

GPG - GNU Privacy Guard

How to use

Károly Erdei

October 7, 2013



1 Why

2 Cryptography

3 PGP

4 KGPG-Assistant

5 -Key-Manager

6 -Editor

7 GPG4Win

8 Enigmail

Agenda

- 1 Why
- 2 Cryptography
- 3 PGP
- 4 KPGG-Assistent
- 5 -Key-Manager
- 6 -Editor
- 7 GPG4Win
- 8 Enigmail

Why to use cryptography in the computer/Internet age

Digital privacy

- keeping your appropriate digital data, files, accessible only by you
- keeping your digital communication not readable, accessible for third party members

Public data

- a data sent through the Internet is public, i.e. readable, accessible by third party members, if the data is not encrypted !

It is your task to take care about your digital privacy !

See also my talk later in the semester:

- Security and Privacy in the Internet

Agenda

1 Why

2 Cryptography

3 PGP

4 KPGG-Assistant

5 -Key-Manager

6 -Editor

7 GPG4Win

8 Enigmail

Cryptography

Cryptography

- you encrypt a readable text (or a file) to an unreadable text (or file) using a key
- you can decrypt the file with a key

Symmetric-key cryptography

- for encryption and decryption the same key will be used

Public-key cryptography (assymetric key cryptography)

- a public key and private key pair will be generated
- the public key is used for encryption
- the private key is used for decryption

Public key cryptography

History

Assymetric key cryptography

- 1976 - the paper of Diffie-Hellman: the theory of it.
 - they could not find such a system

RSA algorithm

- 1978 - Rivest, Shamir, Adleman: a working algorithm for the public key cryptography

PGP - Pretty Good Privacy

- 1991 - Zimmermann: algorithm and computer program

Agenda

1 Why

2 Cryptography

3 PGP

4 KPGG-Assistant

5 -Key-Manager

6 -Editor

7 GPG4Win

8 Enigmail

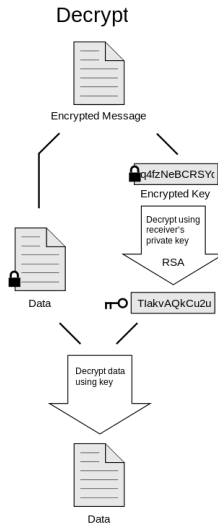
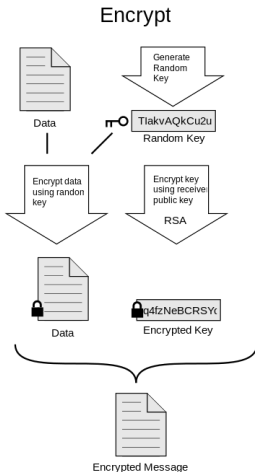
Public key cryptography

PGP features

PGP

- 1991 - Zimmermann: algorithm and computer program:
 - for data encryption and decryption that provides cryptographic privacy and authentication for data communication
 - it uses for encryption a combination of hashing, data compression, symmetric-key cryptography and public-key cryptography
 - the public key is bound to the name and/or email- address
- PGP is used
 - for encryption, decryption and signing ...
 - ... for texts, e-mails, files, directories, and whole disk partitions

How PGP works



PGP, OpenPGP, GPG

PGP

- is available without a fee but is not really free software

OpenPGP

- it is a free software without patent problems
- is a standard of the IETF (Internet Engineering Task Force)
- last version of OpenPGP is defined in RFC 4880 (Nov.2007)

GPG, GnuPG - Gnu Privacy Guard

- a project of the Free Software Foundation
 - OpenPGP specification implemented under GPL
- is freely available together with all source code
- is maintained separatly from GUIs, which use PGP
- <http://www.gnupg.org/>

Versions of GnuPG

GnuPG v-1.4

- compliant with OpenPGP described in RFC 4880.
- the standalone version of OpenPGP
 - no support for S/MIME and for key servers
 - no other tools, usefull for desktop environments
 - mostly used for servers and embedded platforms
- Debian package: gnupg

GnuPG v-2.0

- compliant with OpenPGP described in RFC 2440 (Nov 1998)
- can be set to be compliant to RFC 4880
- the modularized version of OpenPGP
 - support for S/MIME, key servers
 - with tools, usefull for desktop environments
 - used for desktop environments
- Debian package: gnupg2

GUI for GnuPG

GUI for GPG is available for almost all OS

- Linux
 - KGPG - the KDE GUI
 - Seahorse - the GNU GUI
- other OS
 - GPG4Win (MS Windows)
 - MacGPG (Mac OS)
 - iPGMail (iOS)
 - APG (Android)

Enigmail - a Thunderbird plugin which uses GPG

Using GnuPG in Debian and Ubuntu

kgpg - the best GUI

Packages to install

- apt-get install gnupg2
- apt-get install kgpg
- apt-get install seahorse

Packages for use with Mozilla Thunderbird

- apt-get install thunderbird/icedove
- apt-get install enigmail

Agenda

- 1 Why
- 2 Cryptography
- 3 PGP
- 4 KPGG-Assistant
- 5 -Key-Manager
- 6 -Editor
- 7 GPG4Win
- 8 Enigmail

KGPG Assistant

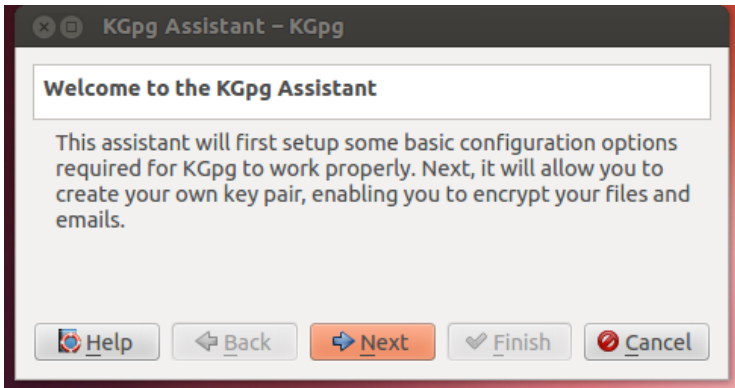
KGPG Assistant

- At the first start of KGPG the Assistant window will be started
- Some basic configuration will be carried out
 - you can confirm the default values for KGPG, by clicking Next, except two values:
- Do unmark the settings for:
 - Generate new key
 - Start KGpg automatically by starting KDE
- Finish configuration

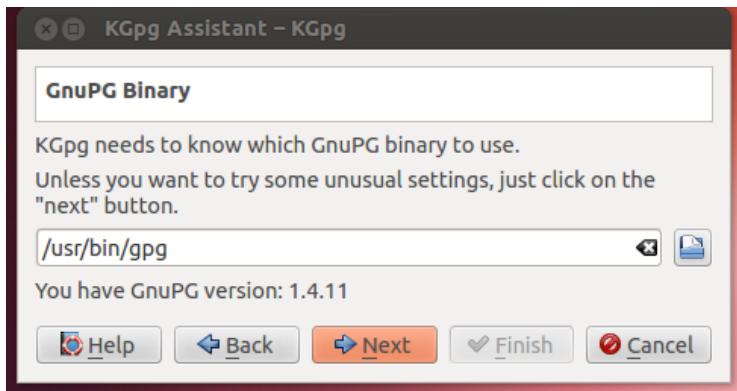
The next slides show you the configuration step-by-step

KGPG Assistant

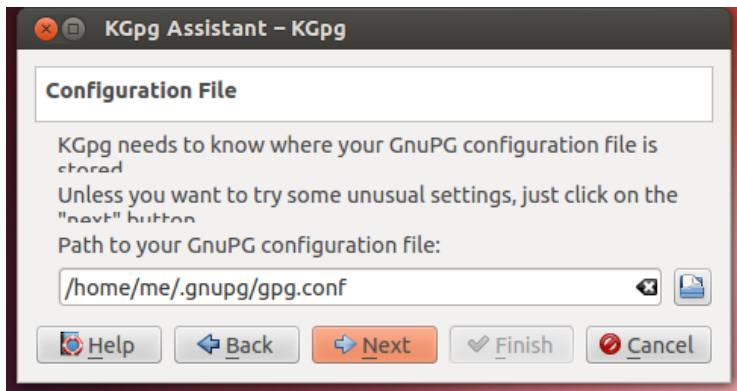
Starting



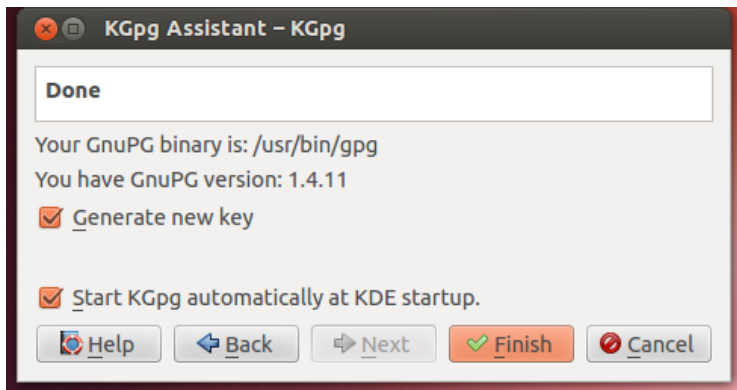
KGPG Assistant



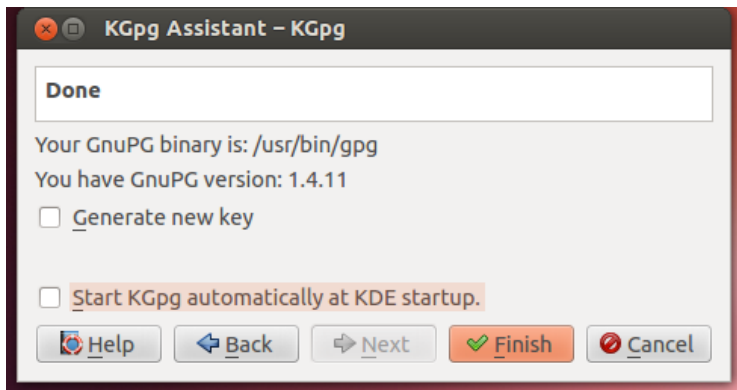
KGPG Assistant



KGPG Assistant



KGPG Assistant



Agenda

- 1 Why
- 2 Cryptography
- 3 PGP
- 4 KPGG-Assistant
- 5 -Key-Manager**
- 6 -Editor
- 7 GPG4Win
- 8 Enigmail

Using KGPG

Parts

Parts of KGPG

- Key Manager
 - start it by: `kgpg -k`
- Editor
 - start it by: `kgpg -d`
- you can start the KGPG Editor from the Key Manager
 - File / Open Editor
- you can start the Key Manager from the Editor
 - File / Open Key Manager

Using KPGP

Key Manager - Main features I.

Features of the Key Manager

- Generation of private/public key pairs
 - extrem important to set a passphrase for the private key
 - choose a long, secure, memorable passphrase
 - if you forgot your passphrase you lost all data which you have/got encrypted (files, emails) - you can not decrypt them anymore !
- Exporting your private/public keys
 - always do it !!
 - write them to a CD and put them in your safe
 - print them and put the printout them in your safe
- Creating revocation certificate for the own public key
 - store it as your private/public key (write to CD/ print it out)
- Changing values in the own public key
 - adding further email addresses
 - changing expiration date
 - adding photo

Using KGPG

Key Manager - Main features II.

Features of the Key Manager

- Importing public keys from files
- Listing public keys and their details
 - name, email address, key-ID, length of the key, expiration date, etc.
- Setting the level of trust for public keys
 - ultimately, fully, marginally, I do NOT trust, I do not know
- Signing public keys
- Using key servers
 - uploading the public key
 - searching for public keys, names, email addresses
 - using more key servers

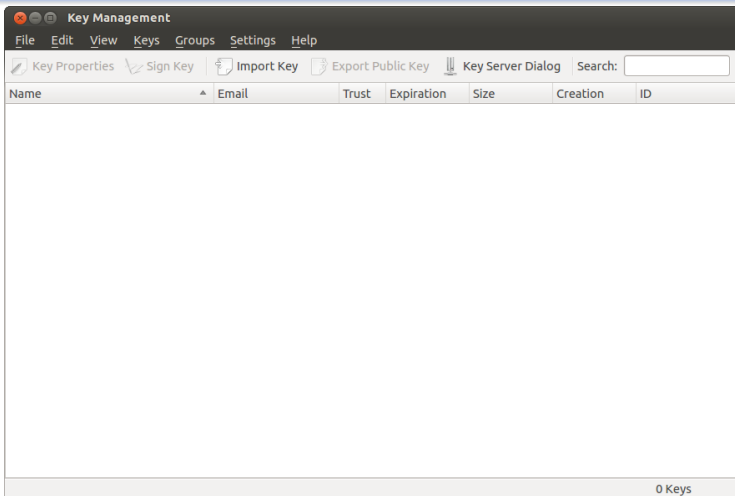
Using KGPG starting

After starting KGPG you get



Using KGPG key manager

Key management window



Menu item: Key / Generate key pairs

Using KGPG key manager

Generate key pair window

Key Generation – KGpg

Generate Key Pair

Name:



Email:

Comment (optional):

Expiration: Never

Key size:

Algorithm: DSA & ElGamal

Expert Mode  Cancel  OK

Using KPGP key manager

Generate key pair window

Key Generation – KGpg

Generate Key Pair

Name:

Email:

Comment (optional):

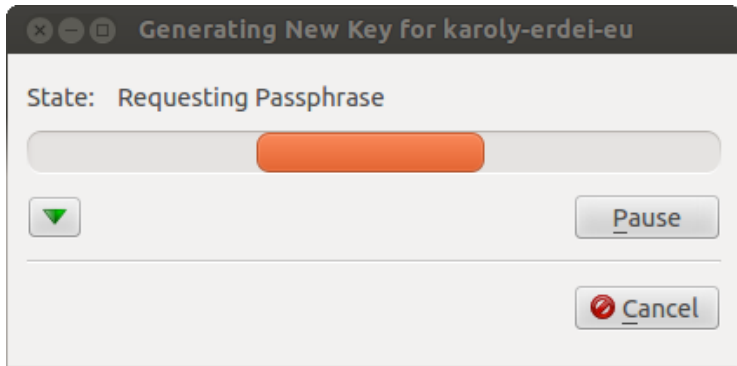
Expiration:
 Never

Key size:

Algorithm:

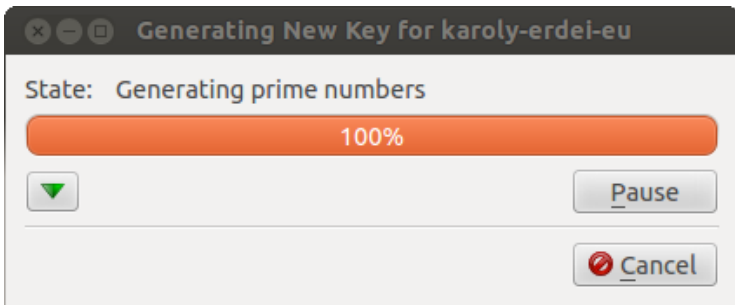
Using KGPG key manager

Generation in progress



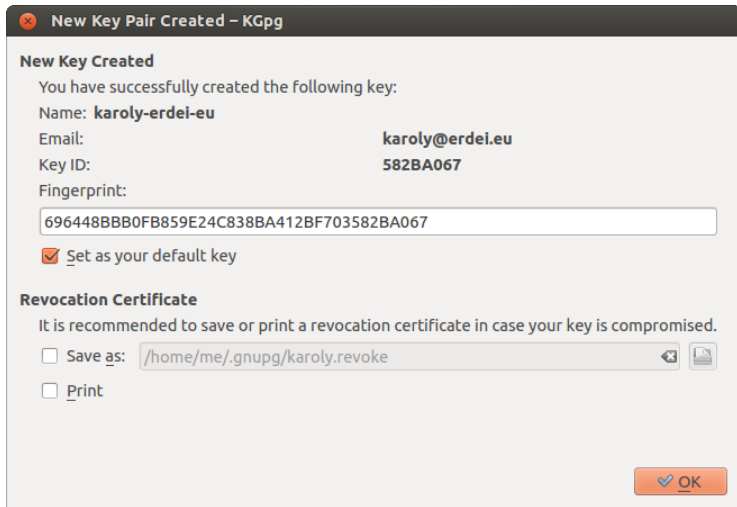
Using KGPG key manager

Generation in progress - prime numbers



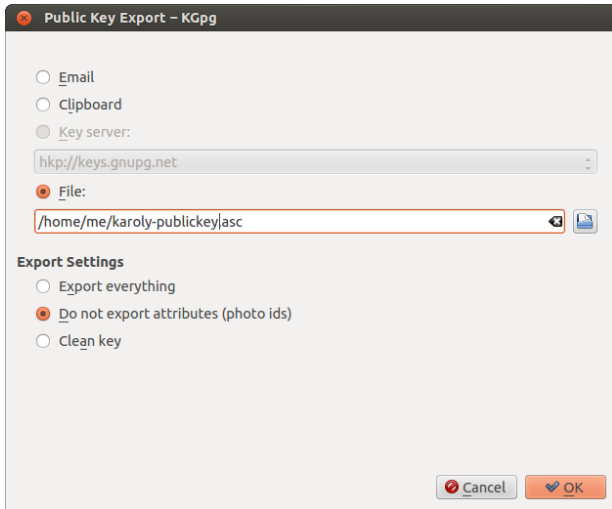
Using KPGP key manager

Properties of the generated key



Using KPGP key manager

Export public key



Agenda

1 Why

2 Cryptography

3 PGP

4 KPGG-Assistant

5 -Key-Manager

6 -Editor

7 GPG4Win

8 Enigmail

Using KPGP

Editor - Main features

Features of the Editor

- is a simple text editor, too
- encrypts, decrypts objects (file, directory)
- signs files and verifies signature

You can create your encrypted file for your internet login data, etc.

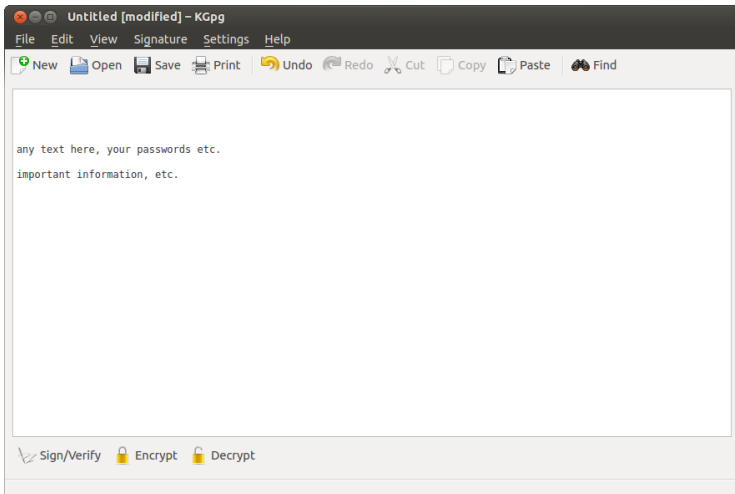
KPGP and file managers

- KPGP work together with file managers
 - konqueror, dolphin, nautilus
- you can encrypt/decrypt files from file manager by getting the menu item by right mouse click

Using KPGP Editor

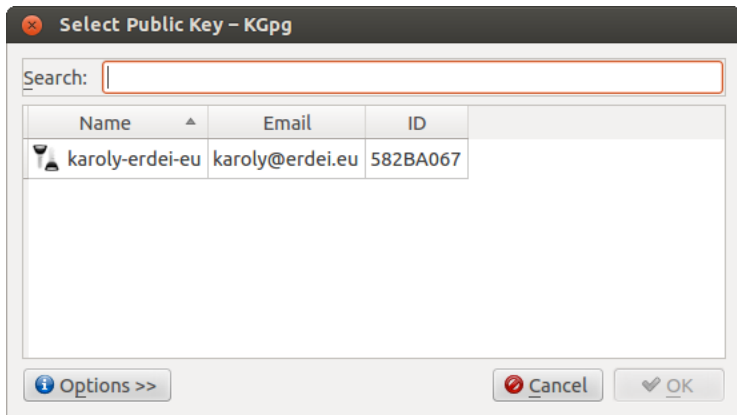
the Editor for encrypt, decrypt files

Type a text in the window and click Encrypt



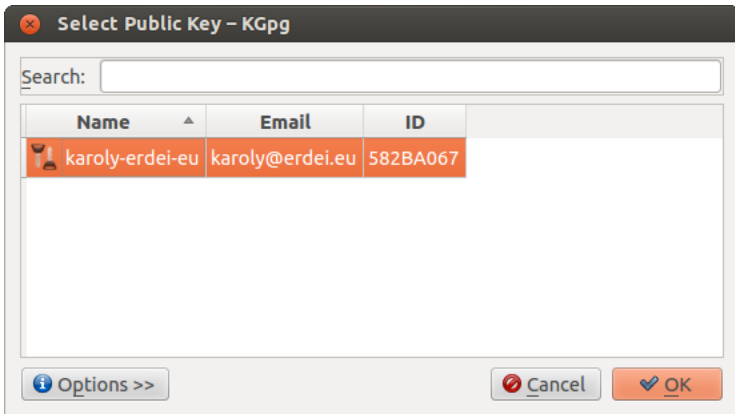
Using KGPG Editor

Open the key files used for encryption



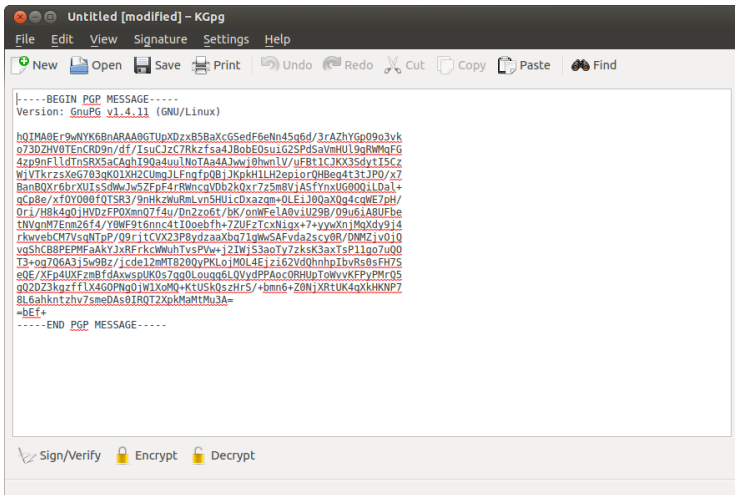
Using KPGP Editor

Select the key used for encryption, click OK



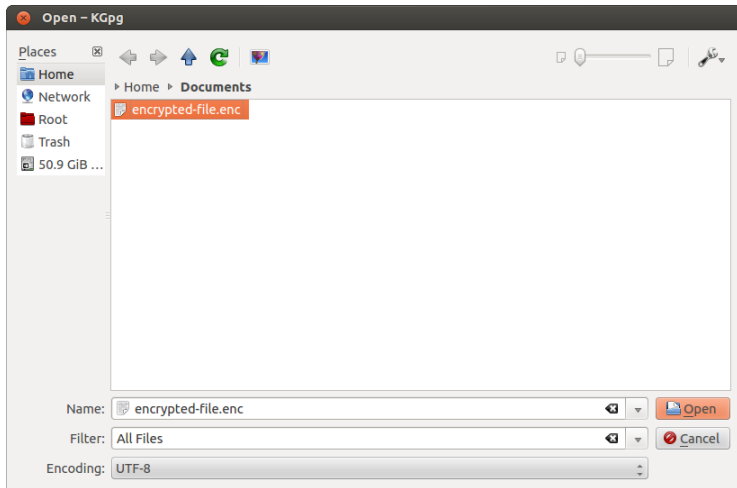
Using KPGP Editor

Here is the encrypted text:



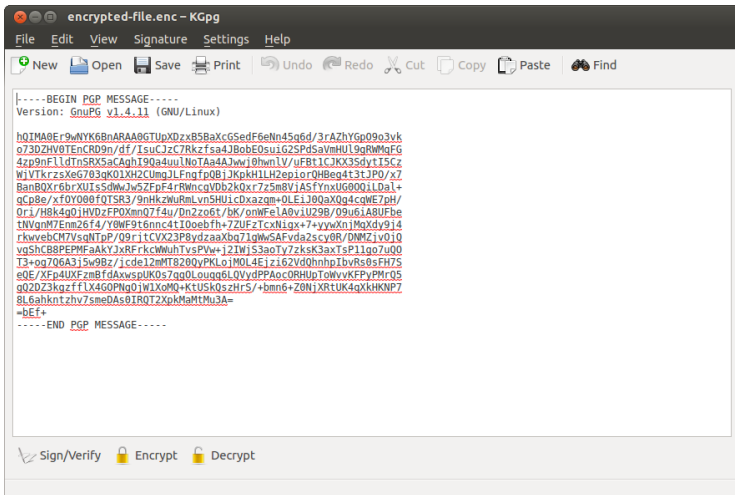
Using KPG Editor

Save the encrypted file (as encrypted-file.enc)



Using KPGP Editor

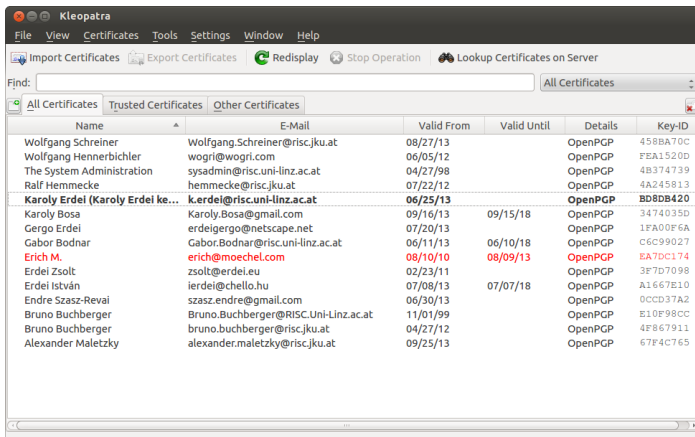
Open the file encrypted-file.enc, the encrypted content will be displayed



Kleopatra

Kleopatra is the KDE Key Manager for GnuPG

- all features, the KPGP has, has Kleopatra, too.
- important is this tool for Windows user



Agenda

- 1 Why
- 2 Cryptography
- 3 PGP
- 4 KPGG-Assistant
- 5 -Key-Manager
- 6 -Editor
- 7 GPG4Win**
- 8 Enigmail

Using GnuPG in MS Windows

GPG4Win

GPG4Win

- <http://www.gpg4win.org/>
- the MS Windows version of GnuPG
- is a free, open source software, under active development
- uses the term **certificate** instead of **key**

Parts of GPG4Win

- GnuPG, the basic software
- Kleopatra, a certificate manager for OpenPGP and S/MIME
- GpgEX, a plugin for Microsoft Explorer (file encryption)
- Claws Mail, a complete email application with crypto support
- Documentation
- GpgOL, plugin for MS Outlook 2003/2007/2010/2013 (email encryption)
- GPA, the Gnu Privacy Assistant

Using GnuPG in MS Windows

Installation, configuration

Installation

- download it from: <http://www.gpg4win.org/download.html>
- current version: Gpg4win 2.2.1 (Released: 2013-10-07)
- download the **full version** which includes the parts listed above
- by the installation unmark: GpgOL, GPA, Claws Mail

Configuration and using Kleopatra

- go to the Webpage at GPG4Win and check the screen shots:
- <http://www.gpg4win.org/screenshots.html>

Enjoy the Gnu Privacy Guard under MS Windows, too !

Agenda

- 1 Why
- 2 Cryptography
- 3 PGP
- 4 KPGG-Assistant
- 5 -Key-Manager
- 6 -Editor
- 7 GPG4Win
- 8 Enigmail**

Using GnuPG in Thunderbird/Icedove

Enigmail add-on

Enigmail

- is a security extension to Mozilla Thunderbird and Seamonkey
- is a plugin, not a standalone program
- it is based on GnuPG, you have to install this first.
 - all features of GnuPG are available

Main features

- Encrypt/sign mail when sending, decrypt/authenticate received mail
- Support for inline-PGP (RFC 4880) and PGP/MIME (RFC 3156)
- Per-Account based encryption and signing defaults
- OpenPGP key management interface
- Per-Recipient rules for automated key selection, and enabling/disabling encryption and signing
- Full features list:
 - <https://www.enigmail.net/documentation/features.php>

Enigmail

Installation, configuration, documentation

Installation

- through the Tools/Add-Ons/ search for Enigmail 1.5.2

Configuration

- see: <https://www.enigmail.net/documentation/basic.php>

Documentation

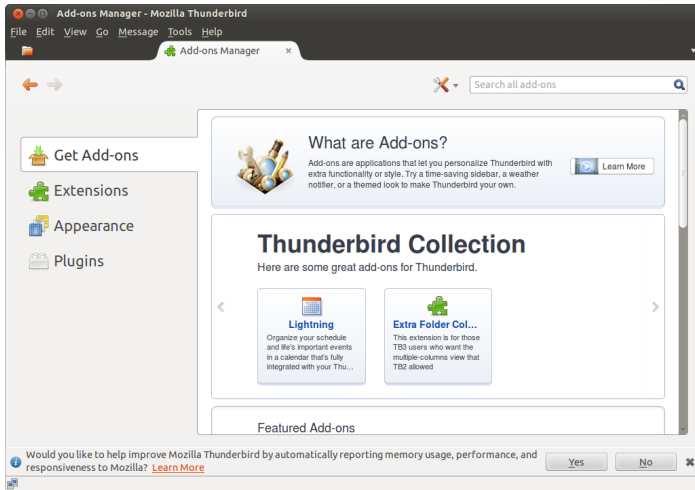
- for new users see the Quick Start Guide:
 - <https://www.enigmail.net/documentation/quickstart.php>
- user manual:
 - <https://www.enigmail.net/documentation/>

The next slides show some of the above steps

Enigmail

Installation I.

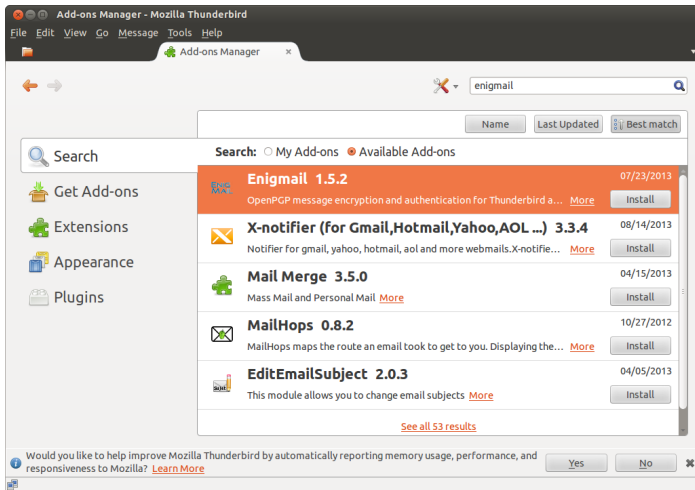
Get the Add-On



Enigmail

Installation II.

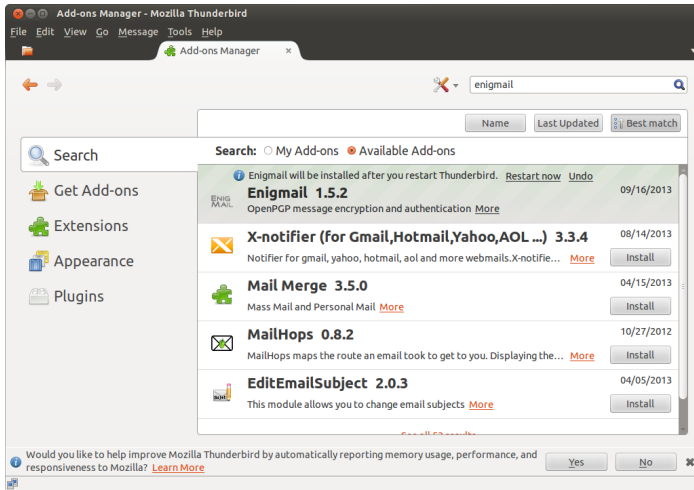
Search for Enigmail



Enigmail

Installation III.

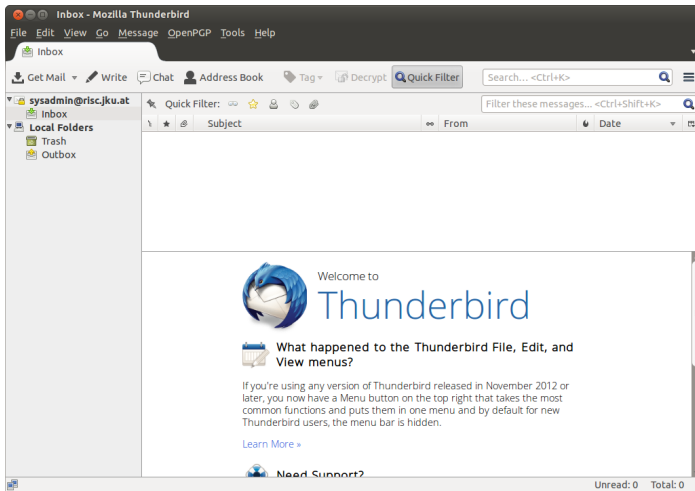
Install it and restart Thunderbird



Enigmail

Installation IV.

You have now the OpenPGP item in the menue list

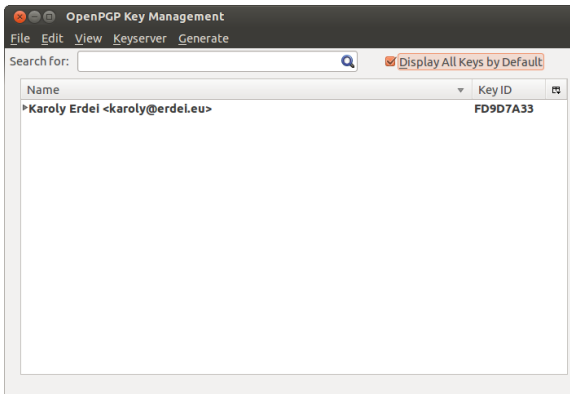


Enigmail - Keys

Start the Key Manager

Menue list: OpenPGP / Key Management

- Always mark: Display All Keys by Default

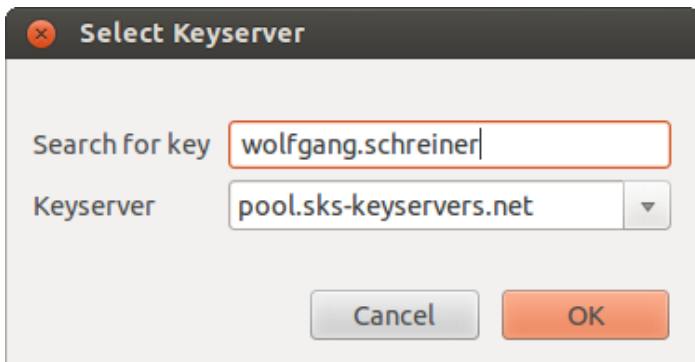


Keyserver / Search for keys

Enigmail - Keys

Select Keyserver Window

Type the name in the Search for key field:



Select Keyserver

Search for key

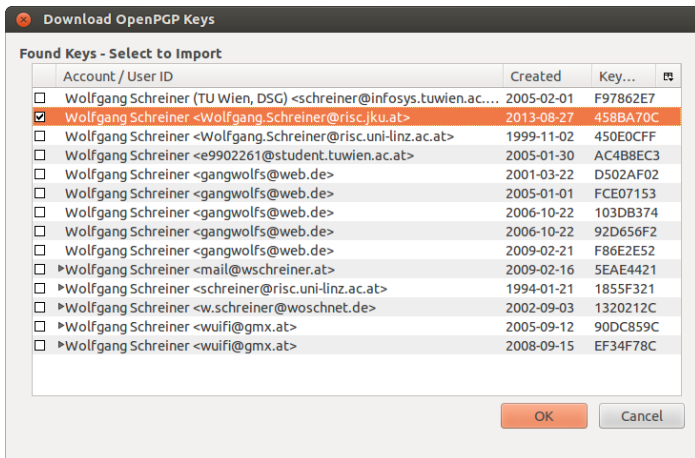
Keyserver ▼

Cancel OK

Enigmail - Keys

Download OpenPGP Keys

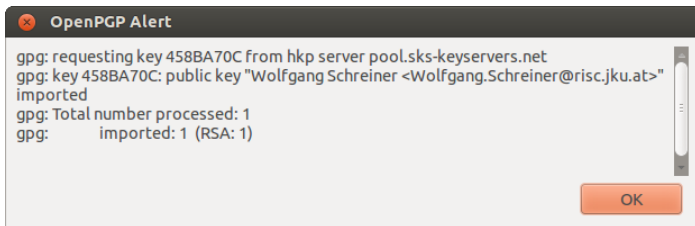
Select the key from the list to download



Enigmail - Keys

OpenPGP Alert

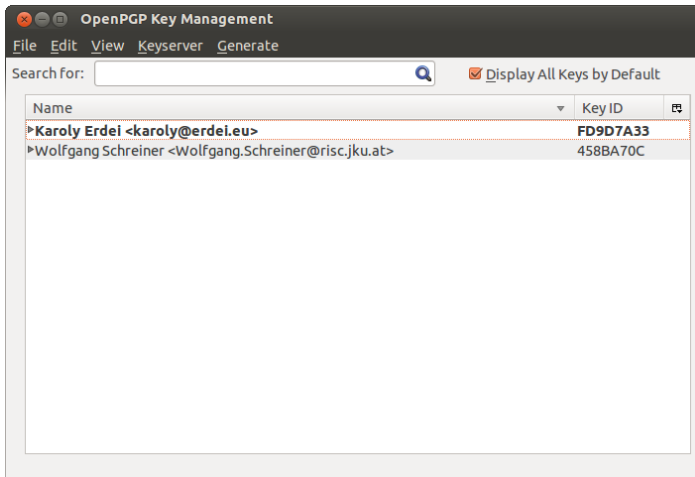
Information about the imported key:



Enigmail - Keys

OpenPGP Key Management Window

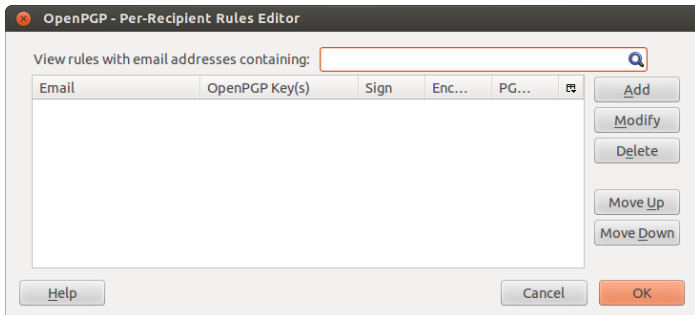
List of the imported keys:



Enigmail

Set up a per recipient rule - I.

OpenPGP / Edit Per Recipient Rules



Click: Add

Enigmail

Set up a per recipient rule - II.

Fill out the fields in the Window: Edit Per Recipient Settings

OpenPGP - Recipient Settings

Set OpenPGP Rules for (Separate several email addresses with spaces)

Apply rule if recipient one of the above addresses

Action

☐ Continue with next rule for the matching address

☐ Do not check further rules for the matching address

☒ Use the following OpenPGP keys:

Defaults for ...

Signing

Encryption

PGP/MIME

(Note: in case of conflicts, 'Never' overrules 'Always')

End of GPG

Enjoy using Enigmail and using encrypted emails !

Thanks for your attention !