

SIX Financial Information

# Manual

Step by Step instructions to implement SSH Key

Cavallin, Maurizio  
5-21-2024

## Contents

Why you need this guidance .....	2
Prerequisite to be able to up- and download files .....	2
SFTP Addresses to use .....	3
Creation of the private and public keys .....	4
Uploading the public key .....	5
How to connect.....	6
DataHub suppliers' migration.....	7

# GUIDANCE HOW TO MIGRATE TO SSH-KEY

## Why you need this guidance

As we have informed you, we will change the security behavior. This will affect the way you transfer files to and from our servers. The current login credentials will no longer work. You will need to use SSH-keys for secure authentication and SFTP for secure file transfer.

This document provides you with the essential instructions and details for performing the migration.

## Prerequisite to be able to up- and download files

SIX is using state of the art algorithms. Please make sure that your SFTP-Client software will handle

A. To connect to the SIX-FTS platform please use this encryption algorithms:

- aes128-ctr
- aes192-ctr
- aes256-ctr
- aes128-gcm
- aes256-gcm

B. For the SFTP key exchange you need one of the following algorithms:

- diffie-hellman-group-exchange-sha256
- diffie-hellman-group15-sha512
- diffie-hellman-group16-sha512
- diffie-hellman-group18-sha512
- rsa2048-sha256
- ecdh-sha2-nistp384

## SFTP Addresses to use

With the new connection, you need to change the FTP/SFTP addresses to the new one. On the table you will find the correspondent new one:

	<b>Environment</b>	<b>Connect via</b>	<b>Address / Port</b>
Old	Production	Internet	s/ftpreghub.six-financial-information.com / 22/21
New	Production	Internet	fts-prod.six-group.com / 22
Old	Production	P2P	s/ftpreghub.p2p.six-financial-information.com / 22/21
New	Production	P2P	fts-prod.p2p.six-group.com / 22
Old	Production	FIP	s/ftpreghub.fip.six-financial-information.com / 22/21
New	Production	FIP	fts-prod.six.ssfm.ch / 22
Old	Quality Assurance	Internet	s/ftpreghubint.six-financial-information.com / 22/21
New	Quality Assurance	Internet	fts-qa.six-group.com / 22
Old	Quality Assurance	P2P	s/ftpreghubint.p2p.six-financial-information.com / 22/21
New	Quality Assurance	P2P	fts-qa.p2p.six-group.com / 22
Old	Quality Assurance	FIP	s/ftpreghubint.fip.six-financial-information.com / 22/21
New	Quality Assurance	FIP	fts-qa.six.ssfm.ch / 22

## Creation of the private and public keys

There are several way/tools to create private and public keys for the SSH protocol, and it will depend on the format you need to use.

In our example we use the common way of generating these keys- we will use openssh utility `ssh-keygen`.

To create an RSA key pair with no passphrase and **4096** bits length the syntax is:

```
ssh-keygen -b 4096 -f <filename> -t rsa -C <comment> -q -N ""
```

Here's what each part of the command means:

**-b 4096**: This specifies the number of bits in the key. The more bits, the more secure the key, but the harder it will be to crack. **4096** is a good balance between security and performance.

**-f <filename>**: This specifies the filename of the key.

**-t rsa**: This specifies the type of key to create. In this case, we're creating an RSA key.

**-C <comment>**: This allows you to add a comment to the key. This can be useful for identifying the key later.

**-q**: This option silences `ssh-keygen`.

**-N ""**: This option sets the passphrase for the key to an empty string, meaning there is no passphrase.

For example, if you want to create a key pair for a client named "**sixfts**", you would use the following command:

```
ssh-keygen -b 4096 -f sixfts.key -t rsa -C key@sixfts -q -N ""
```

This would create two file (file name are example):

- **sixfts.key**: this is the private key to be used from client side to establish a connection.
- **sixfts.key.pub**: this is the public key that must be sent to SIX.

How to upload the key will described in the next chapter.

## Uploading the public key

This step is needed to import the key into the SIX-FTS platform. Only then we are able to guarantee the access to our applications.

Step one: use your https credentials to

Login via internet: <https://portal.six-group.com> or if you still use the finance IP NET then

Login via FIP: <https://portal.fip.six-group.com> or if you have changed to SSFN then

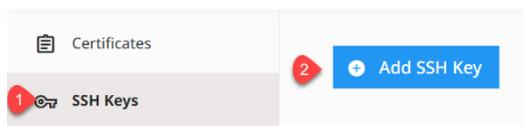
Login via SSFN: <https://portal.six.sfn.ch>.

Step two: were to upload the SSH-Key

After logged in, you will need to choose the certificate application.

Klick on the field named "Cerificates"

Certificates



1. Choose it for the SSH Key
2. For the first time it will show this field to add a new key

A screenshot of the 'Add SSH Key' form. It has two main input fields: 'Description\*' and 'SSH Key\*'. The 'Description\*' field contains the placeholder text 'Description of the SSH Key' and is marked with a red circle and the number '1'. The 'SSH Key\*' field contains the placeholder text 'Paste your SSH Key here' and is marked with a red circle and the number '2'. At the bottom, there are 'Cancel' and 'Add' buttons, with the 'Add' button marked with a red circle and the number '3'.

1. Give a description what kind of key it would be
2. Copy the content of the public key into this field
3. and when finished click on Add.

A screenshot of the 'Add SSH Key' form, now filled out. The 'Description\*' field contains the text 'Test'. The 'SSH Key\*' field contains a long string of text representing a public key, starting with 'ssh-rsa' and ending with 'Fhn2/eEDjx/shLMn2COXp/QP4yV0GavWlpgcFgKfFtsSjPcr00GyU9c96zinye'. The 'Add' button is highlighted with a blue background.

Here is an example of how it could look like:

The following screen will show up if everything went well. :

1 out of 10 SSH Keys available				
Description	Status	User ID	Creation date	Comment
My Key <b>1</b>	Active <b>2</b>	CH12345-techuser <b>3</b>	26 Mar 2024 15:29 <b>4</b>	key@sixfts <b>5</b>

- (1) The description given in the step bevor.
- (2) Certificate status in this case Active.
- (3) The credential of the user where will use the SSH-key.
- (4) The date when this SSH-key was uploaded.
- (5) It shows the comment, when created the SSH-key.

## How to connect

This chapter explains how to establish and verify a connection between your machine and ours. We use command line examples to illustrate the steps:

```
sftp -i <path to private key> -P <port> <user name>@<host name>
```

**-I <path to private key>** : This is the path were you have stored the private key, including the key.

**-P <port>** : We use the standard SFTP port 22

**<user name>** :These are your credentials of the technical user

**<host name>** : The host is depending on which way you log in, please see table with the new URLs on page 3.

Here is an example of how it could look like:

```
sftp -i c:\mykeys\sixfts.key -P 22 CH12345-techuser@fts-prod.six-group.com
```

If the interaction is different, please check the connection by activating the verbose mode in order to debug with adding the **-v** flag before the **-i**.

```
sftp -v -i c:\mykeys\sixfts.key -P 22 CH12345-techuser@fts-prod.six-group.com
```

## DataHub suppliers' migration

Once connected to SIX FTS, files need to be uploaded to the following folder:

Environment	Destination Folder
<b>Production</b>	reghub_delivery
<b>Quality Assurance</b>	reghub_delivery_qa

Always use the folder specified above. Files put in different folders will not be processed by DataHub.

### Note

Do not upload files directly to the root folder of SIX FTS (without changing to the upload directly mentioned above). This is a shared folder and files will not be forwarded and processed by DataHub. Please contact SIX support in case there are technical issues with uploading files to the correct folder.

Uploaded files remain in DataHub upload folder, even if the file is processed by DataHub. Old files will be deleted automatically after a certain time period. There is no need to archive or delete files from the supplier side.



Please feel free to reach out if you need further assistance or clarification!

Via phone please call your local Customer Support, contact details can be found here:

**<https://www.six-group.com/en/contacts/financial-information.html>**.

Or send us your request/question via email to: **[support@six-group.com](mailto:support@six-group.com)**