

Author: Ali Yigit 4th Semester Security 2015

How to:

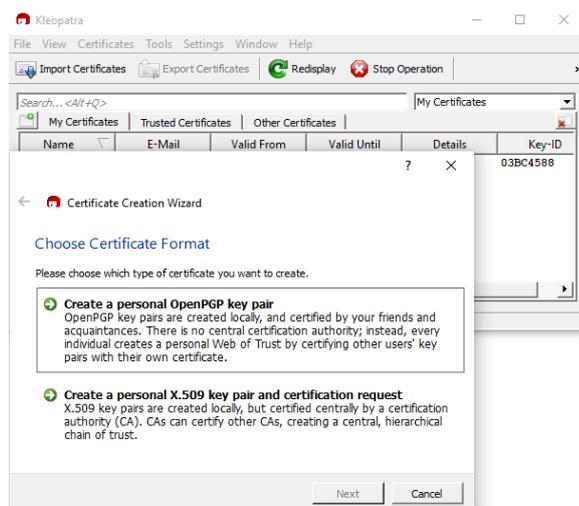
To send and receive encrypted messages you need to create a key pair, which consists of a private and public key.

To send an encrypted message, you need the recipient's public key, which is used to encrypt the message you will send. Your recipient's will then use their own private key to decrypt that message. Your recipient's can send their public key by mail as an attachment file, plain text or they can upload it to a public server from where you can download it from.

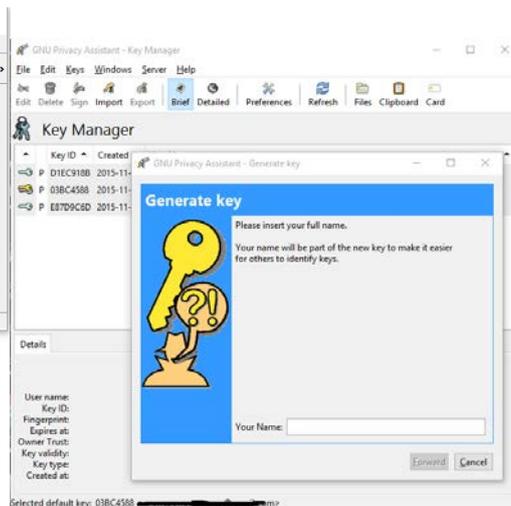
Gpg4win + thunderbird+enigmail - how to

To create a key pair you can use both Kleopatra and GPA, which is included in the Gpg4win software. You must fill in your name, email and a password when creating a new key pair.

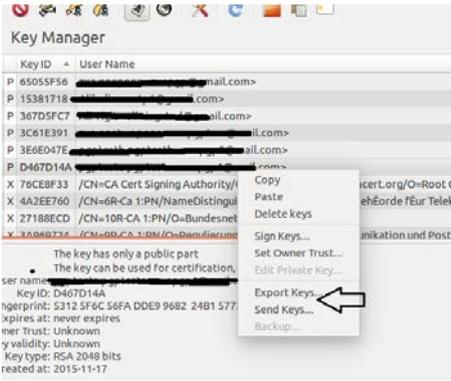
Using Kleopatra



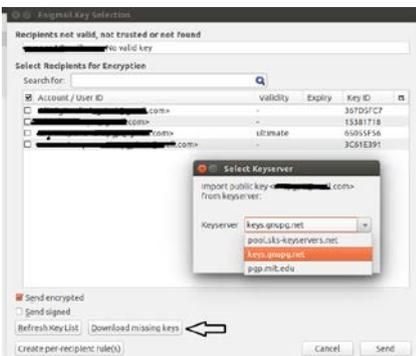
Using GPA



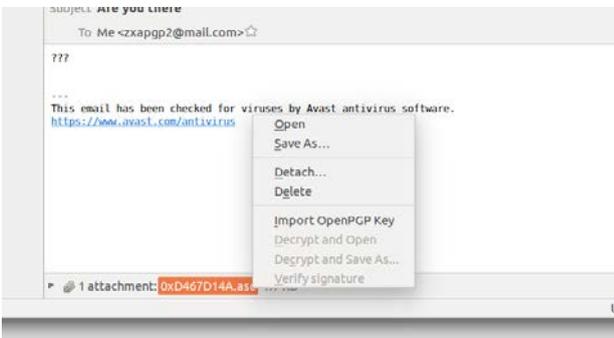
The public key can be exported to uploaded to a public server from both Kleopatra and GPA or be sent using thunderbird. Here it is shown how to do it in GPA:



To import a public key, you can do it within Thunderbird itself, or you can add it manually to your key-manager program. You can search for keys on different public servers:

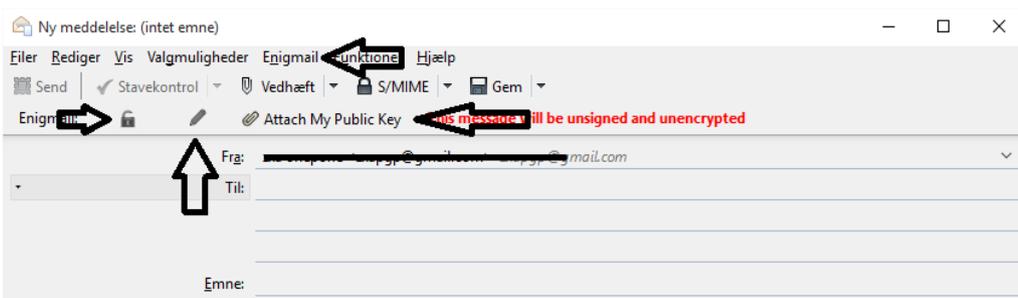


You can import the public key by right clicking on the attached file:

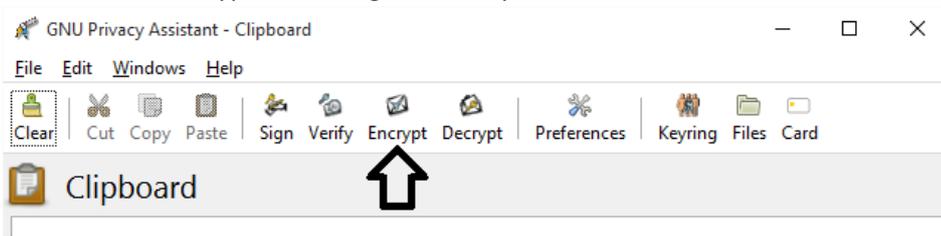


To encrypt your messages, you can use the thunderbird plugin Enigmail which is quite simple to use, or you can your key-manager programs to generate an encrypted message using the recipient's public key.

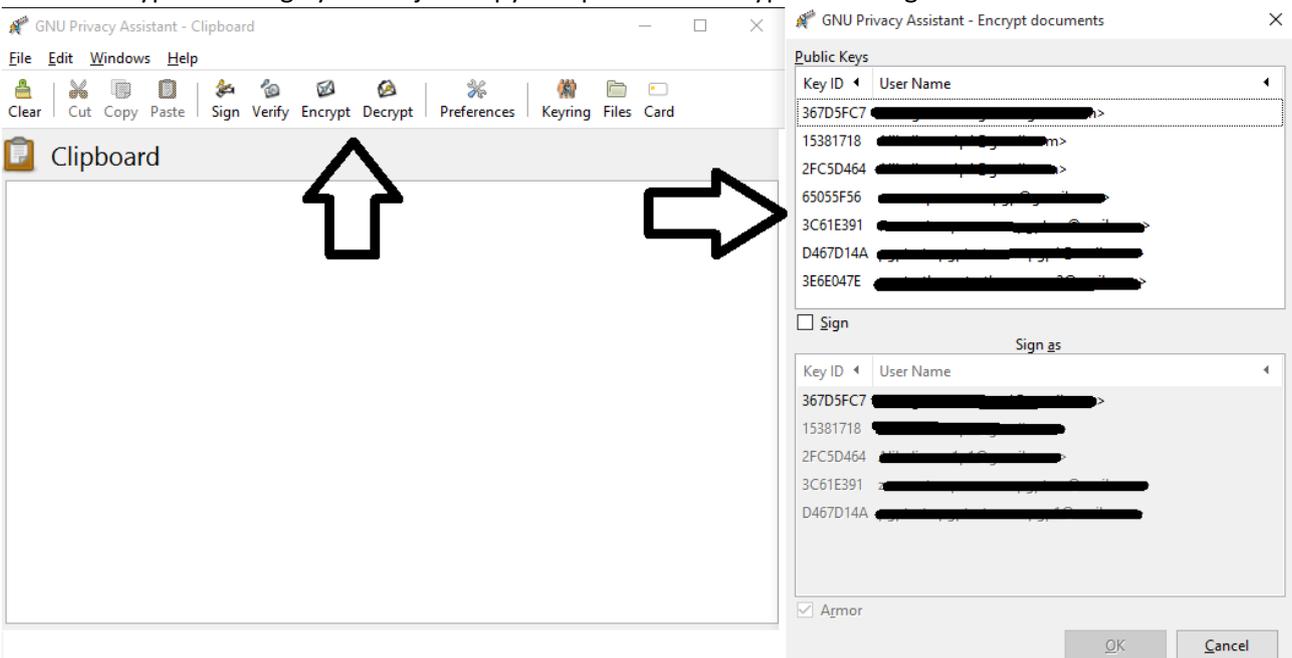
Using Thunderbird:



Or you can do your encryption inside GPA or Kleopatra. When using the gpa clipboard you will have to copy and send the encrypted message manually.



When receiving a mail, Thunderbird will automatically decrypt the messages encrypted with your public because of the addon Enigmail. You can however also decrypt and encrypt the messages inside clipboard within the GPA program: To encrypt a message click the encrypt button and select the recipient's public key and to decrypt a message you can just copy and paste the encrypted message.



Here is what a private key and a public key looks like:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

```
mQENBFZLHM4BCADAaBj5uISgxRA3ouNz5QPSJoxmn4CFwfv00ik551I0wsbd/HZU
J46EjffPhNGcPzLfhYmZgsoTmPHTthNNlDverYlX11jVDCR7Zf2uH48K4G78nzRv
WHgBYMgh5cOPKLGdz1BRyprS8E04B6vd20fvQGC1Iv4HKwvNjs3Hxv0ntuW2njz5
oYF7V356BrPerGjDVvd1ROG68SwHSK50s59ySVj+X/Y/LDP2qRx604LOhvm/YJw5
tCYw15oeL2gaNCJNB9tn71QxUON2845v0IQ5f8VVQ0K6NOjps3077Pptok9uuF10
mkj30k/8X36p3T8uiaKYPZ6b8GosVpdHgttABEBAAG0Hnp4YSBvbWVmb251IDx6
eGFwZ3BAZ21haWwuy29tPokBOQQTAgAIwUCVksCzGIBAwLCOgHAWIBBhUIAgKK
CwQWAgMBAH4BAheAAAJEhXKJf8DvEWI/h8H/06SviwrdsxGQHMU1A/nck1caF/O
X7+OQXOBb1bb9Am2AqYq/Cd0z66OLXcsHy+fr/ayGNEMi5n11NDuHi6baHNin+M4
5AS0PhK/aEczN01xEonAN/MstPFQd5jchp50tTq0RHpyuPKq39ul4shGe4k5FIKk
3tlyCdo2lsTuH9f/rhLTFKaf4HGxu4DmdBqfBMXkUkV24Wm8k2hh1YRYTwh6g1n
bMG04wJo4br9Is6uEzsf48DRhg90F/ujlapFV+jwv7nm0TwrfeeTnmbiXb9Izoy
j4lXBAHQSOsBJKP2b0k10LWn15ixj5NlOmdZ4IdSydBh6XvKqKarKTNhny5AQ0E
VksCzGIEAMkkAR9uw/qAtXBHJU2hYQ1bxy5wCY/okS4XuMMInEUPVR4kznRoKwMR
7Xk8+XvTb0S6f0NPEBRDUNG1Mi61kNuz39eIIQgbotgMXd6uk99mZaUebxEsuZSY
YJ2YtiFMeF3KXNUAAyAhsnL6iWdTHQ9iVZEOG8CgJ5jsITyY2NjvVktiKSw1Qc+z
hi092N4CGrW5z1ScbyB53C87UmURO13w0qgcZsRRW1mr4f17WhSyc6UQTVkjZ9GC
GUKDP5Yka58IBcUXck/kemCYIACjRCLsxf2q0aN0BycJcaLKO+POP0LJxiyysc0
j8lhpshAdrVieZ5iUayoLw+qoFM1SBUAEQEAAYKBHwQYAQgACQCVksCzGIBDAK
CRB15CX/A7xfImj8B/4hElwmKCOAqau9P/XtLJ5r3mG7CJkflAy2x1pRbVMOQMw
A+ycBSsaBx6mPigmZQ4DmGCLq7PB+PwnH296MFEtFhegR9fjkQDHaTsVqd6Tcmrh
NmNvsthnvY35BtFYIRtmt3gXfjCS1l8bpyu27m21Jz+gcwOehwCFUvb1TbglgBa
+KrszY4NVft17pfISLagKYC++zAfCCB0vv90DUYkj+4T3uPDj/UwyTzXFgdqQw2
3MDFNakNxyvmV9YpM5K3L1WaLohP1CtPE4PPNK2ElmKocJHA9ahidWt3nyRYN/ZA
Ot/ZRiyRXFXnEeE0b1v1jEtnt20U05Z8K9nQRg6
=M/mj
```

-----END PGP PUBLIC KEY BLOCK-----

-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: GnuPG v2

```
1Q0+BFZHPxYBCADxOoxQ9pHNM4ke7Yh7iPUYwbygHFkp1p04KQ11QETXzr3/79
03n9/7C0ID0sAz1b8A1RVCMPQcuuyU7e8ZkCcSUPLdSDnAnh2GRJ011r2Mm0wW
wSBHddgQw0S+1XFJNq6ew1TZUKT+Xaklsbs0JGVtZtztjuvAuyyE6W0F76+mZJx/ot|
3s25rVee9FUW1tQKPoVnSjB1Mz3461PsNMK4CKTjfyJwaG091aA3n2qSZK3xmw
B8ar9ttBfCv0LkGHyNeLKrYKlnxt/HBryYRHR5re5s5V0S2fztM3RglA+Ngunnr
/IxNauN4mXaEYy0V1c/RrUAf2RMh7zs477FABEBAAH+AwMC81bmp6c1NtCnhjJ
pdIEuqUE0Yyk4o11crCL1qoDK81PZFH6x10F4h4C8TppxCKUPHP1FtXhIvEtn
6H8oJoxvyIUZyBqRKLXF7yAprN5D98rYKvJJKv9TH4a0D1Ja/KpVoznanHvIqkw
URO++vDvDZKm1kNs8Mqm+TaVed6Qv0ZMsHw0J0Z14162GK5JHRCKJaRvAgT0cFt
2v9wDDCh5iQj75X0s49C/MeNTV0E+F+o5+t0uIReZrLPW0aXp4QXknP185TTPB
BUUbK0ew+aAR1F+qZQJF842pYR0PDoP1MUMmKOpIvRwb2SDR9AJQvJ06vyn9KA0ZpW
BWFg4rDRJXS0JBfUVpnrMFv+idwzJh3RItiKRfug8RxnIKQvJoxFBxQ3YeyTO
ynXariot43j0y5+DsCMtNCK7XAQIKDZQ6YJZtLggycYD1Zdf1W/YHP8isq4u7B
5fQoeF0V3GeH3OHIG1LZikxX50rZsvy7cIk/0uWJrr6mtjJTBO1S0QtB0Z51L
fX0PV+BRBRNaPgJyCyDsG/R94rvGmBpLp0L6eH+uNGW21HtI56q19s1q7idpHboJ
sDax9w1QjfbRb3TrKInzzGFP3M4LQrFy/yin0KRj1/DmBq1Z0Gaa0xZQuGJJ
JMIxMCBN4koZqC1Jg06Fw0oQ5VFnUG1EaJcWd/JrJ2m854Qmi1uLmSPX3d+80Y
ddPSGmqZyh/NOGLPxsG0vI/srbzRWNsTetEmomHZ+SFTV0FAEteZQoERkx+2gZ
jEwOXjKXn1ScMyMshhMM34Kv2CM0MgZywPjthNcMGiGh5BV3NFH20BXquxjEr
C3ay2ZwBuoTVY/T/9931pXoX0x9FDakKb+vJrJzIeJ/Jjcd3TwwvRcGBC3
0LpJtowL9Fu2IhxGVPg978Z0BPG59v+n41w0k9cIAKN91T5rXLyKjdmXkMF1Twc
HyDovhhUzI4r3Ms1A/2pgWryYiFdx8YhTYX1n8yrXX05XnJht4KNDmIgj+0sg14
OUkuMPKXbkjdiFuazphQsQEHXUop4xzRz1IppY0m8z29gWjE0ngVZuJ43yKot1
rQqxIkJozy0VtpLWN71oI31AvPbR841DS3/FTRewZ1zLhQ1kGNG3795AciZyUaZ
rXoBMFOADFtismS/b2iZ08G6e+SpAAXBU/QVoptNaEVmVWZ5tH02FP1A+m9xH
KgCN5ANyowZdGFfaQeH11wF2KsuAFjXaGeJo209ce30mFuT08/M/0/Cm8td/t
17BY11svT7USwa09eHwF2+S8K0dPz2A6w7a+0S8Wd0hDX8CfVdmeW+Aza2A5xJ
ukt2T0GhImId1kTsJwJeaG6nz5bB9dYuknEN0dWahzRvGaaAz200c1v1Zw1id
yJznx01Z/WX+eskMRH56MAtVN/kPnt9LSVKqT18Fv5d58rA2cXDCMQbVyomB90n
ZxDwAYe44IjwUDyY1ztePswq1UWchtHakQvGK4M3GuqE13606T8YyhjqkTSzq
tYvBfvaedd064k8BwQYAQgACQCVkc/FgIbDAAKCRA6B701FTgXGMACADP4G1W
FhxXXzbaX+6ccI41a6tFGC1u8rHg6tSN8PU1oZMj4c+KFI5ZFOtQZyVPGI21WFN
Mzknr108rJA8u6ZK/rLbbK10hN0MteVmpUsEmGhhg0hVlr+FYETdmtcL3T39mVCo
SENQ6GX3+00a17JDL74E1V1hWjBKe55H1A1Z29cYxyvzyRsrXkVYdbCVp+dp
0p7s1nNs5eG0H10hCbEouJ563+M3AZYhTa+83165HAP0828zviwweC+Huh1906d
66u81kL0jU75Q05e5Wi4hGpg0RbPU+4KBUhVXwZ85oEuhsRuyG1CXZ/7winzy4
szKALKJ9P+7I/z0M
=xjP+
```

-----END PGP PRIVATE KEY BLOCK-----