Pretty Good Privacy

PGP

PGP

- Created by Phil Zimmermann in 1991.
- In February 1993 Zimmermann became the target of a criminal investigation by the US Government for "munitions export without a license"
- Cryptosystems with keys larger than 40 bits were considered munitions.
- PGP used 128 bit keys.

PGP

- Zimmerman published the entire source code of PGP in a book (MIT prerss).
- The book could be exported (export of books protected by the first amendment).
- In 1996 the investigation was dropped without charges.
- PGP bought by Symantec in 2010

OpenPGP

- There were initially issues around the RSA patent.
- OpenPGP was defined as a standard by the IETF (started 1997)
- The Free Software Foundation implemented OpenPGP in 1999.
- Known as Gnu Privacy Guard (GPG).

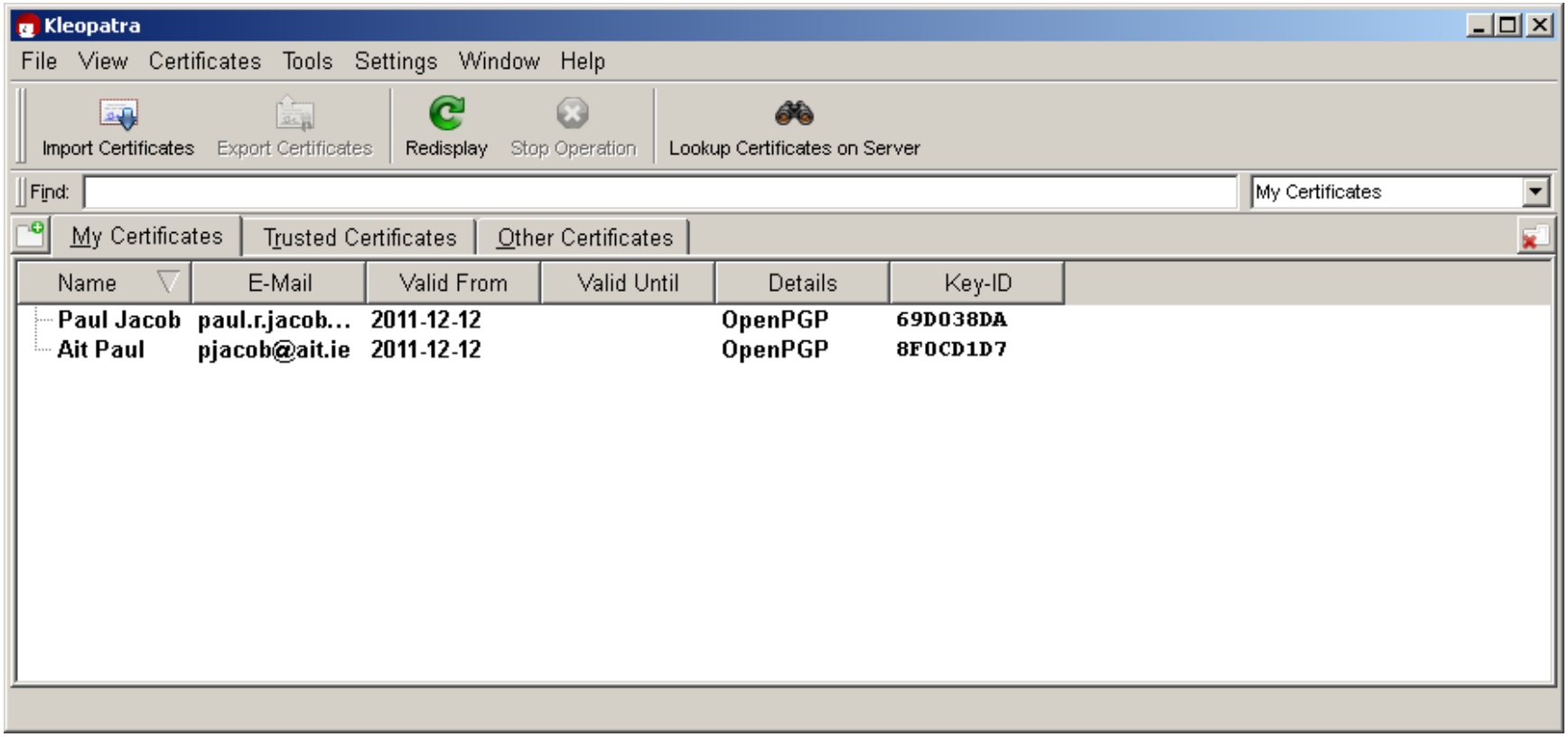
GPG

- http://www.gnupg.org/
- Implemented by FSF in 1999.
- Received major funding from the German government.
- Does not use any patented software.
- Mainly used to encrypt mail and personal files.

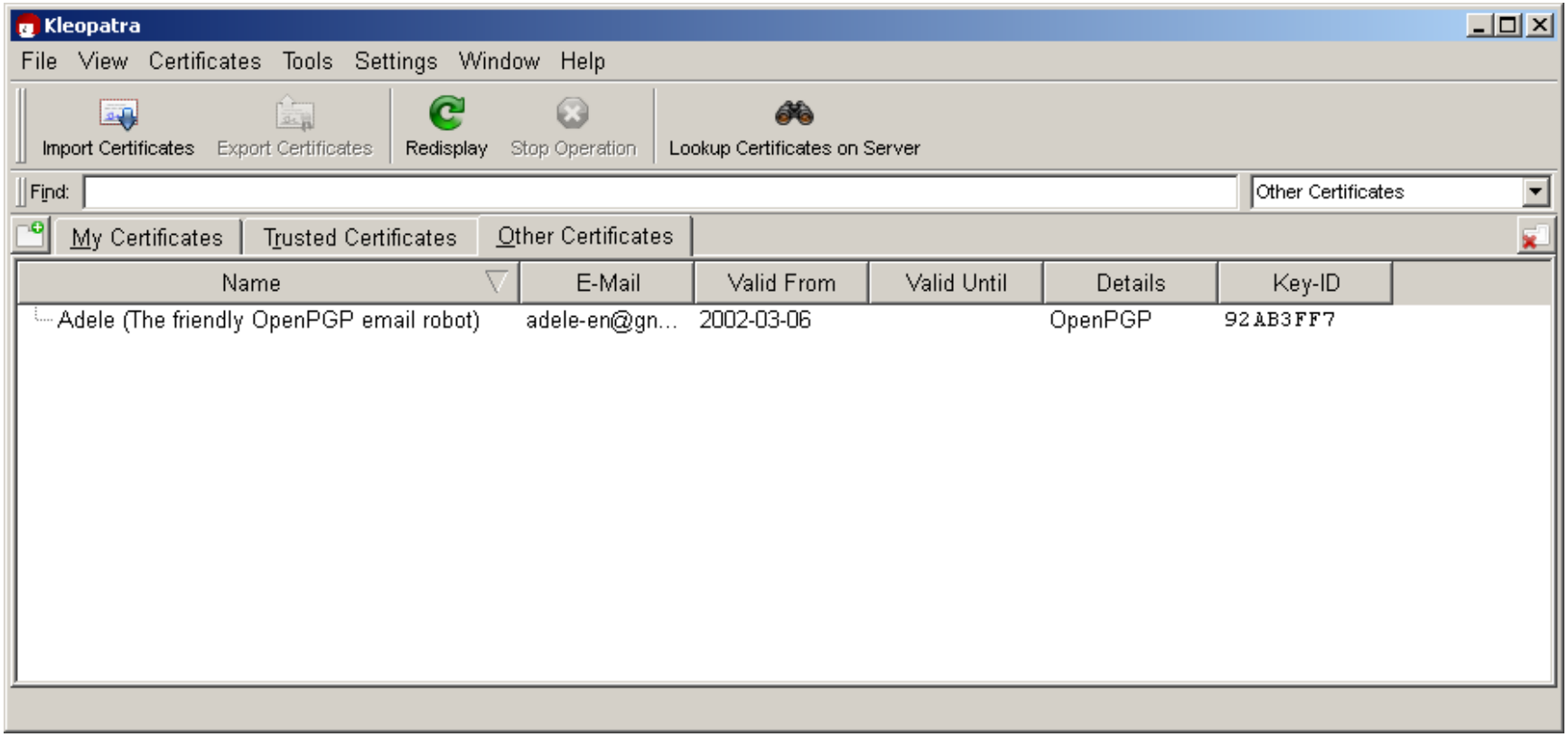
Gpg4win

- Released in 2005.
- Includes
  - WinPT (Windows Privacy Tray)
  - Gnu Privacy Assistant (front end)
  - GPG plugins for Outlook and Windows Explorer.
  - Kleopatra – GUI version.

GPG -Kleopatra



GPG -Kleopatra



GPG - Kleopatra

- Create certificates (OpenPGP key pairs)
- Import certificates.
- Sign/Encrypt Files
- Verify/Decrypt Files

Keys

- You have 2 keys, a public key and a private key.
- You let the people you trust have your public key.
- You encrypt with the public key of whoever you are sending to.
- You decrypt with you own private key.
-

Keys - Confidentiality

- You encrypt with the public key of whoever you are sending to.
- They decrypt with their private key.

Keys - Authentication

- You encrypt with you private key.
- When the recipient decrypts with your public key, that authenticates the message.

Web of Trust

- In contrast to X.509 certificates, which depend on centralized Certificate Authorities, initially PGP depended on a "Web of Trust".
- The concern here is the question
- "How do we know that we have the correct public key of a peer?"

Web of Trust

- A decentralized trust model.
- "OpenPGP identity certificates (which include public key(s) and owner information) can be digitally signed by other users who, by that act, endorse the association of that public key with the person or entity listed in the certificate."

Web of Trust

- [This is in contrast to X509 certificates. Where the certificates are signed by a centralized certificate authority.]
- You can verify over the phone by checking what is know as a public key fingerprint.
- The fingerprint is created by a cryptographic hash function.

Key Servers

- Signed identity certificates uploaded to servers.
- Lots of problems.
- Your information made public (email address!!).
- Analyses can be carried out on who has signed who's certificates.

Web of Trust

- Later versions of PGP can use X509 certificates.

Web of Trust

- Scheme is flexible.
- Decisions are left in the hands of users as to who to trust.
- Users need to make intelligent decisions.