

Kryptographie

Letzte Aktualisierung Montag, 2. Oktober 2006

Ich verwende seit einigen Jahren GnuPG. Einerseits verschlüssele ich damit vertrauenswürdige Daten auf meinen Rechnern, andererseits kommuniziere ich damit verschlüsselt mit einigen anderen. Voraussetzung ist, dass bei einer solchen Kommunikation beide Partner selbst ein zu einander kompatibles Verfahren einsetzen. GnuPG bietet sich an, weil es Open Source und für diverse Plattformen verfügbar ist.

Genauere Erklärungen des Prinzipes von GPG und der asymmetrischen Verschlüsselung finden sich unter anderem bei Wikipedia.

Ich bin überzeugter Anwender des Mailprogrammes Thunderbird (dt.). In Kombination mit dem Plugin Enigmail (dt.), welches GnuPG verwendet, ist das eine ideale und anwenderfreundliche Kombination. Übrigens gilt das sowohl für Linux, als auch für Windows!

Hier nun mein öffentlicher GnuPG-Schlüssel.

Fingerprint: 291F 983C 96F0 FB41 5B5C 6E9F 1FB5 365E A62C 6AF4

Noch eine Bemerkung: Ich unterstütze Open Source, wo es geht. Mit "wo es geht" meine ich einfaches, und schmerzfreies Ausweichen auf freie Software. Ich meine damit nicht endlose Fummelsessions, um irgendetwas ans Laufen zu bekommen. In diesem Sinne kann ich jedem nur empfehlen, sich den Browser Firefox und das Mailprogramm Thunderbird einmal anzusehen. Komplette eingedeutschte und einfachste zu installieren finden sich beide Programme hier. Schon in der Standardausstattung bieten sie alles, was man benötigt. Richtig pfiffig ist aber das Konzept, weitere Funktionen mit Erweiterungen zuzufügen. So kann man sich sein individuelles Werkzeug selbst zusammenstellen - wegen der großen Open-Source-Gemeinschaft komplett kostenfrei.

