

Die Entstehung von GnuPG

(In der Hitze des 29. Juni 2003)



Me and My Boxes

- Hardware, Funkamateure
- TRS-80, Eigenbau, etc.
- PCs in Netzwerken, etwas Mainframe, ...
- Systemhaus, Finanzsoftware, Datenkonvertierungen
- Treiber für PCMCIA Karte

Motivation

- Langeweile
- Die GNU Task List
- Ablauf des DH Patent
- Rede von RMS in Aachen
- Teilhabe am GNU Projekt
- etwas zurückgeben

Erste Schritte

- RFC1991 studiert, einfachen Parser geschrieben
- Mitteilung an den GNU Volunteer Coordinator
- RSA und IDEA implementiert: funktioniert
- RSA und IDEA durch ElGamal und Blowfish ersetzt
- Erste öffentliche Version und gute Rückmeldungen

Helfer

- Wenige Coder, viele Nutzer/Tester
- Übersetzer waren seit Anfang an dabei
- Die Namensdiskussion
 - Aka: Ist "gpg" zu ähnlich zu "pgp"?
- Unterstützung durch die GUUG
 - FTP/CVS Server
 - Veranstaltungen

Der neue Standard

- OpenPGP WG seit Herbst 1997
- Seit Anfang 1998 Umstellung auf OpenPGP
- Neue Algorithmen: DSA, 3DES, CAST5, Twofish
- Implementierung von Subkeys, Web of Trust
- Heute wahrscheinlich die konformste OpenPGP Implementation

Leere Kassen

- Keine Zeit mehr für andere Arbeiten
- Ersparnisse gehen zur Neige
- Einige Monate Projektarbeit
- In dieser Zeit immer stärkere Verbreitung
- Vorträge von Tokyo bis Brasilien

BMWi Förderung

- Nicht mehr um 5 Uhr aufstehen :-)
- Windows Portierung
- Teamarbeit
- Helfer springen ab
- Eingekaufte Programmierer

Nach Ablauf des RSA Patents

- September 2000 lief das RSA Patent ab
- Am nächsten Tag neue Version freigegeben
- Jetzt vollständige PGP 2 Signatur Unterstützung
- Immer noch die Beschwerden über fehlendes IDEA ;-)
- IT Dienstleister gegründet und wieder verlassen

Neue Entwicklungsfirma

- Support
- Portierungen
- Weiterentwicklungen
- Angestellte Mitarbeiter zu meiner Entlastung
- 2. Generation der Helfer
 - Code: Timo, Stefan, David
 - Webseiten: Lolo und andere

Ägypten Projekt

- Ausschreibung des BSI, Zuschlag erhalten
- Trotz sehr knappem Angebot erfolgreich abgeschlossen
- Neue CMS Code Basis
- Fehler in anderen Implementierungen aufgezeigt
- Offizieller Einsatz im BSI und andere Verwaltungen
- Weiterentwicklung?

Wie geht es weiter?

- 3 Entwicklungslinien (stable, devel und NG)
- Ziel: GnuPG 2.0
- Smartcard
- Modular
- S/MIME und OpenPGP
- mal sehen ...

Weitere Informationen

<http://www.gnupg.org>

The logo for g10code, featuring the text 'g10' in a large, bold, black font, with the word 'code' in a smaller, black font positioned above the '0'.

<http://g10code.com>

The logo for fsfeurope, featuring the text 'fsfeurope' in a black, lowercase, sans-serif font, with a horizontal line passing through the middle of the letters.

<http://fsfeurope.org>



<http://www.gnu.org>

- Vielen Dank für Ihre Aufmerksamkeit -