MyPGP
new key

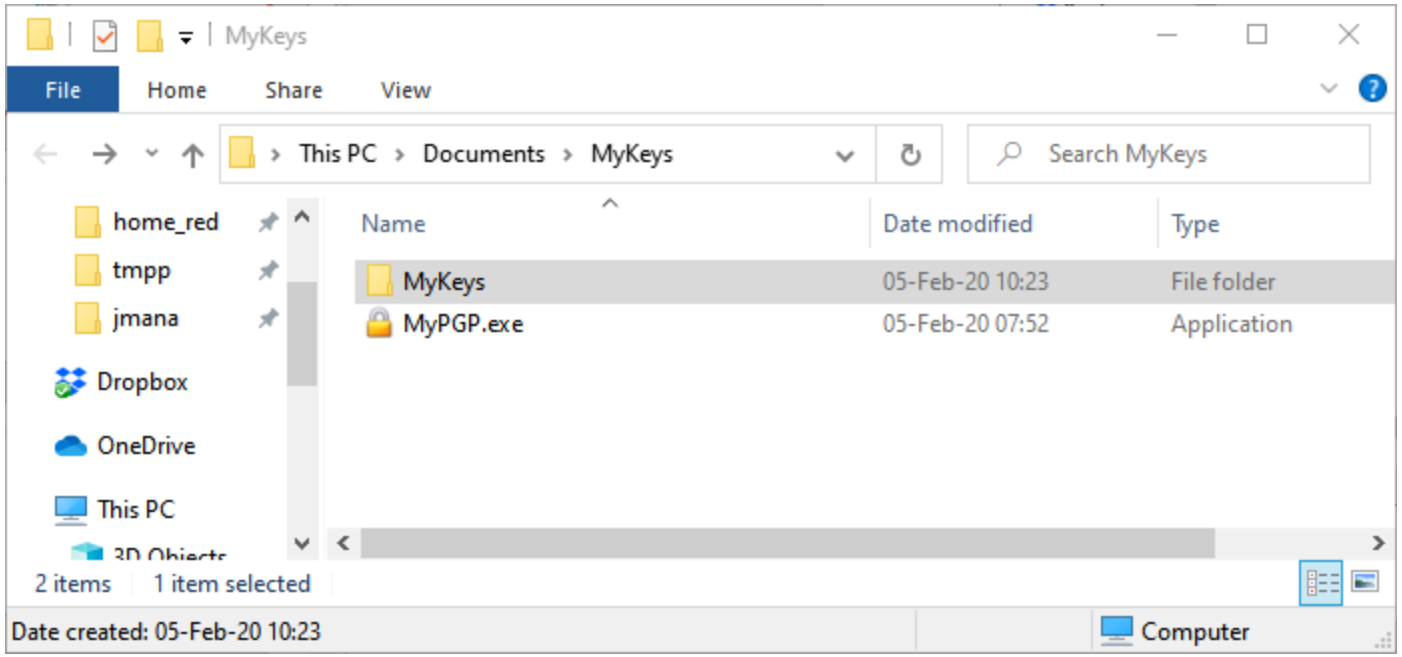
José A. Mañas

https://www.linkedin.com/in/jmanas1/

December 2020

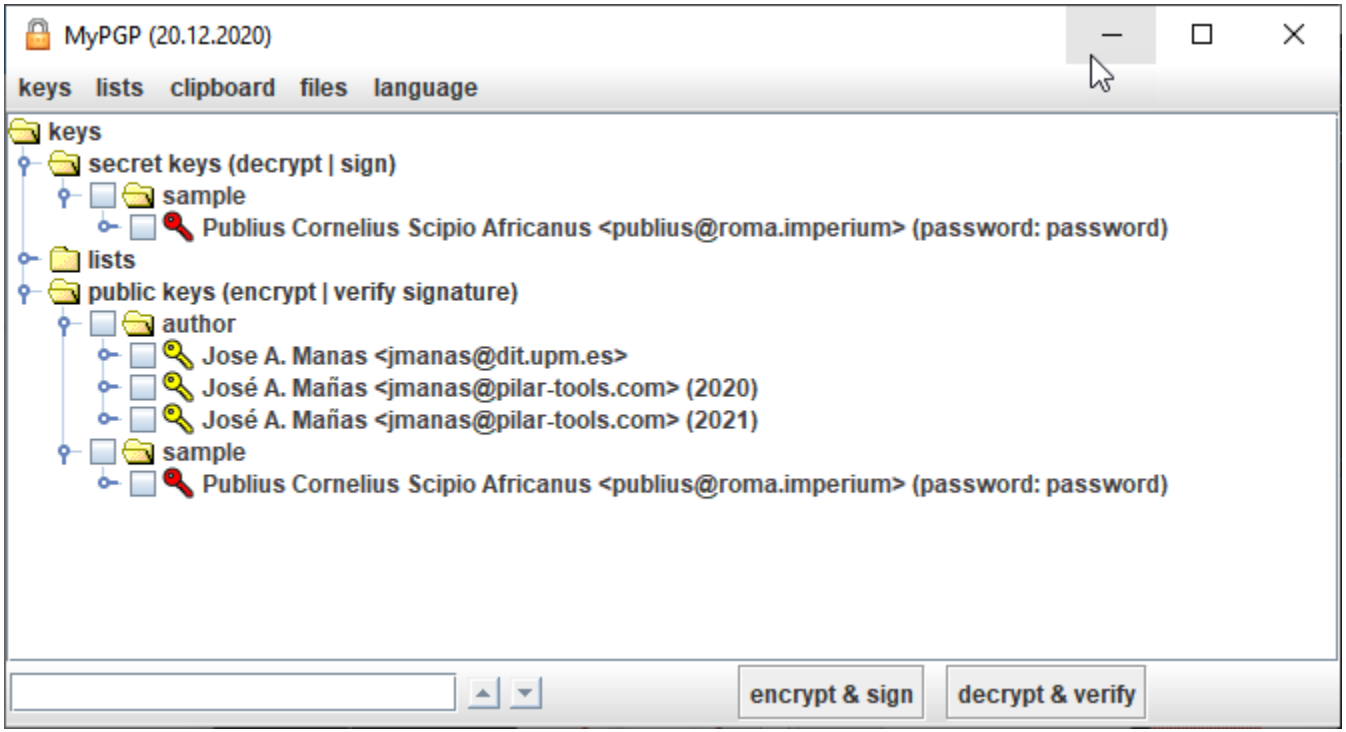
keys directory

- a directory in file system, chosen on start



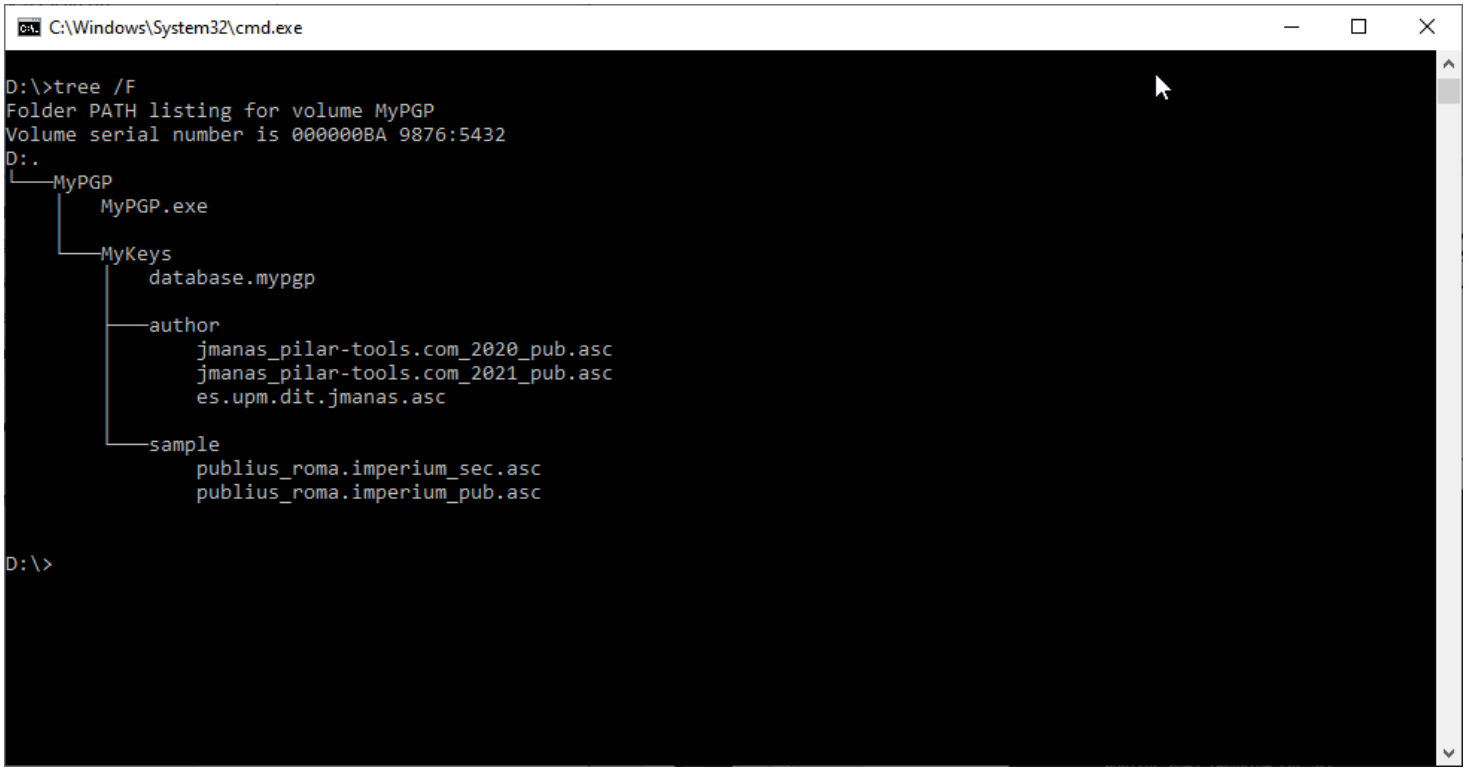
keys directory

- keys are in files
  - *_pub.asc public part
  - *_sec.asc secret part

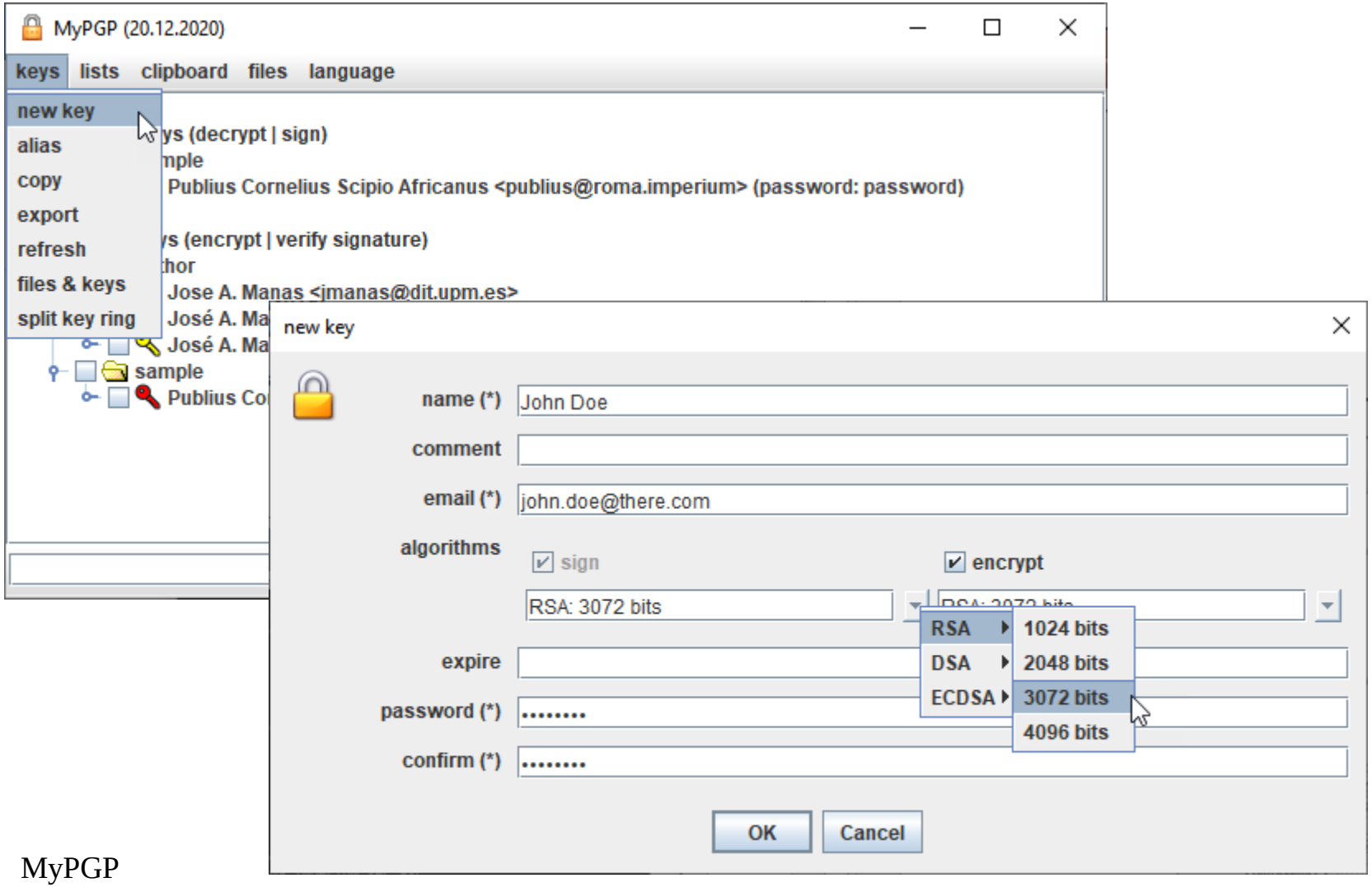


keys directory

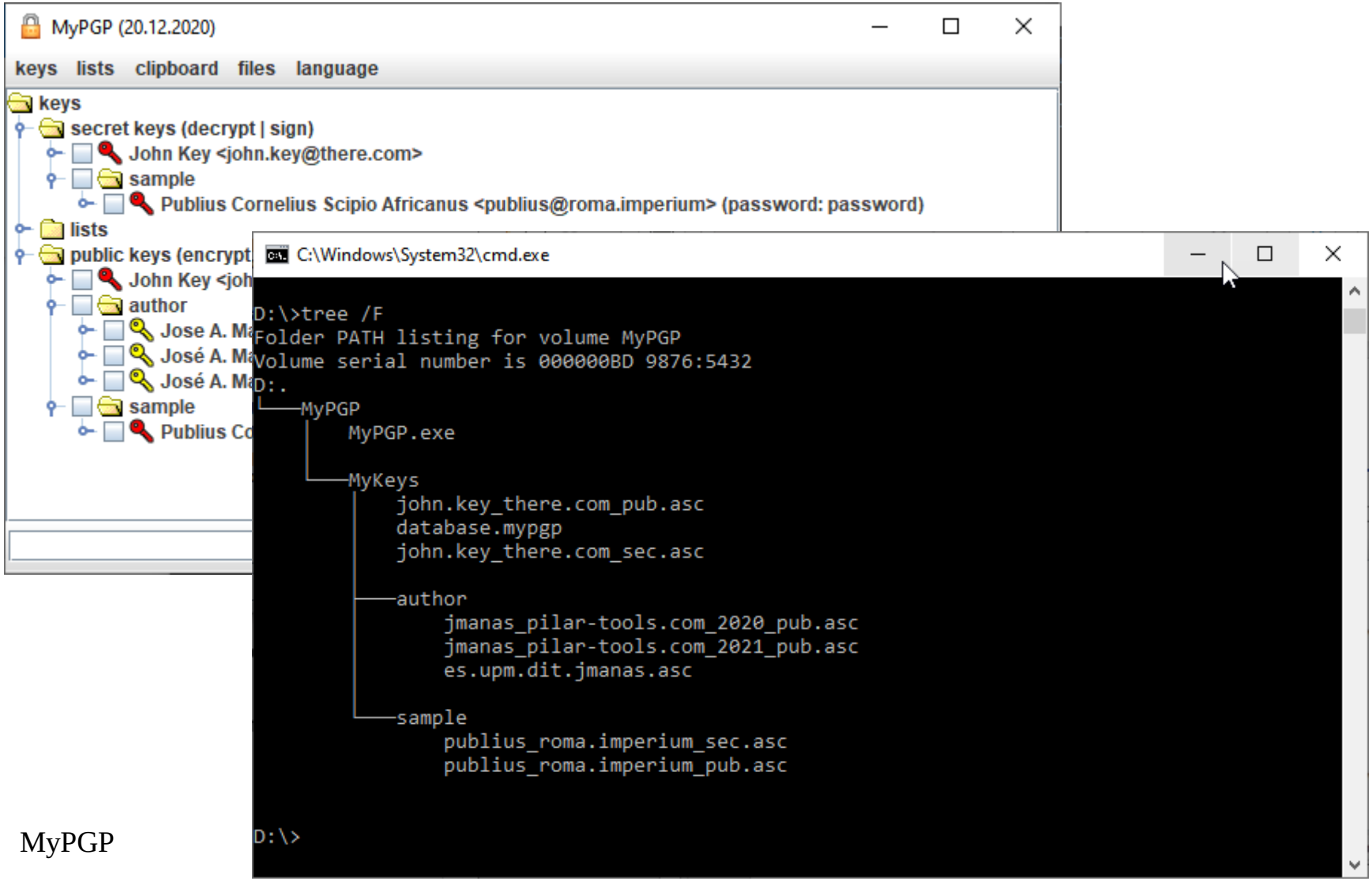
- keys are in files
  - *_pub.asc public part
  - *_sec.asc secret part



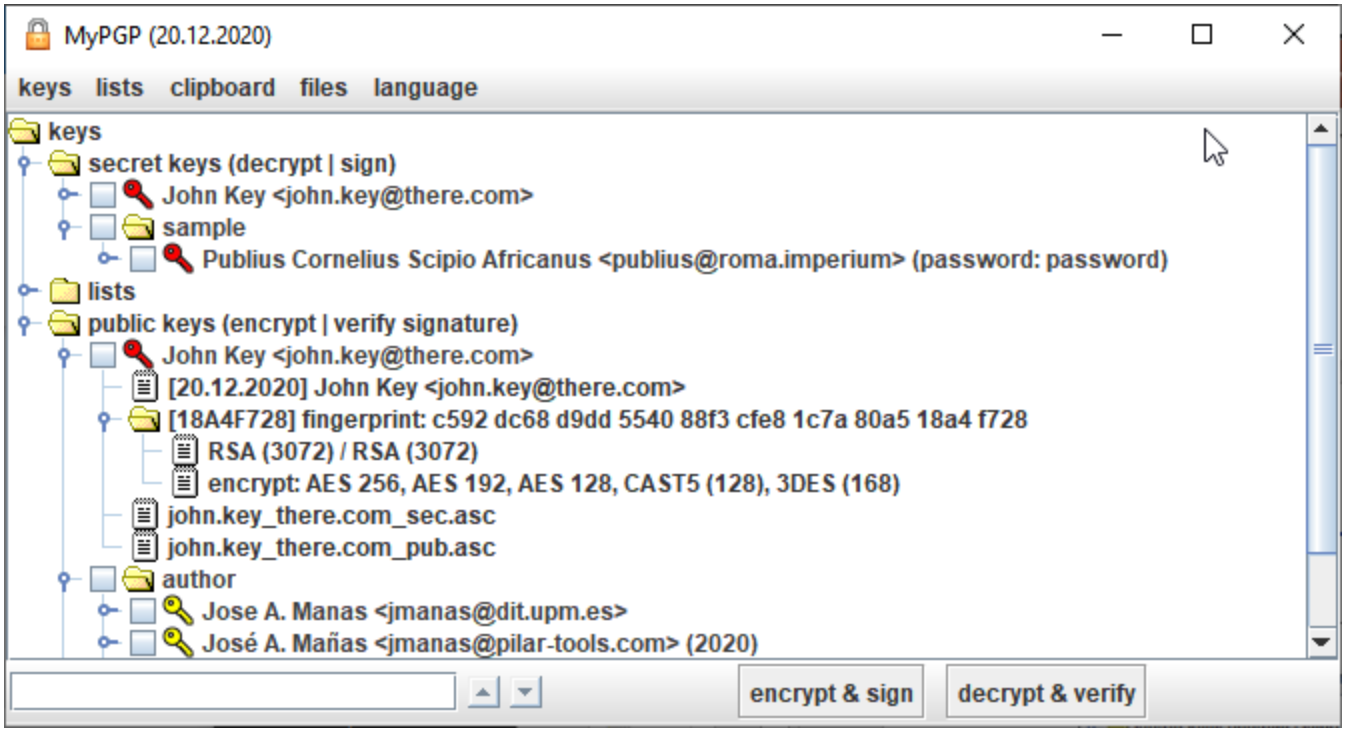
new key /1


MyPGP (20.12.2020)
keys
lists
clipboard
files
language
new key
alias
copy
export
refresh
files & keys
split key ring
ys (decrypt | sign)
nple
Publius Cornelius Scipio Africanus <publius@roma.imperium> (password: password)
ys (encrypt | verify signature)
thor
Jose A. Manas <jmanas@dit.upm.es>
José A. Ma
José A. Ma
sample
Publius Co
new key
name (*)
John Doe
comment
email (*)
john.doe@there.com
algorithms
sign
encrypt
RSA: 3072 bits
RSA
DSA
ECDSA
1024 bits
2048 bits
3072 bits
4096 bits
expire
password (*)
confirm (*)
OK
Cancel

new key /2


MyPGP (20.12.2020)
keys lists clipboard files language
keys
secret keys (decrypt | sign)
John Key <john.key@there.com>
sample
Publius Cornelius Scipio Africanus <publius@roma.imperium> (password: password)
lists
public keys (encrypt
John Key <joh
author
Jose A. Ma
José A. Ma
José A. Ma
sample
Publius Co
C:\Windows\System32\cmd.exe
D:\>tree /F
Folder PATH listing for volume MyPGP
Volume serial number is 000000BD 9876:5432
D:.
└─MyPGP
MyPGP.exe
└─MyKeys
john.key_there.com_pub.asc
database.mypgp
john.key_there.com_sec.asc
└─author
jmanas_pilar-tools.com_2020_pub.asc
jmanas_pilar-tools.com_2021_pub.asc
es.upm.dit.jmanas.asc
└─sample
publius_roma.imperium_sec.asc
publius_roma.imperium_pub.asc
D:\>

new key /3


MyPGP (20.12.2020)
keys lists clipboard files language
keys
secret keys (decrypt | sign)
John Key <john.key@there.com>
sample
Publius Cornelius Scipio Africanus <publius@roma.imperium> (password: password)
lists
public keys (encrypt | verify signature)
John Key <john.key@there.com>
[20.12.2020] John Key <john.key@there.com>
[18A4F728] fingerprint: c592 dc68 d9dd 5540 88f3 cfe8 1c7a 80a5 18a4 f728
RSA (3072) / RSA (3072)
encrypt: AES 256, AES 192, AES 128, CAST5 (128), 3DES (168)
john.key_there.com_sec.asc
john.key_there.com_pub.asc
author
Jose A. Manas <jmanas@dit.upm.es>
José A. Mañas <jmanas@pilar-tools.com> (2020)
encrypt & sign
decrypt & verify

handling

- PUB part is public; you may distribute freely
  - web site
  - email attachment
  - ... make backup copies
- SEC part shall be kept private
  - it is password protected, but keep it in a safe place
- if you lose SEC ...
  - you will not be able to decrypt
  - you will not be able to sign