leser erkennt die für ihn bestimmten Nachrichten selbst. Es ist eine Art schwarzes Brett.

Es ist sinnvoll, die geposteten Nachrichten zu verschlüsseln. Dafür sollte der Empfänger einen OpenPGP-Key bereitstellen, der keine Informationen über seine Identität bietet. Normalerweise enthält ein OpenPGP-Schlüssel die E-Mail Adresse des Inhabers. Verwendet man einen solchen Schlüssel ist der Empfänger natürlich deanonymisiert.

Außerdem sollte man seine Antworten nicht direkt als Antwort auf ein Posting veröffentlichen. Da der Absender in der Regel bekannt ist (falls keine Remailer genutzt wurden) kann aus den Absendern eines zusammengehörenden Thread ein Zusammenhang der Kommunikationspartner ermittelt werden.

3 Mixmaster Remailer

Der Versand einer E-Mail über Remailer-Kaskaden ist mit der Versendung eines Briefes vergleichbar, der in mehreren Umschlägen steckt. Jeder Empfänger innerhalb der Kaskade öffnet einen Umschlag und sendet den darin enthaltenen Brief ohne Hinweise auf den vorherigen Absender weiter. Der letzte Remailer der Kaskade liefert den Brief an den Empfänger aus.

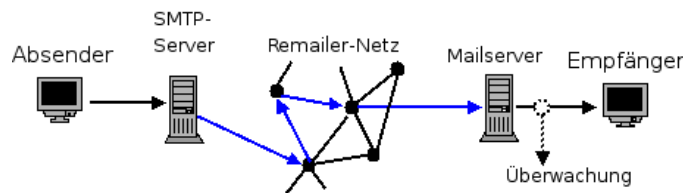


Abbildung 1: Konzept einer anonymen E-Mail

Technisch realisiert wird dieses Prinzip mittels asymmetrischer Verschlüsselung. Der Absender wählt aus der Liste der verfügbaren weltweit verteilten Remailer verschiedene Server aus, verschlüsselt die E-Mail mehrfach mit den öffentlichen Schlüsseln der Remailer in der Reihenfolge ihres Durchlaufes und sendet das Ergebnis an den ersten Rechner der Kaskade. Dieser entschlüsselt mit seinem geheimen Schlüssel den ersten Umschlag, entnimmt dem Ergebnis die Adresse des folgenden Rechners und sendet die jetzt (n-1)-fach verschlüsselte E-Mail an diesen Rechner. Der letzte Rechner der Kaskade liefert die E-Mail an den Empfänger aus.

Mitlesende Dritte können lediglich protokollieren, dass der Empfänger eine E-Mail unbekannter Herkunft und evtl. unbekanntes Inhalt (verschlüsselt

mit OpenPGP oder S/MIME) erhalten hat. Es ist ebenfalls möglich, Beiträge für News-Groups anonym zu posten.

Um die Traffic-Analyse zu erschweren, wird die Weiterleitung jeder E-Mail innerhalb der Kaskade verzögert. Es kann somit 2...12h dauern, ehe die Mail dem Empfänger zugestellt wird! Sollte der letzte Remailer der Kette die Nachricht nicht zustellen können (z.B. aufgrund eines Schreibfehlers in der Adresse), erhält der Absender keine Fehlermeldung. Der Absender ist ja nicht bekannt.

Wichtig: da die E-Mail keine Angaben über den Absender enthält, funktioniert der *Antworten-Button* der Clients auf der Empfängerseite nicht! Der Text der E-Mail sollte einen entsprechenden Hinweis enthalten!

3.1 Remailer-Webinterface nutzen

Die einfachste Möglichkeit, eine anonyme E-Mail zu schreiben, besteht darin, ein Webinterface zu nutzen. Es gibt verschiedene Angebote im Internet:

- <https://www.awxcnx.de/anon-email.htm>
- <https://www.cotse.net/cgi-bin/mixmail.cgi>

Verglichen mit der lokalen Installation eines Remailer Clients ist dies die zweitbeste Möglichkeit, eine anonyme E-Mail zu versenden. Den Betreibern der Server liegen alle Daten im Klartext vor und sie könnten beliebig loggen. Die Installation von Quicksilver (für Windows) oder Mixmaster (für Linux) finden sie in der Online-Version des Privacy-Handbuch.

4 Fake Mailer

Im Webinterface eines Fake-Mailers können sie eine beliebige Absender Adresse angeben. Um anonym zu bleiben, sollte man Fake Mailer nur mit Anonymisierungsdiensten nutzen. Es besteht kein Schutz gegen Aufdeckung des Absenders durch den Betreiber des Dienstes.

- <https://emkei.cz>

Im Gegensatz zu Remalern dauert es nicht mehrere Stunden, bis die Mail zugestellt wird. Es ist aber möglich, dass diese Mails in Spam-Filtern hängen bleiben, da viele Spam-Filter diese Absender Adresse und die IP-Adresse des sendenden Servers in ihre Bewertung einfließen lassen. Man sollte zusätzliche Spam-Merkmale im Text der Nachricht vermeiden.

5 PrivacyBox der GPF

Die PrivacyBox (<https://privacybox.de>) ermöglicht es, anonyme Nachrichten zu empfangen. Sie sollte in erster Linie Journalisten, Bloggern u.a. eine vorratsdatenfreie und anonyme Kontaktmöglichkeit für Informanten bieten, steht

aber allen Interessenten offen. Es können nur Nachrichten empfangen werden. Die Nachrichten müssen auf der Kontaktseite des Empfängers geschrieben werden.

Die PrivacyBox nimmt keine E-Mails an und bietet auch keine Möglichkeit, E-Mails zu versenden. Es ist so etwas, wie ein Toter Briefkasten.

Politische Aktivisten sollten beachten, dass die PrivacyBox von einem deutschen Verein betrieben wird, der bspw. Linken Gruppen keinen Schutz gegen Ermittlungen nach §129a durch das BKA bieten kann. Die PrivacyBox ist ein Single Point, der über fast alle Informationen inklusive unverschlüsselter Inhalte der Nachrichten verfügen kann. Das LulzSec-Fiasco des VPN-Dienstes *Hide my Ass* zeigt, wie leicht Single Points kompromittiert werden können.

Ich habe die PrivacyBox lange Zeit uneingeschränkt empfohlen. Als Administrator und Hauptentwickler konnte ich sicher sein, dass keine Daten gespeichert wurden und es keine Kooperation mit Geheimdiensten gab. Im Sommer 2011 hat der Vorstand der GPF gegen meinen Wunsch einen zweiten Administrator für die PrivacyBox bestätigt, der meiner Meinung nach als informeller Mitarbeiter unter dem Decknamen SSysiphos für die Dienste arbeitet (neusprech: als "Vertrauensperson"). Der Vorschlag, dass alle Mitglieder des Vorstand inkl. des neu bestätigten Admin eine eidesstattliche Erklärung zur Nicht-Kooperation mit Geheimdiensten abgeben, wurde nicht angenommen.

Ich habe die Administration und Weiterentwicklung der PrivacyBox sowie meine Mitgliedschaft in der GPF niedergelegt. Aus heutiger Sicht ist das Projekt PrivacyBox ähnlich wie VPN-Dienste einzustufen. Mehr war mit den bescheidenen Mitteln eines Vereins nicht realisierbar.

Die PrivacyBox bietet viele Sicherheitsfeatures. Sie ist als Tor Hidden Service und I2P eepsite erreichbar und bietet client-seitige Verschlüsselung im Browser. Es liegt aber in der Verantwortung der Nutzer, diese Feature auch zu nutzen!

6 Quicksilver für WINDOWS

Die folgenden Kapitel erläutern den Einsatz von Quicksilver unter WINDOWS zur Versendung anonymer E-Mails. Für den Empfang von E-Mails kann der Standard-Mail-Client genutzt werden, welcher um eine Komponente zur Entschlüsselung von E-Mails erweitert wurde, z.B. Thunderbird (der E-Mail-Client der Mozilla-Foundation) mit dem EnigMail-PlugIn.

6.1 Installation von Quicksilver

Quicksilver für WINDOWS steht als selbstentpackendes Archiv *QS1.2.x.exe* unter folgender Adresse zum Download bereit:

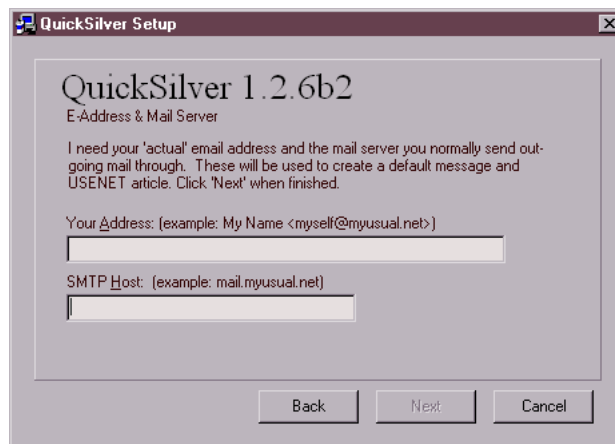


Abbildung 2: Quicksilver Installation

<ftp://ftp.quicksilvermail.net/pub/quicksilver/>

Nach dem Download ist die EXE-Datei zu starten und den Anweisungen des Setup zu folgen. Unter WINDOWS XP sollte das Setup nicht(!) als Administrator sondern unter dem später genutzten Account gestartet werden. Während der Installation ist der für die Versendung zu nutzende E-Mail-Account und SMTP-Server anzugeben (Bild 2). Auf Grundlage dieser Angaben wird ein Template für die Erstellung neuer E-Mails generiert. Dieses Template kann bei Bedarf später modifiziert werden.

Nach dem Abschluss der Installation ist Quicksilver zu starten um die weitere benötigten Komponenten einzurichten. Für das Versenden von E-Mails werden zusätzlich Mixmaster und das PGP-PlugIn benötigt.

Unmittelbar nach dem ersten Start erkennt QS, das Mixmaster noch nicht installiert ist und fordert sie auf, diese Komponente zu installieren. In dem sich öffnenden Dialog sollte *Get Mixmaster* gewählt werden, da ohne diese Komponente Quicksilver nicht nutzbar ist.

Mixmaster ist unter der gleichen FTP-Adresse zu finden wie Quicksilver und der folgende Dialog des Update-Wizard mit der Frage nach dem FTP-Verzeichnis kann mit dem Button *Next* betätigt werden, um das Standard-Verzeichnis zu nutzen.

Sollte der Download mit Quicksilver nicht funktionieren, kann die Datei *Mix2x.zip* mit einem Browser von der angegebenen Quelle geholt und lokal gespeichert werden. In der Drop-Down-Liste ist der Punkt *Local File* an Stelle des FTP-Servers zu wählen, um diese Datei zu installieren. Funktioniert der FTP-Download, ist in der Liste das Mixmaster-Archiv *Mix2x.zip* auszuwählen und die Auswahl mit dem Button *Next* zu bestätigen.

Nach dem Download ist das Setup für Mixmaster auszuführen. Im folgenden Dialog ist der Button *Run Setup* zu wählen.

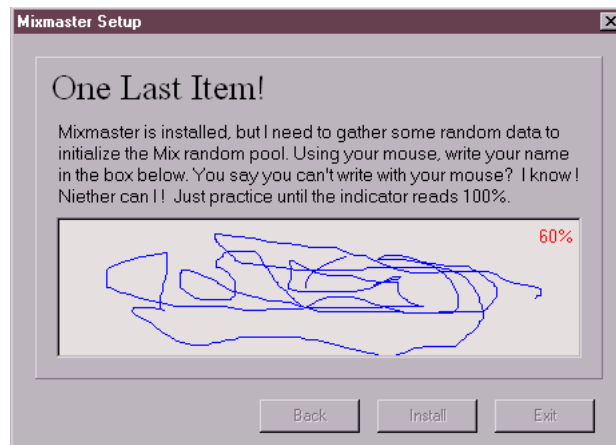


Abbildung 3: Zufallsgenerator initialisieren

Nach der üblichen Auswahl des Installationsverzeichnisses wird Mixmaster installiert und gestartet. Für die Initialisierung des Zufallsgenerators ist es nötig, im folgenden Fenster mit der Maus Bewegungen auszuführen, bis eine hinreichende Entropie angesammelt wurde (100%).

Es ist insbesondere bei der Versendung anonymer E-Mails sinnvoll, diese zu verschlüsseln. Für diese Verschlüsselung ist ein weiteres Plug-In nötig. Quicksilver bietet ein GnuPG-PlugIn für diese Aufgabe, welches über den Menüpunkt *Help - Update Wizard* installiert werden kann.

In dem sich auf die Auswahl des Download-Servers folgend öffnende Dialogbox ist die GnuPG-Komponente *QSpgp1.1.x.zip* zu wählen und die Auswahl mit dem Button *Next* zu bestätigen. (siehe Bild 4)

Nach dem Download ist das Setup mit einem Klick auf den Button *Run Setup* zu starten. Weitere Angaben sind für die Installation des Plug-Ins nicht nötig.

6.2 PGP-Schlüssel verwalten

Soll eine E-Mail verschlüsselt versendet werden, ist es als erstes nötig, den öffentlichen PGP-Schlüssel des Empfängers zu importieren. Die PGP-Schlüsselverwaltung kann über den Menüpunkt *Keyring - Open - Personal Pgp* oder über das Toolbar-Icon mit dem blauen Schlüssel geöffnet werden.

Der öffentliche Schlüssel des Empfängers kann über den Toolbar-Button *Importieren* aus einer Datei oder der Zwischenablage importiert werden. Die einfache Schlüsselverwaltung von Quicksilver bietet keine Möglichkeit, die

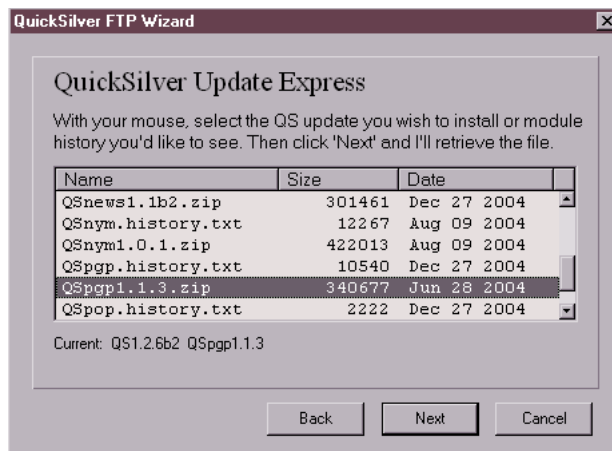


Abbildung 4: PGP-Archiv auswählen

Schlüsselservers im Internet zu durchsuchen.

Komfortabler lassen sich die Schlüssel beispielsweise mit Enigmail für Thunderbird oder dem Tool GPA verwalten. Mit Quicksilver lassen sich diese Schlüsselringe nutzen. Es ist der Konfigurationsdialog unter *Tools -> Options* zu öffnen und auf den Reiter *PGP* zu wechseln (Bild 5). Hier sind die mit anderen Tools verwalteten Schlüsselringe einzutragen.

Diese Schlüsselringe liegen bei der Nutzung von GnuPG normalerweise im Verzeichnis *C:/Dokumente und Einstellungen/ihr Name /Anwendungsdaten/gnupg/* und haben die Endung **.gpg!* Es muss die Option *alle Dateien anzeigen* im Dateiauswahldialog aktiviert werden.

Der Button *Advanced* führt zu einem Dialog, welcher die Auswahl eines alternativen Programms zur Schlüsselverwaltung ermöglicht. Hier könnte zum Beispiel Thunderbird gewählt werden.

6.3 Remailer-Listen aktualisieren

Quicksilver benötigt Informationen über die nutzbaren Remailer, die unterstützten Features und die öffentlichen Schlüssel der Remailer. Diese Informationen werden von mehreren Servern im Internet gesammelt und zum Download bereitgestellt.

Quicksilver benötigt aktuelle Kopien von folgenden Dateien, die nicht älter als 24h sein sollten. Vor dem Senden einer E-Mail oder News sind diese Dateien zu aktualisieren:

mlist.txt Liste der nutzbaren Mixmaster Remailer.

rlist.txt Liste der nutzbaren Cypherpunk Remailer.

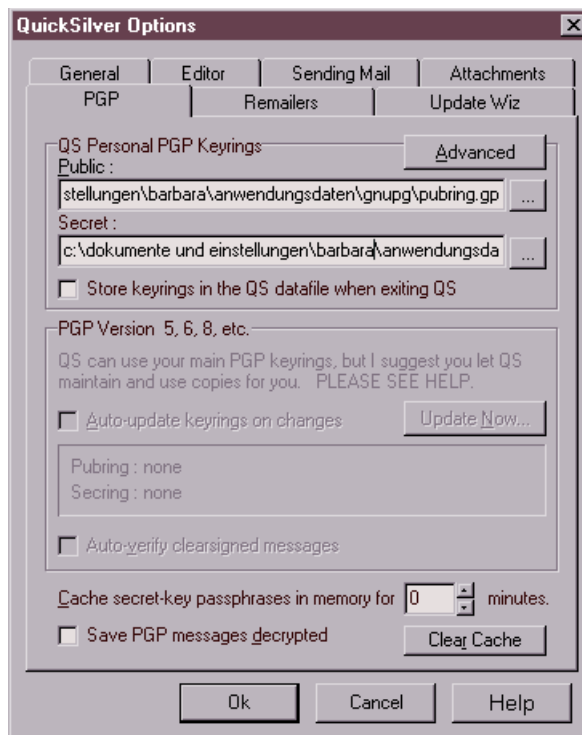


Abbildung 5: PGP-Schlüsselbund auswählen

pubring.mix Schlüsselring der Mixmaster Remailer.

pubring.asc Schlüsselring der Cypherpunk Remailer.

Für das Update der Listen ist der Menüpunkt *Tools - Remailers* zu wählen. In dem sich öffnenden Dialog (Bild 6) sind die Checkboxes wie gezeigt zu aktivieren und der Prozess mit einem Klick auf den Button *Update* zu starten.

Treten Fehler beim Update-Prozess auf, ist evtl. der gewählte Server nicht erreichbar. Es ist für die Quellen ein anderer Server zu wählen und das Update zu wiederholen. Mehrere Server sind standardmäßig bereits konfiguriert. Eine aktuelle Liste bietet <http://www.noreply.org/allpingers/allpingers.txt>. Die dort genannten Downloadquellen können mit dem *URL Manager* der Konfiguration hinzugefügt werden.

Nach dem erfolgreichen Update werden ein oder zwei Fenster zur Verwaltung der Schlüssel geöffnet, wenn neue Schlüssel gefunden wurden. Wird nur ein Fenster *Mixmaster Keyring* geöffnet, ist dieser neue Keyring mit Klick auf das blaue Disketten-Symbol zu speichern und das Fenster kann geschlossen werden.

Werden zwei Fenster geöffnet, sind zuerst im alten *Mixmaster Keyring* die Schlüssel für Remailer zu löschen, für die im zweiten Fenster aktualisierte

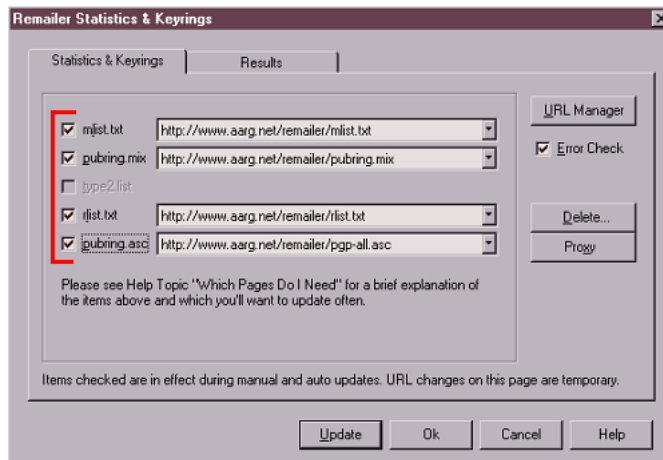


Abbildung 6: Update der Remailer-Listen

Schlüssel bereitgestellt wurden. Anschließend sind die neuen Schlüssel in den *Mixmaster Keyring* zu übernehmen und beide Fenster können geschlossen werden.

6.4 Anonyme E-Mail schreiben

Für das Erstellen einer neuen E-Mail ist das Toolbar-Icon ganz links und der Unterpunkt *Message* zu wählen. Es öffnet sich ein Fenster mit dem gewählten Template (Bild 7). Quicksilver lässt an dieser Stelle den gewohnten Komfort vieler E-Mail-Clients vermissen, ist aber sehr effektiv bedienbar.

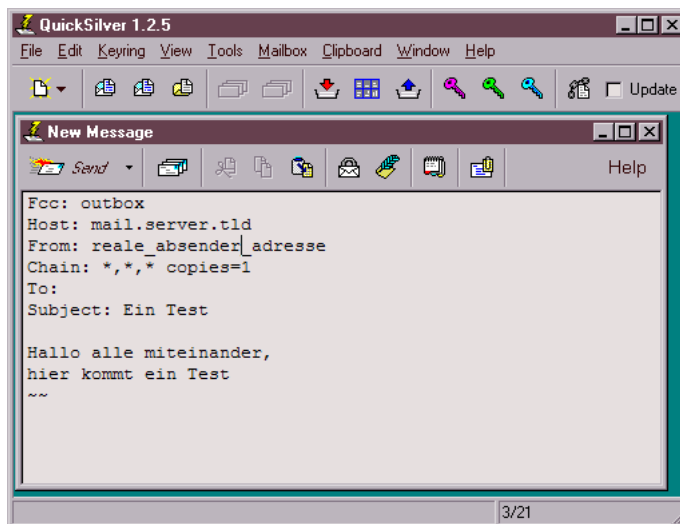


Abbildung 7: Neue E-Mail schreiben

Fcc: outbox

Host: mail.server.tld, ihr SMTP-Host

From: reale Absender-E-Mail-Addr.

Diese wird vom ersten Remailer der Kaskade entfernt. Sie ist aber nötig, um die E-Mail korrekt via SMTP zu senden.

Chain: *,*,*; copies=1

Es wird die Remailer-Kaskade festgelegt, welche für die Versendung genutzt wird. Ein Stern überlässt es Quicksilver, einen beliebigen, verfügbaren Remailer für diese Position auszuwählen. Da es möglich sein könnte, dass eine E-Mail nicht ausgeliefert wird, können bis zu 3 Kopien gesendet werden.

To: E-Mail-Addr. des Empfänger

Subject: Betreff-Zeile

Leerzeile!!!

Inhalt der Nachricht.

Der Text unterhalb der doppelten Tilde wird nicht gesendet. Vor dem Senden der Nachricht ist das Toolbar-Icon für die Verschlüsselung zu aktivieren, wenn die Nachricht OpenPGP-konform verschlüsselt werden soll.

Ein Klick auf den Button *Send* übergibt die E-Mail an Mixmaster, welcher eine Kette für die Versendung auswählt und die Message mehrfach verschlüsselt an den SMTP-Server sendet.

Update: Mit der am 18.4.2007 von Deutschen Bundestag beschlossenen Vorratsdatenspeicherung ist der SMTP-Host des Providers zur Speicherung der Daten aller weitergeleiteten E-Mails verpflichtet. Es wird damit protokolliert, dass man ein verschlüsselte E-Mails an einen Remailer versendet hat. Der reale Empfänger ist nicht protokollierbar.

Um diesen überflüssigen Logeintrag zu vermeiden, kann man die Mail direkt dem ersten Remailer der Kaskade übergeben. Der erste Remailer ist eindeutig festzulegen und als auch als SMTP-Host einzutragen. Eine Übersicht über verfügbare Remailer bietet <http://www.noreply.org/echolot/mlist2.html> Folgende Kombination funktioniert:

Host: awxcnx.de

Chain: awxcnx,*,*,*

6.5 Anonymes News-Posting schreiben

Für das Erstellen eines neuen News-Postings wählen sie das Toolbar-Icon für eine neue Nachricht ganz links, den Unterpunkt *Usenet Article*. Es öffnet sich das in Bild 8 dargestellte Fenster mit dem Template.

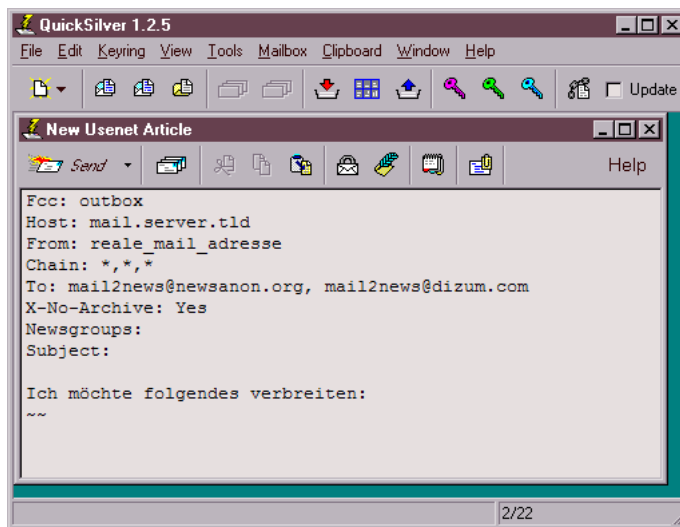


Abbildung 8: Neuen News-Artikel schreiben

Fcc: outbox

Host: mail.server.tld, ihr SMTP-Host

From: reale Absender-E-Mail-Addr.

Diese wird vom ersten Remailer der Kaskade entfernt.

Chain: *,*,*; copies=1

Es wird die Remailer-Kaskade festgelegt, welche für die Versendung genutzt werden. Ein Stern überlässt es Quicksilver, einen beliebigen, verfügbaren Remailer für diese Position auszuwählen. Da es möglich sein könnte, dass eine E-Mail nicht ausgeliefert wird, können bis zu 3 Kopien gesendet werden.

To: mail2news Gateway

Das Posting wird als E-Mail an ein Mail2News-Gateway gesandt. Dieses Gateway wandelt die E-Mail in einen Usenet Artikel um und versendet diesen an die angegebenen Newsgroups. Eine kurzer Liste aktueller Gateways:

- mail2news (at) bananasplit.info
- mail2news (at) dizum.com
- mail2news (at) reece.net.au
- mail2news (at) m2n.mixmin.net

Newsgroups: News-Gruppen in denen das Posting erscheinen soll.

Subject: Betreff-Zeile

Leerzeile!!!

Inhalt des Postings.

Ein anonymes News-Posting wird nicht als Posting an einen News-Server versendet, sondern als E-Mail über eine Remailer-Kaskade anonymisiert und anschließend vom Mail2News-Gateway an einen News-Server gesendet.

6.6 Weitere Features von Quicksilver

SMTP-Authorisierung: Erfordert der für den Versand der E-Mails genutzte Server eine Anmeldung mit Benutzername und Passwort, ist diese unter dem Menüpunkt *Tools - SmtP Authentication* zu konfigurieren. Die nötigen Angaben erfährt man vom Provider oder System-Administrator.

Adressbuch: Quicksilver bietet ein rudimentäres Adressbuch, um Listen häufig genutzter E-Mail-Adressen und News-Groups zu speichern. Das Adressbuch kann über den Menüpunkt *Tools - Adressbook* geöffnet werden. Die hier zeilenweise eingegebenen Adressen stehen beim Schreiben einer neuen E-Mail zur Verfügung und können mit wenigen Mausclicks übernommen werden.

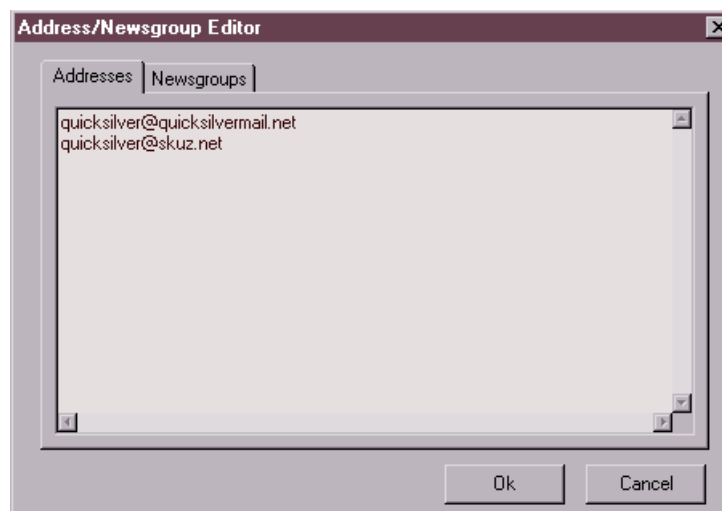


Abbildung 9: Quicksilver Adressbuch

Versand über Mixkaskade: Die Version 2.6 von Quicksilver bietet die Möglichkeit, den externen SMTP-Server für den Versand der E-Mails über Mixkaskaden oder anonymisierende Proxies zu kontaktieren. Dieses Feature dient einer höheren Anonymität gegen mitlesende Dritte auf der Seite des Absenders. In der Toolbar einer neuen E-Mail ist der Button *Proxy* zu finden. Hier kann der zu nutzende Proxy konfiguriert werden. Sinnvoll ist es, das Onion-Router-Netz (TOR) für die Kontaktierung des SMTP-Servers zu nutzen.

7 E-Mails anonym empfangen

7.1 Dauerhafter Nym-Account

Für anonyme Antworten via E-Mail bietet das Mixmaster Netzwerk die Nutzung von Nym-Accounts. Ein Nym-Account ist ein Postfach, welches die Identität des Inhabers versteckt. Eingehende E-Mails werden über eine Remailer Kaskade an die reale Adresse des Nutzers weiter geleitet, wobei jeder Remailer der Kaskade den empfangenen Stoff in einen zusätzlichen kryptografischen Umschlag steckt, den nur der richtige Empfänger öffnen kann.

Der Empfänger erhält eine E-Mail, die mehrfach OpenPGP konform verschlüsselt wurde. Er kann jeden Umschlag mit einem nur ihm bekannten Passwort öffnen und die ursprüngliche Nachricht wieder herstellen.

Die Installation der benötigten Software (Quicksilver bzw. Mixmaster) ist bereits beschrieben worden. Nutzer von Quicksilver für WINDOWS sollten zusätzlich das Modul *Nym* mit Hilfe des Update Wizard installieren. Es vereinfacht die Verwaltung von Nym-Accounts.

Nym-Account einrichten

Die folgende kurze Anleitung nutzt den Nym Wizard von Quicksilver für WINDOWS. Wie man mit Texteditor und GnuPG unter Linux arbeitet, steht unter <http://hp.kairaven.de/quick/quicknym.html>.

1. Als erstes ist ein Nym-Server und ein Name für den Account auszuwählen. Bekannte Server sind z.B. *nym.alias.net*, *hod.aarg.net* oder *nym.komite.net*. An einen dieser Server schickt man eine leer E-Mail an den Account *list*, beispielsweise an *list@nym.alias.net*. Die Antwort enthält alle auf diesem Server gehosteten Accounts. Anhand dieser Antwort kann man einen nicht genutzten Namen wählen.
2. Ein OpenPGP-Schlüsselpaar (Typ: RSA!) ist für den gewählten Namen zu erstellen (z.B. für *pitschie@nym.alias.net*) und der öffentliche Teil auf die Schlüsselserver zu exportieren. Um die Anonymität des Accounts zu gewährleisten, sendet man den öffentlichen Schlüssel per anonymer E-Mail an einen Schlüsselserver oder nutzt einen Hidden Service des Onion Router Netzes. Die Gültigkeitsdauer des Schlüsselpaares sollte nicht *unbegrenzt* sein, sondern der geplanten Nutzungsdauer des Accounts entsprechen.
3. Der öffentliche PGP-Schlüssel des Accounts *config* des gewählten Nym-Servers ist in den Cypherpunk Keyring zu importieren. <http://www.quicksilvermail.net/nymserver.txt> enthält alle Schlüssel. Diese Datei kann nach dem Download in den Cypherpunk Keyring übernommen werden. Nutzer von Quicksilver öffnen den Keyring über den Menüpunkt *Keyring* -> *Open* -> *Cypherpunk* und wählen in der Toolbar *Import*.
4. Ein Reply-Block ist zu erstellen. Der Nym-Wizard von Quicksilver fragt dabei nacheinander die nötigen Angaben ab.

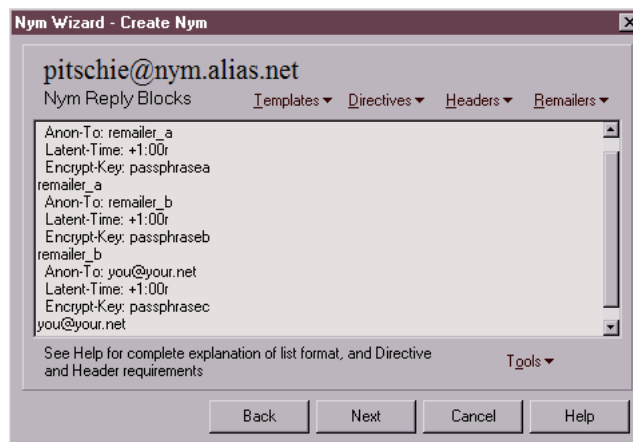


Abbildung 10: Nym-Wizard von Quicksilver

Im in Bild 10 angezeigten Template sind für die Werte *remailer_a* und *remailer_b* zwei gut erreichbare Remailer einzutragen. Die Seiten <http://pinger.bananasplit.info/> oder <http://rlist.ath.cx/mlist2.html> listen verfügbare Remailer auf.

Für *you@your.net* ist die reale E-Mail Adresse und als *passphrasea* ... *passphrasec* sind drei Passwörter einzutragen. Mit diesen Passwörtern verschlüsseln die Remailer die eingehende E-Mail symmetrisch, bevor sie weitergeleitet wird. Die Entschlüsselung erfolgt mit den gleichen Passwörtern in umgekehrter Reihenfolge.

5. Der erstellte Reply-Block ist als anonyme E-Mail an den *config* Account des gewählten Servers zu schicken, z.B. an *config@nym.alias.net*. Diese E-Mail ist mit dem Schlüssel des gewünschten Accounts zu signieren und mit dem Schlüssel des Servers zu verschlüsseln. Der Schlüsselservers überprüft die Signatur anhand des öffentlichen Schlüssels vom Schlüsselservers! Unter Quicksilver übernimmt der Nym Wizard diesen Schritt.
6. Nach 1-2 Tagen erhält man eine Antwort vom Nym-Server. Diese Antwort ist an den Nym-Server als Bestätigung zurückzuschicken (signiert und verschlüsselt).
7. Nach weiteren 1-2 Tagen ist der Account freigeschaltet, was mit einer leeren E-Mail an den *list* Account des Servers überprüfen kann.
8. Die Erreichbarkeit der genutzten Remailer sollte während der Dauer der Nutzung des Accounts regelmäßig überprüft werden. Ist einer der gewählten Remailer nicht mehr erreichbar, muss an den *config* Account des gewählten Servers ein neuer Reply-Block geschickt werden. Einige Pinger stellen die nötigen Informationen über die Erreichbarkeit im Internet bereit, beispielsweise <http://rlist.ath.cx/mlist2.html> oder <http://pinger.bananasplit.info/mlist2>