CHC Cloud GPG Encryption commands

1. Install GPG software

Software installed as part of the Standard Build (NextGen) – Nothing to do here

1. Create a key pair.

cmd: gpg --gen-key

xcxtdbw3q.aetna.com (oracle) CXTQA3::/home/oracle

CXTQA3> **gpg --gen-key 🡸**

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)

Requested keysize is 2048 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) 0 🡸**

Key does not expire at all

**Is this correct? (y/N) y 🡸**

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

Real name: aetna

Email address: [aetna@aetna.com](mailto:aetna@aetna.com)

Comment:

You selected this USER-ID:

    "aetna <[aetna@aetna.com](mailto:aetna@aetna.com)>"

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

1. Export the public key.

cmd: gpg --armor --export aetna --output aetna\_pubkey.asc

CXTQA3> **gpg --armor --export aetna --output aetna\_pubkey.asc 🡸**

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v2.0.22 (GNU/Linux)

mQENBF1v1j0BCADLAFWAVsWxnxbxZW+8AcdmfIuuVjOq+BJ8AcsUvPQ1qCwJ2NM0

8/+Q2ASloKivl9+jcXmNSXTneTHUPNu6zqH2ZbAx1mRD0x36JJALIr1UcnJxcz+3

5RAS3y+YpACbljaW02LbrXMt2h14aJLOh71l82LDXlgil6iMbKma60EXhwnVidm8

05taa8pUJAtK3RxE7C7vnfVpT7TpZBbe9eSyiNBU9vmYSVWd8MFA922paPzhwPwf

69Co05qNPGBK9qOkhggAlLwHSqbeLAe9XmpXD4X4ACmajcu/AAFHSAT7eyS0VXRP

urfarWlNUxbiDYnJg/L0WHxuhkrPPyctXblPABEBAAG0F2FldG5hIDxhZXRuYUBh

ZXRuYS5jb20+iQE5BBMBAgAjBQJdb9Y9AhsDBwsJCAcDAgEGFQgCCQoLBBYCAwEC

HgECF4AACgkQufIDzkrk/48OFQf/YA+B1G4DVO/Akz/ImoojDqbzzo3DdnPYGxaS

qfVzdMeYgTnHhL1poR8909qQonu3ROqoDP5Q9EkHWyKXYAtymZe+8hXl/oWD7NWN

0S9MI/VFztKj0Yn+NDAgkhE844Tvldd8MoYhHJWv5CNq3I0Xex4fF30oXlztbhJq

ujhx8iVXPDnXNgcf+0btpKHHVQ8XHQ+RlUcARZ30A8kWHH+IcgDzKL3a82ZMcTZw

jEjxRhFL0We+XQPsD/k5nBFT6STo9SCt5XBLAJHbvfW18gvRqlpHfJflSJnupfNc

CGf8hoF+ceDeSJdf1Ell5duR7tpLuzU/uncxZIA167igBsZM8rkBDQRdb9Y9AQgA

vc9fRc7tzwaORHUi+2uRyXL2+XkQJHQM2eKMjjqppPgqDcjWFkNV9TFET8vXYg5l

r0JE87V7IfTWzja0YSB0J2+rjotknl9SZekszr8tU2quNuhqOMZI8/6L0dAV+jbE

SUEOHynczN5MUeAFjnxpPb+nv+rugjpdTa49DMY454WrcqWB1LzKp+z+nvICMmZc

XU22rFwDDoDAuPcpFxeW7mbq1bIf2kn7hhCJPxBqw94ejXkrTVICeYW+cj/vWlIy

xA9oWOUDrFyDACSv2f2VAjO45r2whLLm72d3vZcOCaraGU8YUhazMu3SZrfuMmQ1

FjlxGMhr+Y8s3k1SXS0pFwARAQABiQEfBBgBAgAJBQJdb9Y9AhsMAAoJELnyA85K

5P+PwocH/34B9BYG7pJM1F7/AWg7Y5PUDreb0eB/A5NVmoX+iZgr7RMjE0TCt/+M

Tj2DfGBB/OPe0x7CD/TaYHcGfnpav8p9gi9HB/p54LwyJpher407+wRfk69PMidN

mrffP883gWIE5eW70Q8e5JbqLo14dTF6+kA/hayi7pNWMNHVtRGdKS4upIJ+W2YW

WmJqICNBeWnv7y0LnLNAV5qwAEoTx4Yt+Oy1h8D56XigqTApVoA+c2Z/qEgSuLdA

PKenuIediDJGc+jFGJc1cb+vNljxxGle3fmULfi4I2WtCZYexL88Ed7tYK9bp1di

O6I2eGEfG8ahqfP7mjB1baW7eFkOfvU=

=28eM

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

1. Email CHC the public key (above) -- copy/paste into email and wait to receive CHC public key to pair with Aetna.
2. Import CHC public key (CHC will send this via email).

cmd: gpg --import chc\_pub\_key.asc

CXTQA3> **gpg --import chc\_pub\_key.asc 🡸**

gpg: key CCAC2367: public key "CHANGEHEALTHCARE <[changehealthcare@changehealthcare.com](mailto:changehealthcare@changehealthcare.com)>" imported

gpg: Total number processed: 1

gpg:               imported: 1  (RSA: 1)

1. Sign the CHC public key (that was imported) with the Aetna private key that was created above.

gpg -u aetna --sign-key [client@changehealthcare.com](mailto:client@changehealthcare.com)

CXTQA3> **gpg -u aetna --sign-key** [**changehealthcare@changehealthcare.com**](mailto:changehealthcare@changehealthcare.com) **🡸**

pub  2048R/CCAC2367  created: 2019-09-04  expires: never       usage: SC

                     trust: unknown       validity: unknown

sub  2048R/8952735A  created: 2019-09-04  expires: never       usage: E

[ unknown] (1). CHANGEHEALTHCARE <[changehealthcare@changehealthcare.com](mailto:changehealthcare@changehealthcare.com)>

pub  2048R/CCAC2367  created: 2019-09-04  expires: never       usage: SC

                     trust: unknown       validity: unknown

Primary key fingerprint: 7E79 7148 98FD 1402 3F20  3705 2926 F371 CCAC 2367

     CHANGEHEALTHCARE <[changehealthcare@changehealthcare.com](mailto:changehealthcare@changehealthcare.com)>

Are you sure that you want to sign this key with your

key "aetna <[aetna@aetna.com](mailto:aetna@aetna.com)>" (64617CC4)

Really sign? (y/N)**y 🡸**

OK

1. Aetna encrypts the database file(s) using CHC public key.

gpg --homedir c:\encryption --recipient CLIENT --encrypt *export\_file\_name*

CXTQA3> **gpg --recipient** [**changehealthcare@changehealthcare.com**](mailto:changehealthcare@changehealthcare.com)

**--encrypt exp\_histSeed\_CXTQA1\_20190828-0912\_01.dmp 🡸**

1. Aetna uploads the file to S3.