Digitale Selbstverteidigung

eine Einführung

Jens-Wolfhard Schicke-Uffmann

6. September 2013

Grundsätzliches

- Selbst durch gesetzliche Änderungen in Deutschland werden ausländische Geheimdienste ihre Arbeit nicht einstellen
- Digitale Selbstverteidigung ist *ein* Baustein des freien demokratischen Meinungsaustauschs
- Politische Lösungen sind zusätzlich nötig, um die geheimdienstliche Überwachung der Bevölkerung abzustellen

Die eigenen Grenzen kennen

Heutiger Inhalt:

- Tempora (UK), Technikaufwuchsprogramm (DE), SORM-II (RU), u.ä.
- PRISM (US)
- Trojaner, Viren, Würmer
- gezielte Ermittlungsarbeit
- Telefonie, Mobiltelefone

Bei Unsicherheit:

- Die ganz geheimen Dinge bespricht man am besten ohne Handys irgendwo auf einem Feldweg

Das Ziel für heute: Eine Mail schreiben können, ohne dass die Geheimdienste der Welt mitlesen.

Nur weil du verschlüsselst...

... heißt das nicht, dass SIE dich nicht abhören können (aber dass es teurer für SIE ist).

- Absichtlich eingebaute Hintertüren
- Trojaner und Rootkits
- Wanzen, Keylogger
- Elektromagnetische Abstrahlung
- Human Intelligence

Webdiensteanbieter

- Daten bei Dritten sind nie sicher
- PRISM: Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, Apple

Softwareauswahl

OpenSource:

- Jeder kann die Quellen lesen
- Es gibt unabhängige Sicherheitsforscher, die das auch tun
- Trotzdem jede Menge Lücken
- ... die zeitnah behoben werden.

Die Alternative:

- `https://en.wikipedia.org/wiki/NSAKEY`
- `https://en.wikipedia.org/wiki/IBM_Notes#Security`

Mailverschlüsselung

Ungefähre Analogien:

- Unverschlüsselte Mail: Postkarten mit Bleistift beschreiben
- Signierte Mail: Kugelschreiber und Unterschrift
- Verschlüsselte Mail: Brief

Webmail

- Webbasierte Verschlüsselungssoftware ist nicht vertrauenswürdig
- Admins können mitlesen
- Geheimdienste können mitlesen
- Ermittlungsbehörden können mitlesen

Das Problem mit den Metadaten

Mailverschlüsselung bezieht sich nur auf den Inhalt, nicht auf

- Absender
- ... inklusive IPs zwischengeschalteter Server
- Betreff
- Mailclient und andere identifizierende Merkmale
- Zeitpunkt der Kommunikation

Public-Key Kryptographie

Jeder Teilnehmer hat:

- Privaten Schlüssel
- Öffentlichen Schlüssel

Verschlüsselt wird mit dem öffentlichen Schlüssel.

Entschlüsselt wird mit dem privaten Schlüssel.

Signiert wird mit dem privaten Schlüssel.

Public-Key Kryptographie

Jeder Teilnehmer hat:

- Privaten Schlüssel
- Öffentlichen Schlüssel

Verschlüsselt wird mit dem öffentlichen Schlüssel.

Entschlüsselt wird mit dem privaten Schlüssel.

Signiert wird mit dem privaten Schlüssel.

Schlüsselsignaturen (und Netzwerkanalyse)

Um sicher zu stellen, dass man den richtigen Schlüssel hat

- Fingerprints vergleichen
- Signaturen anderer auf dem Schlüssel überprüfen

Problem bei Schlüsselsignaturen: Das soziale Netzwerk wird sichtbar.

PGP & Enigmail

"Pretty Good Privacy"

- `http://openpgp.org/`
- GnuPG als OpenSource-Implementation
- Konkrete Ausgestaltung eines Public-Key Verfahrens

Enigmail

- PGP-Plugin für Thunderbird und SeaMonkey
- Benötigt eine GnuPG-Installation
- `http://www.enigmail.net`

GunPG installieren

- Linux Debian: apt-get install gnupg
- Windows: `http://www.gpg4win.org/`
- Mac OS X: `https://gpgtools.org/`

Enigmail installieren

- Runterladen: `http://www.enigmail.net/download/`
- Plugin installieren: “Tools”, “Add-ons”, “Install”
- Schlüssel erzeugen: “OpenPGP”, “Key Management”, “Generate”, “New Key Pair”
- Passwort setzen
- Revocation Certificate generieren
- Eigenen Schlüssel signieren
- Schlüssel veröffentlichen: Eigene Adresse suchen, “Keyserver”, “Upload public keys”

Andere Systeme

Sehr deutlich nicht empfohlen!
Outlook:

- `https://www.symantec.com/desktop-email-encryption/`
  (Kein Open Source)
- `https://code.google.com/p/outlook-privacy-plugin/`
  (Outlook 2010 und 2013)
- `http://www.gpg4win.org/` und GpgOL
  (Outlook 2003 und 2007)

Mac:

- `https://gpgtools.org/gpgmail/index.html`

Anonymisiertes Browsing

Anwendungsfälle:

- Anonyme Mails schreiben
- Anonyme Veröffentlichungen (z.B. via pastebin)
- Regimekritische Webseiten besuchen

Offensichtliches:

- Cookies, HTML5 Local Storage, Flash Local Storage verhindern
- Nirgends einloggen (außer mit gesonderten Accounts)
- Nicht den eigenen Namen unter Beiträge schreiben
- Keine unnötige private Korrespondenz
- Längere Texte in ungewöhnlichem Stil verfassen

Browser Identification

- `https://panopticlick.eff.org/`
- Browserversion, Plugin-Versionen, Installierte Fonts, Bildschirmgröße, etc.

IP Adresse

- Bei der Einwahl ins Internet wird technisch notwendig eine IP zugewiesen
- Die Zuordnung IP $\leftrightarrow$ Anschluss kann gespeichert werden (“Vorratsdatenspeicherung”, “Mindestspeicherfrist”)
- Die IP einer Anfrage wird routinemäßig bei fast allen Webanbietern abgespeichert

Onion Routing

Anstatt direkt zum Ziel zu verbinden

- Verbindung zu einem ersten Proxy
- ... von dort zu einem zweiten ...
- ... und zu einem dritten, der zum Ziel verbindet.

- Der 1. Proxy: Sieht, wer zum Netzwerk verbunden ist, aber nicht was dort passiert.
- Der 2. Proxy: Sieht, dass überhaupt Netzwerkverkehr vorhanden ist.
- Der 3. Proxy: Sieht, was das Netzwerk im Internet tut, aber nicht wer die Anfrage stellt. ("Exit Nodes")

Tor Browser Bundle

- `https://www.torproject.org/projects/torbrowser.html.en`
- Onion Routing Software TOR + Browser + Voreinstellungen
- Trotzdem(!) kaum Schutz gegen Browser-Version Tracking
- TOR nicht für Aktionen benutzen, die dich identifizieren können
- Genug Exit Nodes werden von Sicherheitsforschern oder Geheimdiensten und anderen Kriminellen betrieben
- ... auch deshalb: Niemals irgendwo (mit relevanten Daten) einloggen.

Fragen???

Jetzt.

Wer es sicherer braucht

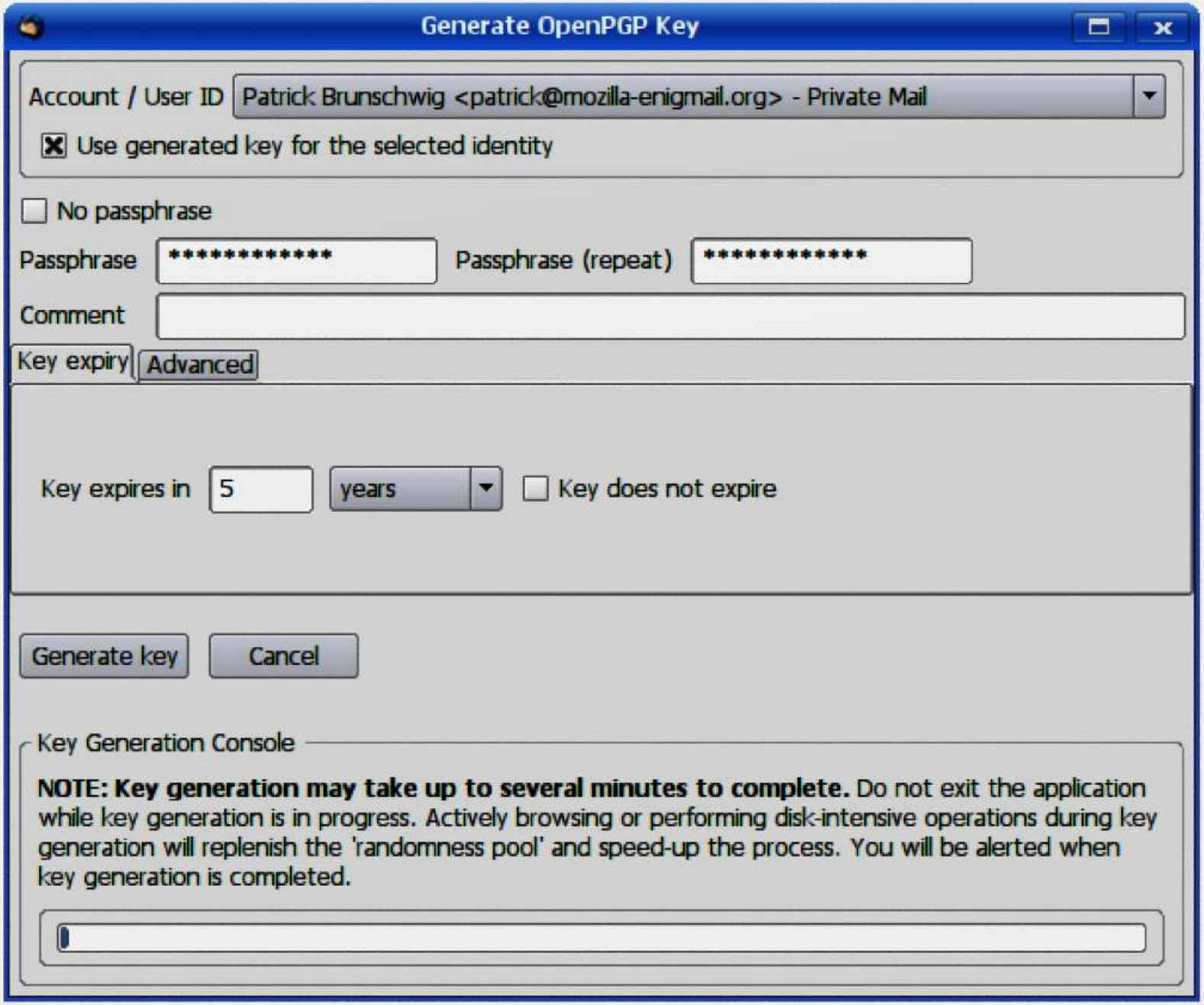
- Selber informieren!
- https://stratum0.org/--HackerspaceBraunschweig
- http://crunchbang.org/forums/viewtopic.php?id=24722
- https://gnunet.org/
- http://wiki.qubes-os.org/trac

Wir üben Mails verschlüsseln

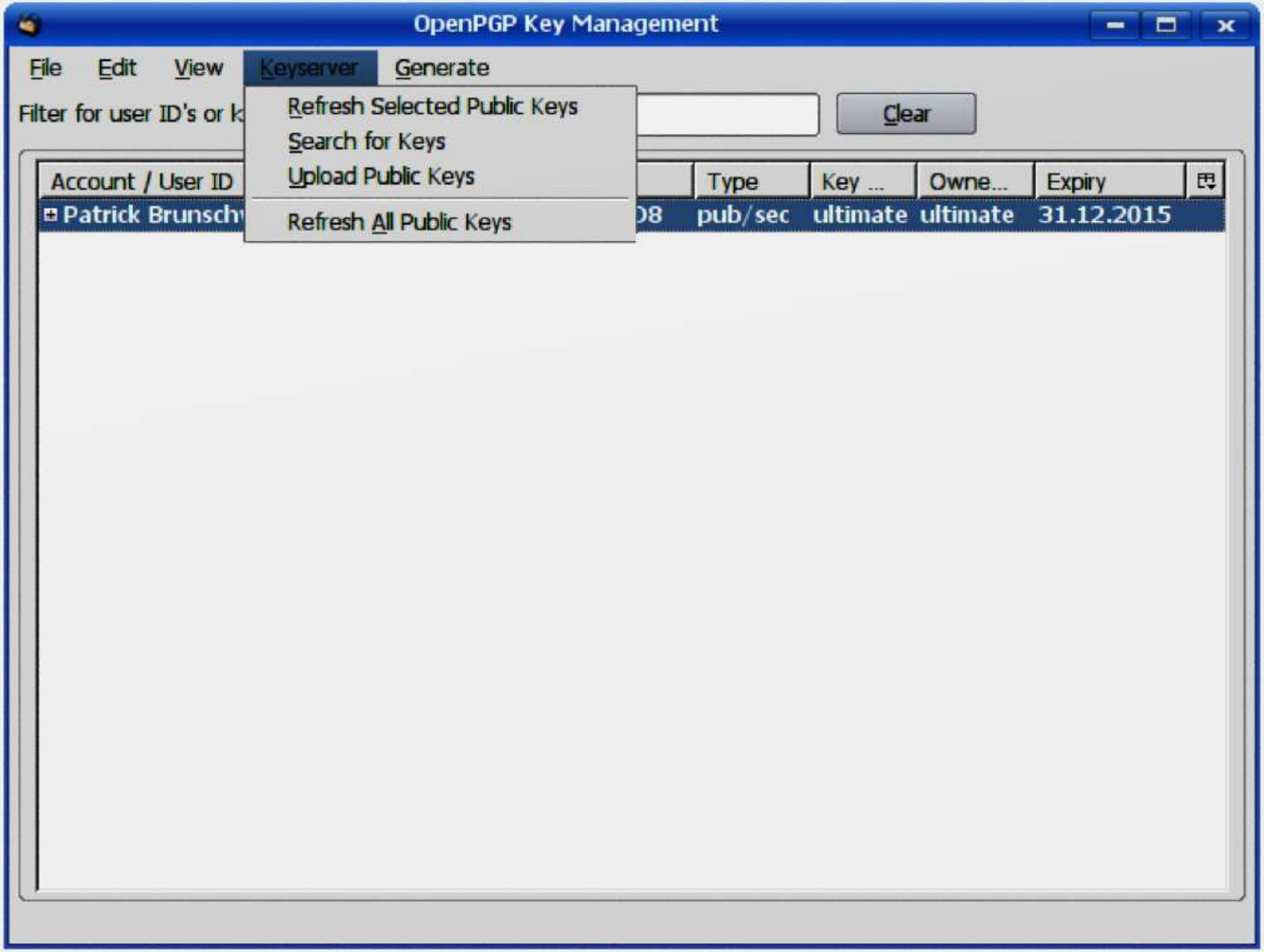
Links unter: `http://drahflow.name/cryptoparty.html`

- Installieren
- Schlüssel erzeugen
- Schlüssel veröffentlichen
- Verschlüsselte und signierte Mail als Test an drahflow@gmx.de
- Verschlüsselte und signierte Antwort erhalten

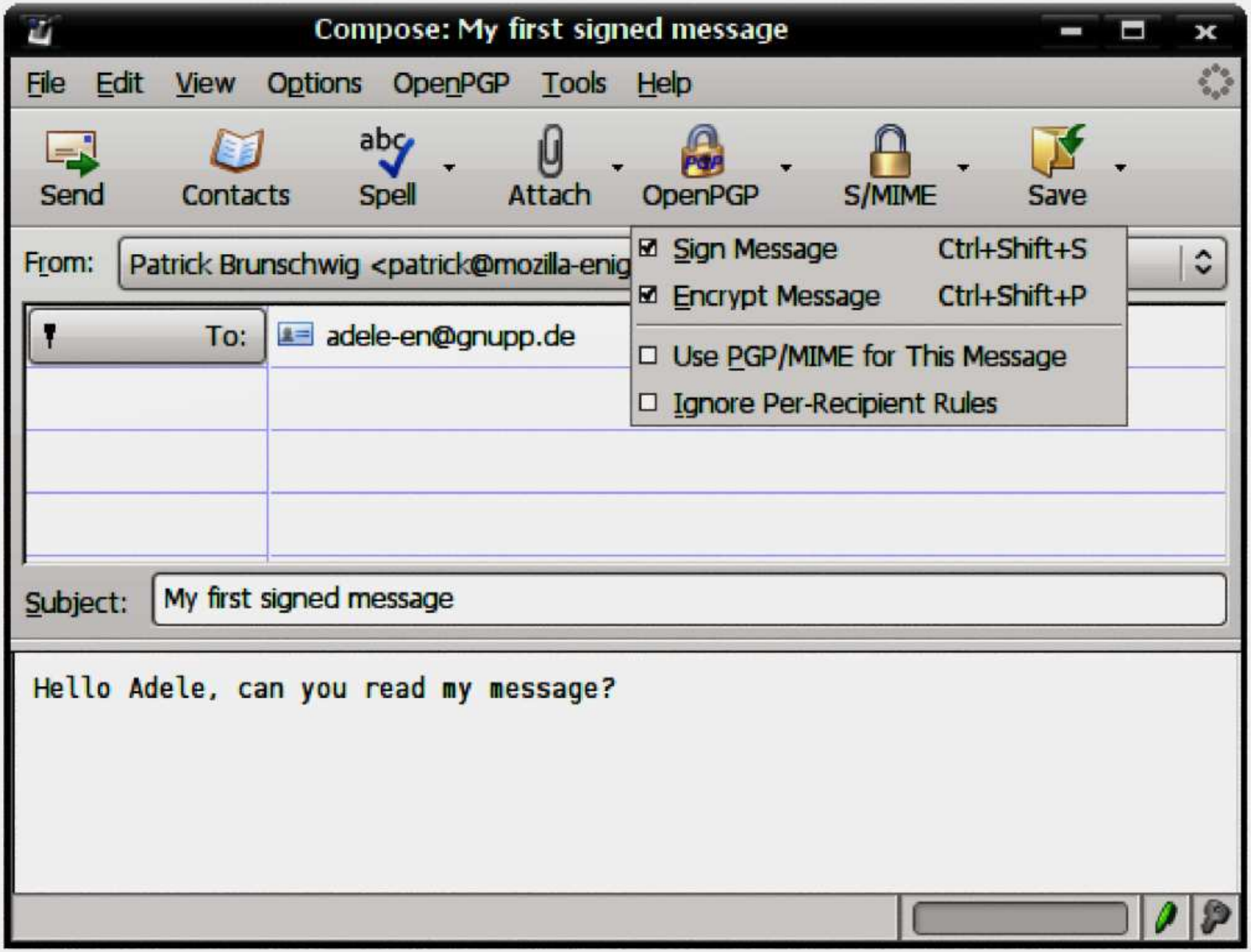
Schlüssel erzeugen



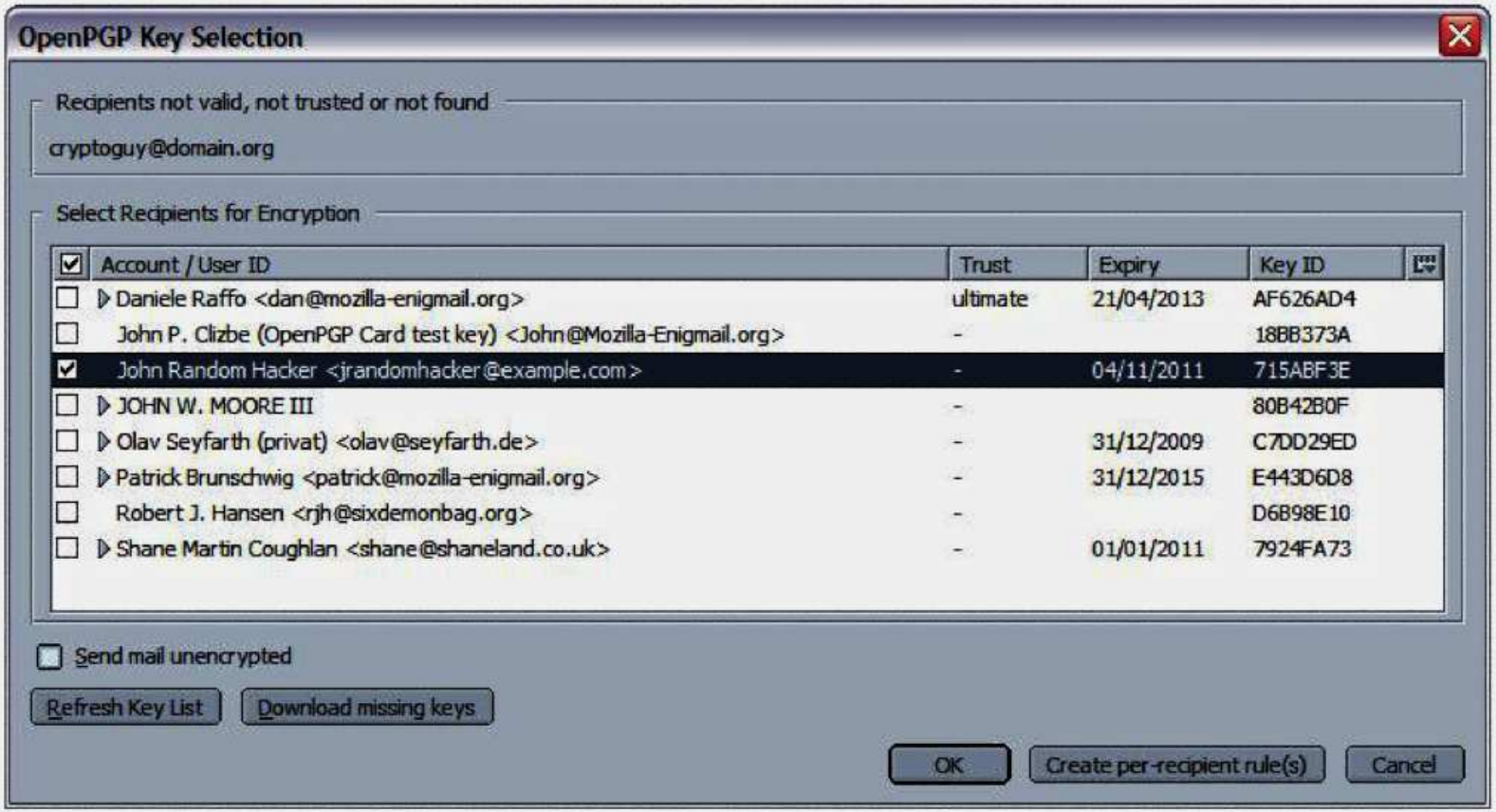
Schlüssel veröffentlichen



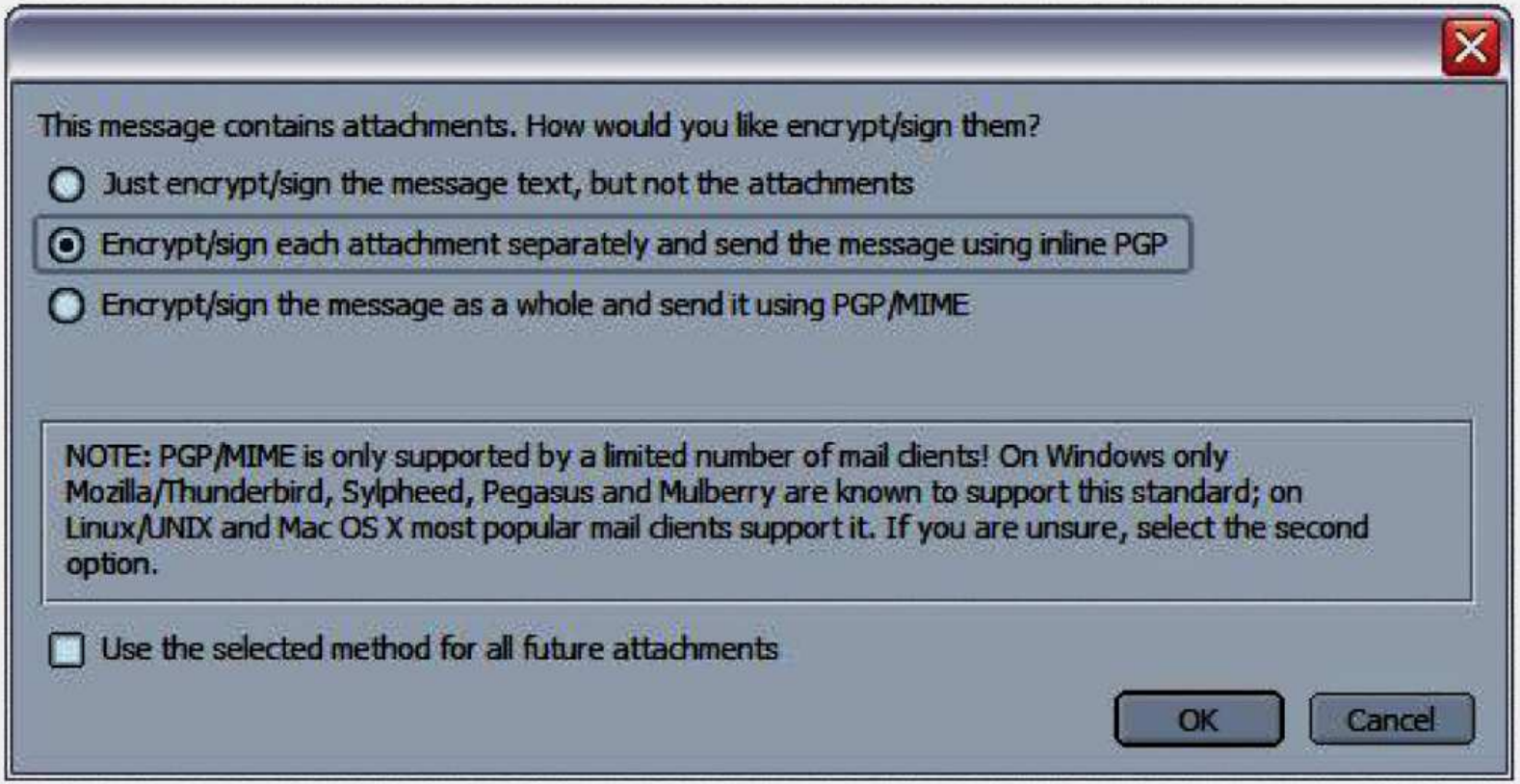
Mail signieren und verschlüsseln



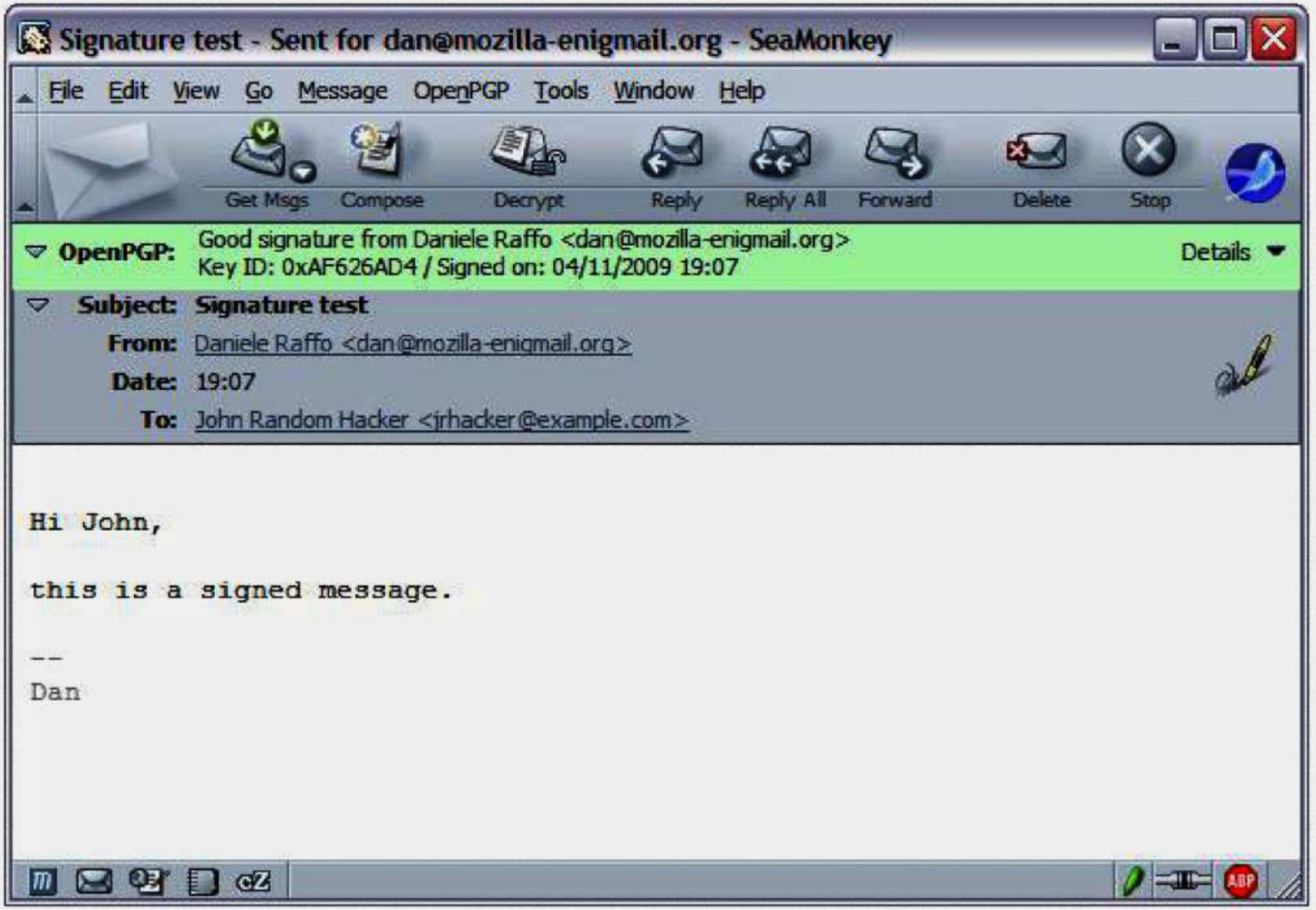
Schlüsselauswahl beim Versandt



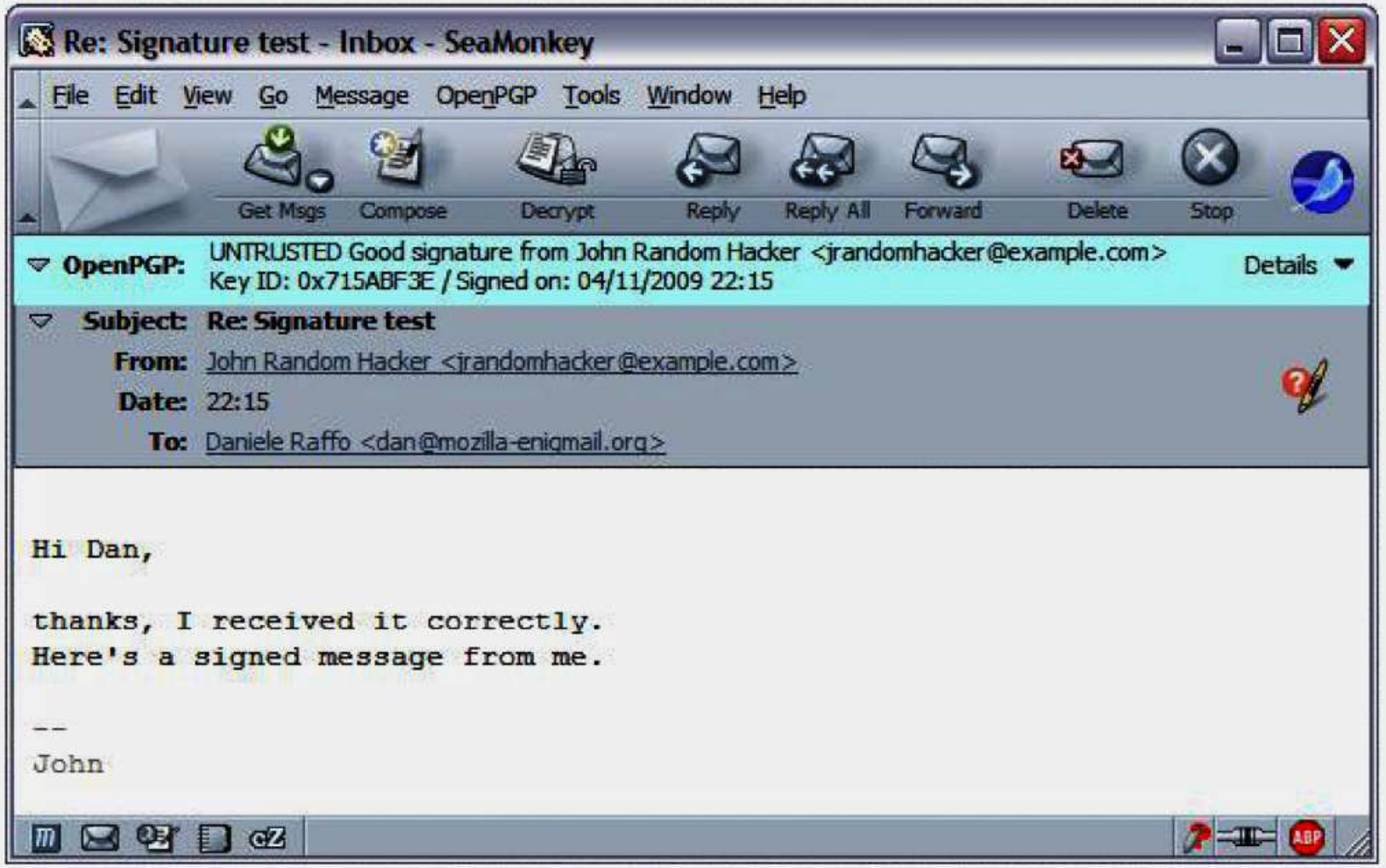
Attachements



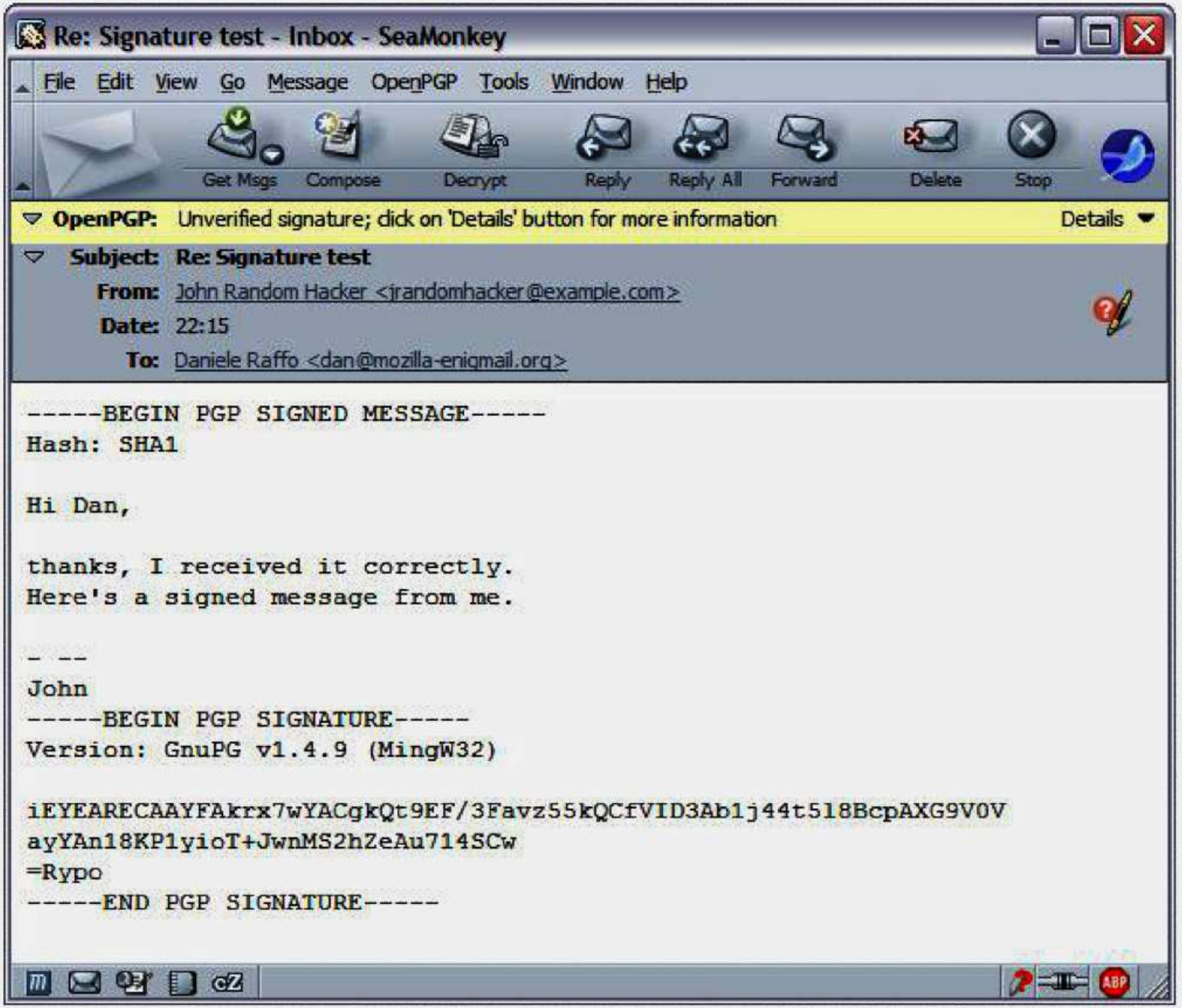
Korrekt signierte Mail



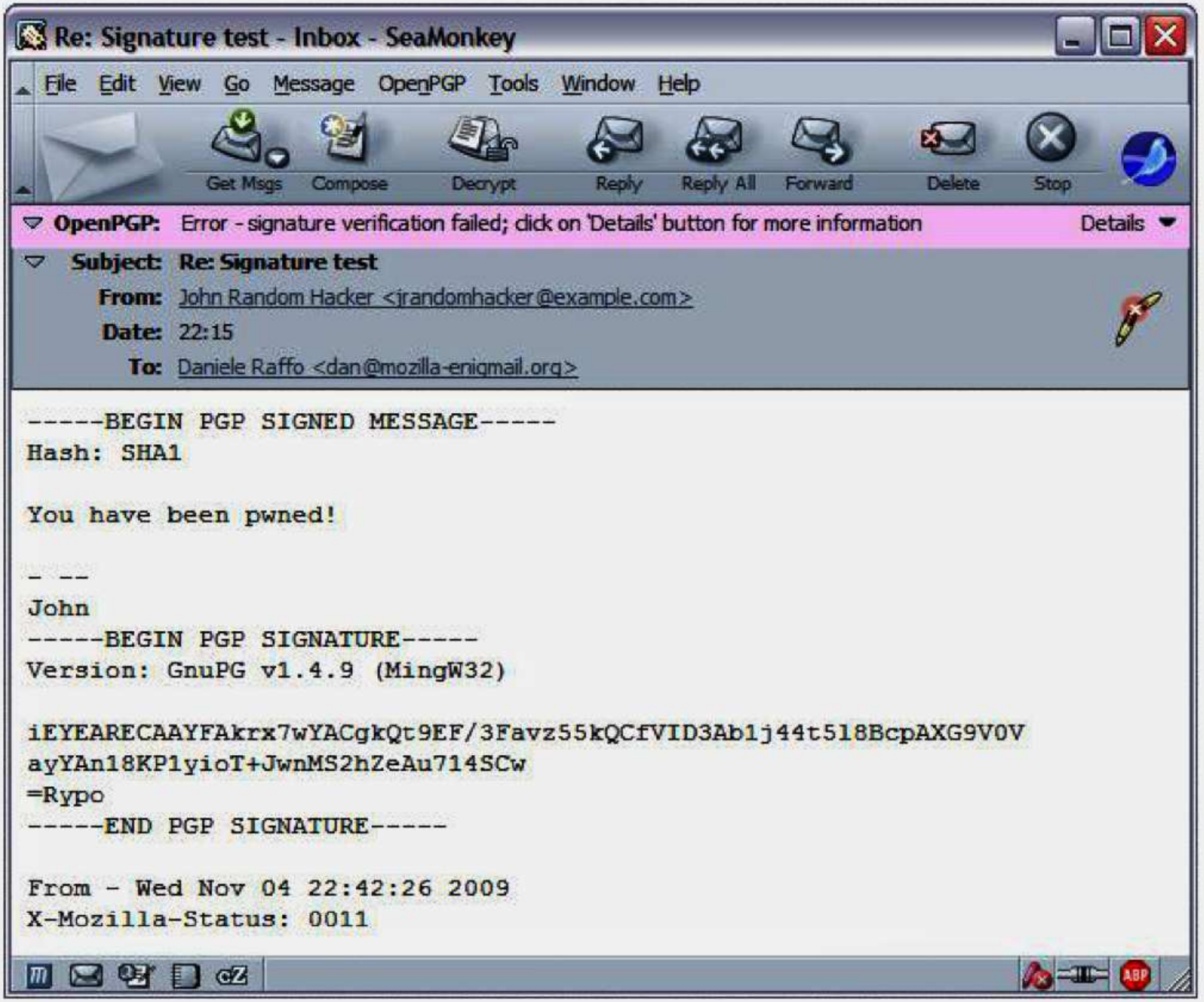
Unvertrauenswürdig signierte Mail



Unbekannt signierte Mail



Fehlerhaft signierte Mail



Wir üben anonym Surfen

- Tor Browser Bundle installieren
- Tor starten
- `http://duckduckgo.com/`
- bzw. `http://3g2upl4pq6kufc4m.onion/`