Magrathea Telecommunications Limited,
5 Commerce Park, Brunel Road, Theale,
Berkshire RG7 4AB

0345 004 0040 info@magrathea-telecom.co.uk

GPG Key Expiry Date Update - Linux

This guide has been created to assist customers with the GPG key renewal process for GPG keys that are due to expire and need updating. When an existing GPG key is due to expire, there are 2 possible options to renew:

Option One –The existing key is updated with a new expiry date and re-uploaded by Magrathea. The current key remains valid and it is just the date that is updated/extended. This is the simplest and recommended option. See below for the steps to take.

Option Two – This is only recommended when Option 1 is not possible. A brand-new key is generated and uploaded by Mag to overwrite the current one. NB This will mean that any files that may have been Downloaded and NOT DECRYPTED, will need to be regenerated as the **NEW KEY** will **NOT** have access to files - This is due to the older files being encrypted by Magrathea using the older key. If required please contact support@magrathea-telecom.co.uk for guidance on Option Two.

The following steps are for option one only and shows command examples and screenshots taken from a Debian 11 host using the standard GPG binaries available on the Debian software repositories, but as the GPG binaries are standard across Linux distributions, there should be not be any issues using them on other Linux distributions.

Steps to follow for Option One:

On the machine and user account previously used to generate the original GPG key, please run a key list using command:

```
gpg -k
```

From the list of keys that you have, pick the one currently used for Magrathea CDR decryption, ie previously provided to Magrathea and note of the GPG key ID (long string of hexadecimals) as it will be needed to update the key.

```
pub   rsa3072 2022-12-02 [SC] [expires: 2024-12-01]
      536E1D3EF83CB33C744752A9A1612752816CB760
uid           [ultimate] Bruno Orfao <bruno@bruno.com>
sub   rsa3072 2022-12-02 [E] [expires: 2024-12-01]
```

Now, enter the key edit mode:

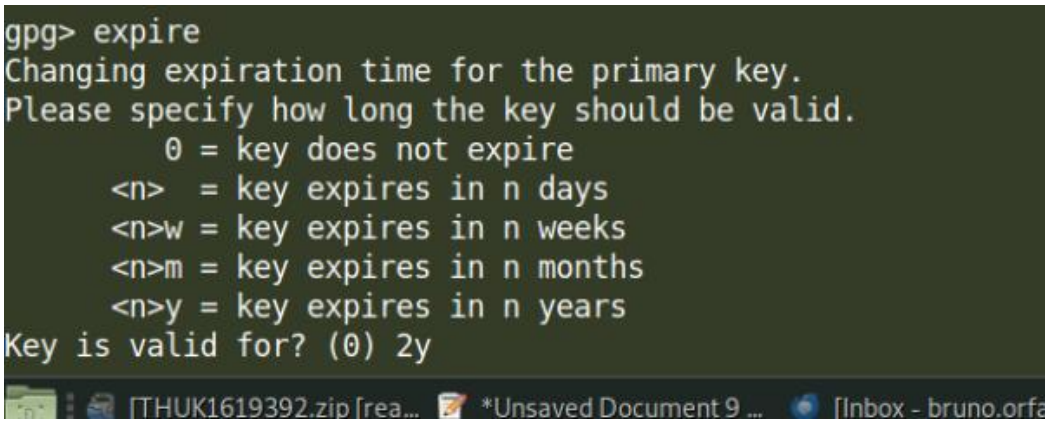
```
gpg --edit-key gpg_key_ID
```

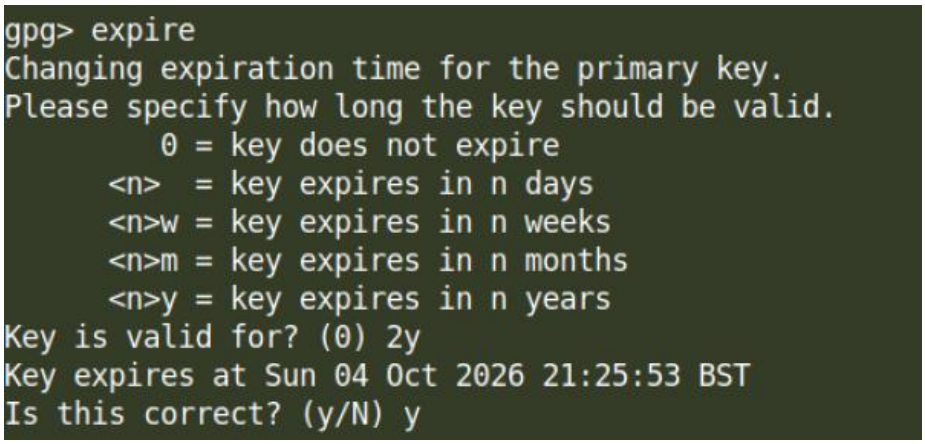
```
brunoo@mdh-prod-xrdp-01:~$ gpg --edit-key 536E1D3EF83CB33C744752A9A1612752816CB760
```

Afterwards, you will need to change the expiry dates of the GPG key, which is a normally a two- stage process, as you will need to update both the primary key and its subkeys. The primary key is normally **key 0** and does **not** to be selected, so we can just enter command

expire

Select the amount of time that you wish to extend the GPG key expire date, Magrathea recommends 2 years maximum and confirm the changes





If you setup a GPG key passphrase with the original key, you will be prompted to insert it so that the GPG key expiry date update process continues.

Now **quit** and **save the changes**

```
Key is valid for? (0) 2y
Key expires at Sun 04 Oct 2026 21:35:04 BST
Is this correct? (y/N) y

sec  rsa3072/A1612752816CB760
     created: 2022-12-02  expires: 2026-10-04  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/4177651F83B549F1
     created: 2022-12-02  expires: 2024-12-01  usage: E
[ultimate] (1). Bruno Orfao <bruno@bruno.com>

gpg> quit
Save changes? (y/N) y
```

Once completed we can now proceed with updating the **subkey**, which as normally keys only have 1 subkey, you can access it by typing '**key 1**'. The subkey is the key actually used for encryption, so it is quite important to update it, as you can see by the screenshot the 1st phase only updated the expiry date on the primary key.

```
brunoo@mdh-prod-xrdp-01:~$ gpg --edit-key 536E1D3EF83CB33C744752A9A1612752816CB760
gpg: keyserver option 'binddn' is unknown
gpg: keyserver option 'bindpw' is unknown
gpg: keyserver option 'tls' is unknown
gpg: keyserver option 'verbose' is unknown
gpg (GnuPG) 2.2.27; 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  rsa3072/A1612752816CB760
     created: 2022-12-02  expires: 2026-10-04  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/4177651F83B549F1
     created: 2022-12-02  expires: 2024-12-01  usage: E
[ultimate] (1). Bruno Orfao <bruno@bruno.com>

gpg>
```

Now select the secondary key ahead of changing its expiry date

key 1

```
brunoo@mdh-prod-xrdp-01:~$ gpg --edit-key 536E1D3EF83CB33C744752A9A1612752816CB760
gpg: keyserver option 'binddn' is unknown
gpg: keyserver option 'bindpw' is unknown
gpg: keyserver option 'tls' is unknown
gpg: keyserver option 'verbose' is unknown
gpg (GnuPG) 2.2.27; 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  rsa3072/A1612752816CB760
     created: 2022-12-02  expires: 2026-10-04  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/4177651F83B549F1
     created: 2022-12-02  expires: 2024-12-01  usage: E
[ultimate] (1). Bruno Orfao <bruno@bruno.com>

gpg> key 1

sec  rsa3072/A1612752816CB760
     created: 2022-12-02  expires: 2026-10-04  usage: SC
     trust: ultimate      validity: ultimate
ssb* rsa3072/4177651F83B549F1
     created: 2022-12-02  expires: 2024-12-01  usage: E
[ultimate] (1). Bruno Orfao <bruno@bruno.com>

gpg>
```

Afterwards, run the **expire** command again using the same value for key expiration as per previous step and do note that if you setup passphrase on the primary key, you will get prompted again.

```
gpg> expire
Changing expiration time for a subkey.
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
```

Finally, we will quit and save the changes:

quit
(When prompted to save please choose **y**)

```
Is this correct? (y/N) y

sec  rsa3072/A1612752816CB760
     created: 2022-12-02  expires: 2026-10-04  usage: SC
     trust: ultimate      validity: ultimate
ssb* rsa3072/4177651F83B549F1
     created: 2022-12-02  expires: 2026-10-04  usage: E
[ultimate] (1). Bruno Orfao <bruno@bruno.com>

gpg> quit
Save changes? (y/N) y
```

The final step is to export the public key ahead of sending it to Magrathea using a command based on the syntax below, but please note that you will need to replace the output path to a path on your system where you can retrieve the key (/tmp is normally a good option) and the email address with the relevant email address associated with your key.

gpg --output /path/to/store/outputfile.asc --export --armour email_address@email.com

```
brunoo@mdh-prod-xrdp-01:~$ gpg --output /tmp/customer_pub_key.asc --export --armour bruno@bruno.com
```

The final step is to send the exported public key file to Magrathea via email to support@magrathea-telecom.co.uk following the guidelines:

Subject line: "*Customer name" - GPG*
Attach: (GPG Public key file)