GPG - GNU Privacy Guard

How to use

Károly Erdei

October 15, 2014

Agenda

1 Why

2 Cryptography

3 PGP

4 KGPG-Assistant

5 -Key-Manager

6 -Editor

7 GPG4Win

8 Enigmail

Why to use cryptography in the computer/Internet age

Privacy

- Privacy and digital privacy is a human right

Digital privacy means

- keeping your appropriate digital data, files, accessable only by you
- keeping your digital comminication not readable, accessable by third party members (trough encrypting the information before sending)

Public data

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

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

- Nobody else, but YOU, have interest in it !

Agenda

1 Why

2 Cryptography

3 PGP

4 KGPG-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 decript 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 KGPG-Assistant

5 -Key-Manager

6 -Editor

7 GPG4Win

8 Enigmail

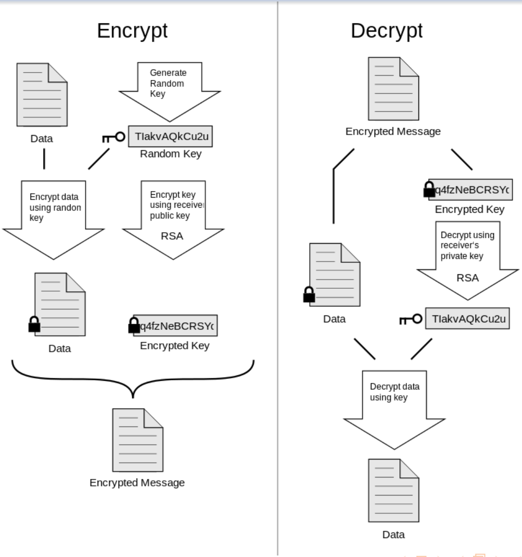
Public key cryptography

PGP features

PGP

- 1991 - Zimmermann: algorithm and computer program:
  - for data encryption and decription 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 GPG
- 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. **KGPG-Assistant**
5. -Key-Manager
6. -Editor
7. GPG4Win
8. Enigmail

KGPG Assistant

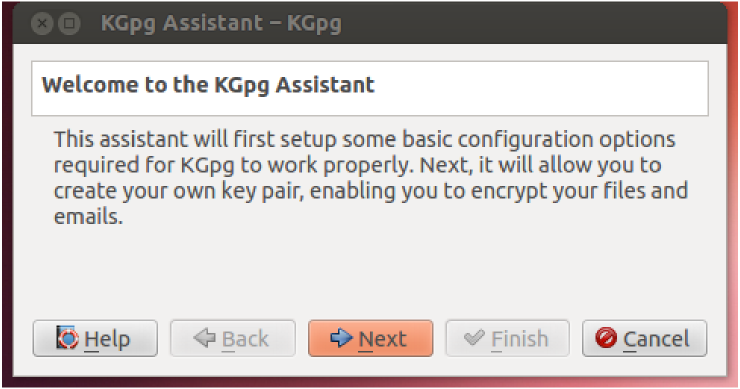
KGPG Assistant

- 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

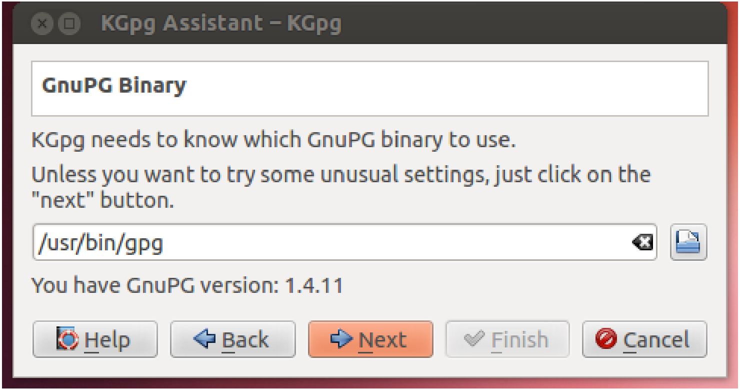
Starting



Welcome to the KGpg Assistant

This assistant will first setup some basic configuration options required for KGpg to work properly. Next, it will allow you to create your own key pair, enabling you to encrypt your files and emails.

KGPG Assistant



KGpg Assistant – KGpg

GnuPG Binary

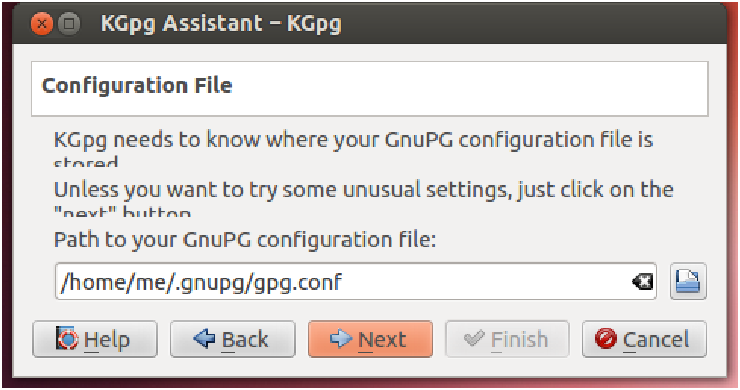
KGpg needs to know which GnuPG binary to use.

Unless you want to try some unusual settings, just click on the "next" button.

/usr/bin/gpg

You have GnuPG version: 1.4.11

KGPG Assistant



KGpg Assistant – KGpg

Configuration File

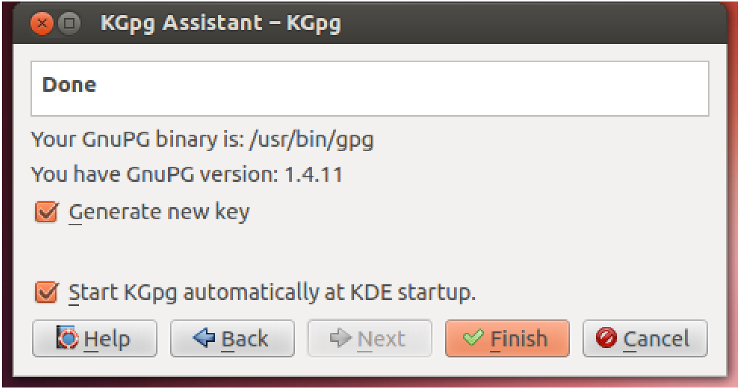
KGpg needs to know where your GnuPG configuration file is stored

Unless you want to try some unusual settings, just click on the "next" button

Path to your GnuPG configuration file:

/home/me/.gnupg/gpg.conf

KGPG Assistant



KGpg Assistant – KGpg

Done

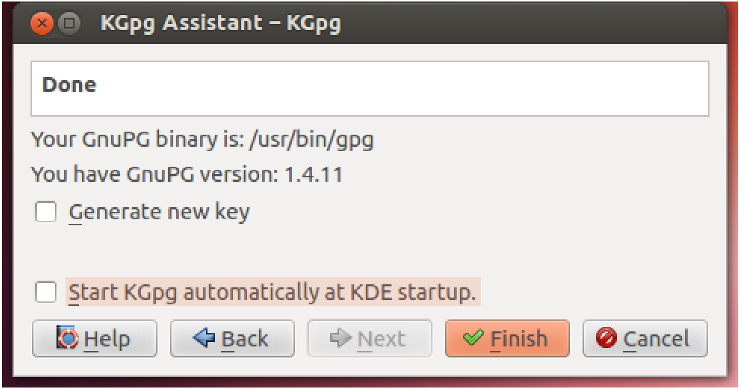
Your GnuPG binary is: /usr/bin/gpg

You have GnuPG version: 1.4.11

☑ Generate new key

☑ Start KGpg automatically at KDE startup.

KGPG Assistant



Your GnuPG binary is: /usr/bin/gpg

You have GnuPG version: 1.4.11

☐ Generate new key

☐ Start KGpg automatically at KDE startup.

Agenda

1 Why

2 Cryptography

3 PGP

4 KGPG-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 KGPG

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, memorizable 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.

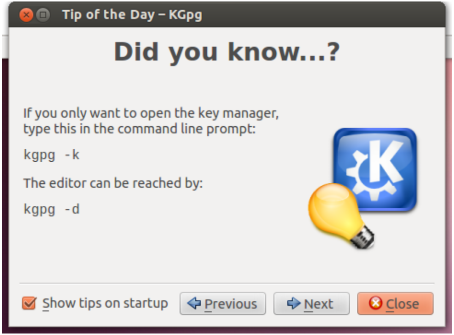
Features of the Key Manager

- 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
  - ultimatly, 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



Tip of the Day – KGpg

Did you know...?

If you only want to open the key manager, type this in the command line prompt:

```
kgpg -k
```

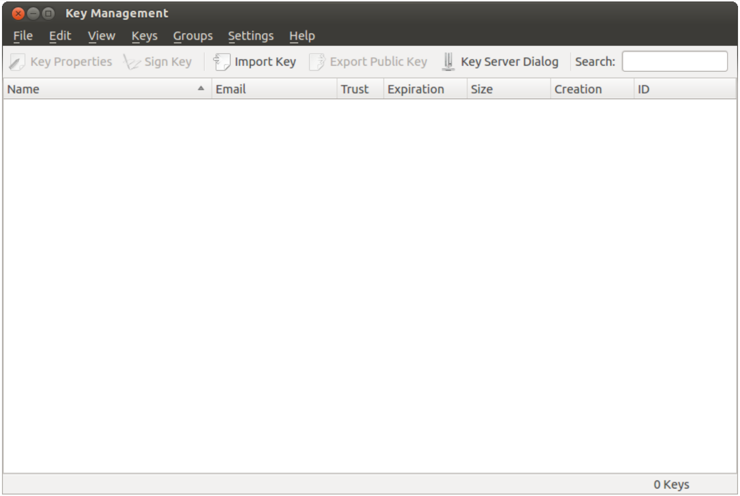
The editor can be reached by:

```
kgpg -d
```

☑ Show tips on startup

Using KGPG key manager

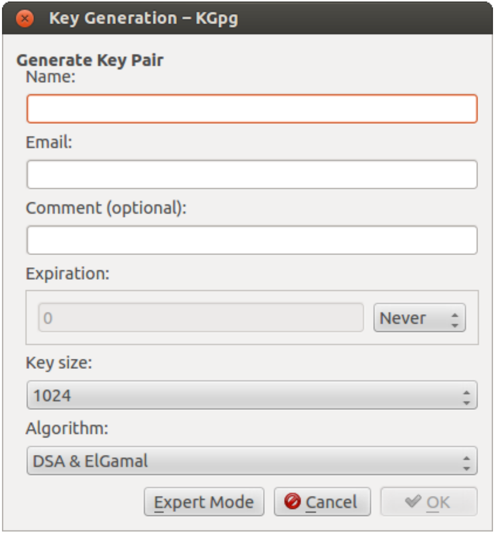
Key management window



Menue item: Key / Generate key pairs

Using KGPG key manager

Generate key pair window



Key Generation – KGpg

Generate Key Pair

Name:

Email:

Comment (optional):

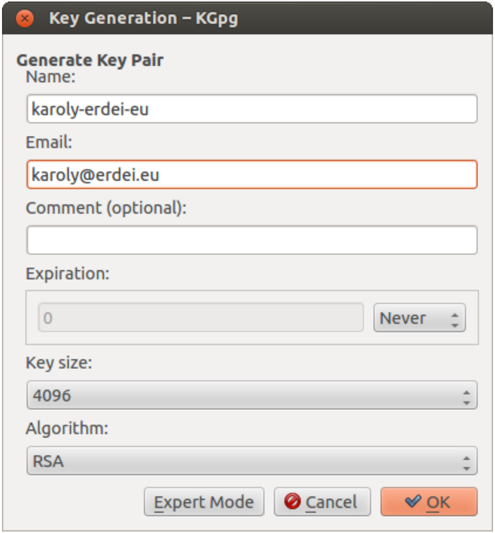
Expiration: 0 Never

Key size: 1024

Algorithm: DSA & ElGamal

Using KGPG key manager

Generate key pair window



Key Generation – KGpg

Generate Key Pair

Name: karoly-erdei-eu

Email: karoly@erdei.eu

Comment (optional):

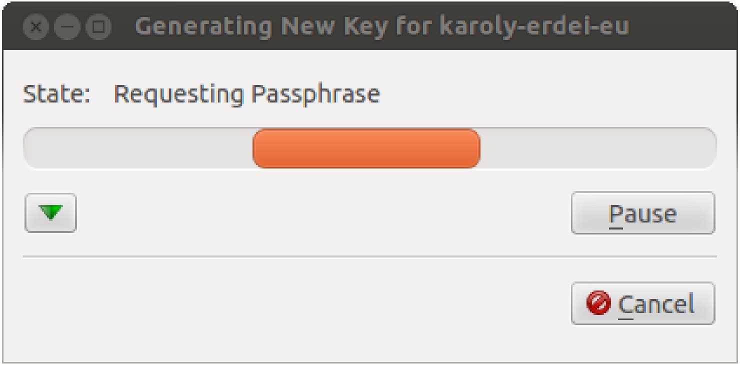
Expiration: 0 Never

Key size: 4096

Algorithm: RSA

Using KGPG key manager

Generation in progress

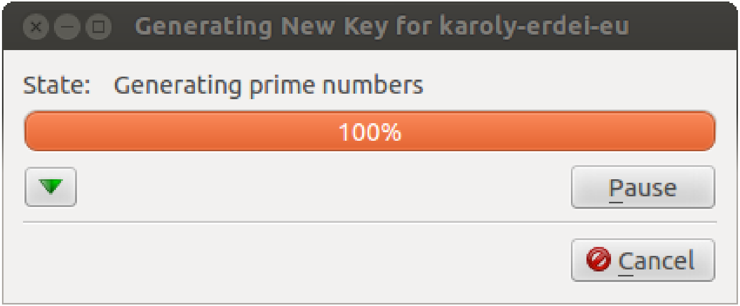


Generating New Key for karoly-erdei-eu

State: Requesting Passphrase

Using KGPG key manager

Generation in progress - prime numbers



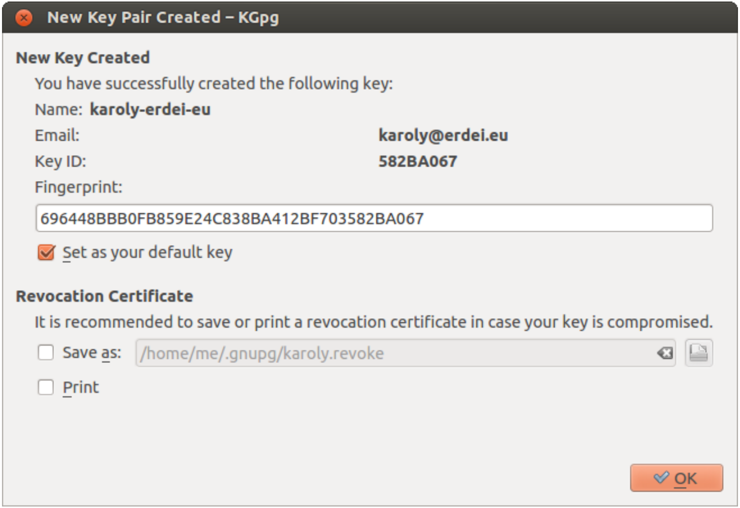
Generating New Key for karoly-erdei-eu

State: Generating prime numbers

100%

Using KGPG key manager

Properties of the generated key



New Key Pair Created – KGpg

New Key Created

You have successfully created the following key:

Name: **karoly-erdei-eu**

Email: **karoly@erdei.eu**

Key ID: **582BA067**

Fingerprint:

696448BBB0FB859E24C838BA412BF703582BA067

☑ Set as your default key

Revocation Certificate

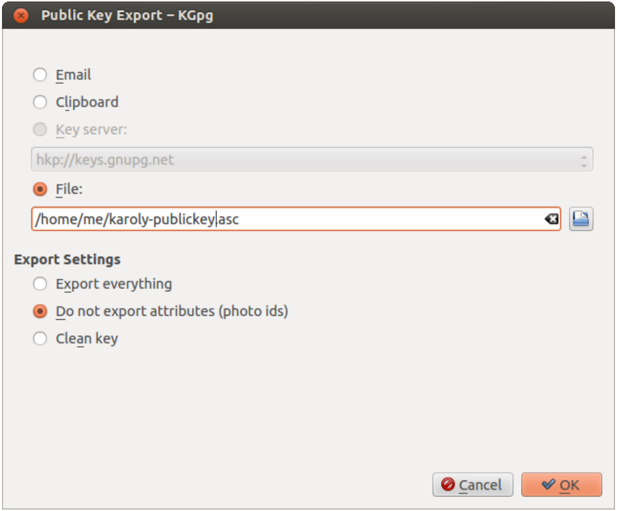
It is recommended to save or print a revocation certificate in case your key is compromised.

☐ Save as: /home/me/.gnupg/karoly.revoke

☐ Print

Using KGPG key manager

Export public key



Public Key Export – KGpg

○ Email

○ Clipboard

○ Key server:

hkp://keys.gnupg.net

● File:

/home/me/karoly-publickey.asc

Export Settings

○ Export everything

● Do not export attributes (photo ids)

○ Clean key

Agenda

1 Why

2 Cryptography

3 PGP

4 KGPG-Assistant

5 -Key-Manager

6 -Editor

7 GPG4Win

8 Enigmail

Using KGPG

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.

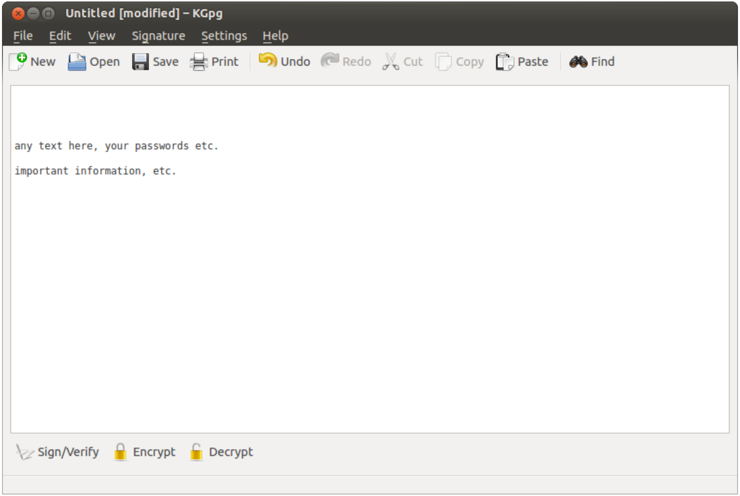
KGPG and file managers

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

Using KGPG Editor

the Editor for encrypt, decrypt files

Type a text in the window and click Encrypt

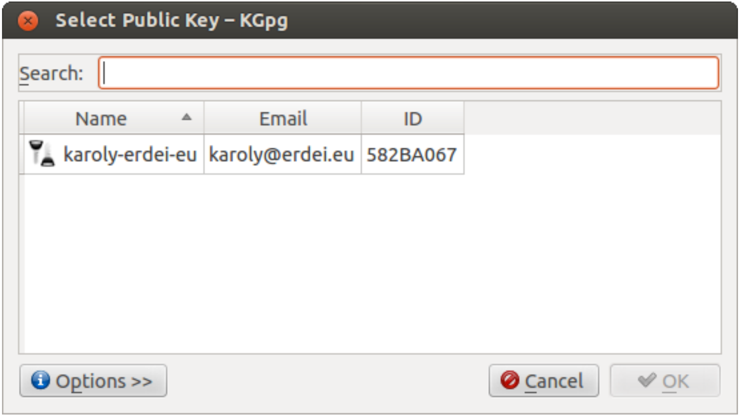


```
any text here, your passwords etc.

important information, etc.
```

Using KGPG Editor

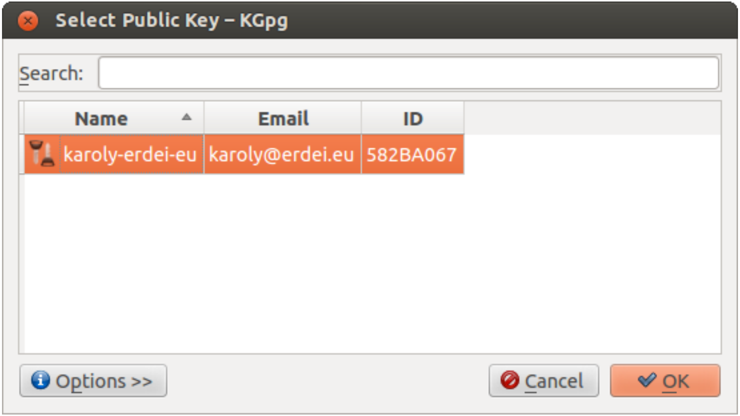
Open the key files used for encryption



Name	Email	ID
karoly-erdei-eu	karoly@erdei.eu	582BA067

Using KGPG Editor

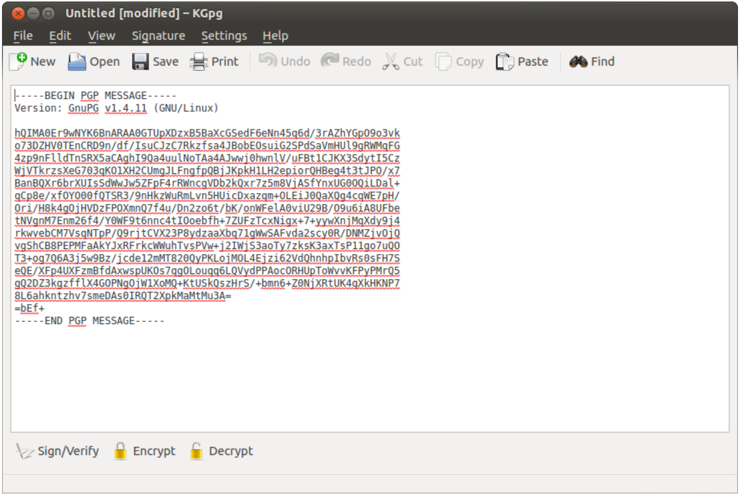
Select the key used for encryption, click OK



Name	Email	ID
karoly-erdei-eu	karoly@erdei.eu	582BA067

Using KGPG Editor

Here is the encrypted text:

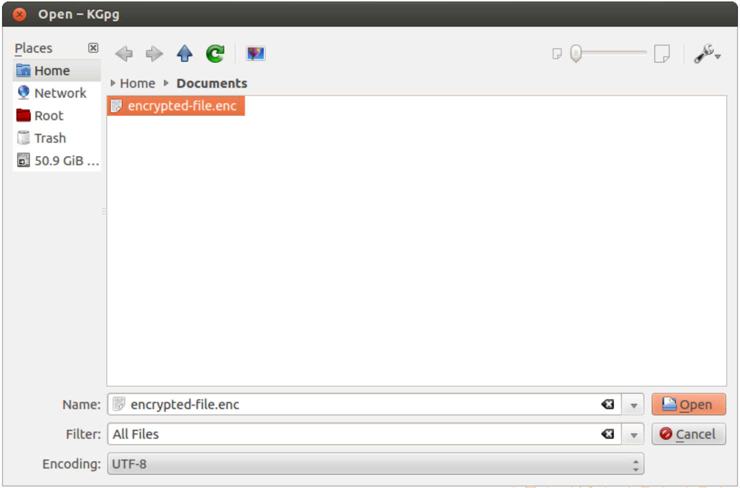

Untitled [modified] – KGpg
File Edit View Signature Settings Help
New Open Save Print Undo Redo Cut Copy Paste Find
Sign/Verify Encrypt Decrypt

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.11 (GNU/Linux)

hQIMA0Er9wNYK6BnARAA0GTUpXDzxB5BaXcGSedF6eNn45q6d/3rAZhYGpO9o3vk
o73DZHV0TEnCRD9n/df/IsuCJzC7Rkzfsa4JBobEOsuiG2SPdSaVmHUl9gRWMqFG
4zp9nFlldTnSRX5aCAghI9Qa4uulNoTAa4AJwwj0hwnlV/uFBt1CJKX3SdytI5Cz
WjVTkrzsXeG703qKO1XH2CUmgJLFngfpQBjJKpkH1LH2epiorQHBeg4t3tJPO/x7
BanBQXr6brXUIsSdWwJw5ZFpF4rRWncgVDb2kQxr7z5m8VjASfYnxUG0OQiLDal+
qCp8e/xfOYO00fQTSR3/9nHkzWuRmLvn5HUicDxazqm+OLEiJ0QaXQg4cqWE7pH/
Ori/H8k4gOjHVDzFPOXmnQ7f4u/Dn2zo6t/bK/onWFelA0viU29B/O9u6iA8UFbe
tNVgnM7Enm26f4/Y0WF9t6nnc4tIOoebfh+7ZUFzTcxNigx+7+yywXnjMqXdy9j4
rkwvebCM7VsqNTpP/Q9rjtCVX23P8ydzaaXbq71gWwSAFvda2scy0R/DNMZjvOjQ
vgShCB8PEPMFaAkYJxRFrkcWWuhTvsPVw+j2IWjS3aoTy7zksK3axTsP11go7uQO
T3+og7Q6A3j5w9Bz/jcde12mMT82OQyPKLojMOL4Ejzi62VdQhnhpIbvRs0sFH7S
eQE/XFp4UXFzmBfdAxwspUKOs7qgOLouqq6LQVydPPAocORHUpToWvvKFPyPMrQ5
gQ2DZ3kgzfflX4GOPNgOjW1XoMQ+KtUSkQszHrS/+bmn6+Z0NjXRtUK4qXkHKNP7
8L6ahkntzhv7smeDAs0IRQT2XpkMaMtMu3A=
=bEf+
-----END PGP MESSAGE-----
```

Using KGPG Editor

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



Open – KGpg

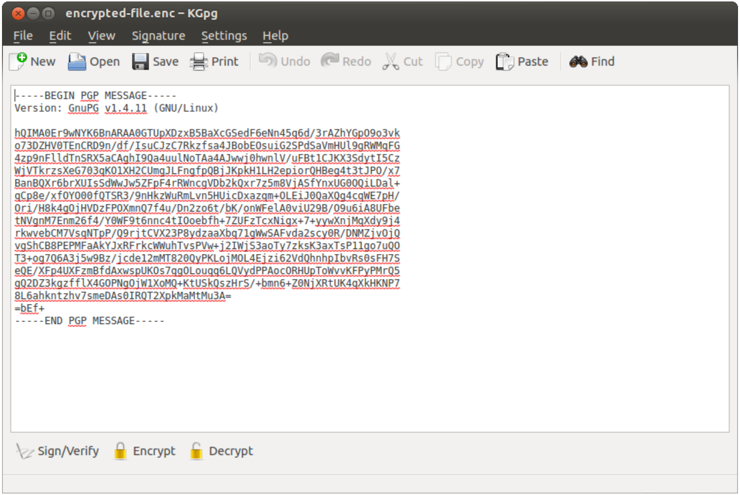
Name: encrypted-file.enc

Filter: All Files

Encoding: UTF-8

Using KGPG Editor

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


encrypted-file.enc – KGpg
File Edit View Signature Settings Help
New Open Save Print Undo Redo Cut Copy Paste Find
Sign/Verify Encrypt Decrypt

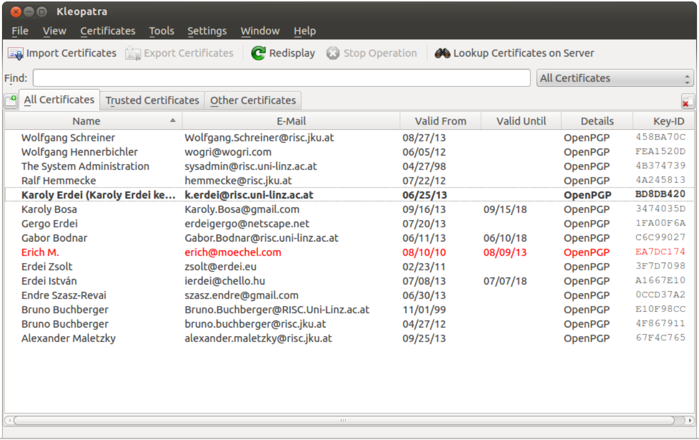
```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.11 (GNU/Linux)

hQIMA0Er9wNYK6BnARAA0GTUpXDzxB5BaXcGSedF6eNn45q6d/3rAZhYGpO9o3vk
o73DZHV0TEnCRD9n/df/IsuCJzC7Rkzfsa4JBobEOsuiG2SPdSaVmHUl9gRWMqFG
4zp9nFlldTnSRX5aCAghI9Qa4uulNoTAa4AJwwj0hwnlV/uFBt1CJKX3SdytI5Cz
WjVTkrzsXeG703qKO1XH2CUmgJLFngfpQBjJKpkH1LH2epiorQHBeg4t3tJPO/x7
BanBQXr6brXUIsSdWwJw5ZFpF4rRWncgVDb2kQxr7z5m8VjASfYnxUG0OQiLDal+
qCp8e/xfOYO00fQTSR3/9nHkzWuRmLvn5HUicDxazqm+OLEiJ0QaXQg4cqWE7pH/
Ori/H8k4gOjHVDzFPOXmnQ7f4u/Dn2zo6t/bK/onWFelA0viU29B/O9u6iA8UFbe
tNVgnM7Enm26f4/Y0WF9t6nnc4tIOoebfh+7ZUFzTcxNigx+7+yywXnjMqXdy9j4
rkwvebCM7VsqNTpP/Q9rjtCVX23P8ydzaaXbq71gWwSAFvda2scy0R/DNMZjvOjQ
vgShCB8PEPMFaAkYJxRFrkcWWuhTvsPVw+j2IWjS3aoTy7zksK3axTsP11go7uQO
T3+og7Q6A3j5w9Bz/jcde12mMT820QyPKLojMOL4Ejzi62VdQhnhpIbvRs0sFH7S
eQE/XFp4UXFzmBfdAxwspUKOs7qgOLouqq6LQVydPPAocORHUpToWvvKFPyPMrQ5
gQ2DZ3kgzfflX4GOPNgOjW1XoMQ+KtUSkQszHrS/+bmn6+Z0NjXRtUK4qXkHKNP7
8L6ahkntzhv7smeDAs0IRQT2XpkMaMtMu3A=
=bEf+
-----END PGP MESSAGE-----
```

Kleopatra

Kleopatra is the KDE Key Manager for GnuPG

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



Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Wolfgang Schreiner	Wolfgang.Schreiner@risc.jku.at	08/27/13		OpenPGP	458BA70C
Wolfgang Hennerbichler	wogri@wogri.com	06/05/12		OpenPGP	FEA1520D
The System Administration	sysadmin@risc.uni-linz.ac.at	04/27/98		OpenPGP	4B374739
Ralf Hemmecke	hemmecke@risc.jku.at	07/22/12		OpenPGP	4A245813
Karoly Erdei (Karoly Erdei ke...	**k.erdei@risc.uni-linz.ac.at**	**06/25/13**		**OpenPGP**	**BD8DB420**
Karoly Bosa	Karoly.Bosa@gmail.com	09/16/13	09/15/18	OpenPGP	3474035D
Gergo Erdei	erdeigergo@netscape.net	07/20/13		OpenPGP	1FA00F6A
Gabor Bodnar	Gabor.Bodnar@risc.uni-linz.ac.at	06/11/13	06/10/18	OpenPGP	C6C99027
Erich M.	erich@moechel.com	08/10/10	08/09/13	OpenPGP	EA7DC174
Erdei Zsolt	zsolt@erdei.eu	02/23/11		OpenPGP	3F7D7098
Erdei István	ierdei@chello.hu	07/08/13	07/07/18	OpenPGP	A1667E10
Endre Szasz-Revai	szasz.endre@gmail.com	06/30/13		OpenPGP	0CCD37A2
Bruno Buchberger	Bruno.Buchberger@RISC.Uni-Linz.ac.at	11/01/99		OpenPGP	E10F98CC
Bruno Buchberger	bruno.buchberger@risc.jku.at	04/27/12		OpenPGP	4F867911
Alexander Maletzky	alexander.maletzky@risc.jku.at	09/25/13		OpenPGP	67F4C765

Agenda

1 Why

2 Cryptography

3 PGP

4 KGPG-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 certifikate 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 2.2.2 (Released: 2014-09-04)
- 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 KGPG-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 1.7.2

Configuration

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

Documentation

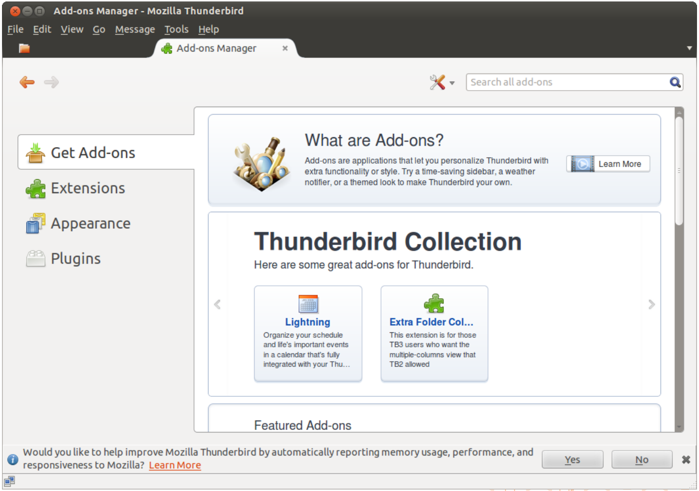
- for new users see the Quick Start Guide:
    - https://www.enigmail.net/documentation/quickstart.php
- user manual:
    - https://www.enigmail.net/documentation/

The next slides show some of the above steps

Enigmail

Installation I.

Get the Add-On



What are Add-ons?

Add-ons are applications that let you personalize Thunderbird with extra functionality or style. Try a time-saving sidebar, a weather notifier, or a themed look to make Thunderbird your own.

Thunderbird Collection

Here are some great add-ons for Thunderbird.

Lightning

Organize your schedule and life's important events in a calendar that's fully integrated with your Thu…

Extra Folder Col…

This extension is for those TB3 users who want the multiple-columns view that TB2 allowed

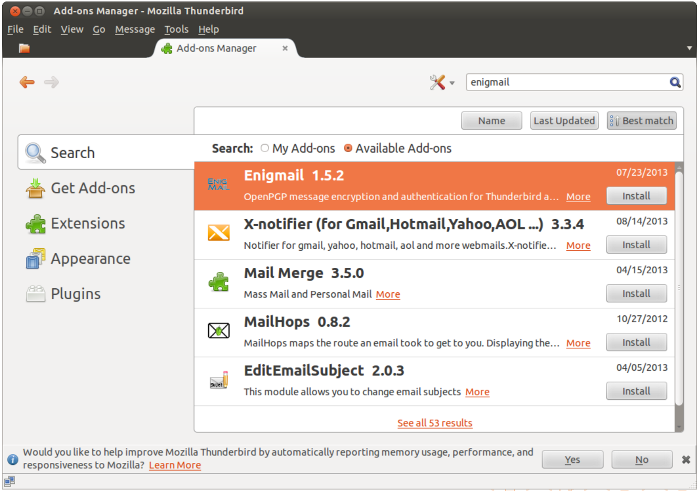
Featured Add-ons

Would you like to help improve Mozilla Thunderbird by automatically reporting memory usage, performance, and responsiveness to Mozilla? Learn More

Enigmail

Installation II.

Search for Enigmail



Add-ons Manager - Mozilla Thunderbird

enigmail

Search: ○ My Add-ons ● Available Add-ons

Add-on	Description	Date	
Enigmail 1.5.2	OpenPGP message encryption and authentication for Thunderbird a... More	07/23/2013	Install
X-notifier (for Gmail,Hotmail,Yahoo,AOL ...) 3.3.4	Notifier for gmail, yahoo, hotmail, aol and more webmails.X-notifie... More	08/14/2013	Install
Mail Merge 3.5.0	Mass Mail and Personal Mail More	04/15/2013	Install
MailHops 0.8.2	MailHops maps the route an email took to get to you. Displaying the... More	10/27/2012	Install
EditEmailSubject 2.0.3	This module allows you to change email subjects More	04/05/2013	Install

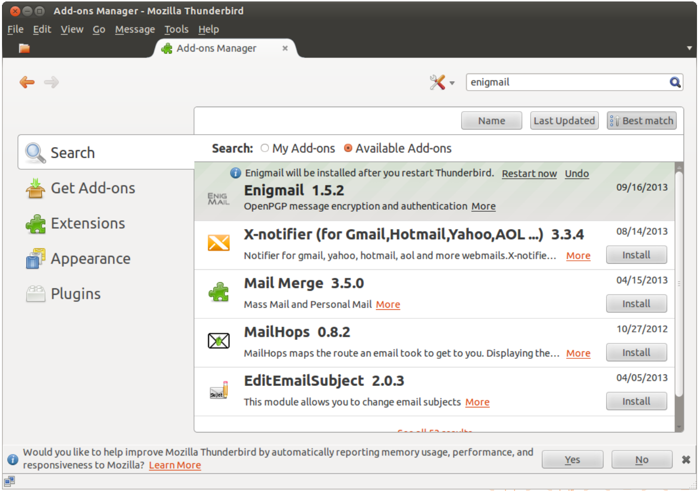
See all 53 results

Would you like to help improve Mozilla Thunderbird by automatically reporting memory usage, performance, and responsiveness to Mozilla? Learn More

Enigmail

Installation III.

Install it and restart Thunderbird



Search: ○ My Add-ons ● Available Add-ons

Enigmail will be installed after you restart Thunderbird. Restart now Undo

Enigmail 1.5.2 — 09/16/2013
OpenPGP message encryption and authentication More

X-notifier (for Gmail,Hotmail,Yahoo,AOL ...) 3.3.4 — 08/14/2013
Notifier for gmail, yahoo, hotmail, aol and more webmails.X-notifie... More

Mail Merge 3.5.0 — 04/15/2013
Mass Mail and Personal Mail More

MailHops 0.8.2 — 10/27/2012
MailHops maps the route an email took to get to you. Displaying the... More

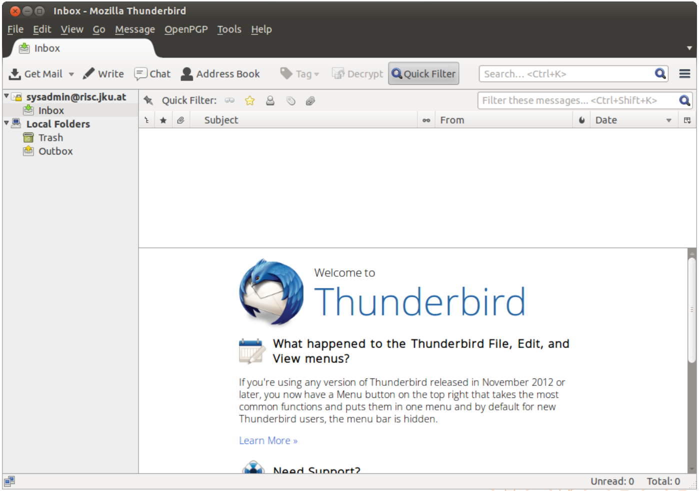
EditEmailSubject 2.0.3 — 04/05/2013
This module allows you to change email subjects More

Would you like to help improve Mozilla Thunderbird by automatically reporting memory usage, performance, and responsiveness to Mozilla? Learn More

Enigmail

Installation IV.

You have now the OpenPGP item in the menue list



Welcome to Thunderbird

What happened to the Thunderbird File, Edit, and View menus?

If you're using any version of Thunderbird released in November 2012 or later, you now have a Menu button on the top right that takes the most common functions and puts them in one menu and by default for new Thunderbird users, the menu bar is hidden.

Learn More »

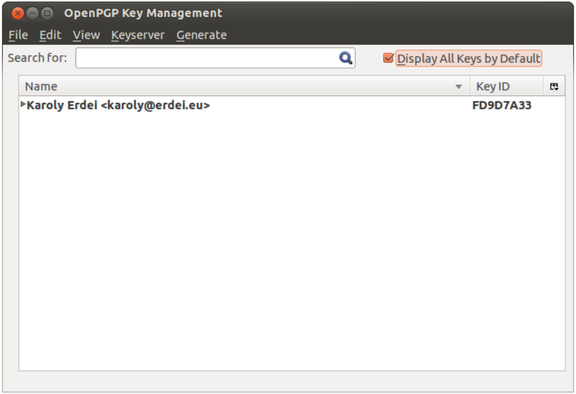
Need Support?

Enigmail - Keys

Start the Key Manager

Menue list: OpenPGP / Key Management

- Always mark: Display All Keys by Default



Search for:

☑ Display All Keys by Default

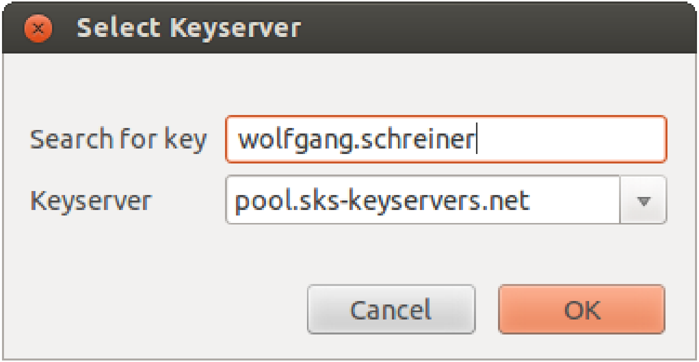
Name	Key ID
Karoly Erdei <karoly@erdei.eu>	FD9D7A33

Keyserver / Search for keys

Enigmail - Keys

Select Keyserver Window

Type the name in the Search for key field:



Select Keyserver

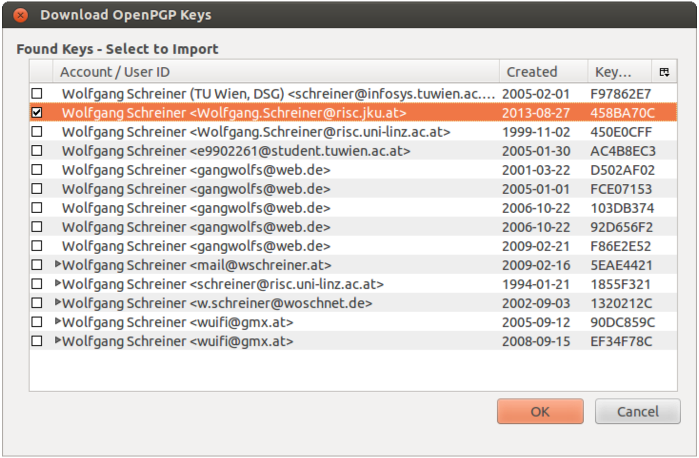
Search for key: wolfgang.schreiner

Keyserver: pool.sks-keyservers.net

Enigmail - Keys

Download OpenPGP Keys

Select the key from the list to download



Download OpenPGP Keys

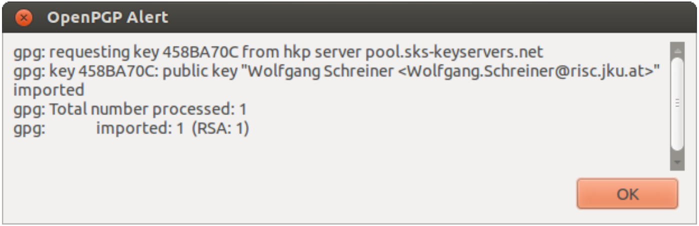
Found Keys - Select to Import

	Account / User ID	Created	Key...
□	Wolfgang Schreiner (TU Wien, DSG) <schreiner@infosys.tuwien.ac....	2005-02-01	F97862E7
☑	Wolfgang Schreiner <Wolfgang.Schreiner@risc.jku.at>	2013-08-27	458BA70C
□	Wolfgang Schreiner <Wolfgang.Schreiner@risc.uni-linz.ac.at>	1999-11-02	450E0CFF
□	Wolfgang Schreiner <e9902261@student.tuwien.ac.at>	2005-01-30	AC4B8EC3
□	Wolfgang Schreiner <gangwolfs@web.de>	2001-03-22	D502AF02
□	Wolfgang Schreiner <gangwolfs@web.de>	2005-01-01	FCE07153
□	Wolfgang Schreiner <gangwolfs@web.de>	2006-10-22	103DB374
□	Wolfgang Schreiner <gangwolfs@web.de>	2006-10-22	92D656F2
□	Wolfgang Schreiner <gangwolfs@web.de>	2009-02-21	F86E2E52
□	▸Wolfgang Schreiner <mail@wschreiner.at>	2009-02-16	5EAE4421
□	▸Wolfgang Schreiner <schreiner@risc.uni-linz.ac.at>	1994-01-21	1855F321
□	▸Wolfgang Schreiner <w.schreiner@woschnet.de>	2002-09-03	1320212C
□	▸Wolfgang Schreiner <wuifi@gmx.at>	2005-09-12	90DC859C
□	▸Wolfgang Schreiner <wuifi@gmx.at>	2008-09-15	EF34F78C

Enigmail - Keys

OpenPGP Alert

Information about the imported key:



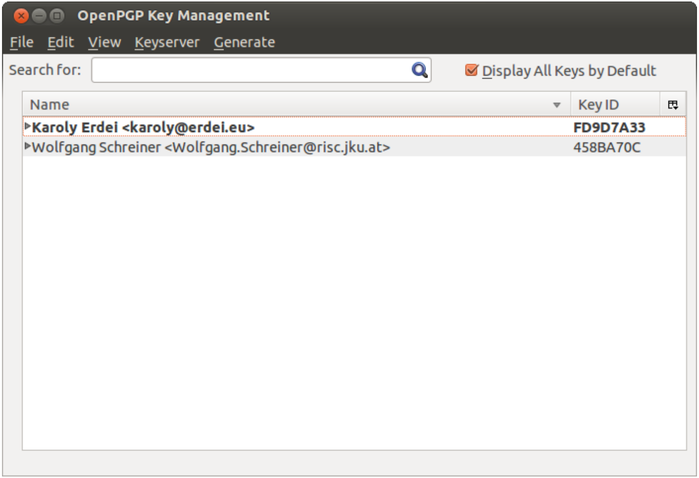
OpenPGP Alert

```
gpg: requesting key 458BA70C from hkp server pool.sks-keyservers.net
gpg: key 458BA70C: public key "Wolfgang Schreiner <Wolfgang.Schreiner@risc.jku.at>"
imported
gpg: Total number processed: 1
gpg:          imported: 1  (RSA: 1)
```

Enigmail - Keys

OpenPGP Key Management Window

List of the imported keys:

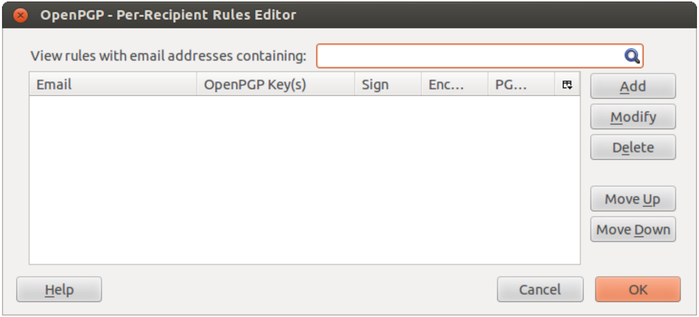

OpenPGP Key Management
File Edit View Keyserver Generate
Search for:
☑ Display All Keys by Default

Name	Key ID
Karoly Erdei <karoly@erdei.eu>	**FD9D7A33**
Wolfgang Schreiner <Wolfgang.Schreiner@risc.jku.at>	458BA70C

Enigmail

Set up a per recipient rule - I.

OpenPGP / Edit Per Recipient Rules

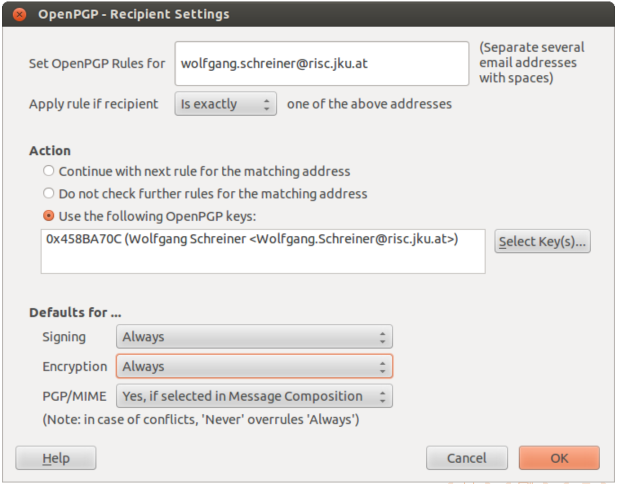

OpenPGP - Per-Recipient Rules Editor
View rules with email addresses containing:
Email
OpenPGP Key(s)
Sign
Enc...
PG...
Add
Modify
Delete
Move Up
Move Down
Help
Cancel
OK

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: wolfgang.schreiner@risc.jku.at (Separate several email addresses with spaces)

Apply rule if recipient: Is exactly 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:

0x458BA70C (Wolfgang Schreiner <Wolfgang.Schreiner@risc.jku.at>)

Defaults for ...

Signing: Always

Encryption: Always

PGP/MIME: Yes, if selected in Message Composition

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

End of GPG

Enjoy using Enigmail and using encrypted emails !

Thanks for your attention !