User Guide to
PGP Encryption

UPDATED ON 1 JULY 2016

Table of Contents

About this guide

For the purposes of SCV Verification, FSCS accepts SCV files encrypted with its PGP public key. FSCS's public key is available on our website:

http://www.fscs.org.uk/industry/single-customer-view/

For guidance on other available submission methods please refer to the FSCS Guide to SCV which is also available on our website. There is also a separate user guide available for the SCV Verification Services portal which you can obtain by contacting:

fasterpayoutenquiries@fscs.org.uk

About PGP

PGP is an encryption program that works on most computing platforms. It is fairly easy to use, and there are viable free versions available in addition to the commercial version. The open-source version of PGP, known as the GPG (Gnu Privacy Guard) program, adheres to the OpenPGP standard and is interoperable with all versions of PGP, and is not restricted to non-commercial use. There are numerous front end applications available for GPG to facilitate encryption of files, and it can also be executed completely on the command line. The tools listed in this guide are the most commonly used.

GPG command line (open-source)

GPG is a complete and free implementation of the OpenPGP standard as defined by RFC4880. GPG allows you to encrypt and sign your data and communication. It is a command line tool with features for easy integration with other applications.

Please follow these steps to encrypt your file using the Windows Command Prompt.

1. Import FSCS's public key:

    - Download FSCS's public key, entitled "FSCS Verification Services.asc" from our website:

        http://www.fscs.org.uk/industry/single-customer-view/

    - Create a folder on the C:\ drive entitled "FSCS".

    - Copy the "FSCS Verification Services.asc" public key to the "FSCS" folder on the C:\ drive.

    - Run the following commands:

```
C:\> cd \FSCS
C:\FSCS>
C:\FSCS>
C:\FSCS>gpg --import "c:\FSCS\FSCS Verification Services.asc"
imported
gpg: Total number processed: 1
gpg:               imported: 1   (RSA: 1)
C:\FSCS>
```

2. Encrypt your SCV file:

    - Use the command below encrypt the SCV file (replace "YourSCVFile.csv" with the actual name and extension of your file):

```
C:\FSCS > gpg --recipient   "FSCS Verification Services
<bhupendra.kc@fscs.org.uk>" --armor --output
"C:\Temp\YourSCVFile.pgp" --encrypt  "C:\SCV\YourSCVFile.csv"
```

3. Submit your SCV file to FSCS:

    - Refer to FSCS SCV Guide and FSCS Verification Services Web Portal User Manual for guidance on the SCV submission process.

GPG graphical user interface (open-source)

GPG is also available as a tool with a graphical user interface.

Please follow these steps to encrypt your file using this version of the tool.

1. Import FSCS's public key:

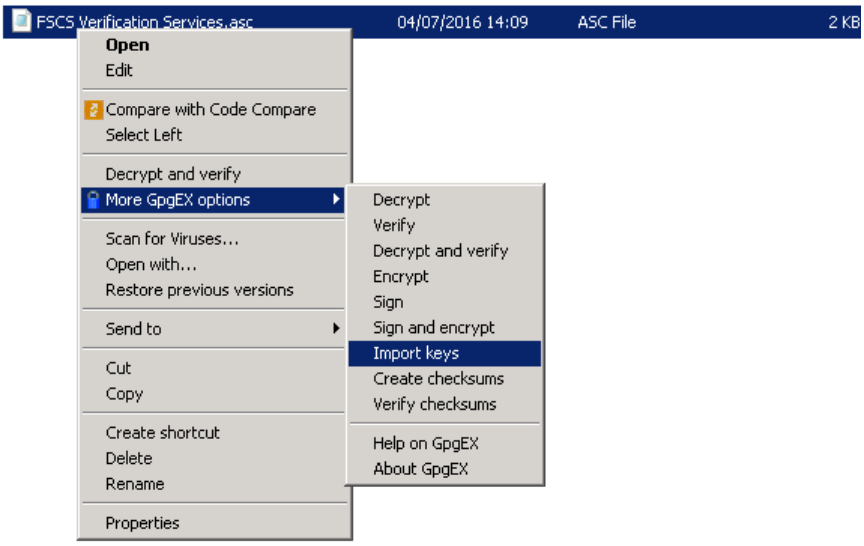
    - Download FSCS's public key, entitled "FSCS Verification Services.asc" from our website:

      http://www.fscs.org.uk/industry/single-customer-view/

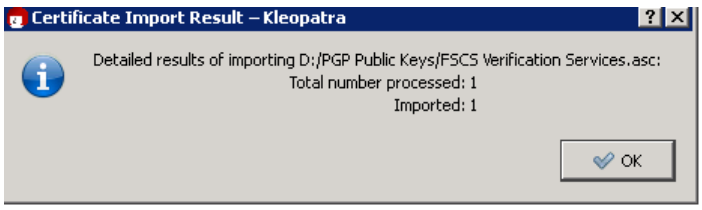
    - Create a folder on the C:\ drive entitled "FSCS".

    - Copy the "FSCS Verification Services.asc" public key to the "FSCS" folder on the C:\ drive.

    - Right-click on the "FSCS Verification Services.asc" public key in the folder "FSCS" folder and click on "More GpgEX options >", followed by "Import keys".

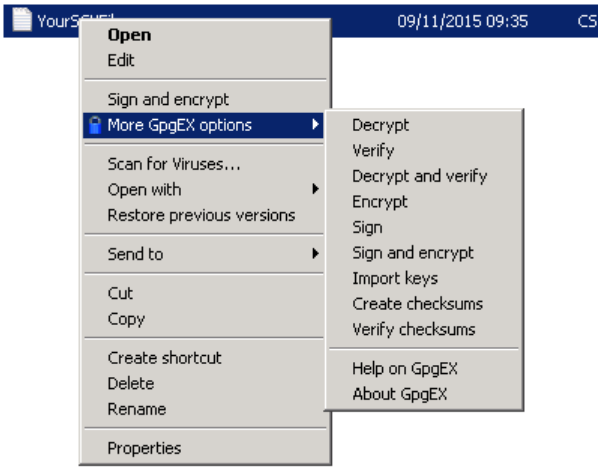


    - A dialog box will appear showing that the public key has been successfully imported.

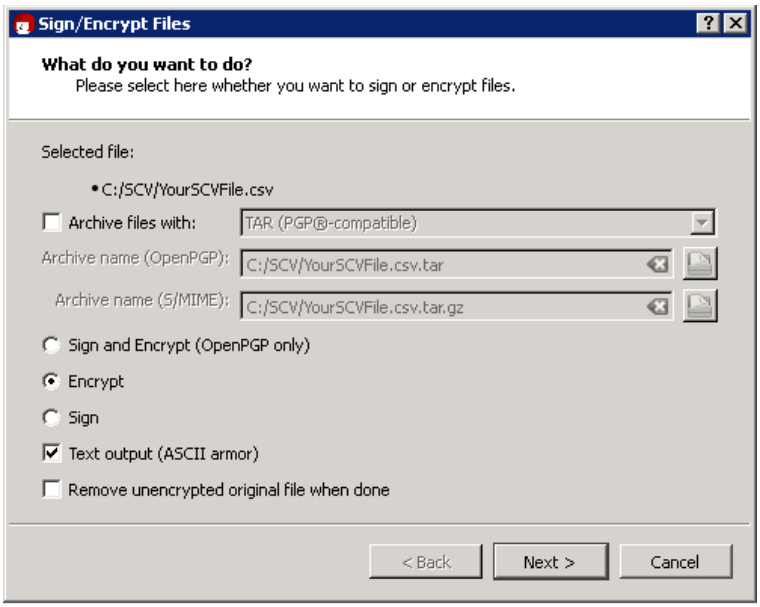


2. Encrypt your SCV file:

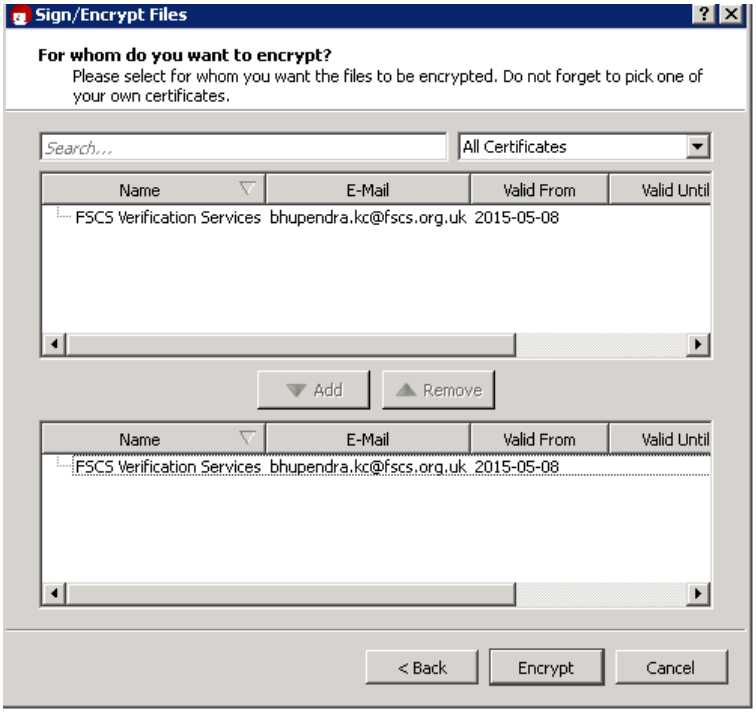
- Right-click on the file that you want to encrypt and click “More GpgEX options >” followed by “Encrypt”.



- Tick “Text output (ASCII armor)” and click “Next >” button.



- Add FSCS's public key and click "Encrypt".



- Rename the File extension to ".PGP".

3. Submit your SCV file to FSCS:

    - Refer to FSCS SCV Guide and FSCS Verification Services Web Portal User Manual for guidance on the SCV submission process.

Symantec Encryption Desktop

Please use instructions below to encrypt your file using Symantec Encryption Desktop for Windows (version 10.3.2).

1. Import FSCS's public key:

    - Download FSCS's public key, entitled "FSCS Verification Services.asc" from our website:

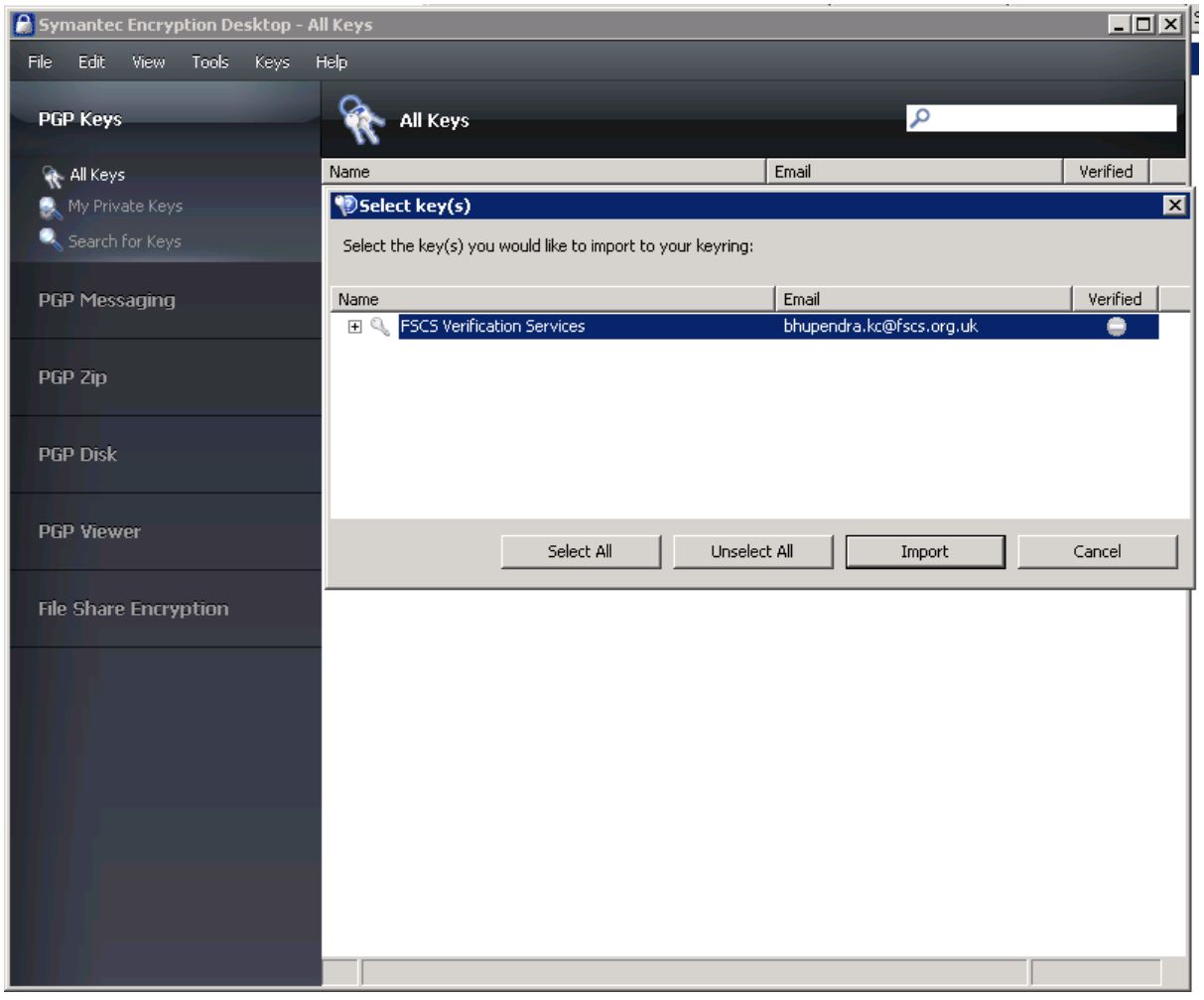
      http://www.fscs.org.uk/industry/single-customer-view/

    - Create a folder on the C:\ drive entitled "FSCS".

    - Copy the "FSCS Verification Services.asc" public key to the "FSCS" folder on the C:\ drive.

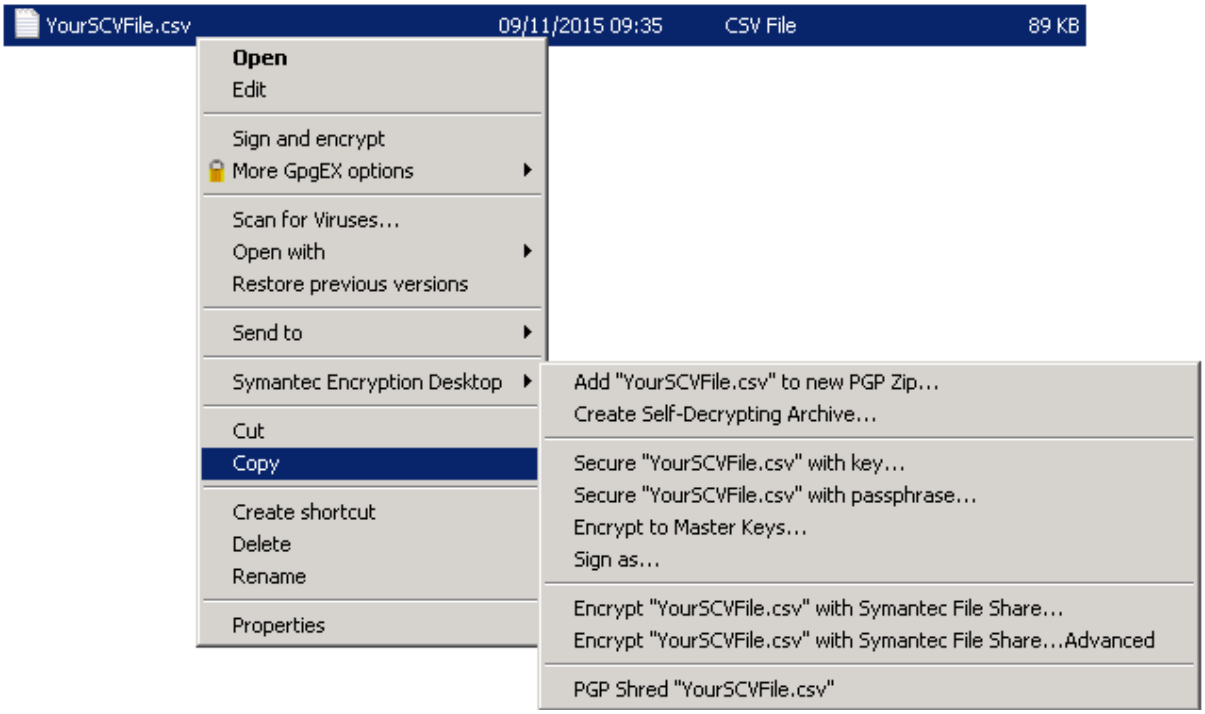
    - Open the Symantec Encryption Desktop application.

    - Click "File" followed by "Import", and then select the public key to import it.

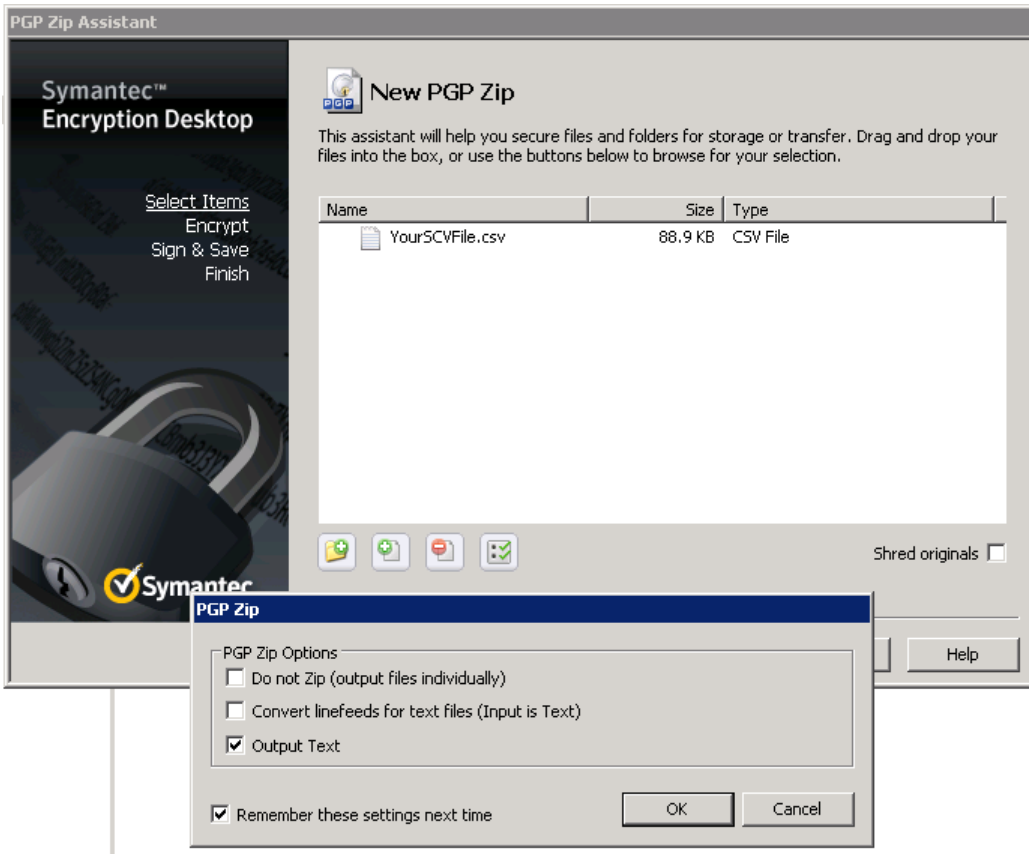


2. Encrypt your SCV File:

- Right click on the file you want to encrypt and select “Add **YourSCVFile.csv** to new PGP Zip …”.

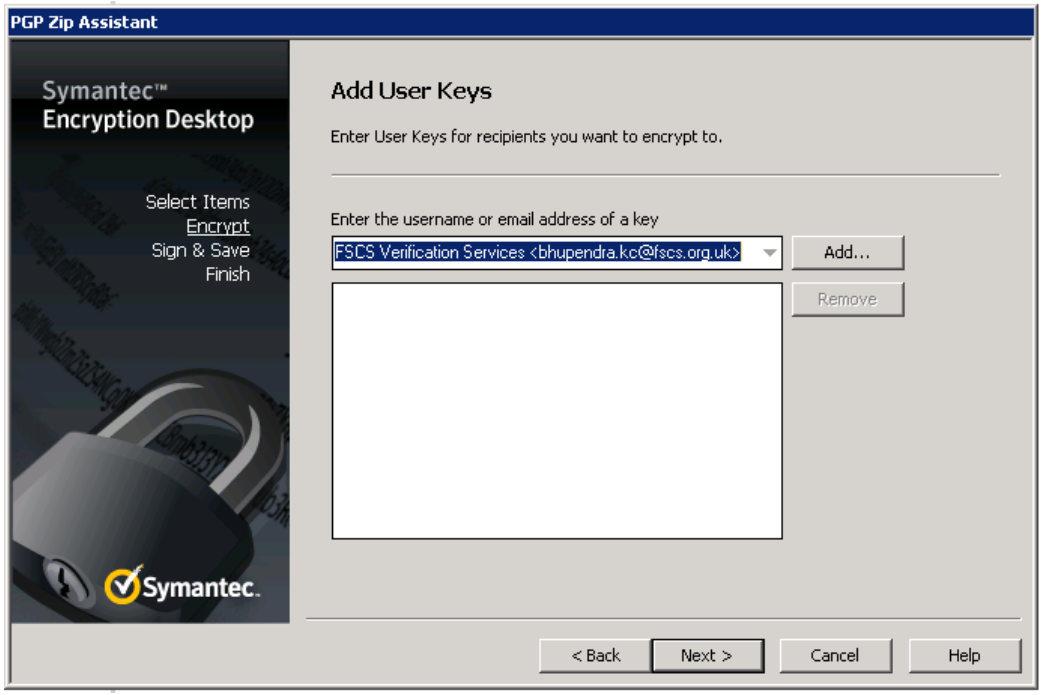


- Click on Advanced Options and select “Output Text”.



- Choose “Recipient Keys” and click “Next >”.

- Select FSCS’s public key from the dropdown list and click “Add”, then click “Next”, and finally click “Finish” in the step that follows.



3. Submit your SCV file to FSCS:

    - Refer to FSCS SCV Guide and FSCS Verification Services Web Portal User Manual for guidance on the SCV submission process.