E-mail privacy with GnuPG and Mozilla in eComStation

- The problem: How can we achieve e-mail privacy on the unsecure Internet?

E-mail privacy with GnuPG and Mozilla in eComStation

- The problem: How can we achieve e-mail privacy on the unsecure Internet?
- E-mails are normally open documents that could be read by anybody like postcards.

E-mail privacy with GnuPG and Mozilla in eComStation

- The problem: How can we achieve e-mail privacy on the unsecure Internet?
- E-mails are normally open documents that could be read by anybody like postcards.
- Most e-mails are of a none private type but there are situations when it can be welcome with read protection from others than the ”real” recepients.

E-mail privacy with GnuPG and Mozilla in eComStation

- The problem: How can we achieve e-mail privacy on the unsecure Internet?
- E-mails are normally open documents that could be read by anybody like postcards.
- Most e-mails are of a none private type but there are situations when it can be welcome with read protection from others than the ”real” recepients.
- Solution: Start to protect important e-mails with signing and encryption.

E-mail privacy with signing and encryption

- Encryption is nothing new in the computing age, it has been around for centries but modern form of encryption is from the world of spys and military Secret Agencies.
- In times of war and terrorism it is easy to understand why certain things has to be keept secret.
- For companies and private users it's different but there is other types of situations that can motivate privacy. Business secrets, political discussions, contacts with lawyers etc.
- So why not take up the technique and use it when it's motivated? It's free and easy to use.

E-mail privacy with signing and encryption

- How does signing and encryption work and which tools and software do I need?

E-mail privacy with signing and encryption

- How does signing and encryption work and which tools and software do I need?
- Is it complicated and is there any alternatives available on the market for eCS?
- Do I have to pay for something?
- Let us first talk about the technique.

E-mail privacy with signing and encryption

- The most wellknown software for these tasks is Pretty Good Privacy that was developed by an American, Mr Philip Zimmerman. Hi wanted to protect himself from the American authorities and his point was to achieve privacy.
- As a result hi was procecuted by the American society but luckily enough they could not punish him.
- The first versions was command-line based and also available for OS/2 up to version 5.
- It could be used from within a mail client like PM Mail/2 but thanks to license issues, the company behind PM Mail/2 was forbidden to add real documentation and even to point out where to find PGP!!

E-mail privacy with signing and encryption

- Then PGP became a commercial application and there is no later version for OS/2 available. Unfortunately newer versions has broken compatibility with version 5 so it's not useful anymore.
- Since a few years a free alternative to PGP has been brought to Internet users in form of an Open Source software called GnuPG, short for Gnu Privacy Guard. Like other Open Source it's mostly intended for use on Unix and Linux computers. But thanks to the Open Source model it's possible to port to other platforms and that is also the case for OS/2.
- The reason that could make it free is it's not dependent of any patented algoritms like PGP.

E-mail privacy with signing and encryption from Enigmail

- Like earlier PGP's, GnuPG is a command-line tool and thanks to that fact, a little difficult to use for average users. It can be used from PM Mail/2 but it's not that easy.
- Since a couple of years there is a modern Plug-In for the different Mozillas called Enigmail. That Plug-In is nothing more than a graphical shell for GnuPG and adds itself to the menus of Mozilla suite or Thunderbird. Then it's suddenly very easy to use the basics of GnuPG.
- And finally, both these tools are available for OS/2 or eCS so nothing stops you from using modern encryption with full compatibilty to other platforms with the latest version and that is not always the case for eCS users?

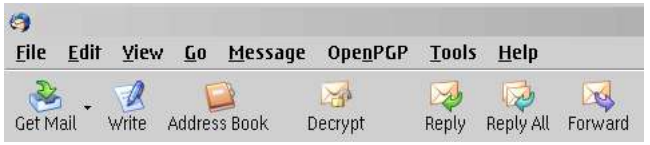
Install GnuPG and reboot the system

- GnuPG for OS/2 is ported from the world of UNIX and it needs a few things on the computer to work.
- First, a runtime of EMX that is standard on eCS.
- Second, a home directory where the keys is going to be stored.
  Eg. c:\home\default\.gnupg
- Third, a UNIX-root argument in config.sys.
  Eg. SET UNIXROOT=c:\unixos2
- Download GnuPG for OS/2 from Internet and start the installation by dropping the wpi-file over the WarpIN-icon. You need to reboot to make the changes in config.sys active.

Install Enigmail to your needs, either for the Mozilla suite or Thunderbird

- Enigmail can handle the basics of GnuPG from your e-mail software. It can only handle the most common tasks but the design gools for Enigmail has never been to cover every odd command.
- Enigmail is available in different version for complete Mozilla suite or Thunderbird use. Download the version you need with your browser and save the file. Then open your mail application and go to Tools and Extensions. Browse for the file and after restart of the mail application, it will show up as new alternative on the menu.
- You can also get Enigmail in different NLS-versions. Download it from Internet and install together with the base code, you should use the same langauge as in Mozilla suite or Thunderbird!

Enigmail Plug-In

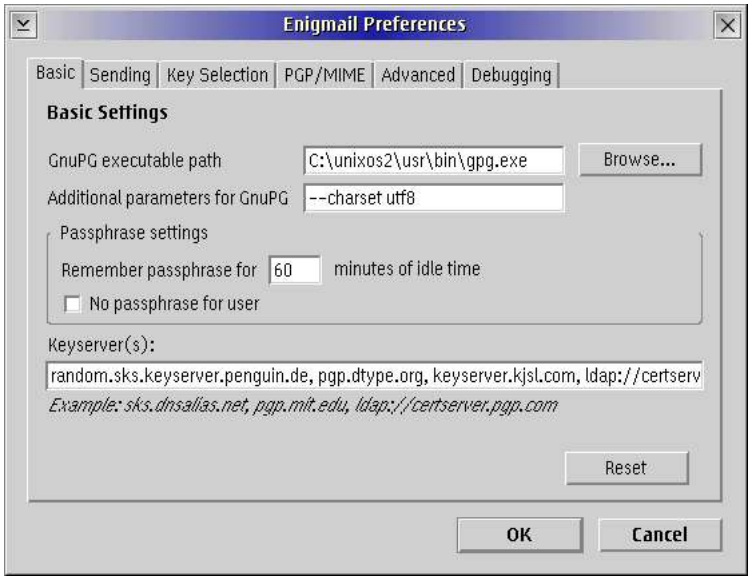


After installation of Enigmail it adds itself to the menu, in this case with the name OpenPGP in Mozilla Thunderbird, earlier versions got the name Enigmail.

There is also a new icon on the tools field called Decrypt.

P.S. It is very important to run Enigmail in the same language as the mail program! Otherwise it can behave very strange and destroy menus and dialogboxes.

Enigmail settings



The most important setting is of cource the path to the binary gpg.exe file.

Remember, don't mark No passphrase for user! Then it would be a lot more unsecure.

The latest Enigmail, 0.93, has a Wizard that can help you with basic configuration. The other settings are not critical and can be changed later if needed. In case of problems it can be useful to activate debugging. The resulting logfiles contains information that could be of great value for developers when helping users.

E-mail privacy with signing and encryption

- Modern encryption is using keys in a combination of one private and one public. The main reason for using two keys is you use the private key for your own encryptions and your recepients needs your public to be able to decrypt your messages.
- The private key should never leave your system, but your public key is free for everybody who wants it. The best is to upload it to a public keyserver. You can also attach it to your mails.
- My recommendation: Don't add it to just any mail, it will only confuse recepients that knows nothing about GnuPG!

E-mail privacy with signing

- What is the difference between signing and encryption?
- A signed mail is given an electronic guarantee that the mail origins from you, made by GnuPG using your e-mail address!
- Remember, your e-mail adress was used to create your pair of keys. The e-mail is not going to be encrypted.
- Signing of a mail uses your private key.
- When the mail arrives, the recepient uses your public key to confirm that it's sent from you and that is possible only if you did it from a system with GnuPG and your keys on it.

E-mail privacy with encryption

- What is the difference between signing and encryption?
- An encrypted mail can only be composed to a recepient that is part of your public keyring. That means you have to download a public key from a keyserver or it could have been sent to you in an e-mail.
- When adding a public key to your system, it grows from only one key to a complete keyring that contains all your contacts that uses GnuPG.
- P.S. It would be of no use to send an encrypted mail to a person that can't open it, that's the reason you must have access to his public key before sending an encrypted mail!

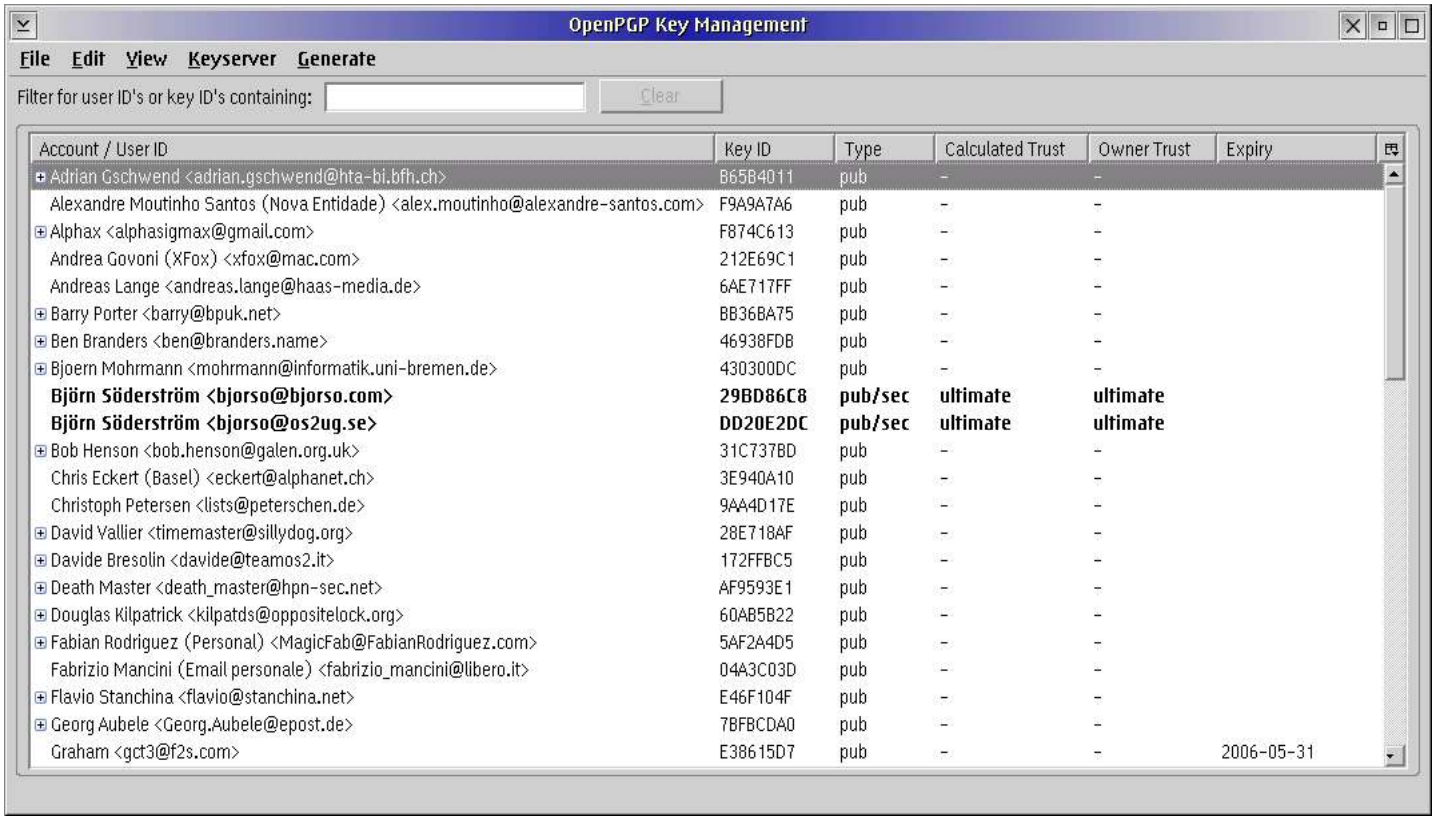
E-mail privacy with signing and encryption

- What is the difference between signing and encryption?
- It is also possible to combine encryption and signing. Then it's going to use both your private key and the recepients public key when composing and sending a mail.
- This is a very strong method for achieving real privacy.
- In Enimail it's possible to set rules for individual recepients. Use that if you are sending GnuPG mail to persons with the same settings every time and to aviod further questions from your mail software.

Sending attachments in e-mails that is signed or encrypted?

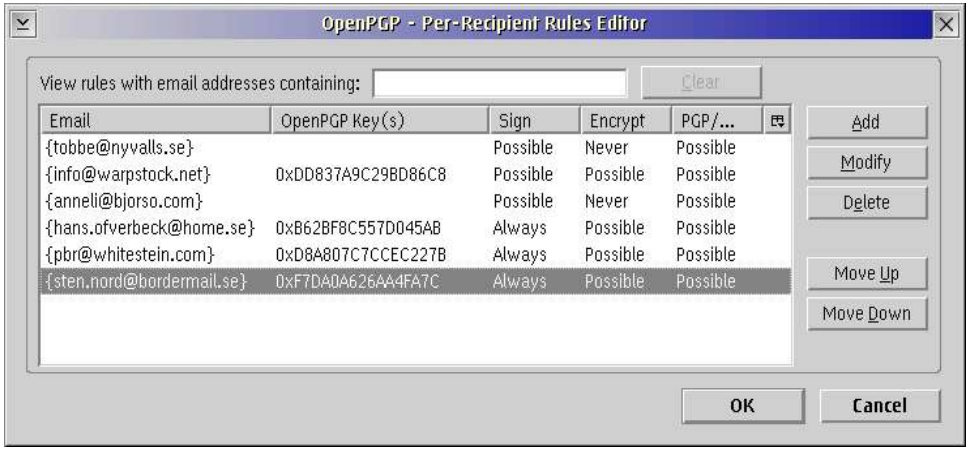
- Earlier version of PGP like 5.0, that was the last for OS/2, could not encrypt attachments to mails like pictures, documents etc.
- When using GnuPG it is possible to include attachments and have the them encrypted as well and there are two different methods available, INLINE and PGP/MINE.
- Use PGP/MIME for compatibility with other software or if you are not sure.
- INLINE is a more modern method but not supported on every e-mail software. Eg. MS Outlook is not supported. There is a Plug-In available on Internet for GnuPG use in MS Outlook but it's not possible to use Enigmail.

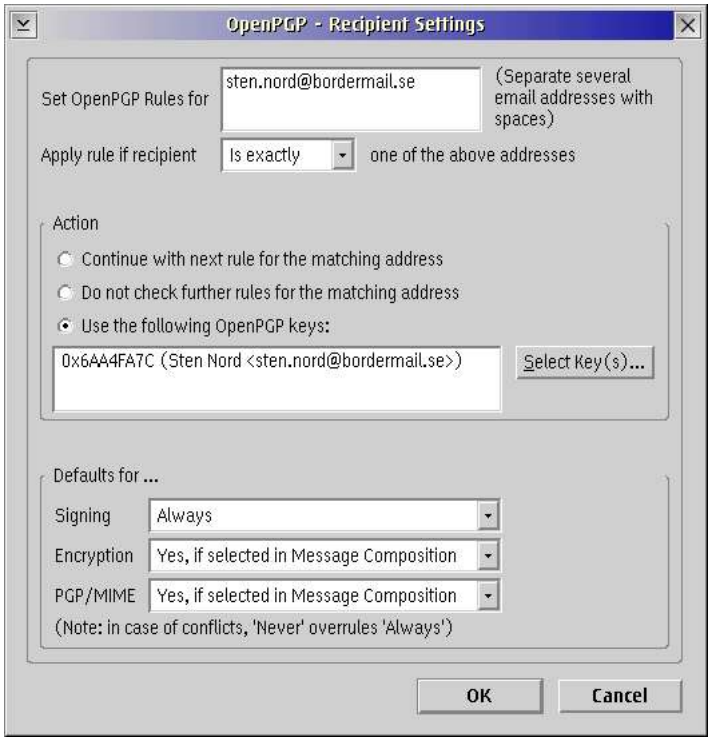
Enigmail keyring management



From this window you can control everything that concerns keys like creation, editing and set trust. One special thing about public keys is that it's not possible to delete them from keyservers. Instead, you have to create a revokation certificate and upload it if you want to cancel your key.

Enigmail per-recepient settings





If you have contacts that you are exchanging mails with regulary, it's easy to add rules for each person so you don't have to answer questions every time.

GnuPG = Pretty Good Privacy the GNU way

- Author of Enigmail for OS/2: Davide Bresolin
  E-mail: davide@teamos2.it
  Web: http://www.dimi.uniud.it/bresolin/warpzilla/
- GnuPG organisation:
  Web: http://www.gnupg.org
- Author of GnuPG for OS/2: Tobias Hürlimann
  E-mail: tobias@tobiashuerlimann.de
  Web: http://www.tobiashuerlimann.de/software/GnuPG/
- Enigmail organisation:
  Web: http://enigmail.mozdev.org

Author of this presentation

- Björn Söderström: Telecommunication engineer employed at Eltel Networks AB in Sweden.
- Have been using OS/2, eCS since 1992 and forward. Been active in translation of sofware since -97. Done XWorkplace, Ghostview, PMView and a lot of other programs including major parts of helpfiles for Mozilla into Swedish.
- Member of Swedish OS/2 User Group http://www.os2ug.se
- E-mail: bjorso@bjorso.com
- Web: http://www.bjorso.com