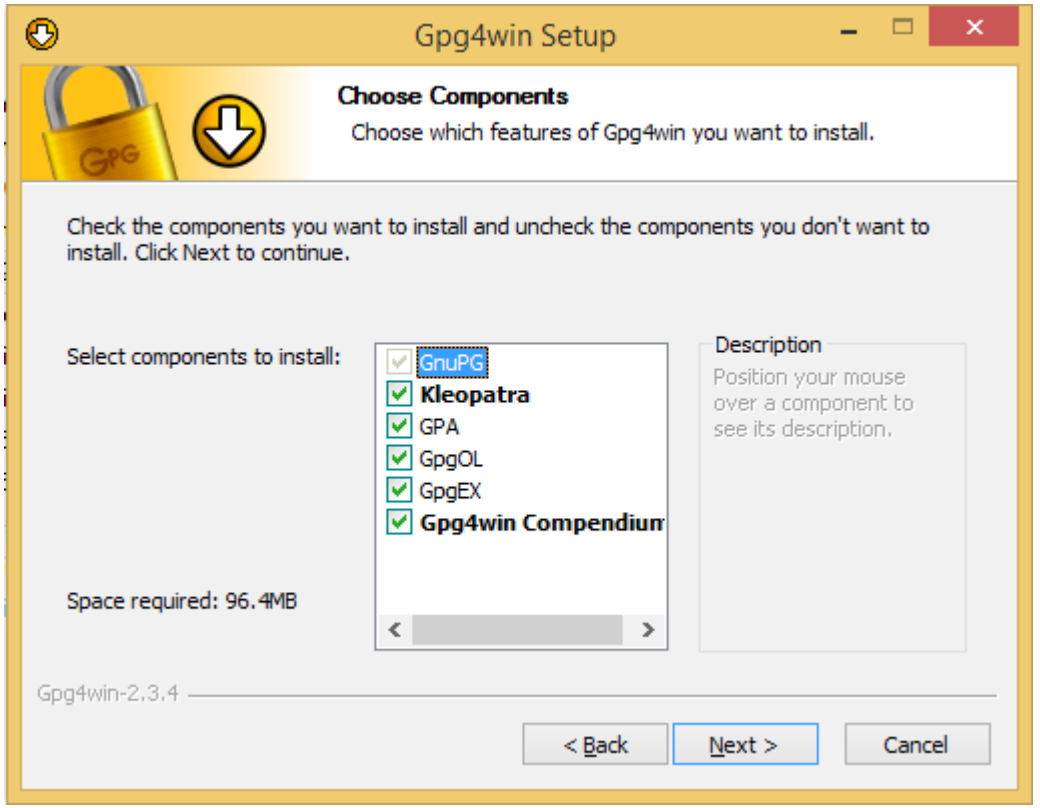
gPGP

Installing and using gPGP

Required Software

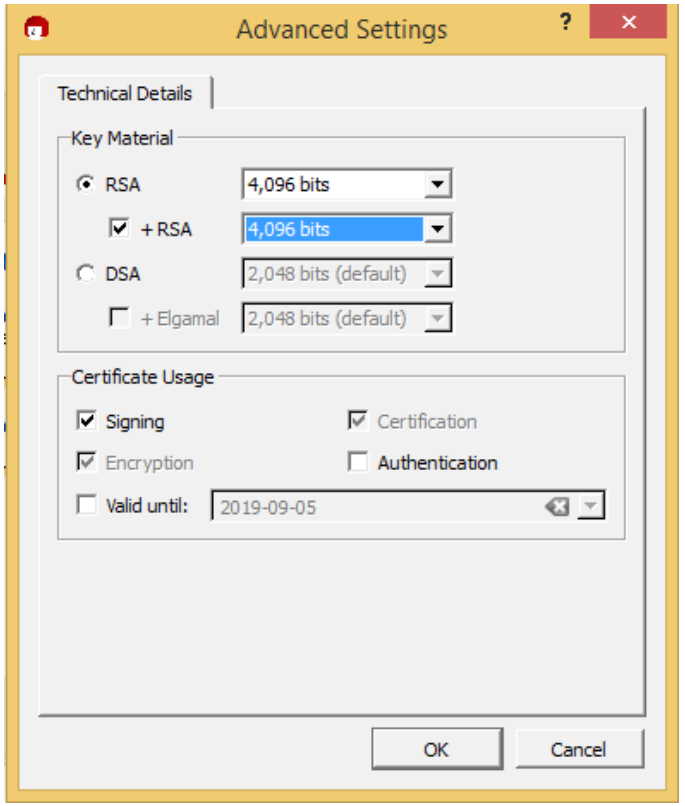
- Windows: Gpg4win
  `http://tznog.sns.tznog.or.tz/tznog5/sns/pgp/gpg4win-2.3.4.exe`
- Mac: GPG Suite
  `http://tznog.sns.tznog.or.tz/tznog5/sns/pgp/GPG_Suite-2016.10_v2.dmg`
- Linux: GnuPG2
  `(apt|yum|emerge) gnupg2`

Installation gpg4win



Generate a key pair

- Start Kleopatra
- CTRL+N (File – New Certificate – Create new personal GnuPGP key pair)



Or with the command line

```
tznog@localhost:~$ gpg2 --gen-key
gpg (GnuPG) 2.0.22; Copyright (C) 2013 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
```

- RSA keys may be between 1024 and 4096 bits long.
- What keysize do you want? (2048) 4096
- Requested keysize is 4096 bits
- Please specify how long the key should be valid.
- 0 = key does not expire
- <n> = key expires in n days
- <n>w = key expires in n weeks
- <n>m = key expires in n months
- <n>y = key expires in n years
- Key is valid for? (0) 5y
- Key expires at Sun 04 Sep 2022 08:40:29 AM UTC
- Is this correct? (y/N) y
-
- GnuPG needs to construct a user ID to identify your key.
-
- Real name: TZNOG5
- Email address: tznog5@ict-pros.co.tz
- Comment:
- You selected this USER-ID:
- "TZNOG5 <tznog5@ict-pros.co.tz>"
-
- Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o

```
GnuPG needs to construct a user ID to identify your key.

Real name: TZNOG5
Email address: tznog5@ict-pros.co.tz
Comment:
You selected this USER-ID:
    "TZNOG5 <tznog5@ict-pros.co.tz>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o
```

```
You need a Passphrase to protect your secret key.


We need to generate a lot of random bytes. It is a good idea to
perform

some other action (type on the keyboard, move the mouse, utilize the

disks) during the prime generation; this gives the random number

generator a better chance to gain enough entropy.

We need to generate a lot of random bytes. It is a good idea to
perform

some other action (type on the keyboard, move the mouse, utilize the

disks) during the prime generation; this gives the random number

generator a better chance to gain enough entropy.

gpg: /home/tznog/.gnupg/trustdb.gpg: trustdb created

gpg: key 88BC02B7 marked as ultimately trusted

public and secret key created and signed.
```

```
gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2022-09-04
pub   4096R/88BC02B7 2017-09-05 [expires: 2022-09-04]
      Key fingerprint = 5002 FB78 1ABF 4592 56BD  5567 C6B1 9EB0 88BC 02B7
uid                  TZNOG5 <tznog5@ict-pros.co.tz>
sub   4096R/183CE2B8 2017-09-05 [expires: 2022-09-04]
```

Next Steps

- Crate a backup of the key

```
gpg2 --export-secret-keys --armor -o <filename>.asc tznog5@ict-pros.co.tz
```

- Create a revocation key for the case that should not happen….

  This steps are similar in Linux and Windows: Command line:

Revocation key

- Find you key ID

```
tznog@localhost:~$ gpg2 -k
/home/tznog/.gnupg/pubring.gpg
------------------------------
pub   4096R/C7A44C7B 2017-09-05 [expires: 2022-09-04]
uid                  TZNOG5 <tznog5@ict-pros.co.tz>
sub   4096R/6A089451 2017-09-05 [expires: 2022-09-04]

tznog@localhost:~$
```

Generate revocation key

```
tznog@localhost:~$ gpg2 --gen-revoke -o tznog.ict-pros.co.tz_revoke.asc C7A44C7B

sec  4096R/C7A44C7B 2017-09-05 TZNOG5 <tznog5@ict-pros.co.tz>

Create a revocation certificate for this key? (y/N) y

You need a passphrase to unlock the secret key for
user: "TZNOG5 <tznog5@ict-pros.co.tz>"
4096-bit RSA key, ID 88BC02B7, created 2017-09-05

ASCII armored output forced.
Revocation certificate created.
```

Export your public key

- You might need it.
  And you can distribute it wherever you want.

```
gpg2 –export –armor -o public_key.asc tznog5@ictpros.co.tz
```

What to do with this keys?

- Keep the backup key and the revocation key on a safe and secret place!

  Hint: Printing as QR code
- Upload the public key to the key servers

Plugins addons for MUA

- Thunderbird: Enigmail
  https://addons.mozilla.org/en-US/thunderbird/addon/enigmail/
- Outlook: Comes with pgp4win
- iPhone/iPad: iPGMail
- Android: K9-Mail + OpenKeychain (APGP is not longer supported!)
- Browser (Firefox and Chrome): Mailvelope
  https://www.mailvelope.com/en