Warum brauchen wir neue PGP Keyserver

Vortrag gehalten beim Belwue Netzdienste AK
am 8. Juli 1999

Peter Gietz,
DFN-Directory Services,
Zentrum für Datenverarbeitung, Universität Tübingen

Agenda

- Vorzüge von PGP
- Probleme des existierenden PGP Keyserver
- Was bisher geschah
- Probleme bei der Speicherung von PGP Keys im Directory
- Anforderungen

Vorzüge von PGP

- Augenblicklich meistgenutzte Public Key Infrastruktur
- Geeignet zum Signieren, Integritätssicherung, Verschlüsseln (asymmetrisch und symmetrisch), Authentifizierung
- Flexibles Format: verschiedene Algorithmen und Schlüssellängen, Subkeys
- CA Trustmodell anwendbar

Probleme des existierenden PGP Keyserver

- Die klassische Lösung: PKS von Marc Horrowitz (http://www.mit.edu/afs/net.mit.edu/project/pks/thesis/paper/thesis.html)
- Kein verteiltes System: Alle Keys auf allen Servern
- Nicht beliebig skalierbar
- Probleme bei der Replikation der Schlüssel

Was bisher geschah

- Hedberg: „Definition of X.500 Attribute Types and a Object Class to hold public PGP keys“ Februar 1996 (seit September 1996 obsolet)
- AMBIX-PGP@mail500.uni-tuebingen.de
- pgp-directory@dante.org.uk
  (http://www.dante.net/np/listarchives/pgp)
- OpenKeyServer von Highware
  (http://www.highware.com/main-oks.html)
- NAI PGP Certificate Server
  (http://www.nai.com/products/security/commercial.asp)

Probleme bei der Speicherung von PGP Keys im Directory

- Eine Person kann mehrere Keys haben
- Ein Key kann mehrere UserIds haben
- Ein Key kann mehrere Subkeys haben

Anforderungen

- Standardisierte Lösung
- Keys müssen nach verschiedenen Kriterien suchbar sein
- CA Zertifizierung muss intergierbar sein
- Zertifizierungspfad muss verfolgt werden können
- Key-Status muss abfragbar sein
- Key Information müssen sowohl unter einem Personeneintrag als auch in einem eigenen Keyspace gespeichert werden können