

A guide to accessing and decrypting data logs

Ref: [v.1.01]

Contents

Contents	1
1. Introduction.....	2
2. Requirements	2
3. Generate keys.....	3
4. Export keys	3
5. Import keys	3
6. Decrypt files.....	3
7. Encrypt files.....	3
8. SE Labs public key	4

Revisions:

1.01 Corrected minor typo; updated company address 27/06/2018

1. Introduction

This guide is designed to help you decrypt logs provided following a test.

This version of the document explains how to get up and running with GnuPG (GPG) and should be compatible with other command-line versions of GPG/PGP.

If you just need to gain access to some logs quickly, without wanting to set up a system for long term use please read the Windows Quick Start guide on page three.

If you plan to handle logs sent by SE Labs more regularly you may find the list of commands in the rest of this short guide helpful.

2. Requirements

To decrypt logs provided by SE Labs you will need the following:

2.1. A system* configured with:

- GnuPG (aka GPG) (<https://www.gnupg.org/>) or
- Any other OpenPGP-compatible encryption application (<http://openpgp.org/>)

GPG is almost certainly already installed if you use one of the common Linux distributions. If you want to process logs on a Windows system please consider our Windows Quick Start guide below.

* GPG's commands are the same regardless of your choice of operating system. This guide is compatible with all versions of Windows, Linux and MacOS X.

Windows Quick Start

GPG's default installation package for Windows includes a few things you may not want, including a certificate manager and context menu integration. If you only want to process logs sent by us you might prefer the basic installer. When we use Windows we use GPG's 'Vanilla' installation, which works from the command line and can perform all normal GPG tasks without slowing Windows down with extra services etc.

You can find different Windows GPG versions at <https://www.gpg4win.org/>.

At the time of writing the latest version of the Vanilla installation was available from:

<https://files.gpg4win.org/gpg4win-vanilla-2.3.3.exe>

- Download and install the software, following the familiar Wizard-driven process.
- Generate a key pair. Type the following from the Command Prompt, choosing the default options:

```
gpg --gen-key
```

- Export your public key. During the step above you will have entered an email address – most likely the catch-all account for your own internal lab. In this example that email address is labs@vendor.tld:

```
gpg --armor --export labs@vendor.tld > lab.pub.asc
```

- Copy and paste the public key into an email, or attach the file generated above, before sending to us at aux@selabs.uk.
- When you want to decrypt a downloaded log file (e.g. 2017Q1-LAB-001.tar.gpg) use the following command, replacing the filenames as appropriate and, when requested, entering the passphrase you specified when generating your key pair:

```
gpg -d 2017Q3-LAB-001.tar.gpg > 2017Q3-LAB-001.tar
```

3. Generate keys

The command to generate a pair of public and private keys is:

```
gpg --gen-key
```

Use the default options unless you have good reason to choose others.

4. Export keys

The command to export your public key for use by others is:

```
gpg --armor --export labs@vendor.tld > lab.pub.asc
```

(where labs@vendor.tld is your own lab's email address)

5. Import keys

The command to import a public key so you can encrypt files for another organisation is:

```
gpg --import selabs-aux.txt
```

6. Decrypt files

6.1 Decrypt a single file

The command to decrypt a single file supplied by SE Labs:

```
gpg -d 2017Q3-LAB-001.tar.gpg > 2017Q3-LAB-001.tar
```

(where 2017Q3-LAB-001.tar.gpg is the name of the file provided.)

6.2 Decrypt multiple files

```
gpg --decrypt-files *.gpg
```

7. Encrypt files

7.1 Encrypt one file for SE Labs only:

```
gpg -e -r selabs file.txt
```

7.2. Encrypt one file for SE Labs and your own organisation:

```
gpg -e -r selabs -r vendor file.txt
```

7.3 Encrypt multiple files for SE Labs and your own organisation:

```
gpg --encrypt-files -r selabs -r vendor *.txt
```

8. SE Labs public key

You can download our public key from <https://selabs.uk/download/selabs-aux.txt> or paste the following code into a text file and import it as explained in 5. Import keys.

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

Version: GnuPG v2

```
mQINBFa55UwBEACmr2VcjbI7C8nuJ0w3ijwrHsFYGmQRjf4ca8DHr/Er+ey7tL07
TFQVHsNUU6aI9rIN5EIAU36PnKhEP84MS5NUBTIWBQIKbah85e1B5nrb1nrIBsKn
oORKuWfZ82/KDIEvp+bMaP9JC8gDJs6elv1Vf4JpppIKAq+dg8uQG5agkBD914EX
R+FtmdSS1fsQDD7BmUDFA4YsFD0bAMLi8bTboXU31g01/P1yU/H5+upLLB8S4CRB
C4J+z24TC4jIARqH+3oS707h4NjXlg4jC4oXN4p+hHCZIX1Qg/D5hgJavJcSF4Yn
8QGjB/BupEkN3GySk+D2JtranEz0xpl8l8IwY0snDgigdVZhKmZuJ2LF3W14N0
DxstKitU815Dpa17cyRLqewDAwldlNkCLOXK98hagBTOXIrjR8ak07Hz73I2Stqc
AfYcYcqmhDw491QsqwU/vUG619YlxCHPYCDdIAvWuE3vS455tjY207+SgCTHRwN
2yWmFK10kjpUBngblzQwJm6foB3meRRojS4eWuMgRh4hP6xAeCludgJQcjSzHWDW
sQcLPfmD++N4DFAQ5YIbIRCMwaTK/VvPqLjV1A21imjxv+NTwvpThspX4EE76ev/
C4+SPZ10LHjJONwWAS2BqrByIA9HcMeqjhleaBJXm0ssaOfqW2kyNpQQhQARAQAB
tCVTRSBMYWJzIEZ0ZCAoR2VvZXJhbCkgPGF1eEBzZWxhYnMudWw+iQI4BBMBAgAi
BQJWueVMAhsDBgsJCAcDAGYVCAIJCgsEFGIDAQIeAQIXgAAKCRDzIc+ujRN/MSbe
D/4javh5rSecqt/Adstc01MTMOyVXIvN818zj2ZRIMYWRJFTwY0BKKUk6eYe8ZF9
5YSx0tQTAObtWEKJwDnbnesLnqPIb173invge8N/Lrhh2HyInD0yhMvfxhoKKNK
IABISXhRfRWU9uV1sGTjXkzIpxXUGE4tD+Ciq4xgeQuYQuNCRE25goj4yMT+Ij8h
1/yTO9Y+aT+SeITaKs+7lv17DQstDqZOTaODc9ZjWh7t+K1XSXoEe+/0Sn25Glul
qSNZLQYFhQpSKgsgQwYtMFTFN0ovIppmJcvKuV3Rjbo44BuA0VApIG6wzbuhHUKO
S2R193fSF9c+ASa0q0+gK6lxIKSPJ0yVrf8+ODZAVa13GOgwltha/uj9AIBF3hcW
JN7uLXDA9B6CXyIPcEyJHP5qFdiuQuedGCKnPMTXnjPR/qqaH43rUL5JundogBp3
3tRurmlQGFbq8hhsG7rMzUX5DP3p1rxd4nET5S+qzhXoUSjBbxyB0Z/5o1JgueM
6lHcgZsNWx+4X3DoxT/0w2TWzf95tteOr3VVV6Q2h2ldd4YAwQO1/M+Ug1XxTjL
PWJk00osStK9tdRfKcVrkqmr+SYFkZ/sRkLmuNWeUCq4RhkSQgsdvgMZ5Ldl1TL0
Us9UByaK64jauagnFoqu++MwD2oAzL5CwuaR7aQ/x6QIN7kCDQRWueVMARAAwygg
6JBL1YSmr3WLGJ5xXPHjKNFwGSt1t7ez1ZBdDvvs9aWz657iHsrBz/BGQxSvVo
v+X3yXelvP2NPqTklNzpj/OvwiKVzV1UyagZr11cFbWBq2MPemZmRulv4P8odWHR
3FtFvXmJmVz1hC9Zlyy01MNTJ8EwAMCSTSF8QxAlifftqEq7CIsvhAKMZ+CemfS
xfr4BJWCdwOb8BXpKCh8MQRnTZTFQKHC9XIV6qdbhkszNW5YeTyX3Ja6nOyswBA
kclFo2vBhA/DhTA1p905pUOKTD3VuSVvXUA/Chi2BBKmj6toCmXZ12NvmZs1RQq
WOQVtoMLcN0V7E0i29zpFtnwq1ERdipm41b/QZfYSQxo5XTI2rM16f+R0y9+XmM4
4H6iXuRp0lKgonCsDIIE1ohDEgtdWoE6vNJ+Hihu3aZVrsqOle8v/6QgCb3g+16e
HgJABM6K6h0KzrRSUR85XHnCQzLStKqAsT2S2y2jz6VYQ5wDO5T7bY9risxEB4Np
DqWRHG4mMuU4ZgGLR6c3of0oPb7Om82db5g4OgGiEa4ZCVPVtS9umyB30xGCJf90
O8i03jxnXoRgsL17oZLO1ukco/LduZU4u4iie4yQFHVXvddN1mjRXHx0FLA6GC9T
JLrK14zgYbGogsIj1jB5CvR1IbTz0KS5j+k3icAEQEAAyKCHwQYAQIACQUCVrnl
TAIbDAACKRDzIc+ujRN/MVB1D/4sed5yxjvpK9m9mAFYjKAsF12VjKod/FLddzXsK
d2kpWKbsNIZNFwWpSXCtXaBGKsfRDVZxVv1gZBfsHz1z+A+6Mmij3nzi0YXokKmK
DxlQP+QvQS7cny5HBsedTFEGBWckbRTau112givK1yCDC2+AbNRsRVg4D8G5oKUz
Zz52myEeT2ENknjpXgn7rNwd2LWJU2C5/SrgpWtmf340cLw/+SDroKzO9PUN/kk
50sDYpNppWyUny/8InZa2lHyA9HtXKy1/Tp5mv8utQlLA8tyyQULK9EixAq8H/gp
U1d3N0ox4+CM92eXerXmC0VDrT9FWrAwh4cmGYIHL64AIY39Sx9NPAHxo5cquwWK
yC3UfeiFax2innNiz5TD+RhBvWYpebWq0baUp97gXs0A0sUZ1oyjdpCgnVtw+H87
R2NcEspEamJBsr4CcEKrpeTE5Ovb9BNQ9/4oTneAQIVAj4tS4/QShGFq64QeY5V
dDepBml+ApbyeVOB3tll7Zkdo5RQDiYp6o2W9hGJfsr0FjQlC9Rbdo6rFO/T3ZT6
FQftOI3aklA/cXD4q1+lwrhJf4OekQ8c6CEERnh3Axp64VQxP8Rm/+V4te59wjNr
B3xv2YhVjfpNfe536WtSECV9AsPMfSX16CLcQC11+Zkdbkc/6vAIR+mywLwW+7V
61hbPQ==
=xgmk
-----END PGP PUBLIC KEY BLOCK-----
```

SE LABS LTD

4 Cromwell Court, New Street, Aylesbury, Buckinghamshire, HP20 2PB, United Kingdom.

Registered in England: 9688006.

Tel: +44(0)203 875 5000; Email: aux@selabs.uk