EQUIFAX

Equifax Managed File Transfer

Key Creation TIF

OpenPGP Key Creation Technical Information Form

Equifax Midtown Office in Atlanta

Author:
Change Authority: EFX Data Protection/NIST
Change Forecast: As needed per NIST Standards

This document will be kept under revision control.

Change History

Version No.	Issue Date	Status	Reason for Change
4880.1	2023-02-24	Submitted	Initial Release

Reviewer History

Reviewer's Details	Version No.	Date
Nick Fuller	4880.1	2023-02-24
Ben Hale	4880.1	2023-02-27

Introduction

Purpose

The purpose of this document is to inform external business partners on how to properly create OpenPGP keys to adequately secure sensitive data that is to be exchanged with Equifax. This Technical Information Form (TIF) should serve as a point of reference for official key creation/rotation documentation that Equifax would leverage for secure data exchange. As cryptography standards are updated, this document is subject to change to align with industry best practices.

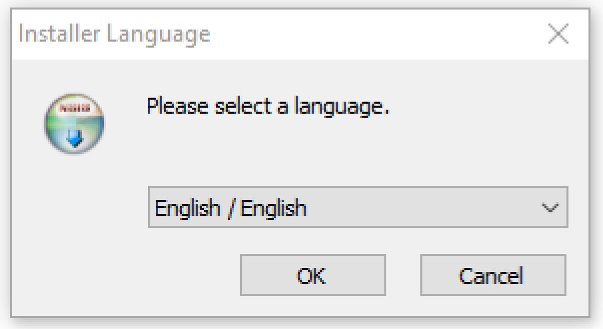
Objectives & Scope

The objective of this document is to enhance the data security levels according to the latest industry standards . To ensure PGP keys are compatible with Equifax services, client PGP keys need to be equipped with certain elements such as key validity, sub-key validity, streamlining the ciphers, etc.

The scope of this document is to demonstrate how to set up PGP keys locally with all the necessary features so they meet industry best practices as well as Equifax services. The steps documented below include the generation of a PGP key with all the required elements, removal of unnecessary elements, validating the final key meets requirements, and export key to send to Equifax.

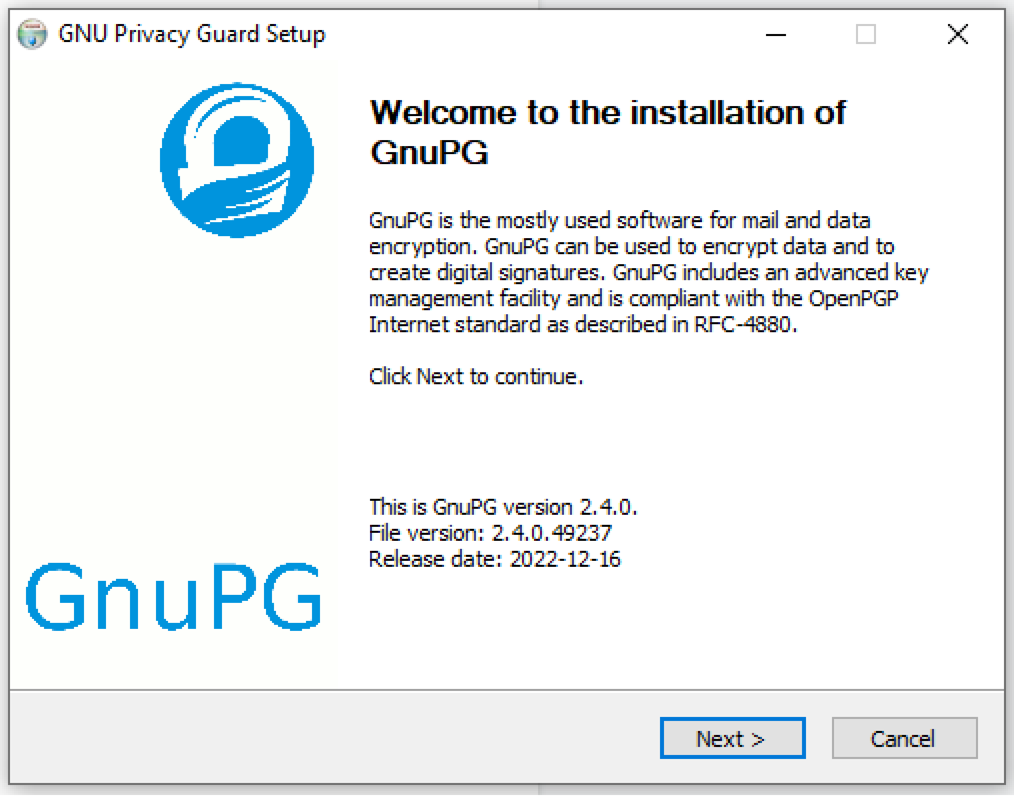
Recommended GPG Tools

- gpg (GnuPG) 2.3.8
  libgcrypt 1.10.1
  Copyright (C) 2021 Free Software Foundation, Inc.
- https://gnupg.org/ for latest releases (GnuPG version 2.4.0 is latest as of Dec 2022)
- Before you perform the steps below you need the GnuPG command line tool. Normally you don't need administrator permissions to install the GnuPG tool. If required administrator permissions you need to check with your system administrator.
- Browse into https://gnupg.org/download/index.html and download the latest version of gnupg-w32-2.4.0_20221216.exe file. Install the .exe file.
- Installation steps:



Please select a language.

English / English

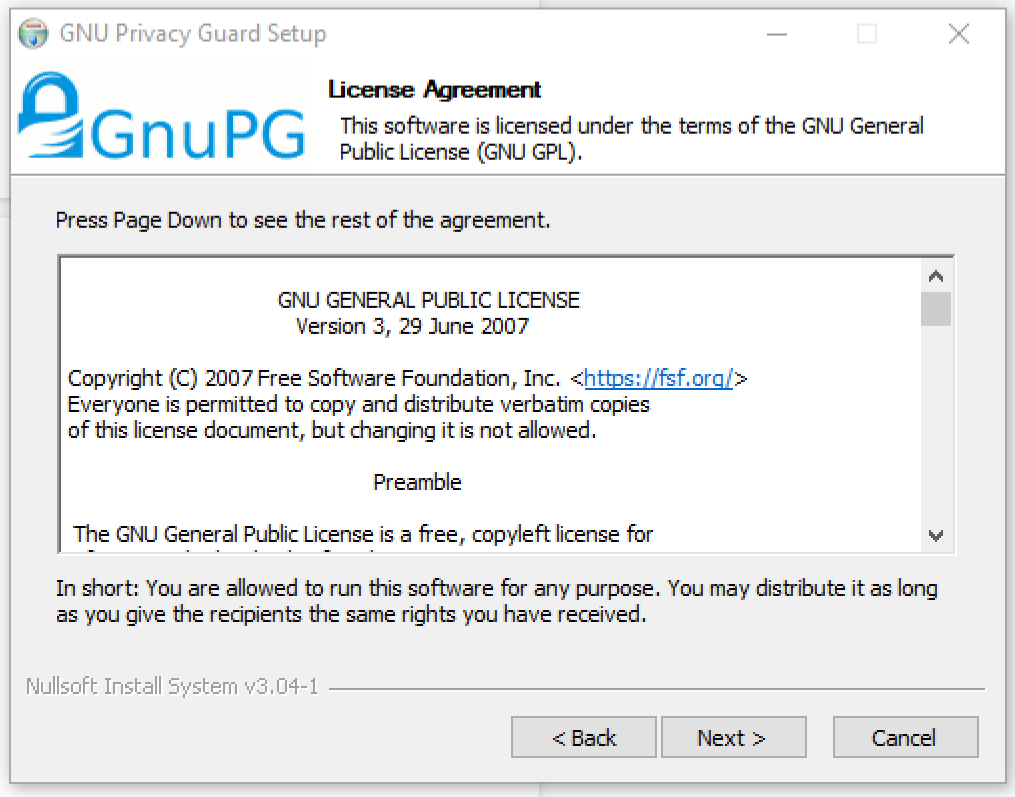


Welcome to the installation of GnuPG

GnuPG is the mostly used software for mail and data encryption. GnuPG can be used to encrypt data and to create digital signatures. GnuPG includes an advanced key management facility and is compliant with the OpenPGP Internet standard as described in RFC-4880.

Click Next to continue.

This is GnuPG version 2.4.0.
File version: 2.4.0.49237
Release date: 2022-12-16



License Agreement

This software is licensed under the terms of the GNU General Public License (GNU GPL).

Press Page Down to see the rest of the agreement.

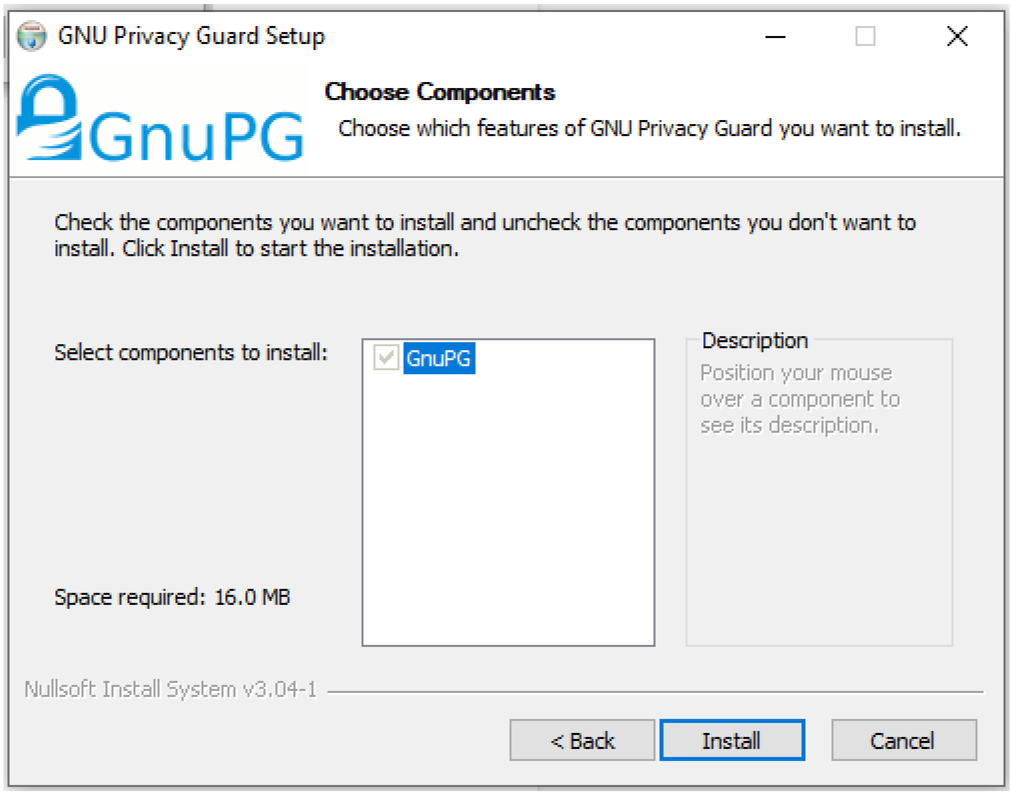
GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <https://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for

In short: You are allowed to run this software for any purpose. You may distribute it as long as you give the recipients the same rights you have received.



Choose Components

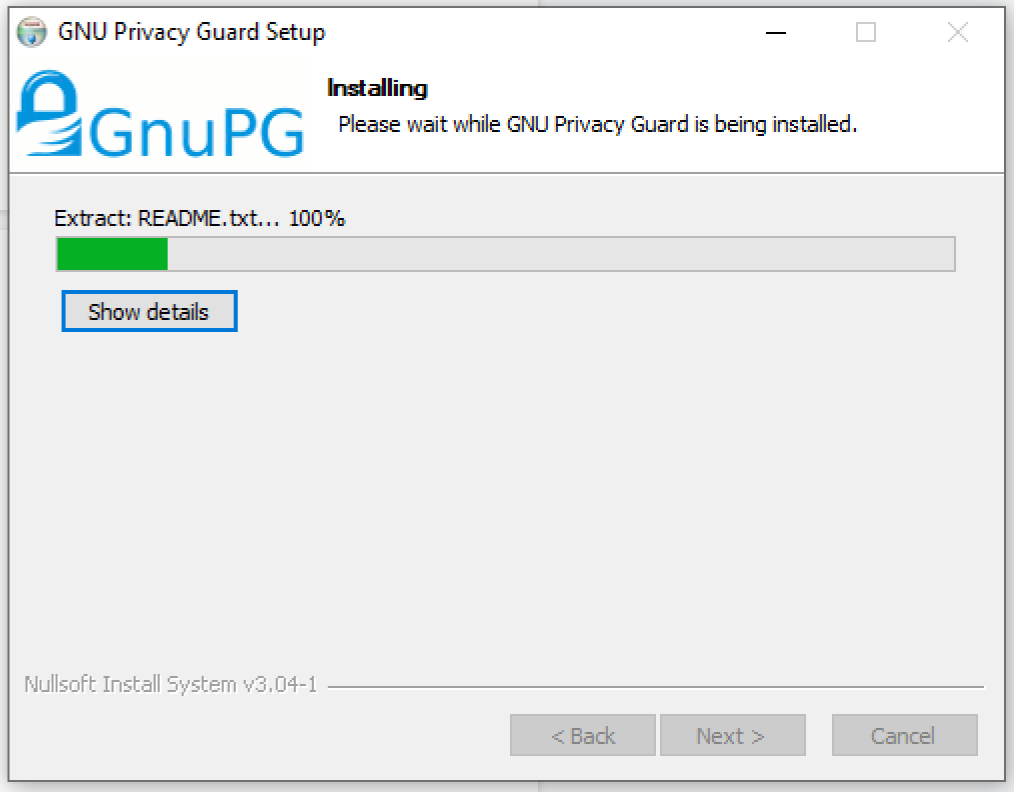
Choose which features of GNU Privacy Guard you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Install to start the installation.

Select components to install: ☑ GnuPG

Space required: 16.0 MB

Description
Position your mouse over a component to see its description.

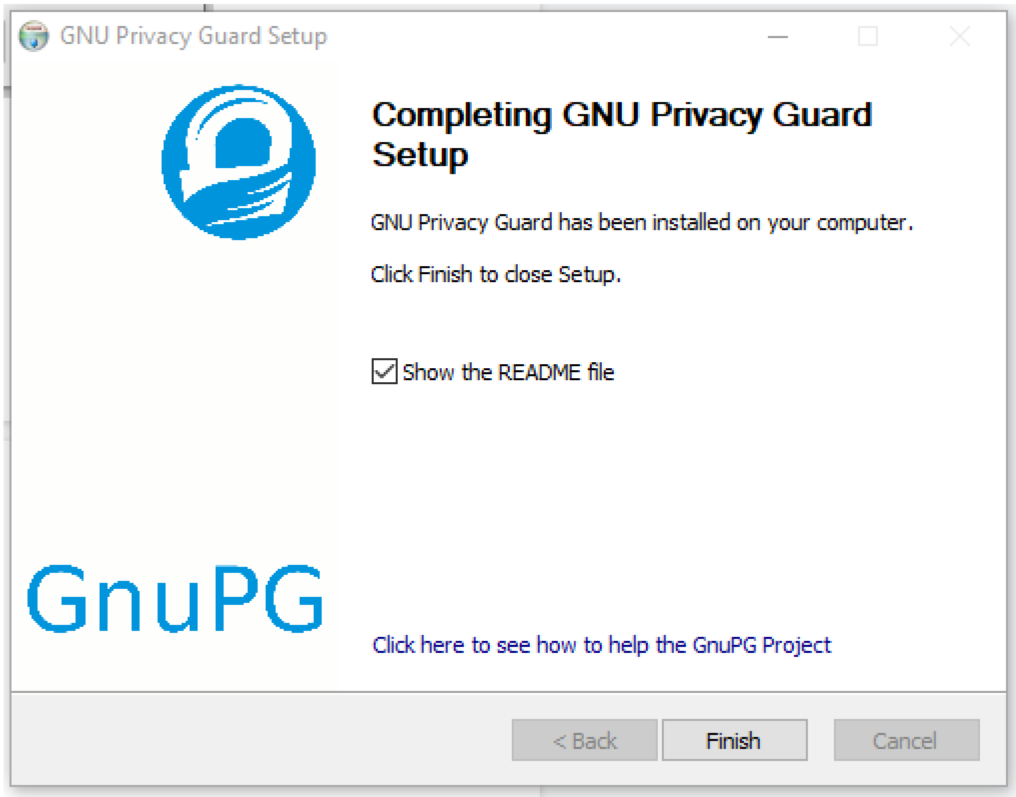


GNU Privacy Guard Setup

Installing

Please wait while GNU Privacy Guard is being installed.

Extract: README.txt... 100%



GNU Privacy Guard Setup

Completing GNU Privacy Guard Setup

GNU Privacy Guard has been installed on your computer.

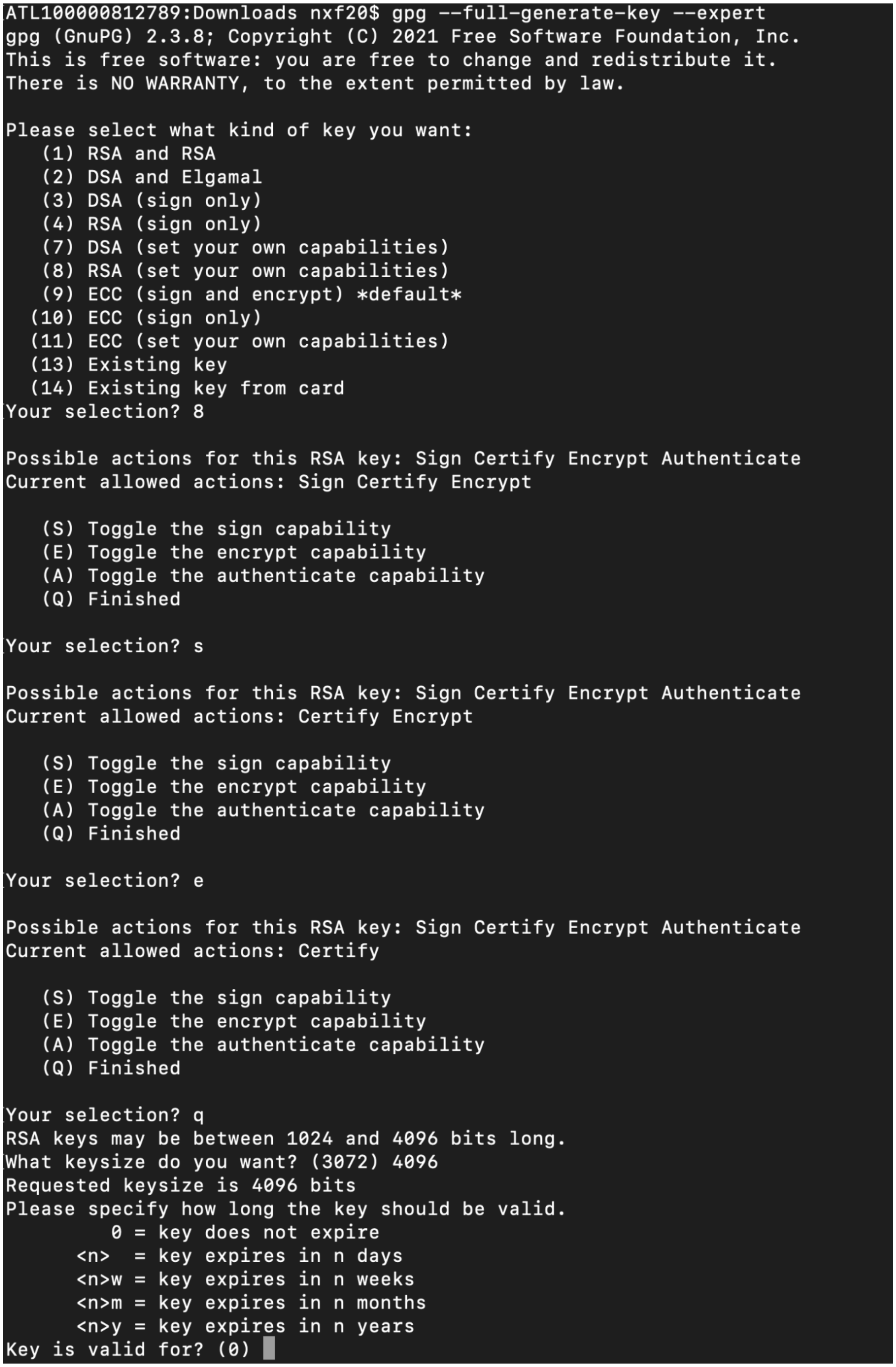
Click Finish to close Setup.

☑ Show the README file

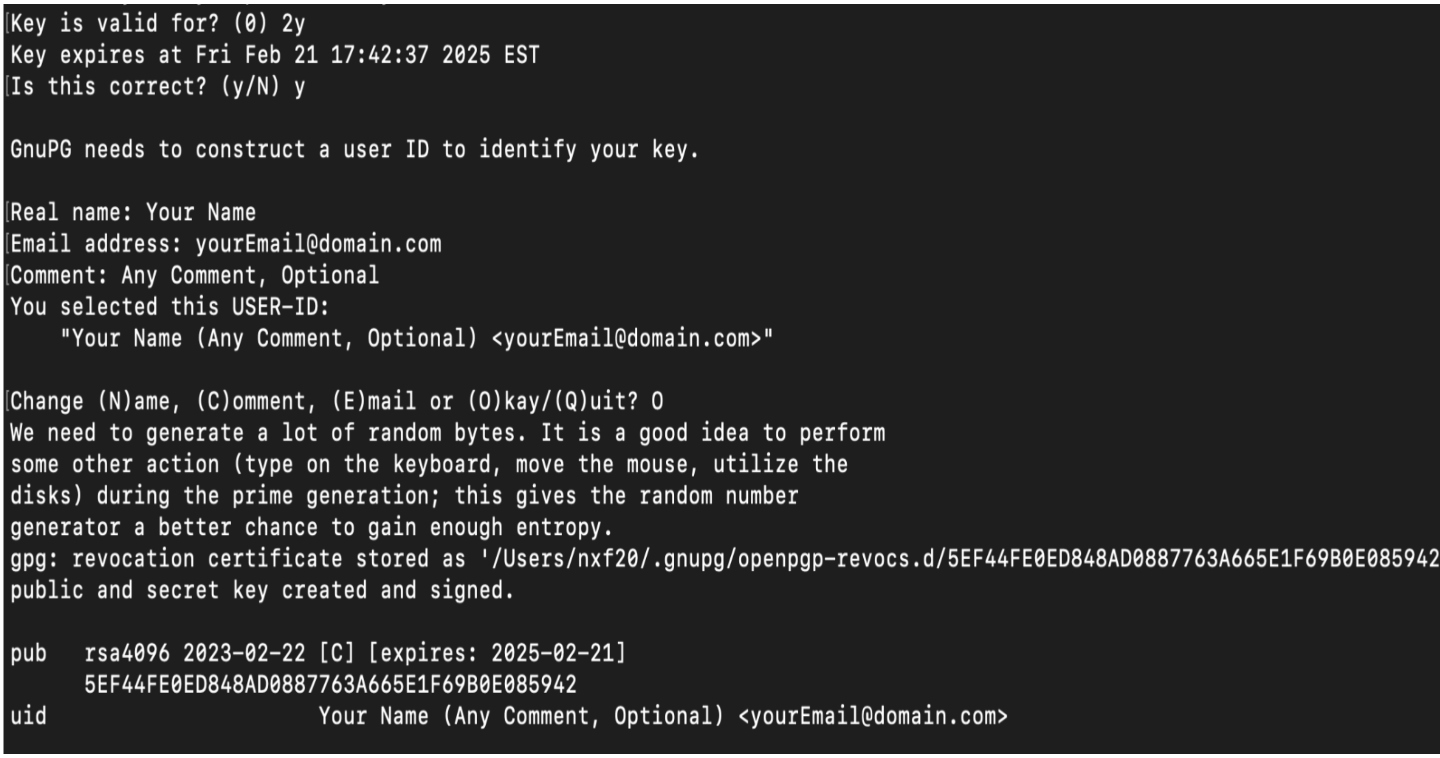
Click here to see how to help the GnuPG Project

After installation you need to go to the CMD (command line) and go to the GnuPG installation directory. Example: C:\XXX\XXXX\GnuPG\bin

Set Capabilities

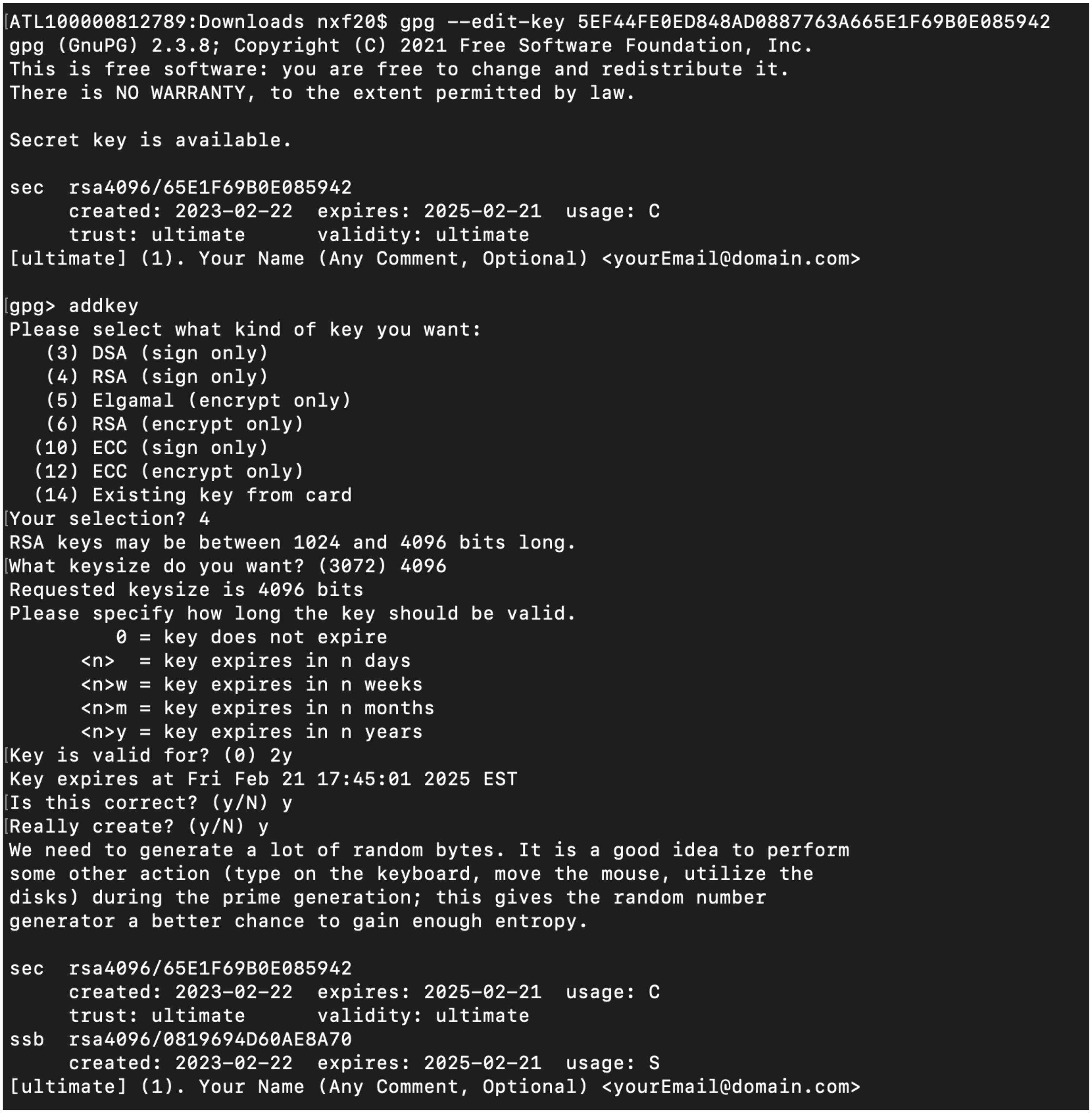


```
ATL100000812789:Downloads nxf20$ gpg --full-generate-key --expert
gpg (GnuPG) 2.3.8; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
   (7) DSA (set your own capabilities)
   (8) RSA (set your own capabilities)
   (9) ECC (sign and encrypt) *default*
  (10) ECC (sign only)
  (11) ECC (set your own capabilities)
  (13) Existing key
  (14) Existing key from card
Your selection? 8

Possible actions for this RSA key: Sign Certify Encrypt Authenticate
Current allowed actions: Sign Certify Encrypt

   (S) Toggle the sign capability
   (E) Toggle the encrypt capability
   (A) Toggle the authenticate capability
   (Q) Finished

Your selection? s

Possible actions for this RSA key: Sign Certify Encrypt Authenticate
Current allowed actions: Certify Encrypt

   (S) Toggle the sign capability
   (E) Toggle the encrypt capability
   (A) Toggle the authenticate capability
   (Q) Finished

Your selection? e

Possible actions for this RSA key: Sign Certify Encrypt Authenticate
Current allowed actions: Certify

   (S) Toggle the sign capability
   (E) Toggle the encrypt capability
   (A) Toggle the authenticate capability
   (Q) Finished

Your selection? q
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072) 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)
```



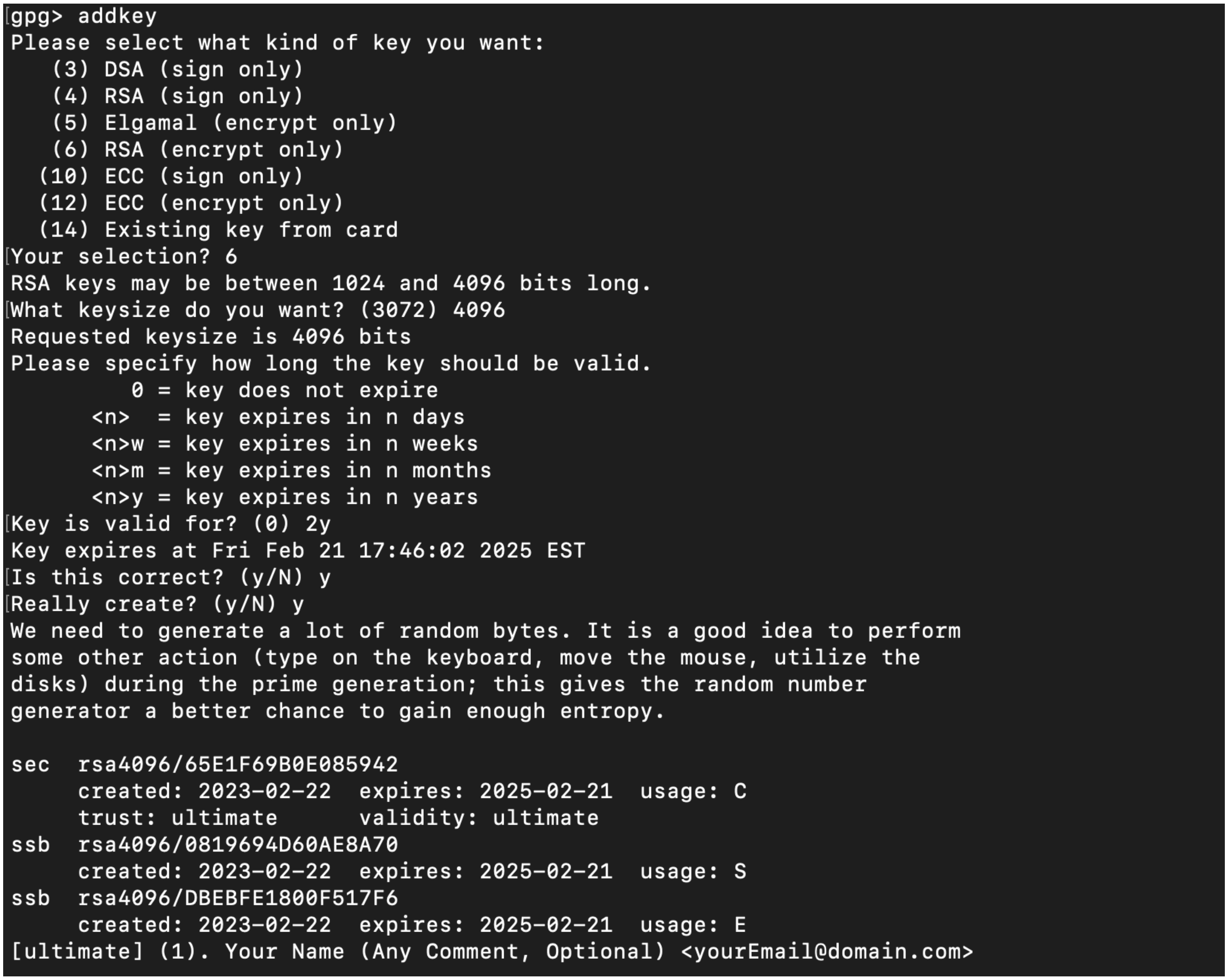
```
[Key is valid for? (0) 2y
 Key expires at Fri Feb 21 17:42:37 2025 EST
[Is this correct? (y/N) y

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

[Real name: Your Name
[Email address: yourEmail@domain.com
[Comment: Any Comment, Optional
 You selected this USER-ID:
     "Your Name (Any Comment, Optional) <yourEmail@domain.com>"

[Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
 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: revocation certificate stored as '/Users/nxf20/.gnupg/openpgp-revocs.d/5EF44FE0ED848AD0887763A665E1F69B0E085942
 public and secret key created and signed.

 pub   rsa4096 2023-02-22 [C] [expires: 2025-02-21]
       5EF44FE0ED848AD0887763A665E1F69B0E085942
 uid                      Your Name (Any Comment, Optional) <yourEmail@domain.com>
```

Sign Only (Optional)



```
[ATL100000812789:Downloads nxf20$ gpg --edit-key 5EF44FE0ED848AD0887763A665E1F69B0E085942
gpg (GnuPG) 2.3.8; Copyright (C) 2021 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.

Secret key is available.

sec  rsa4096/65E1F69B0E085942
     created: 2023-02-22  expires: 2025-02-21  usage: C
     trust: ultimate      validity: ultimate
[ultimate] (1). Your Name (Any Comment, Optional) <yourEmail@domain.com>

[gpg> addkey
Please select what kind of key you want:
   (3) DSA (sign only)
   (4) RSA (sign only)
   (5) Elgamal (encrypt only)
   (6) RSA (encrypt only)
  (10) ECC (sign only)
  (12) ECC (encrypt only)
  (14) Existing key from card
[Your selection? 4
RSA keys may be between 1024 and 4096 bits long.
[What keysize do you want? (3072) 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) 2y
Key expires at Fri Feb 21 17:45:01 2025 EST
[Is this correct? (y/N) y
[Really create? (y/N) y
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.

sec  rsa4096/65E1F69B0E085942
     created: 2023-02-22  expires: 2025-02-21  usage: C
     trust: ultimate      validity: ultimate
ssb  rsa4096/0819694D60AE8A70
     created: 2023-02-22  expires: 2025-02-21  usage: S
[ultimate] (1). Your Name (Any Comment, Optional) <yourEmail@domain.com>
```

Encrypt Only

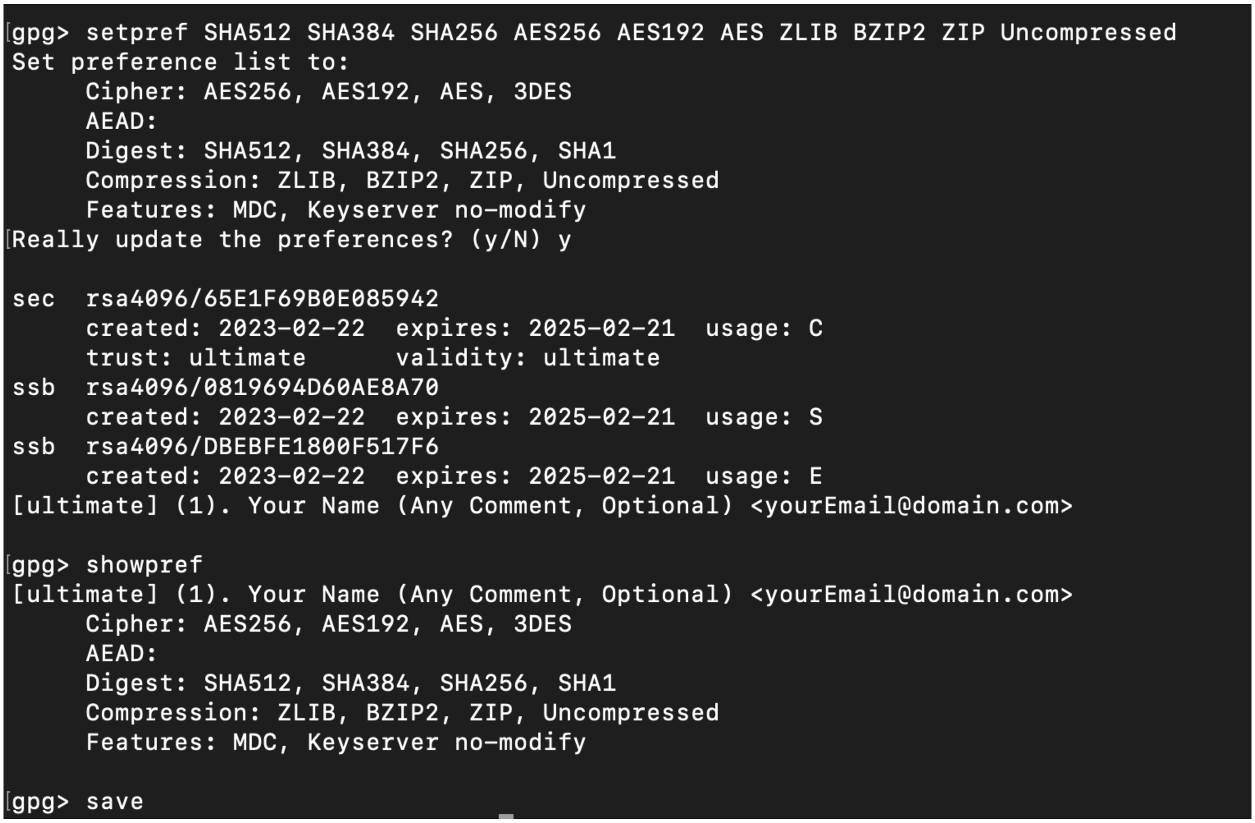


```
[gpg> addkey
Please select what kind of key you want:
   (3) DSA (sign only)
   (4) RSA (sign only)
   (5) Elgamal (encrypt only)
   (6) RSA (encrypt only)
  (10) ECC (sign only)
  (12) ECC (encrypt only)
  (14) Existing key from card
[Your selection? 6
RSA keys may be between 1024 and 4096 bits long.
[What keysize do you want? (3072) 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) 2y
Key expires at Fri Feb 21 17:46:02 2025 EST
[Is this correct? (y/N) y
[Really create? (y/N) y
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.

sec  rsa4096/65E1F69B0E085942
     created: 2023-02-22  expires: 2025-02-21  usage: C
     trust: ultimate      validity: ultimate
ssb  rsa4096/0819694D60AE8A70
     created: 2023-02-22  expires: 2025-02-21  usage: S
ssb  rsa4096/DBEBFE1800F517F6
     created: 2023-02-22  expires: 2025-02-21  usage: E
[ultimate] (1). Your Name (Any Comment, Optional) <yourEmail@domain.com>
```

Key Preferences

- Prerequisite step is to run:

  gpg –edit-keys <KEYID of YOURKEY>

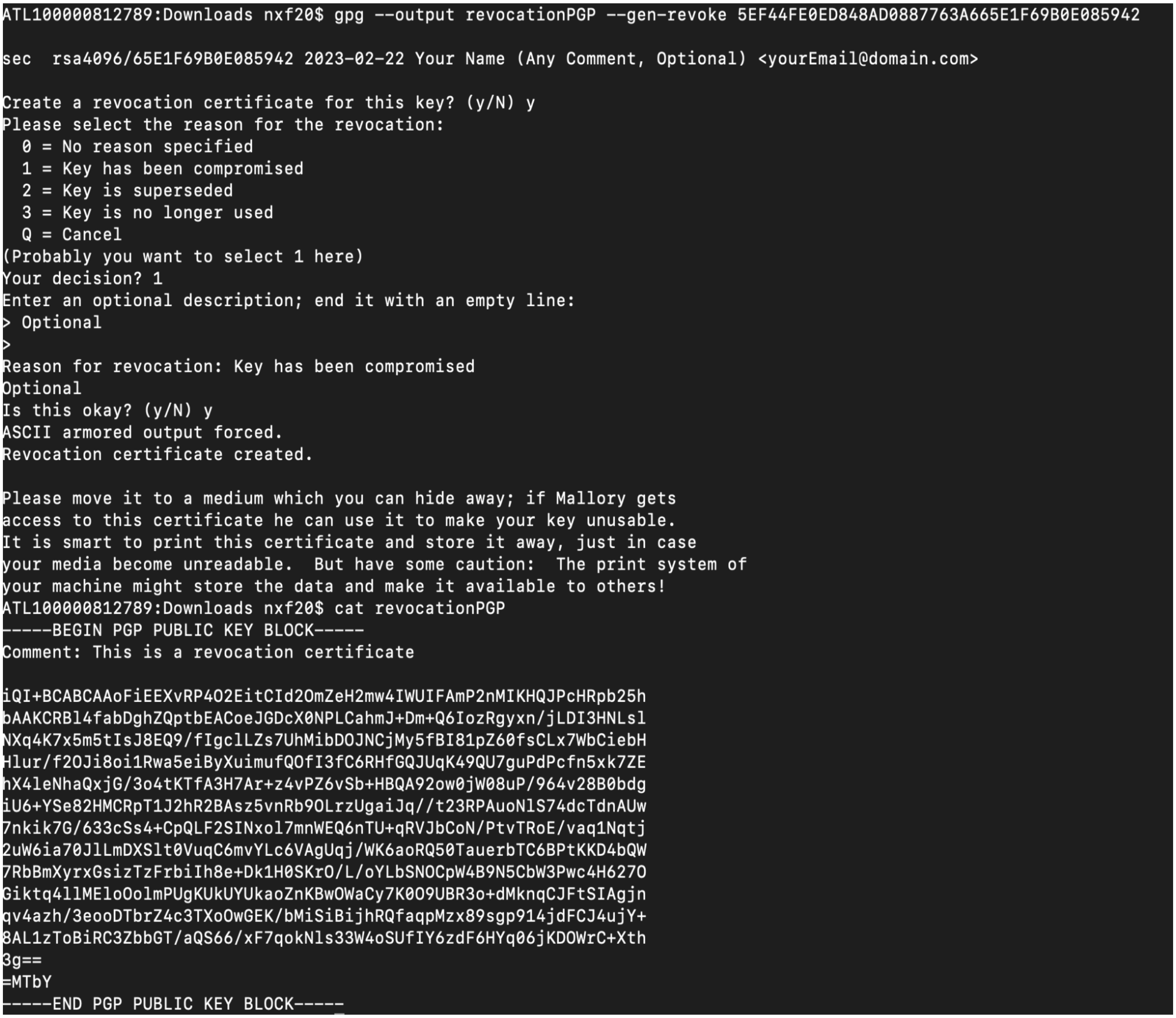


```
[gpg> setpref SHA512 SHA384 SHA256 AES256 AES192 AES ZLIB BZIP2 ZIP Uncompressed
 Set preference list to:
      Cipher: AES256, AES192, AES, 3DES
      AEAD:
      Digest: SHA512, SHA384, SHA256, SHA1
      Compression: ZLIB, BZIP2, ZIP, Uncompressed
      Features: MDC, Keyserver no-modify
[Really update the preferences? (y/N) y

 sec  rsa4096/65E1F69B0E085942
      created: 2023-02-22  expires: 2025-02-21  usage: C
      trust: ultimate      validity: ultimate
 ssb  rsa4096/0819694D60AE8A70
      created: 2023-02-22  expires: 2025-02-21  usage: S
 ssb  rsa4096/DBEBFE1800F517F6
      created: 2023-02-22  expires: 2025-02-21  usage: E
 [ultimate] (1). Your Name (Any Comment, Optional) <yourEmail@domain.com>

[gpg> showpref
 [ultimate] (1). Your Name (Any Comment, Optional) <yourEmail@domain.com>
      Cipher: AES256, AES192, AES, 3DES
      AEAD:
      Digest: SHA512, SHA384, SHA256, SHA1
      Compression: ZLIB, BZIP2, ZIP, Uncompressed
      Features: MDC, Keyserver no-modify

[gpg> save
```

**NOTE 3DES and SHA1 cannot be removed but they will not be used since they are last in the preferences list

OPTIONAL STEPS:

Revocation Cert



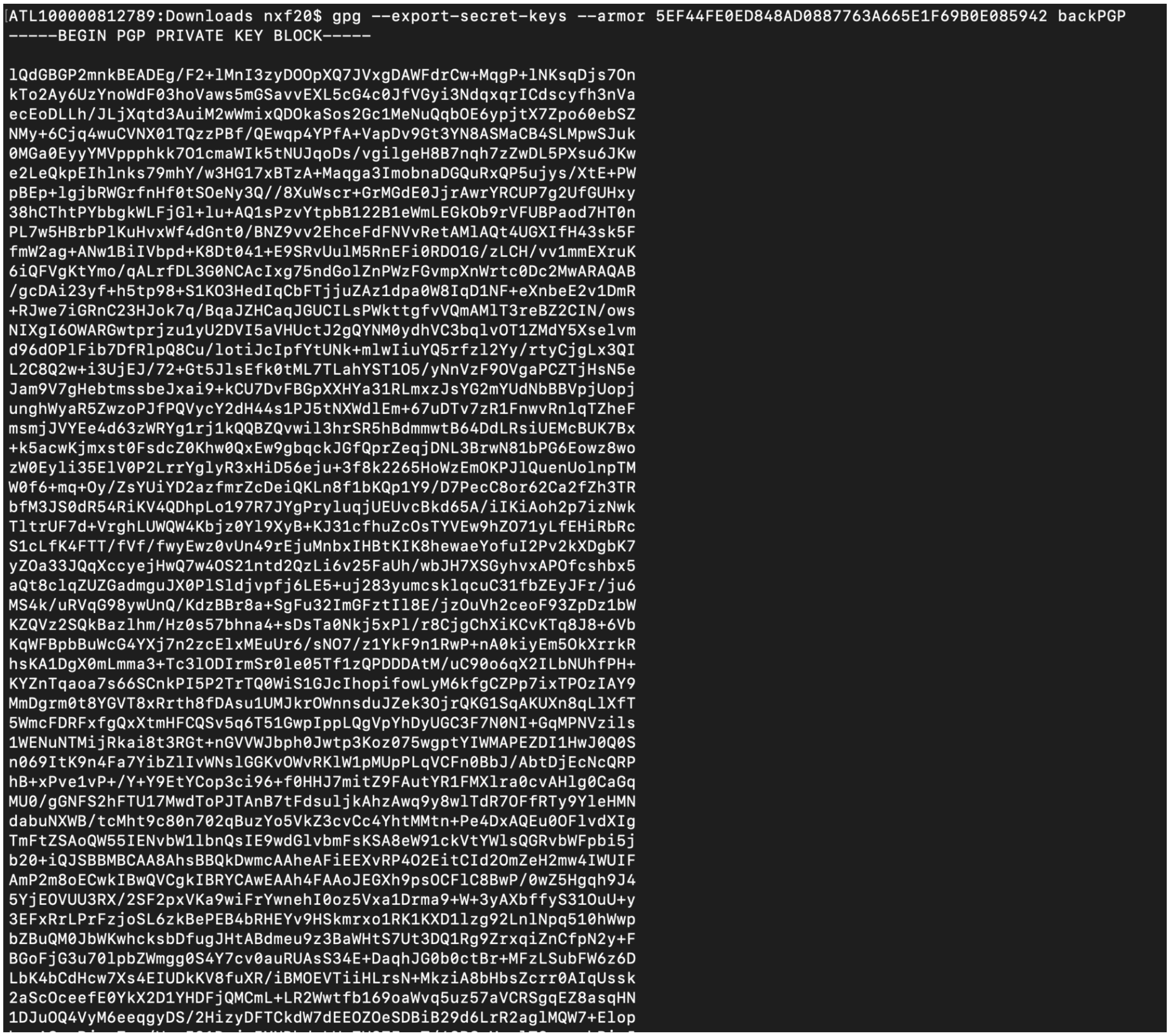
```
ATL100000812789:Downloads nxf20$ gpg --output revocationPGP --gen-revoke 5EF44FE0ED848AD0887763A665E1F69B0E085942

sec  rsa4096/65E1F69B0E085942 2023-02-22 Your Name (Any Comment, Optional) <yourEmail@domain.com>

Create a revocation certificate for this key? (y/N) y
Please select the reason for the revocation:
  0 = No reason specified
  1 = Key has been compromised
  2 = Key is superseded
  3 = Key is no longer used
  Q = Cancel
(Probably you want to select 1 here)
Your decision? 1
Enter an optional description; end it with an empty line:
> Optional
>
Reason for revocation: Key has been compromised
Optional
Is this okay? (y/N) y
ASCII armored output forced.
Revocation certificate created.

Please move it to a medium which you can hide away; if Mallory gets
access to this certificate he can use it to make your key unusable.
It is smart to print this certificate and store it away, just in case
your media become unreadable.  But have some caution:  The print system of
your machine might store the data and make it available to others!
ATL100000812789:Downloads nxf20$ cat revocationPGP
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: This is a revocation certificate

iQI+BCABCAAoFiEEXvRP4O2EitCId2OmZeH2mw4IWUIFAmP2nMIKHQJPcHRpb25h
bAAKCRBl4fabDghZQptbEACoeJGDcX0NPLCahmJ+Dm+Q6IozRgyxn/jLDI3HNLsl
NXq4K7x5m5tIsJ8EQ9/fIgclLZs7UhMibDOJNCjMy5fBI81pZ60fsCLx7WbCiebH
Hlur/f2OJi8oi1Rwa5eiByXuimufQOfI3fC6RHfGQJUqK49QU7guPdPcfn5xk7ZE
hX4leNhaQxjG/3o4tKTfA3H7Ar+z4vPZ6vSb+HBQA92ow0jW08uP/964v28B0bdg
iU6+YSe82HMCRpT1J2hR2BAsz5vnRb9OLrzUgaiJq//t23RPAuoNlS74dcTdnAUw
7nkik7G/633cSs4+CpQLF2SINxol7mnWEQ6nTU+qRVJbCoN/PtvTRoE/vaq1Nqtj
2uW6ia70JlLmDXSlt0VuqC6mvYLc6VAgUqj/WK6aoRQ50TauerbTC6BPtKKD4bQW
7RbBmXyrxGsizTzFrbiIh8e+Dk1H0SKrO/L/oYLbSNOCpW4B9N5CbW3Pwc4H627O
Giktq4llMEloOolmPUgKUkUYUkaoZnKBwOWaCy7K0O9UBR3o+dMknqCJFtSIAgjn
qv4azh/3eooDTbrZ4c3TXoOwGEK/bMiSiBijhRQfaqpMzx89sgp914jdFCJ4ujY+
8AL1zToBiRC3ZbbGT/aQS66/xF7qokNls33W4oSUfIY6zdF6HYq06jKDOWrC+Xth
3g==
=MTbY
-----END PGP PUBLIC KEY BLOCK-----
```

```
-------------------------- CREATE KEY -----------------------
gpg --full-generate-key --expert
Please select what kind of key you want: 8
Possible actions for a RSA key: <toggle off s and e> <q to finish>
What keysize do you want? <key size, 4096 recommended>
```

```
Please specify how long the key should be valid. <select desired
expiration, 2y recommended>
Real name: <enter desired user name, will be used to build userid>
Email address: <enter desired e-mail, will be used to build userid>
Comment: <enter desired comment> <O to finish>

-------- EDIT KEY (add sub keys and set preferences) ----------
gpg --edit-key <KEYID>
addkey
Please select what kind of key you want: 4
What keysize do you want? <key size, 4096 recommended>
Key is valid for? <select desired expiration, 2y recommended>
Is this correct? y
Really create? y
addkey
Please select what kind of key you want: 6
What keysize do you want? <key size, 4096 recommended>
Key is valid for? <select desired expiration, 2y recommended>
Is this correct? y
Really create? y
setpref SHA512 SHA384 SHA256 AES256 AES192 AES ZLIB BZIP2 ZIP Uncompressed
Really update the preferences? y
save

----- GENERATE REVOCATION CERTIFICATE !!!!!!!!STORE SECURELY
OFFLINE!!!!!!!! -----
gpg --output <DESIRED_FILE_NAME> --gen-revoke <KEY_ID>
Create a revocation certificate for this key? y
Please select the reason for the revocation: 1
Enter an optional description; end it with an empty line: <desired
comment, blank recommended>
Is this okay? y

------------ BACKUP KEYS !!!!!!!!STORE SECURELY OFFLINE!!!!!!!!
-------------
gpg --export-secret-keys --armor <KEY_ID> > <DESIRED_FILE_NAME>
gpg --export --armor <KEY_ID> > <DESIRED_FILE_NAME>

----------------------- REMOVE CERTIFICATION PRIVATE KEY
---------------------
mkdir -p tmp/gpg
gpg --export-secret-subkeys <KEY_ID> > tmp/gpg/subkeys
gpg --delete-secret-key <KEY_ID>
Delete this key from the keyring? y
This is a secret key! - really delete? y
gpg --import tmp/gpg/subkeys
rm -Rf tmp
```

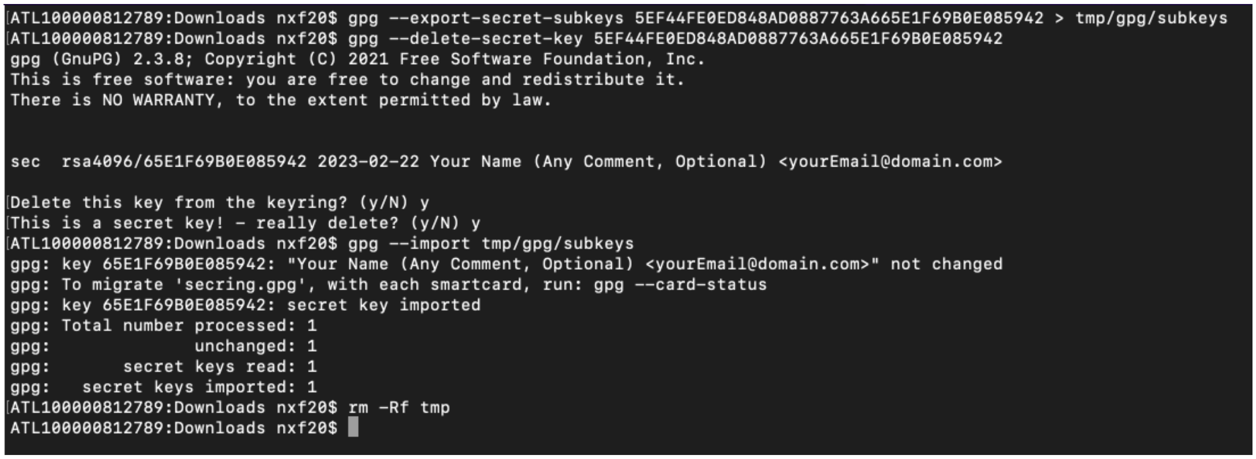
```
----------------- EXPORT PUBLIC AND PRIVATE PEM -------------------
gpg --armor --output <DESIRED_FILE_NAME> --export <KEY_ID>
gpg --armor --output <DESIRED_FILE_NAME> --export-secret-keys <KEY_ID>
```

Backup PGP



```
ATL100000812789:Downloads nxf20$ gpg --export-secret-keys --armor 5EF44FE0ED848AD0887763A665E1F69B0E085942 backPGP
-----BEGIN PGP PRIVATE KEY BLOCK-----

lQdGBGP2mnkBEADEg/F2+lMnI3zyDOOpXQ7JVxgDAWFdrCw+MqgP+lNKsqDjs7On
kTo2Ay6UzYnoWdF03hoVaws5mGSavvEXL5cG4c0JfVGyi3NdqxqrICdscyfh3nVa
ecEoDLLh/JLjXqtd3AuiM2wWmixQDOkaSos2Gc1MeNuQqbOE6ypjtX7Zpo60ebSZ
NMy+6Cjq4wuCVNX01TQzzPBf/QEwqp4YPfA+VapDv9Gt3YN8ASMaCB4SLMpwSJuk
0MGa0EyyYMVppphkk7O1cmaWIk5tNUJqoDs/vgilgeH8B7nqh7zZwDL5PXsu6JKw
e2LeQkpEIhlnks79mhY/w3HG17xBTzA+Maqga3ImobnaDGQuRxQP5ujys/XtE+PW
pBEp+lgjbRWGrfnHf0tSOeNy3Q//8XuWscr+GrMGdE0JjrAwrYRCUP7g2UfGUHxy
38hCThtPYbbgkWLFjGl+lu+AQ1sPzvYtpbB122B1eWmLEGkOb9rVFUBPaod7HT0n
PL7w5HBrbPlKuHvxWf4dGnt0/BNZ9vv2EhceFdFNVvRetAMlAQt4UGXIfH43sk5F
fmW2ag+ANw1BiIVbpd+K8Dt041+E9SRvUulM5RnEFi0RDO1G/zLCH/vv1mmEXruK
6iQFVgKtYmo/qALrfDL3G0NCAcIxg75ndGolZnPWzFGvmpXnWrtc0Dc2MwARAQAB
/gcDAi23yf+h5tp98+S1KO3HedIqCbFTjjuZAz1dpa0W8IqD1NF+eXnbeE2v1DmR
+RJwe7iGRnC23HJok7q/BqaJZHCaqJGUCILsPWkttgfvVQmAMlT3reBZ2CIN/ows
NIXgI6OWARGwtprjzu1yU2DVI5aVHUctJ2gQYNM0ydhVC3bqlvOT1ZMdY5Xselvm
d96dOPlFib7DfRlpQ8Cu/lotiJcIpfYtUNk+mlwIiuYQ5rfzl2Yy/rtyCjgLx3QI
L2C8Q2w+i3UjEJ/72+Gt5JlsEfk0tML7TLahYST1O5/yNnVzF9OVgaPCZTjHsN5e
Jam9V7gHebtmssbeJxai9+kCU7DvFBGpXXHYa31RLmxzJsYG2mYUdNbBBVpjUopj
unghWyaR5ZwzoPJfPQVycY2dH44s1PJ5tNXWdlEm+67uDTv7zR1FnwvRnlqTZheF
msmjJVYEe4d63zWRYg1rj1kQQBZQvwil3hrSR5hBdmmwtB64DdLRsiUEMcBUK7Bx
+k5acwKjmxst0FsdcZ0Khw0QxEw9gbqckJGfQprZeqjDNL3BrwN81bPG6Eowz8wo
zW0Eyli35ElV0P2LrrYglyR3xHiD56eju+3f8k2265HoWzEmOKPJlQuenUolnpTM
W0f6+mq+Oy/ZsYUiYD2azfmrZcDeiQKLn8f1bKQp1Y9/D7PecC8or62Ca2fZh3TR
bfM3JS0dR54RiKV4QDhpLo197R7JYgPryluqjUEUvcBkd65A/iIKiAoh2p7izNwk
TltrUF7d+VrghLUWQW4Kbjz0Yl9XyB+KJ31cfhuZcOsTYVEw9hZO71yLfEHiRbRc
S1cLfK4FTT/fVf/fwyEwz0vUn49rEjuMnbxIHBtKIK8hewaeYofuI2Pv2kXDgbK7
yZOa33JQqXccyejHwQ7w4OS21ntd2QzLi6v25FaUh/wbJH7XSGyhvxAPOfcshbx5
aQt8clqZUZGadmguJX0PlSldjvpfj6LE5+uj283yumcsklqcuC31fbZEyJFr/ju6
MS4k/uRVqG98ywUnQ/KdzBBr8a+SgFu32ImGFztIl8E/jzOuVh2ceoF93ZpDz1bW
KZQVz2SQkBazlhm/Hz0s57bhna4+sDsTa0Nkj5xPl/r8CjgChXiKCvKTq8J8+6Vb
KqWFBpbBuWcG4YXj7n2zcElxMEuUr6/sNO7/z1YkF9n1RwP+nA0kiyEm5OkXrrkR
hsKA1DgX0mLmma3+Tc3lODIrmSr0le05Tf1zQPDDDAtM/uC90o6qX2ILbNUhfPH+
KYZnTqaoa7s66SCnkPI5P2TrTQ0WiS1GJcIhopifowLyM6kfgCZPp7ixTPOzIAY9
MmDgrm0t8YGVT8xRrth8fDAsu1UMJkrOWnnsduJZek3OjrQKG1SqAKUXn8qLlXfT
5WmcFDRFxfgQxXtmHFCQSv5q6T51GwpIppLQgVpYhDyUGC3F7N0NI+GqMPNVzils
1WENuNTMijRkai8t3RGt+nGVVWJbph0Jwtp3Koz075wgptYIWMAPEZDI1HwJ0Q0S
n069ItK9n4Fa7YibZlIvWNslGGKvOWvRKlW1pMUpPLqVCFn0BbJ/AbtDjEcNcQRP
hB+xPve1vP+/Y+Y9EtYCop3ci96+f0HHJ7mitZ9FAutYR1FMXlra0cvAHlg0CaGq
MU0/gGNFS2hFTU17MwdToPJTAnB7tFdsuljkAhzAwq9y8wlTdR7OFfRTy9YleHMN
dabuNXWB/tcMht9c80n702qBuzYo5VkZ3cvCc4YhtMMtn+Pe4DxAQEu0OFlvdXIg
TmFtZSAoQW55IENvbW1lbnQsIE9wdGlvbmFsKSA8eW91ckVtYWlsQGRvbWFpbi5j
b20+iQJSBBMBCAA8AhsBBQkDwmcAAheAFiEEXvRP4O2EitCId2OmZeH2mw4IWUIF
AmP2m8oECwkIBwQVCgkIBRYCAwEAAh4FAAoJEGXh9psOCFlC8BwP/0wZ5Hgqh9J4
5YjEOVUU3RX/2SF2pxVKa9wiFrYwnehI0oz5Vxa1Drma9+W+3yAXbffyS31OuU+y
3EFxRrLPrFzjoSL6zkBePEB4bRHEYv9HSkmrxo1RK1KXD1lzg92LnlNpq510hWwp
bZBuQM0JbWKwhcksbDfugJHtABdmeu9z3BaWHtS7Ut3DQ1Rg9ZrxqiZnCfpN2y+F
BGoFjG3u70lpbZWmgg0S4Y7cv0auRUAsS34E+DaqhJG0b0ctBr+MFzLSubFW6z6D
LbK4bCdHcw7Xs4EIUDkKV8fuXR/iBMOEVTiiHLrsN+MkziA8bHbsZcrr0AIqUssk
2aScOceefE0YkX2D1YHDFjQMCmL+LR2Wwtfb169oaWvq5uz57aVCRSgqEZ8asqHN
1DJuOQ4VyM6eeqgyDS/2HizyDFTCkdW7dEEOZOeSDBiB29d6LrR2aglMQW7+Elop
```

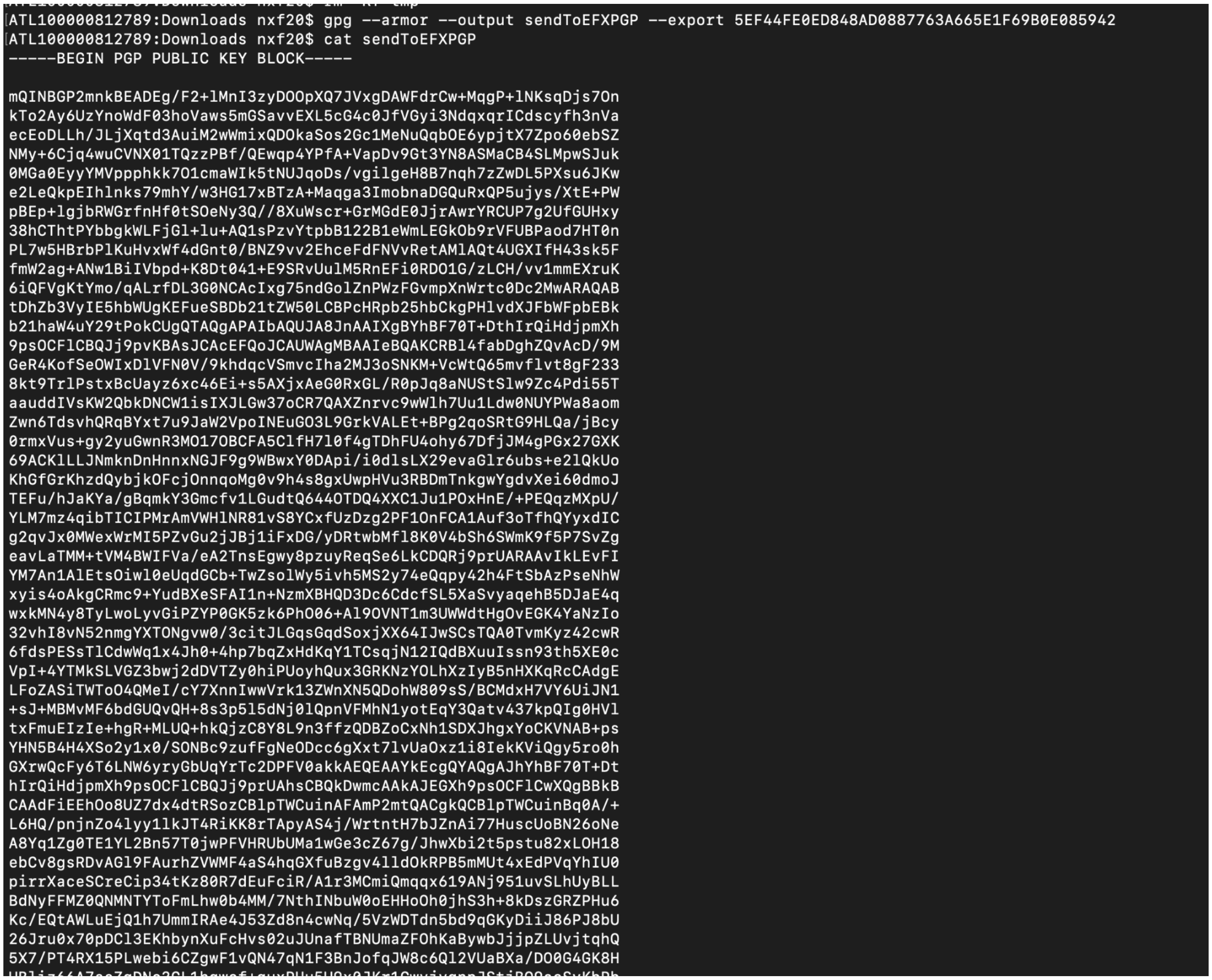
Remove the master/primary key



```
[ATL100000812789:Downloads nxf20$ gpg --export-secret-subkeys 5EF44FE0ED848AD0887763A665E1F69B0E085942 > tmp/gpg/subkeys
[ATL100000812789:Downloads nxf20$ gpg --delete-secret-key 5EF44FE0ED848AD0887763A665E1F69B0E085942
 gpg (GnuPG) 2.3.8; Copyright (C) 2021 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.


 sec  rsa4096/65E1F69B0E085942 2023-02-22 Your Name (Any Comment, Optional) <yourEmail@domain.com>

[Delete this key from the keyring? (y/N) y
[This is a secret key! - really delete? (y/N) y
[ATL100000812789:Downloads nxf20$ gpg --import tmp/gpg/subkeys
 gpg: key 65E1F69B0E085942: "Your Name (Any Comment, Optional) <yourEmail@domain.com>" not changed
 gpg: To migrate 'secring.gpg', with each smartcard, run: gpg --card-status
 gpg: key 65E1F69B0E085942: secret key imported
 gpg: Total number processed: 1
 gpg:              unchanged: 1
 gpg:       secret keys read: 1
 gpg:   secret keys imported: 1
[ATL100000812789:Downloads nxf20$ rm -Rf tmp
 ATL100000812789:Downloads nxf20$ 
```

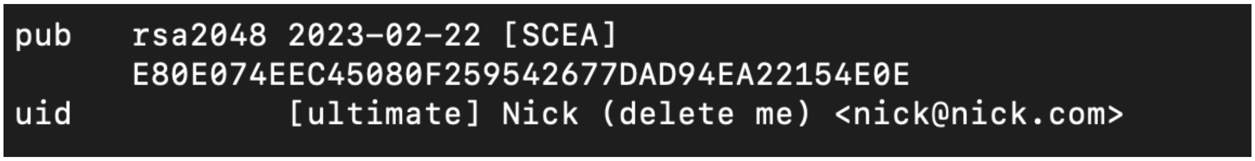
Command to export and then send to EFX

NOTE: It is Recommended (but optional) to removing master/primary for security reasons (see previous section for instructions)



```
[ATL100000812789:Downloads nxf20$ gpg --armor --output sendToEFXPGP --export 5EF44FE0ED848AD0887763A665E1F69B0E085942
[ATL100000812789:Downloads nxf20$ cat sendToEFXPGP
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGP2mnkBEADEg/F2+lMnI3zyDOOpXQ7JVxgDAWFdrCw+MqgP+lNKsqDjs7On
kTo2Ay6UzYnoWdF03hoVaws5mGSavvEXL5cG4c0JfVGyi3NdqxqrICdscyfh3nVa
ecEoDLLh/JLjXqtd3AuiM2wWmixQDOkaSos2Gc1MeNuQqbOE6ypjtX7Zpo60ebSZ
NMy+6Cjq4wuCVNX01TQzzPBf/QEwqp4YPfA+VapDv9Gt3YN8ASMaCB4SLMpwSJuk
0MGa0EyyYMVppphkk7O1cmaWIk5tNUJqoDs/vgilgeH8B7nqh7zZwDL5PXsu6JKw
e2LeQkpEIhlnks79mhY/w3HG17xBTzA+Maqga3ImobnaDGQuRxQP5ujys/XtE+PW
pBEp+lgjbRWGrfnHf0tSOeNy3Q//8XuWscr+GrMGdE0JjrAwrYRCUP7g2UfGUHxy
38hCThtPYbbgkWLFjGl+lu+AQ1sPzvYtpbB122B1eWmLEGkOb9rVFUBPaod7HT0n
PL7w5HBrbPlKuHvxWf4dGnt0/BNZ9vv2EhceFdFNVvRetAMlAQt4UGXIfH43sk5F
fmW2ag+ANw1BiIVbpd+K8Dt041+E9SRvUulM5RnEFi0RDO1G/zLCH/vv1mmEXruK
6iQFVgKtYmo/qALrfDL3G0NCAcIxg75ndGolZnPWzFGvmpXnWrtc0Dc2MwARAQAB
tDhZb3VyIE5hbWUgKEFueSBDb21tZW50LCBPcHRpb25hbCkgPHlvdXJFbWFpbEBk
b21haW4uY29tPokCUgQTAQgAPAIbAQUJA8JnAAIXgBYhBF70T+DthIrQiHdjpmXh
9psOCFlCBQJj9pvKBAsJCAcEFQoJCAUWAgMBAAIeBQAKCRBl4fabDghZQvAcD/9M
GeR4KofSeOWIxDlVFN0V/9khdqcVSmvcIha2MJ3oSNKM+VcWtQ65mvflvt8gF233
8kt9TrlPstxBcUayz6xc46Ei+s5AXjxAeG0RxGL/R0pJq8aNUStSlw9Zc4Pdi55T
aauddIVsKW2QbkDNCW1isIXJLGw37oCR7QAXZnrvc9wWlh7Uu1Ldw0NUYPWa8aom
Zwn6TdsvhQRqBYxt7u9JaW2VpoINEuGO3L9GrkVALEt+BPg2qoSRtG9HLQa/jBcy
0rmxVus+gy2yuGwnR3MO17OBCFA5ClfH7l0f4gTDhFU4ohy67DfjJM4gPGx27GXK
69ACKlLLJNmknDnHnnxNGJF9g9WBwxY0DApi/i0dlsLX29evaGlr6ubs+e2lQkUo
KhGfGrKhzdQybjkOFcjOnnqoMg0v9h4s8gxUwpHVu3RBDmTnkgwYgdvXei60dmoJ
TEFu/hJaKYa/gBqmkY3Gmcfv1LGudtQ644OTDQ4XXC1Ju1POxHnE/+PEQqzMXpU/
YLM7mz4qibTICIPMrAmVWHlNR81vS8YCxfUzDzg2PF1OnFCA1Auf3oTfhQYyxdIC
g2qvJx0MWexWrMI5PZvGu2jJBj1iFxDG/yDRtwbMfl8K0V4bSh6SWmK9f5P7SvZg
eavLaTMM+tVM4BWIFVa/eA2TnsEgwy8pzuyReqSe6LkCDQRj9prUARAAvIkLEvFI
YM7An1AlEtsOiwl0eUqdGCb+TwZsolWy5ivh5MS2y74eQqpy42h4FtSbAzPseNhW
xyis4oAkgCRmc9+YudBXeSFAI1n+NzmXBHQD3Dc6CdcfSL5XaSvyaqehB5DJaE4q
wxkMN4y8TyLwoLyvGiPZYP0GK5zk6PhO06+Al9OVNT1m3UWWdtHgOvEGK4YaNzIo
32vhI8vN52nmgYXTONgvw0/3citJLGqsGqdSoxjXX64IJwSCsTQA0TvmKyz42cwR
6fdsPESsTlCdwWq1x4Jh0+4hp7bqZxHdKqY1TCsqjN12IQdBXuuIssn93th5XE0c
VpI+4YTMkSLVGZ3bwj2dDVTZy0hiPUoyhQux3GRKNzYOLhXzIyB5nHXKqRcCAdgE
LFoZASiTWToO4QMeI/cY7XnnIwwVrk13ZWnXN5QDohW809sS/BCMdxH7VY6UiJN1
+sJ+MBMvMF6bdGUQvQH+8s3p5l5dNj0lQpnVFMhN1yotEqY3Qatv437kpQIg0HVl
txFmuEIzIe+hgR+MLUQ+hkQjzC8Y8L9n3ffzQDBZoCxNh1SDXJhgxYoCKVNAB+ps
YHN5B4H4XSo2y1x0/SONBc9zufFgNeODcc6gXxt7lvUaOxz1i8IekKViQgy5ro0h
GXrwQcFy6T6LNW6yryGbUqYrTc2DPFV0akkAEQEAAYkEcgQYAQgAJhYhBF70T+Dt
hIrQiHdjpmXh9psOCFlCBQJj9prUAhsCBQkDwmcAAkAJEGXh9psOCFlCwXQgBBkB
CAAdFiEEhOo8UZ7dx4dtRSozCBlpTWCuinAFAmP2mtQACgkQCBlpTWCuinBq0A/+
L6HQ/pnjnZo4lyy1lkJT4RiKK8rTApyAS4j/WrtntH7bJZnAi77HuscUoBN26oNe
A8Yq1Zg0TE1YL2Bn57T0jwPFVHRUbUMa1wGe3cZ67g/JhwXbi2t5pstu82xLOH18
ebCv8gsRDvAGl9FAurhZVWMF4aS4hqGXfuBzgv4lldOkRPB5mMUt4xEdPVqYhIU0
pirrXaceSCreCip34tKz80R7dEuFciR/A1r3MCmiQmqqx619ANj951uvSLhUyBLL
BdNyFFMZ0QNMNTYToFmLhw0b4MM/7NthINbuW0oEHHoOh0jhS3h+8kDszGRZPHu6
Kc/EQtAWLuEjQ1h7UmmIRAe4J53Zd8n4cwNq/5VzWDTdn5bd9qGKyDiiJ86PJ8bU
26Jru0x70pDCl3EKhbynXuFcHvs02uJUnafTBNUmaZFOhKaBywbJjjpZLUvjtqhQ
5X7/PT4RX15PLwebi6CZgwF1vQN47qN1F3BnJofqJW8c6Ql2VUaBXa/DO0G4GK8H
```

What it should NOT look like:

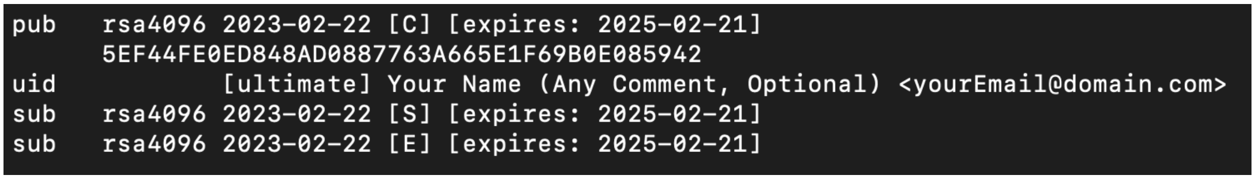


```
pub   rsa2048 2023-02-22 [SCEA]
      E80E074EEC45080F259542677DAD94EA22154E0E
uid           [ultimate] Nick (delete me) <nick@nick.com>
```

This key can do everything and does not follow RFC specifications

- https://www.ietf.org/rfc/rfc4880.txt

What the key should look like:



```
pub   rsa4096 2023-02-22 [C] [expires: 2025-02-21]
      5EF44FE0ED848AD0887763A665E1F69B0E085942
uid           [ultimate] Your Name (Any Comment, Optional) <yourEmail@domain.com>
sub   rsa4096 2023-02-22 [S] [expires: 2025-02-21]
sub   rsa4096 2023-02-22 [E] [expires: 2025-02-21]
```

This has a separate subkey for encryption and one for signing (optional) and the top level key is for certification