

Ex 9 – PGP - GPG4Win

Public-Private Key Generation and Backup:

GNU Privacy Assistant - Generate key

Generate key




Please insert your full name.

Your name will be part of the new key to make it easier for others to identify keys.

Your Name:

GNU Privacy Assistant - Generate key

Generate key

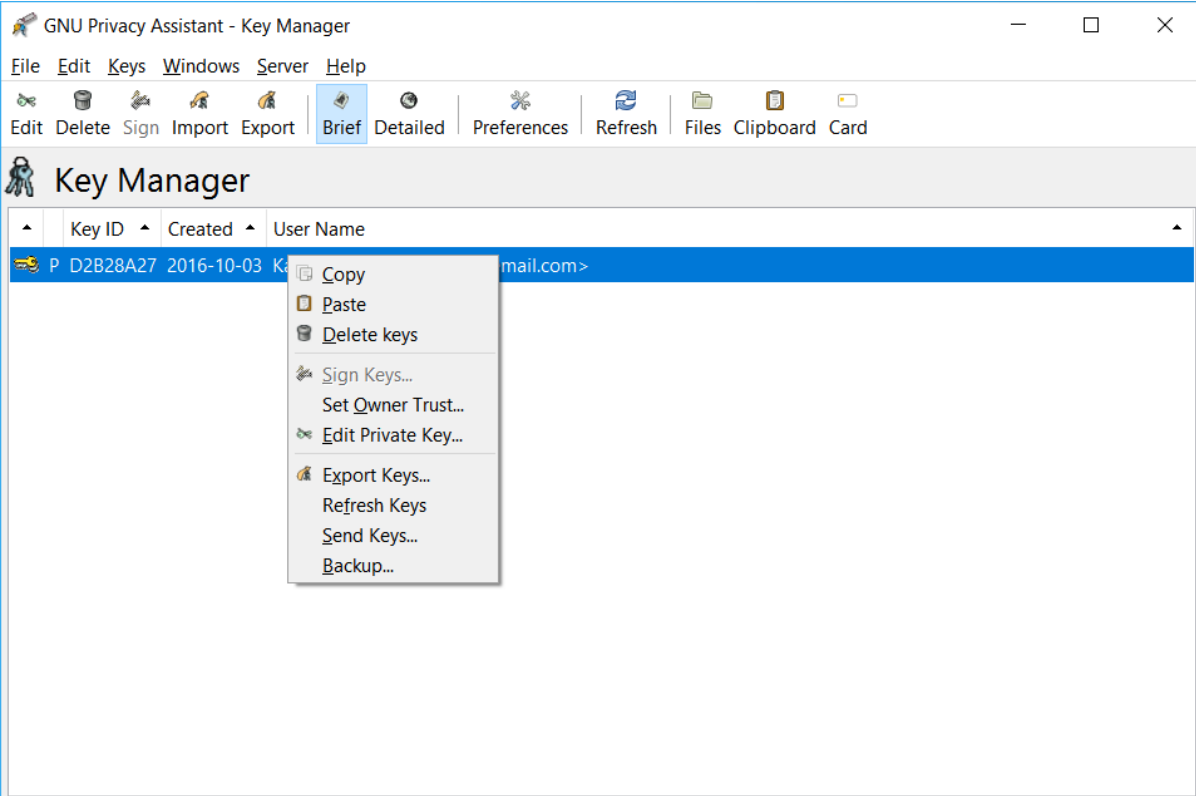


Please insert your email address.

Your email address will be part of the new key to make it easier for others to identify keys. If you have several email addresses, you can add further email addresses later.

Your Email Address:

Distributing Public Key using [hkp://keys.gnupg.net](http://keys.gnupg.net) Public Key server:



GNU Privacy Assistant - Key Manager

File Edit Keys Windows Server Help

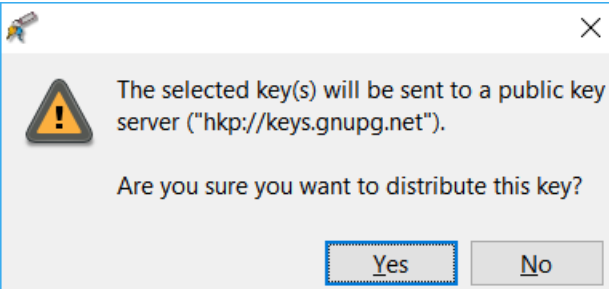
Edit Delete Sign Import Export Brief Detailed Preferences Refresh Files Clipboard Card


Key Manager

Key ID	Created	User Name
P D2B28A27	2016-10-03	KarthikMAM <karthik@fakemail.com>

The key has both a private and a public part
The key can be used for certification, signing and encryption.
User name: KarthikMAM <karthik@fakemail.com>
Key ID: D2B28A27
Fingerprint: 8299 8C7F A92B 7244 2098 A51D 985A FECE D2B2 8A27
Expires at: never expires
Owner Trust: Ultimate
Key validity: Fully Valid
Key type: RSA 2048 bits
Created at: 2016-10-03

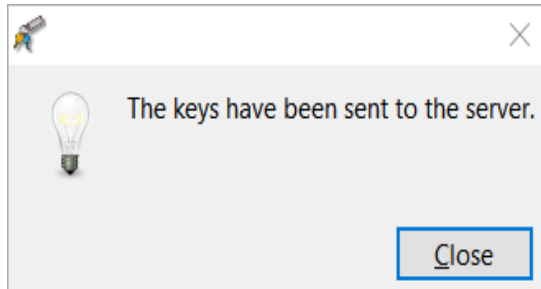
Selected default key: D2B28A27 KarthikMAM <karthik@fakemail.com>




 The selected key(s) will be sent to a public key server ("[hkp://keys.gnupg.net](http://keys.gnupg.net)").

Are you sure you want to distribute this key?

Yes No



 The keys have been sent to the server.

Close

Retrieve keys from the server:

gpa.exe

Which key do you want to import? (The key must be specified by key ID).

Key ID:



1 public keys read
1 public keys imported
0 public keys unchanged
0 secret keys read
0 secret keys imported
0 secret keys unchanged

GNU Privacy Assistant - Key Manager

File Edit Keys Windows Server Help

Edit Delete Sign Import Export Brief Detailed Preferences Refresh Files Clipboard Card

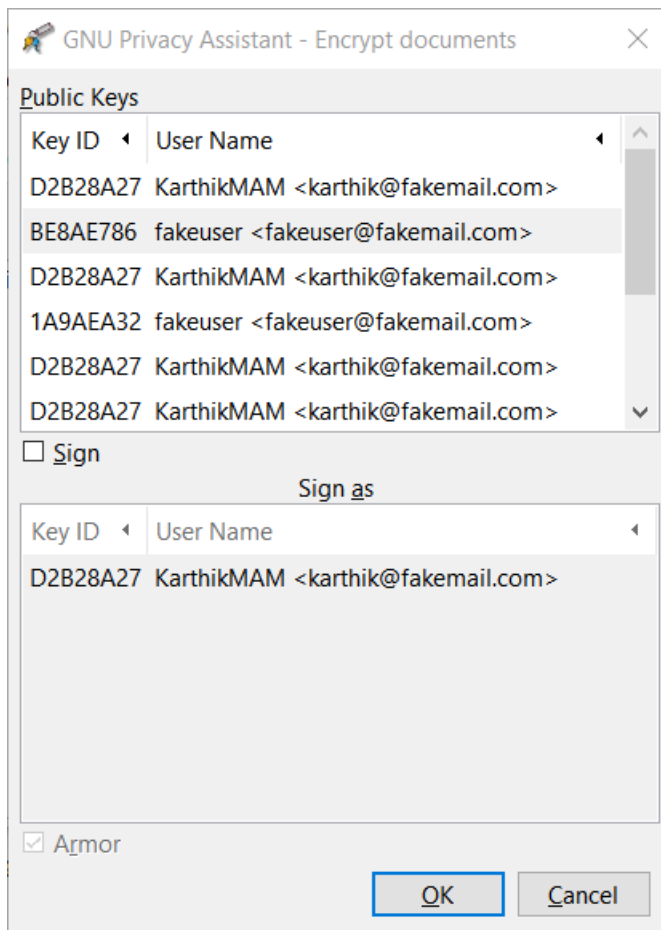
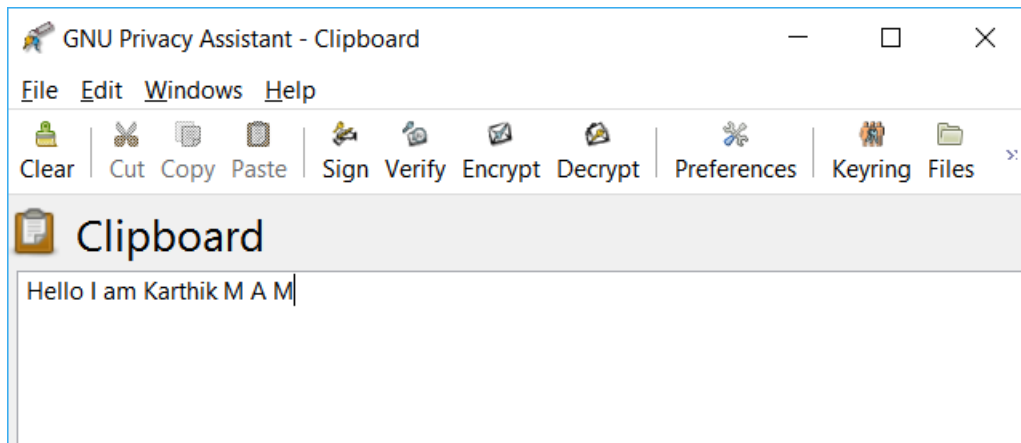
Key Manager

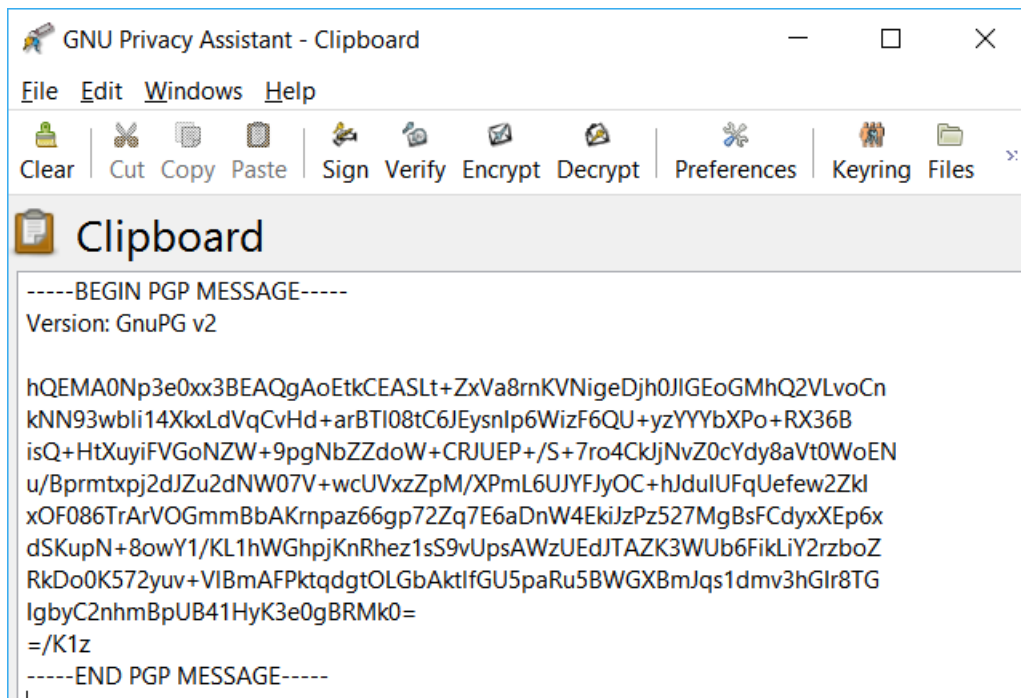
	Key ID	Created	User Name
 P	D2B28A27	2016-10-03	KarthikMAM <karthik@fakemail.com>
 P	1A9AEA32	2016-10-03	fakeuser <fakeuser@fakemail.com>

The key has both a private and a public part
The key can be used for certification, signing and encryption.
User name: fakeuser <fakeuser@fakemail.com>
Key ID: 1A9AEA32
Fingerprint: 8D59 24B4 AE6C B4D3 DB6D FD9F 0C9C 9913 1A9A EA32
Expires at: never expires
Owner Trust: Unknown
Key validity: Unknown
Key type: RSA 2048 bits
Created at: 2016-10-03

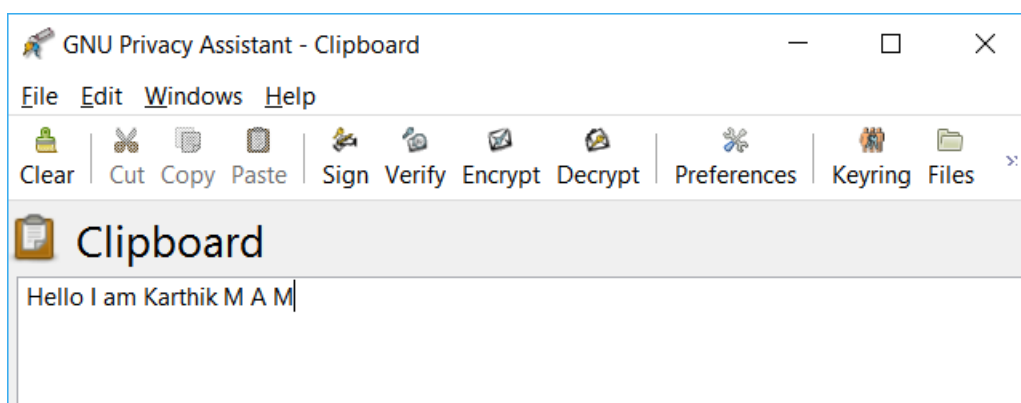
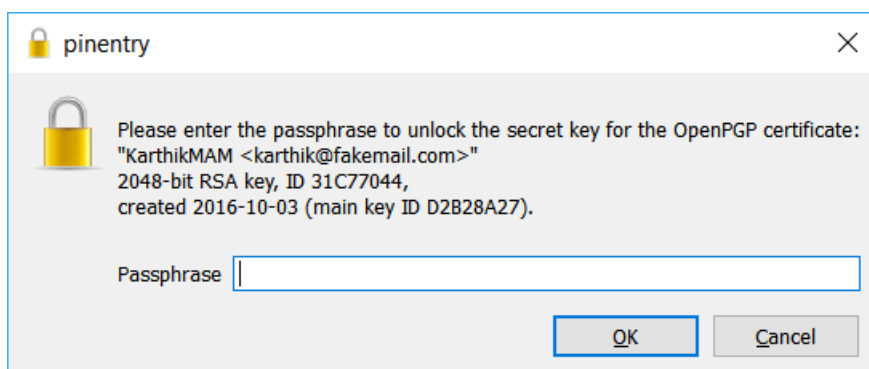
Selected default key: D2B28A27 KarthikMAM <karthik@fakemail.com>

Encrypting at Sender side:





Decrypting at receiver side:



Result:

The GPA tool was used to

- Create public – private key pair
- Share and retrieve public keys
- Encrypt and decrypt using them.