BANK OF ENGLAND

Sterling Money Market Data Collection: Technical instructions for the transmission of form SMMD

Version 5.0

February 2017

Contents page

Document version and change control

Version no.	Date applicable	Change log
1.0	1 July 2016	Initial publication.
2.0	18 August 2016	Clarified IP requirements for address whitelisting. Clarified TCP Port requirements. Updated to include further details on submission via an SFTP client tool.
3.0	12th September 2016	Added further information on MFT response files to Annex 1. Added Annex 2 – MFT response file naming conventions. Added Annex 3 – MFT minimum testing requirements.
4.0	20th January 2017	Corrections to MFT file paths Additional notes on error handling
5.0	9th February 2017	Clarification of domain and LEI mapping in relation to MFT account email addresses.

1. Introduction

In order to secure and improve the information available to it on conditions in sterling money markets, the Bank of England collects money market data from banks, building societies and major investment firms on their secured and unsecured sterling money market activity*. Part of this process is the transmission of data from firms to the Bank and also the return of status and data quality information back to the firms for notification purposes and for continuous improvement.

This document explains how to implement machine to machine based transfers of files to the Bank of England using the SFTP transfer protocol and retrieval of response files from the Bank of England. It also documents how security will work within the platform and the file system structure of the platform from an end user perspective. The same basic process will be valid for both secured and unsecured transaction submissions.

This document does not include details on the use of the interactive HTTPS portal. The Bank will provide further information on the timeframe for the implementation of this functionality during H1 2017.

*For further details please refer to the Sterling Money Market Data Collection Reporting Instructions which can be found on our web site:

http://www.bankofengland.co.uk/statistics/Documents/reporters/defs/instructions_smmd_combined.zip

2. Transfer Process

In its simplest form the sending system will create an SFTP connection to the Bank of England transfer server, using a username, password and key for authentication. Once an authenticated connection is established a file can either be sent to the server using an SFTP PUT or received from the server using an SFTP GET.

2.1. Sending files

Automated submissions must be carried out via SFTP using two factor authentication based on firm generated public keys which will need to be generated and supplied to the Bank of England based on SSH-2-RSA SSH-2-DSA standards with 2048 Bit key length. A username / password combination will also be required.

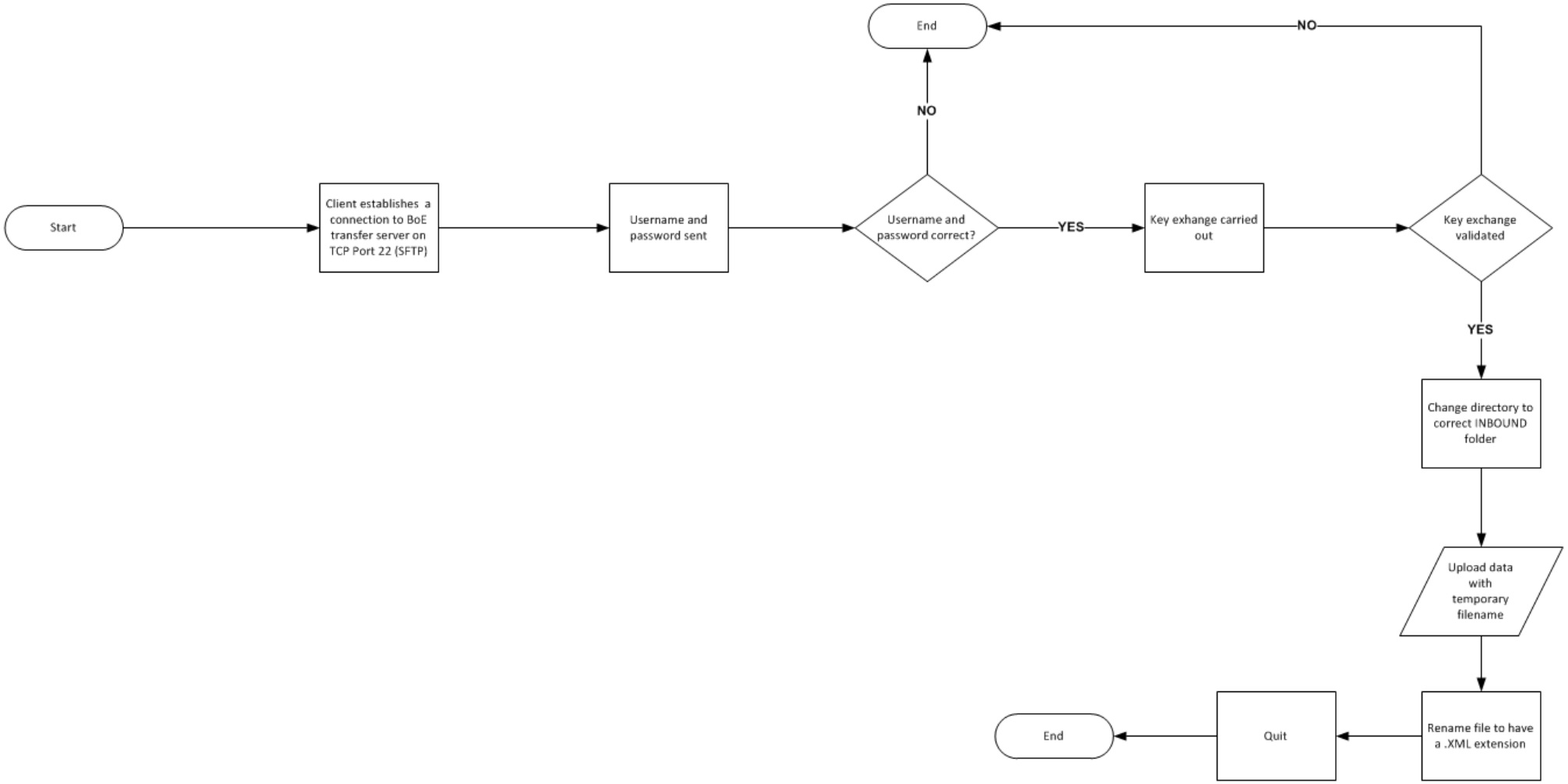
For each submission type, Secured and Unsecured, there will be a unique account which must be used for the correct type of submission. When uploading a file it must be placed in the INBOUND folder on the SFTP server.

In order to ensure that an upload is completed the file should be uploaded with a temporary extension (.TMP or .PART) and renamed to a .XML extension after the upload is complete. Only .XML files will be processed and using this method ensures all data is sent before the processing of the file commences. Files that do not have the extensions .XML, .PART or .TMP will be automatically deleted if they are uploaded.

The file will be removed from the INBOUND folder when it is processed. It is not possible for the submitting firm to retrieve or delete files from the INBOUND folder once they have been uploaded.

Please note that the INBOUND folder is a virtual path, the underlying folder structure is related to the account used for login and determines whether the file is processed as an unsecured or secured instrument submission.

2.2. File submission workflow

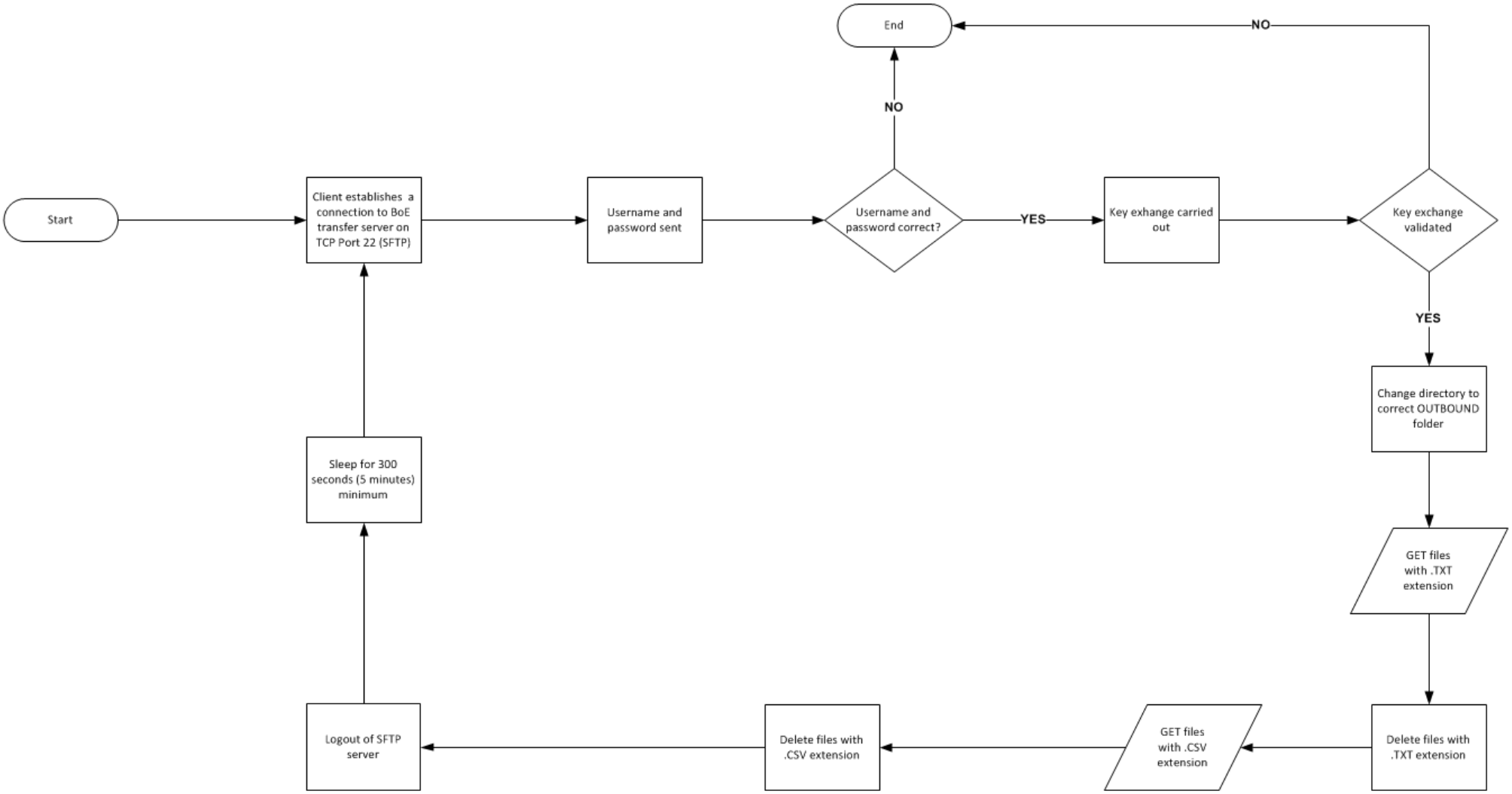


2.3. Receiving files

Responses from the Bank of England to a firm will be available by the same transport method. Response files will be posted to an OUTBOUND folder for collection over SFTP. It is the responsibility of the firm to collect response files and the Bank of England recommends the firm deletes the file after collecting it. For security reasons this folder will be purged daily of files more than seven days old.

The Bank of England will also continue to send responses by secure email to named contacts in the same manner as occurs for email submissions.

2.4. Response retrieval workflow



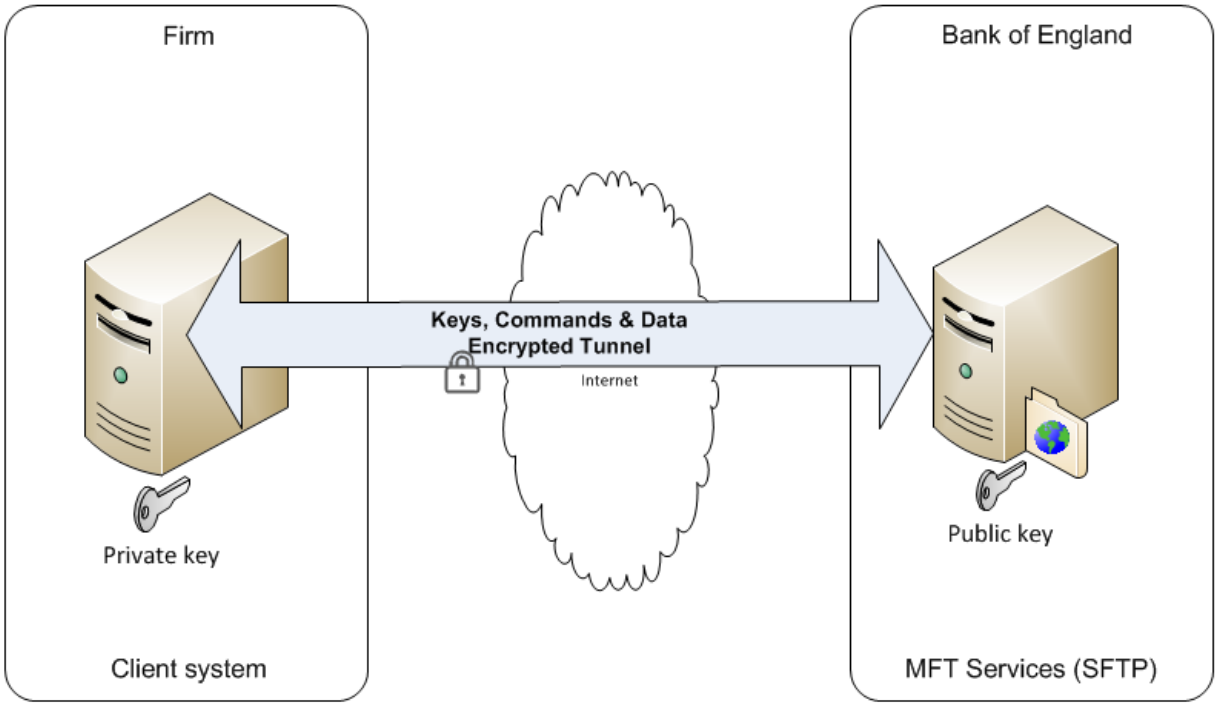
3. Security

In order to give the highest level of protection to any data all files will be encrypted in transit and not decrypted until they are within Bank controlled infrastructure. At this point files will be scanned for malware and automatically rejected and destroyed if found to be present. An email notification will be sent back to the sending system if any form of malware is discovered.

Each submission type will require a unique username, password and public/private key pair with the private key also being protected by the firm internally using a passphrase. The generated public /private key pair needs to be either the SSH-2-RSA or the SSH-2-DSA standard with 2048-bit key length.

Machine generated passwords will be emailed via secure email to the addresses supplied to the Bank of England as part of the on-boarding process. The email addresses supplied must be unique and must be able to receive inbound email by one of the following secured methods (TLS, PGP, PGP Web Messenger).

3.1. The connection security model



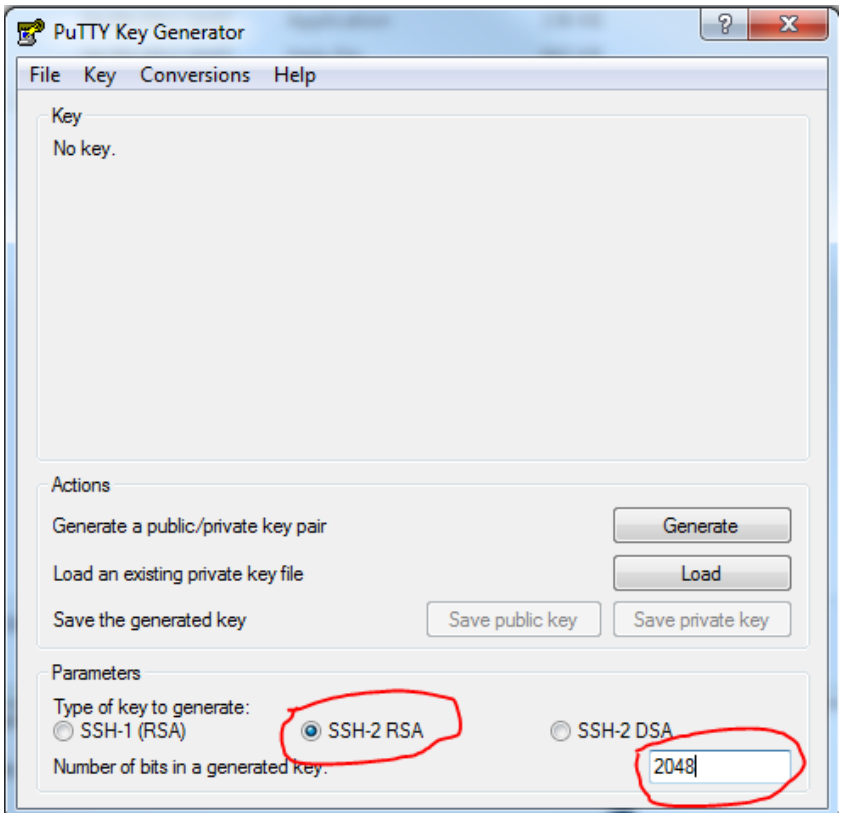
4. Generating public / private key pairs

Key generation mechanisms will differ depending on the software platform used by firms to carry out transfers. The example below uses the open source PuTTygen utility to act as guidance. The Bank of England is not endorsing the use of this specific tool. The pertinent factor is that the key must be of the type SSH-2-RSA or SSH-2-DSA with a 2048-bit key length.

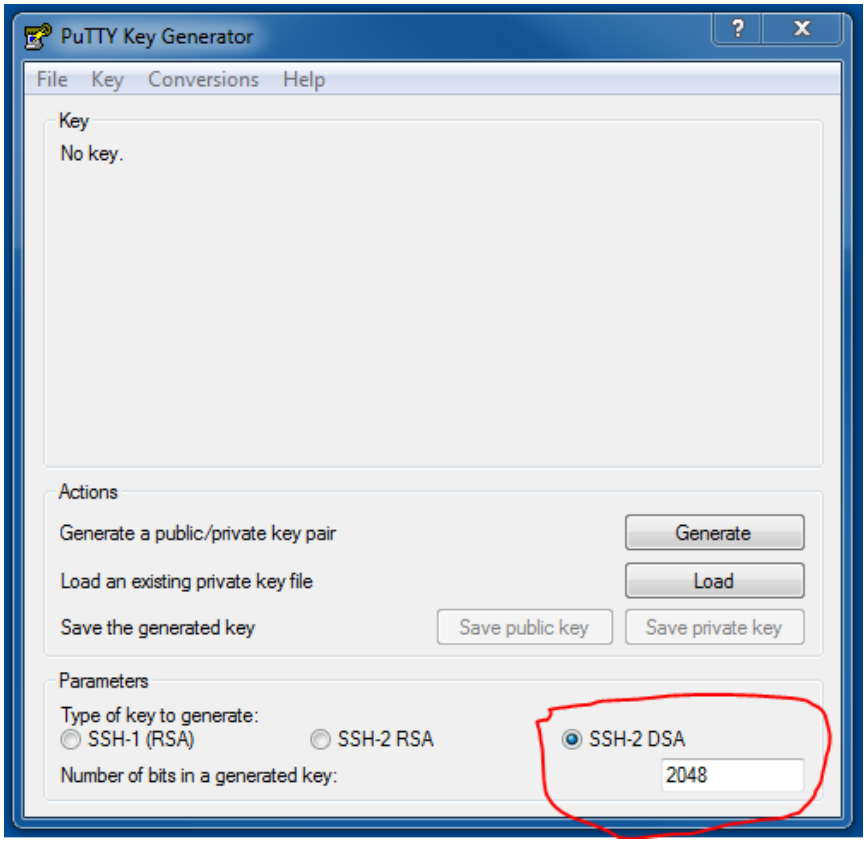
4.1. Generating a public/private key pair

The following steps allow you to generate a public/private key pair.

1. Start Puttygen and update the key type and the key length to be one of those highlighted in the next two screenshots.

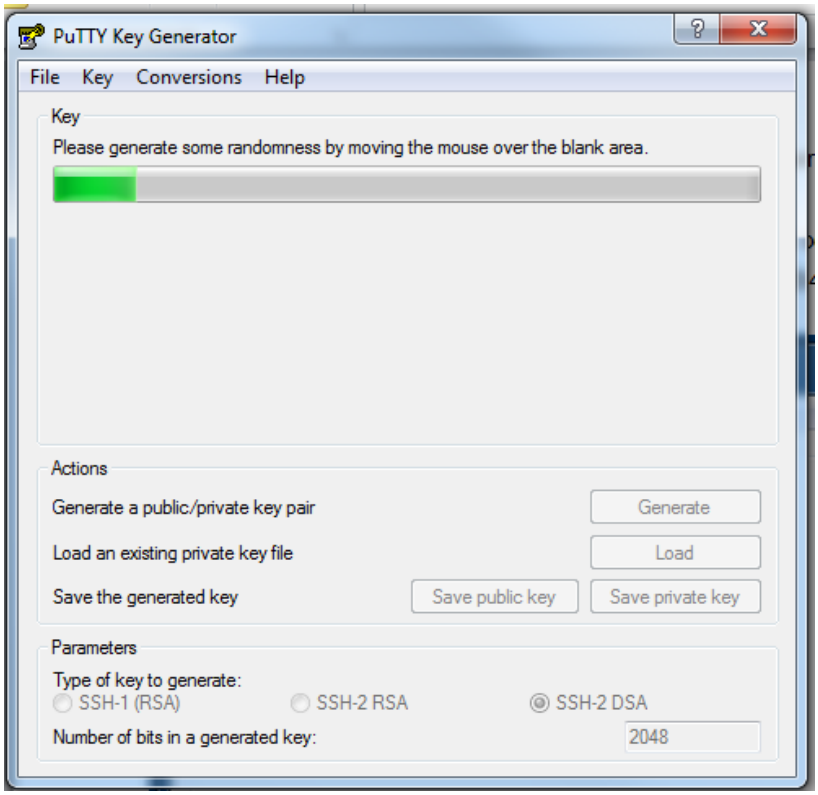


Key type = SSH-2-RSA, number of bits in generated key = 2048

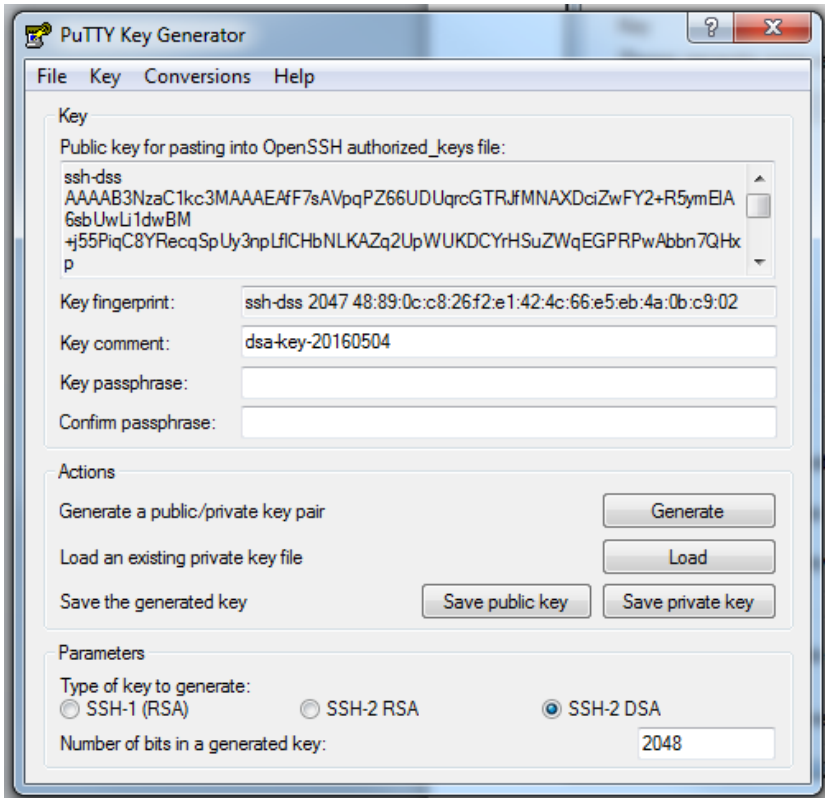


Key type = SSH-2-DSA, number of bits in generated key = 2048

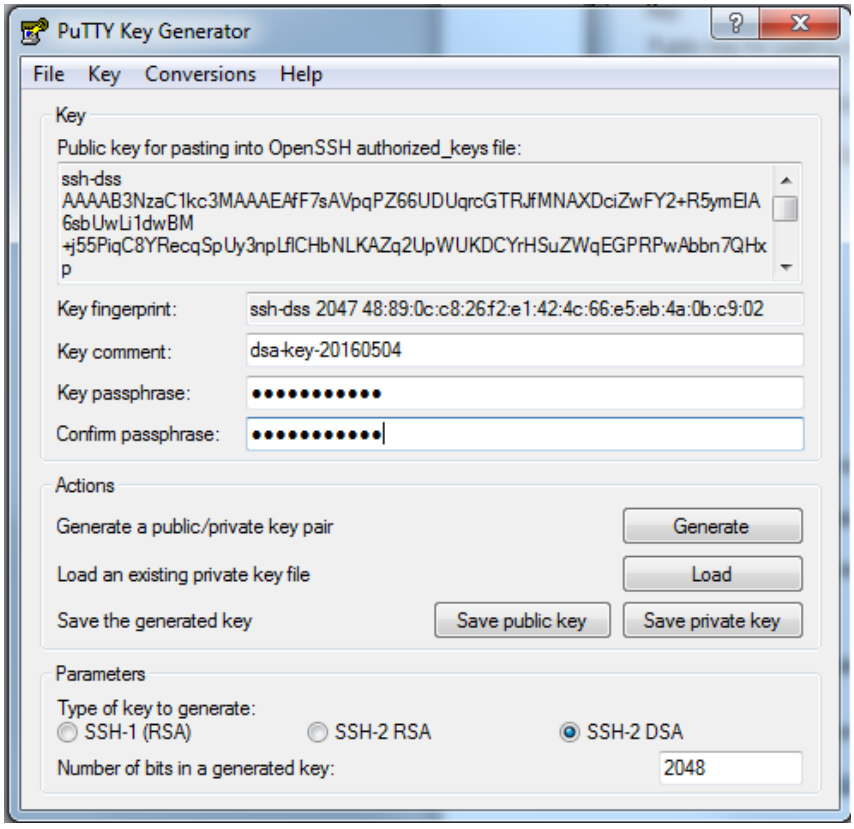
2. Click the 'Generate' button.



3. Move the mouse over the blank area to produce a random key.



4. Add a passphrase (which will also need to be stored safely by the firm for later use in transmissions).



5. Save the public key with the naming convention **Submission_type_environment_firm_name.key** , for example for unsecured submissions into UAT for reporting institution X the filename would be **unsecured_UAT_Institution_X.key** the equivalent name for a production key would be **unsecured_PROD_ Institution_X.key** .
6. Save the private key with the naming convention **Submission_type_environment_ Institution _name.ppk** , for example for unsecured submissions for firm X into UAT the filename would be **unsecured_UAT Institution _X.ppk** . It is the responsibility of the firm to ensure their keys are stored securely and only used for the transmission of files for the purpose intended.

At this point the key pair has been generated and you can exit PuTTygen.

4.2. Supplying public keys to the Bank of England

Public keys should be sent to the Bank of England over secure email. The email address to send them to is SMM_KEYS@bankofengland.co.uk .

Ideally keys should be sent from the “system” email address that will be making submissions (to confirm the email address) although this is not a compulsory requirement.

5. System connection information

There are two entirely independent points of entry, one for UAT and certification purposes and the other for the LIVE system. The host names for the two systems are as follows:

Environment	Hostname	Public IP Address
UAT	Transferuat.bankofengland.co.uk	194.61.186.43
LIVE production	Transfer.bankofengland.co.uk	194.61.186.42

Accounts must be different for UAT and LIVE with separate public keys. Usernames and email addresses should also be unique between secured and un-secured submission types as well as environments.

All SFTP connections will be on the default SFTP TCP Port, 22.

6. Details required to setup accounts

The following tables will need to be completed and submitted to the Bank of England along with the public keys of the submitting firms. This form should then be returned with the correct public keys to smm_keys@bankofengland.co.uk . Firms will then be informed of the correct usernames and password via secure email.

6.1. Users

Each environment and submission type should have a unique user email address:

Environment	Submission type	Email address
UAT	Secured	
UAT	Un-secured	
LIVE	Secured	
LIVE	Un-Secured	

Note:

Where a firm is submitting files via MFT for both secured and un-secured submissions using the same organisation Legal Entity Identifier (LEI) the domain name associated with the email addresses must be the same for both secured and un-secured systems .

6.2. IP Addresses

Public facing IP addresses are required for whitelisting purposes. These should be static IP addresses and should include addresses for business continuity as well as normal running. A maximum of four addresses are allowed per system.

Environment	Submission type	IP Addresses
UAT	Secured	
UAT	Un-secured	
LIVE	Secured	
LIVE	Un-Secured	

Any IP addresses supplied must be specific host addresses and not ranges or subnets. Any attempt to request the whitelisting of an IP range with a mask will be rejected.

7. Sample SFTP command scripts

The sample scripts below are based on use of the open source WINSCP utility and are for example purposes only. The Bank of England does not endorse any specific product that must be used to carry out the transfer, it may be delivered via a firms in-house development or utilise one of many commercially available SFTP clients or managed file transfer solutions.

Good development practices recommend that any hostname, paths and usernames are parameterised configurable values in case of future change. Password and passphrases should be stored in an encrypted form where practical.

7.1. Sending files

7.1.1. Unsecured trade submission

The example below would be used for uploading a submission for an UNSECURED return (please watch out for word wrapping):

```
open SFTP://unsecured_firm_user:password@transfer.bankofengland.co.uk/ -privatekey="
un_secured_firm_user_priv_key.ppk "

cd /INBOUND

put my_submission_file.part

mv my_submission_file.part my_submission_file.xml

exit
```

The actions occurring in the above script are as follows:

1. Open connection to server and login passing private key
2. Change to the correct inbound directory
3. Upload your file with a .PART extension
4. Rename the uploaded .PART file to a .XML file
5. Exit closing the connection

7.1.2. Secured trade submission

The example below would be used for uploading a submission for a SECURED return (please watch out for word wrapping):

```
open SFTP://secured_firm_user:password@transfer.bankofengland.co.uk/ -
privatekey="secured_firm_user_priv_key.ppk"

cd /INBOUND

put my_submission_file.part
```

```
mv my_submission_file.part my_submission_file.xml

exit
```

The actions occurring in the above script are the same as those used to submit an unsecured trade file in section 7.1.1 apart from the change to the username and keyfile.

7.2. Receiving files

7.2.1. Receiving unsecured submission responses

The example below would be used for receiving response files for UNSECURED submissions (be aware of word wrapping).

```
open SFTP://unsecured_firm_user:password@transfer.bankofengland.co.uk/ -privatekey="
un_secured_firm_user_priv_key.ppk "

cd /OUTBOUND

get –delete *.txt  \local_path_to_store_files\

get –delete *.csv  \local_path_to_store_files\

exit
```

The actions occurring in the above script are as follows:

1. Open connection to server and login passing private key
2. Change to the correct outbound directory
3. Get text files from the inbound directory and delete them after retrieval (equivalent content to email notifications)
4. Get CSV files from the inbound directory and delete them after retrieval (error reports)
5. Exit closing the connection

7.2.2. Receiving secured submission responses

The example below would be used for receiving response files for SECURED submissions (watch out for word wrapping).

```
open SFTP://secured_firm_user:password@transfer.bankofengland.co.uk/ -privatekey="
secured_firm_user_priv_key.ppk "

cd /OUTBOUND

get –delete *.txt  \local_path_to_store_files\

get –delete *.csv  \local_path_to_store_files\

exit
```

The actions occurring in the above script are the same as those used to retrieve responses for an unsecured trade file in section 7.2.1 apart from the change to the username and keyfile.

8. Manual interaction downloads over SFTP

Should the event arise whereby a firm needs to carry out a manual transfer over the same protocol as used for machine to machine transfers it is possible to do this using an SFTP client that supports public / private key and password authentication.

If firms chooses to use this method they remain responsible for the protection of their own private keys and this should be handled in a secure manner. Also as whitelisting is to be used the connection should be from the same public IP addresses as used for the automated transfers.

Use of an SFTP client would offer similar functionality to the web based MFT portal.

This section of the document explains how to use an SFTP client to carry out transfers in an interactive manual basis in the same way as could be achieved through a portal but by using an SFTP client as an alternative mechanism. This documentation is based around the use of the open source WINSCP product however other software clients are available and it is not a specific software endorsement.

The content of this section is aimed at technical specialists to educate them in understanding the context of the solution and is not in itself a reference design to address the challenge.

8.1. Prerequisites

Before attempting to carry out any transfers via an SFTP client a firm will need to have first carried out the procedures to generate SSH keys and request accounts as described earlier in this document.

The accounts used by the SFTP client will be those requested as system accounts; no other specific user accounts will be allowed. The source IP of the SFTP client will need to be one of the ones supplied from the above account request process. The most appropriate way to do this would be to use source NAT addressing.

Any IP addresses supplied must be specific host addresses and not ranges or subnets. Any attempt to request the whitelisting of an IP range with a mask will be rejected.

You will need to have a copy of the private key generated using the earlier described process and must also know the passphrase of the certificate as well as the usernames and passwords supplied by the Bank of England.

Please note the security and protection of a reporting firm's private key and supplied user credentials remains the responsibility of the reporting firm at all times. It should be appropriately secured according to a reporting firm's own security policies relating to these types of accounts.

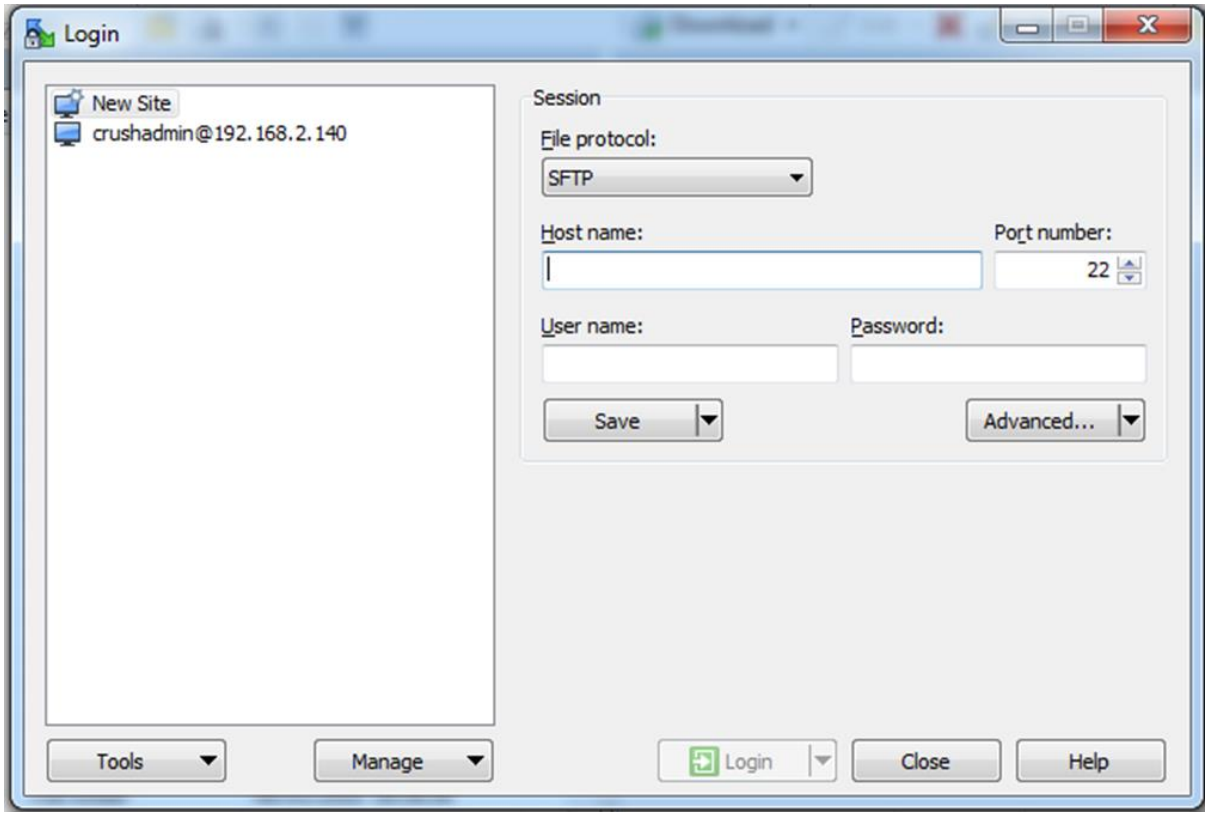
8.2. Configuring and using WINSCP

WINSCP is an open source FTP/S and SFTP client with both a graphical and command line interface. For the purposes of manual transfers by a user this document will only refer to the graphical interface and the use of SFTP.

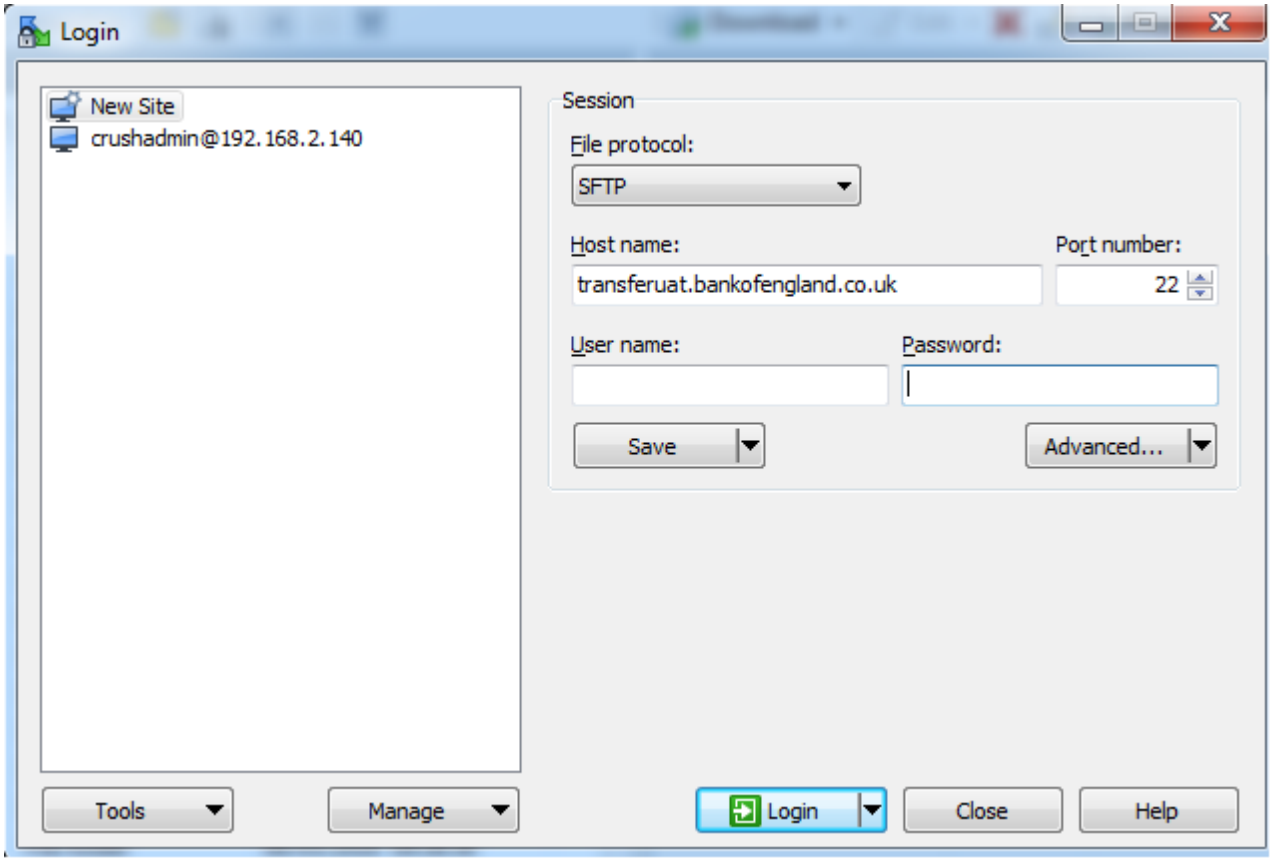
The following steps explain how to configure WINSCP with a pre-generated private SSH key and connect to the Bank of England MFT server after you have installed the WINSCP client according to your company's software policies.

Ensure that you have your pre-generated private key, passphrase, username and password to hand for this process.

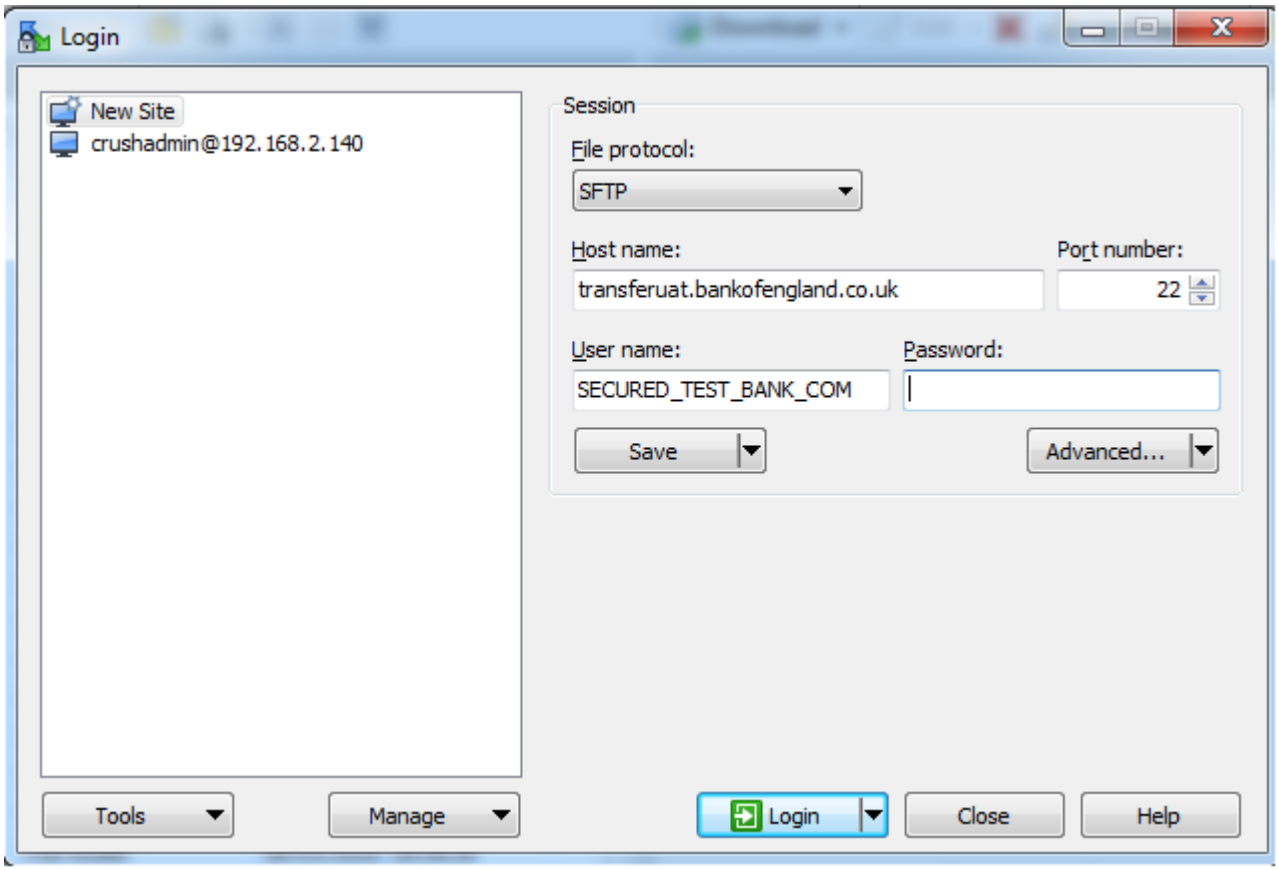
1. Start WINSCP and choose new site.



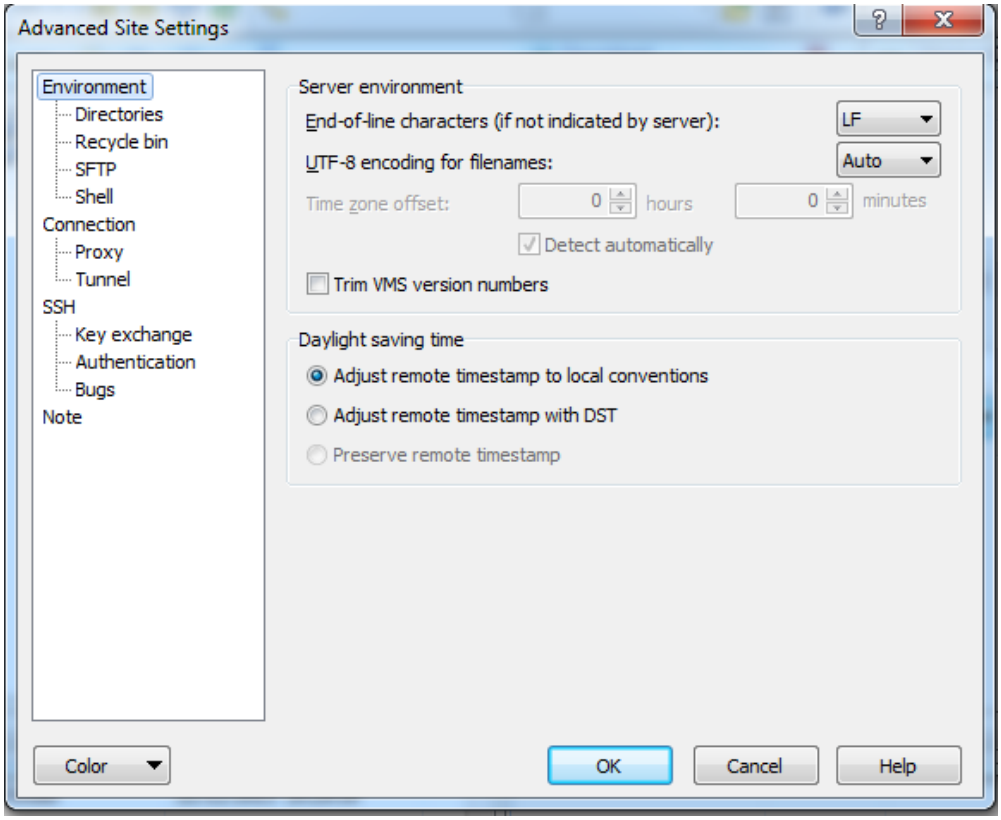
2. Add the name of the site you are connecting to in the hostname field (details of hostnames are in the system connection information section of this document).



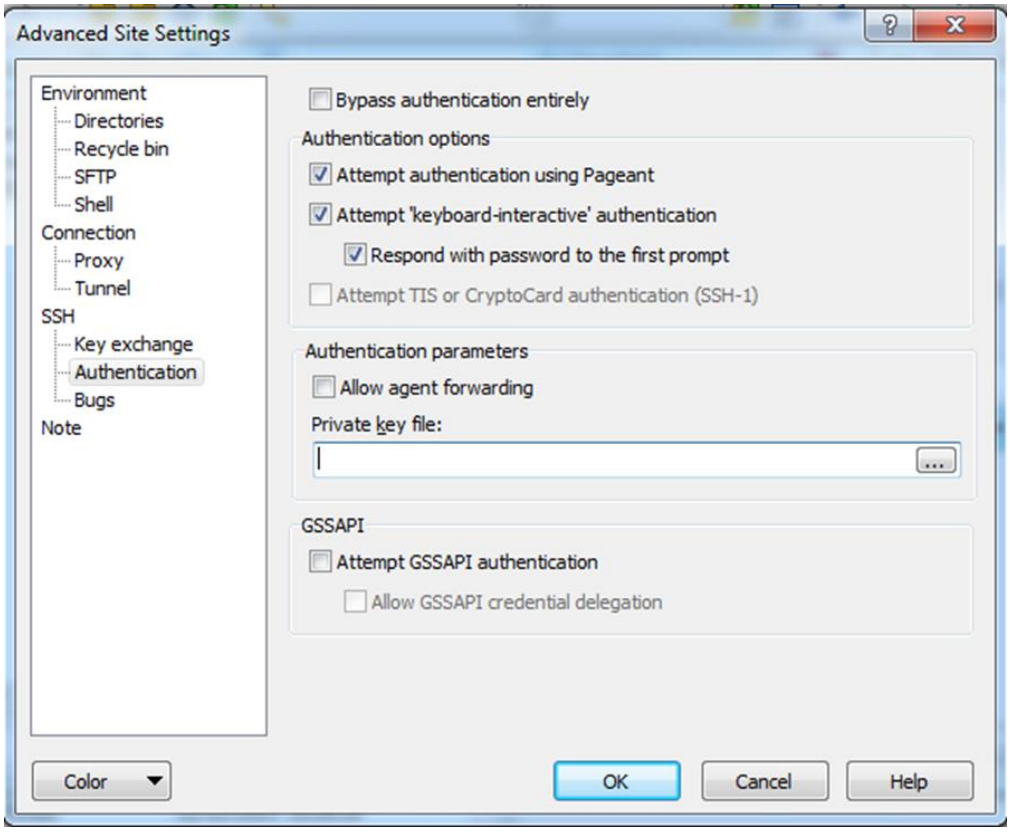
3. Ensure the file protocol is set to **SFTP** and the Port Number **22.**
4. Enter the supplied username of the system account into the username field.



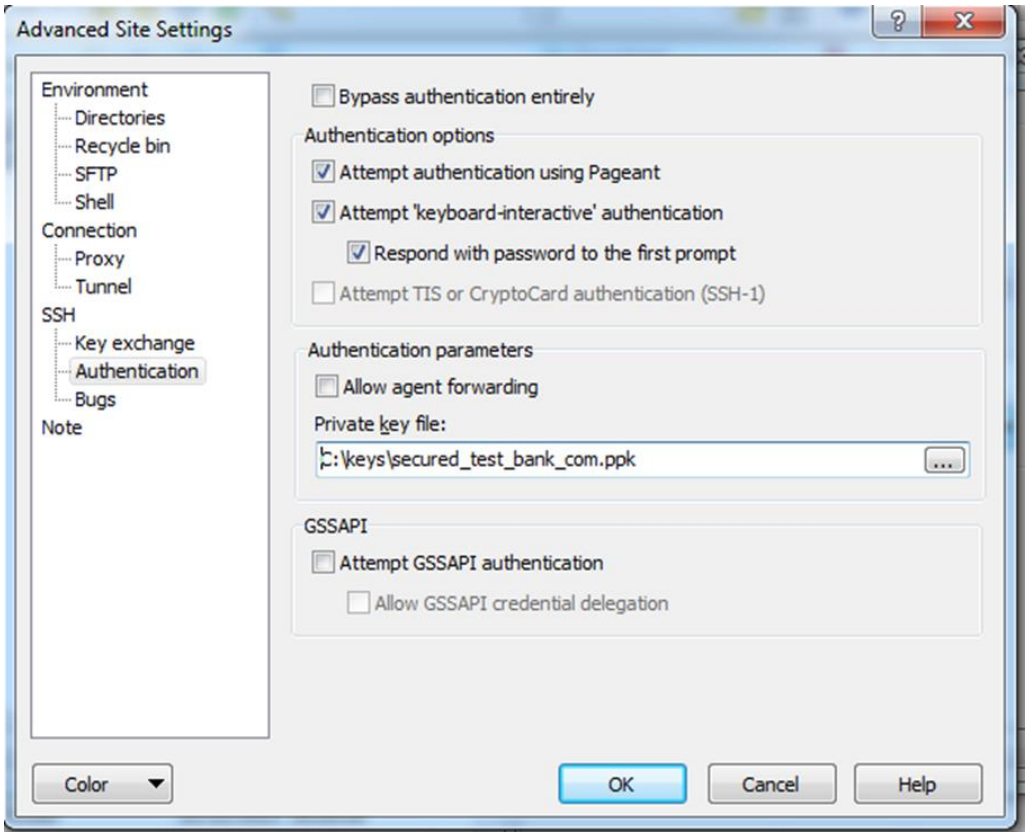
5. Click the **Advanced…..** Button.
6. You will be presented with the following screen.



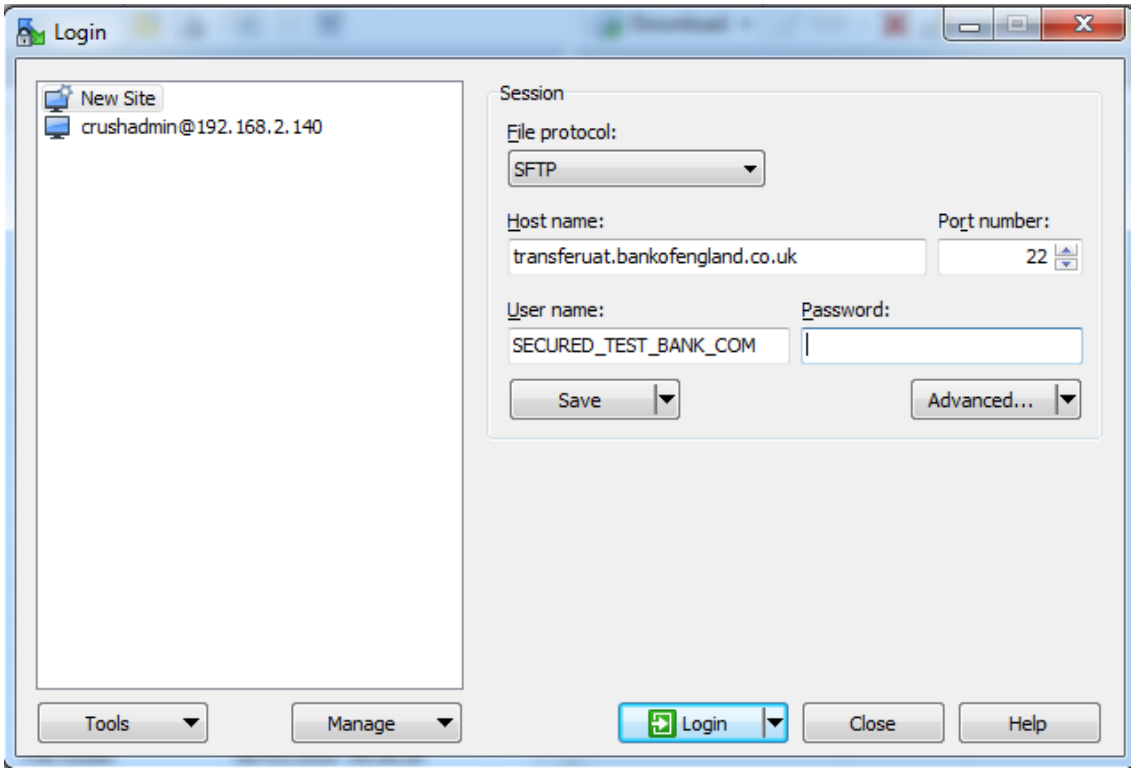
7. You need to select **Authentication** on the left hand menu.



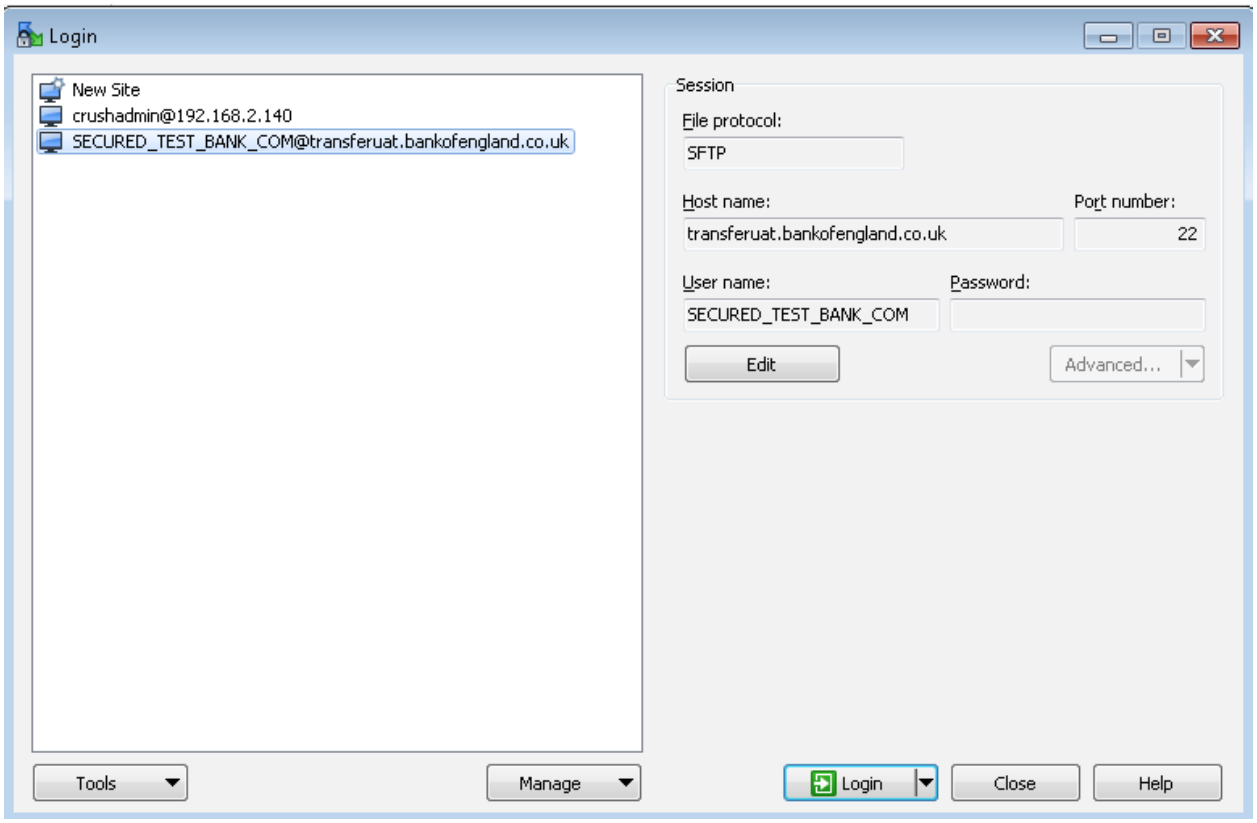
8. Browse to or type in the location of your **Private key File.**



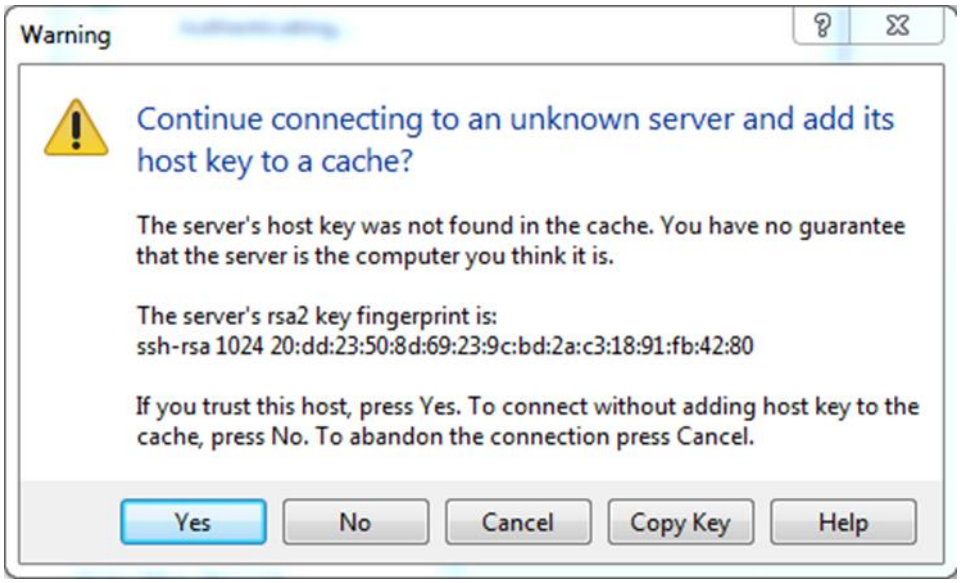
9. Click **OK** to return to the main screen.



10. Click **Save** in order to save the session settings for future use. Choose a name and it will appear in the left hand list.



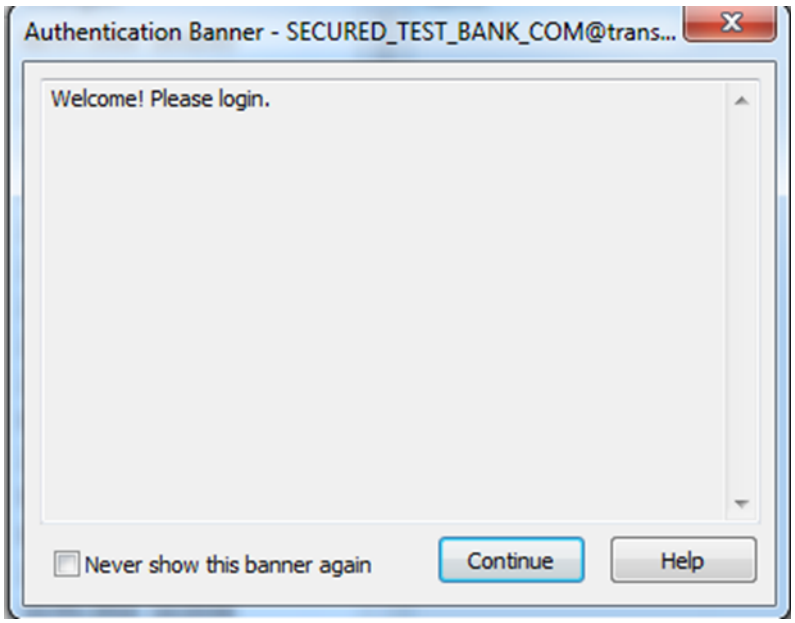
11. You have successfully created a saved session. It is now time to test the login.
12. Ensure that the correct session is loaded from the left hand menu (by clicking on it) then press the login button.
13. The first time you attempt to login you will receive a prompt regarding the remote hosts SSH footprint.



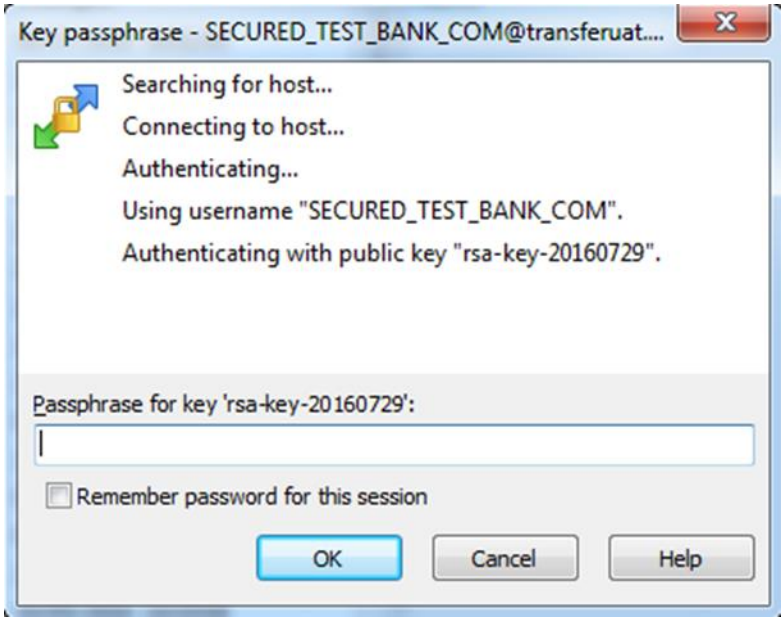
14. You will need to check this matches the “key fingerprint” that the Bank of England will supply to you.

Please note the above is an example and not the actual fingerprint.

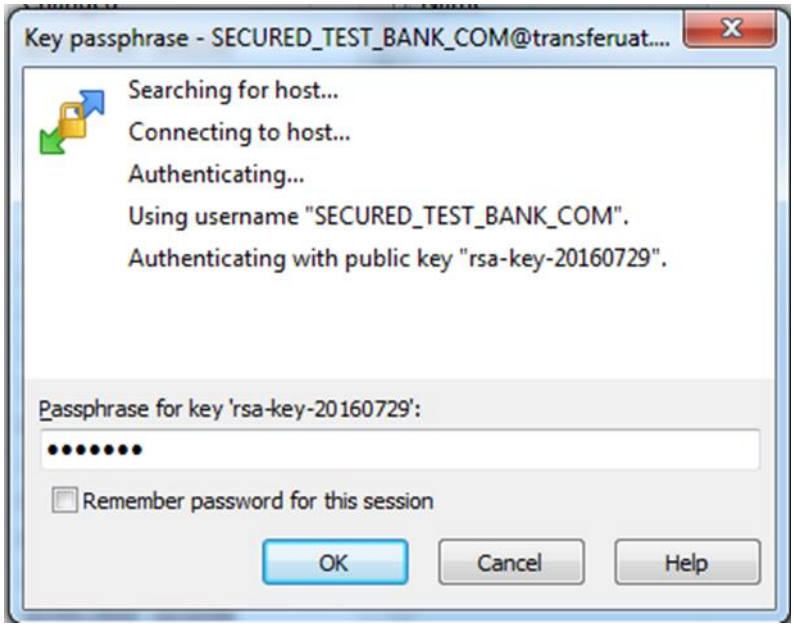
15. After confirming this you should click **Yes** to continue. A welcome banner will appear.



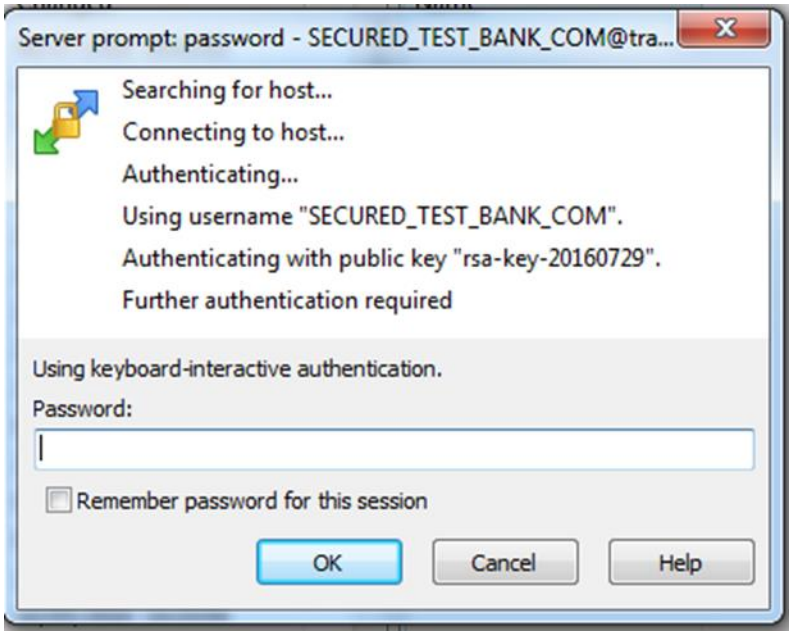
16. Click **Continue.**
17. You will now be prompted for the passphrase for your private key.



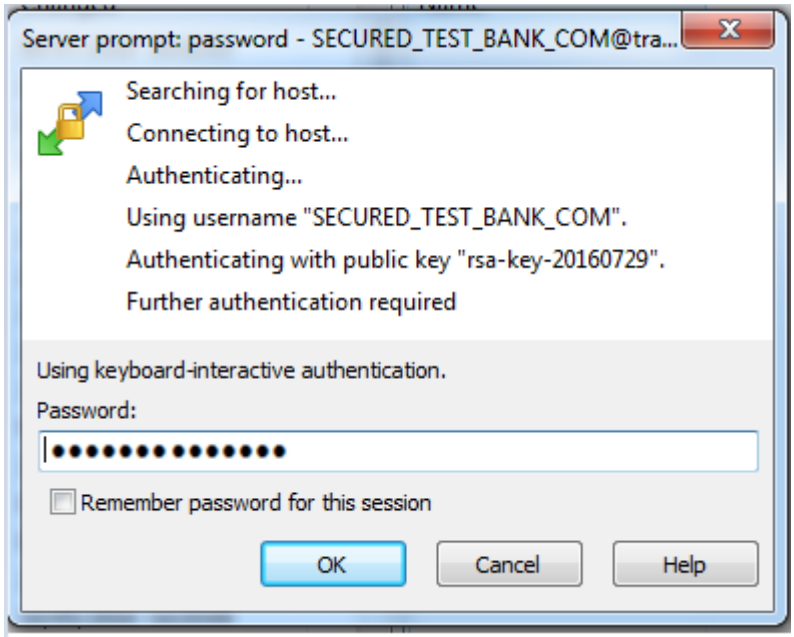
18. Enter the passphrase.



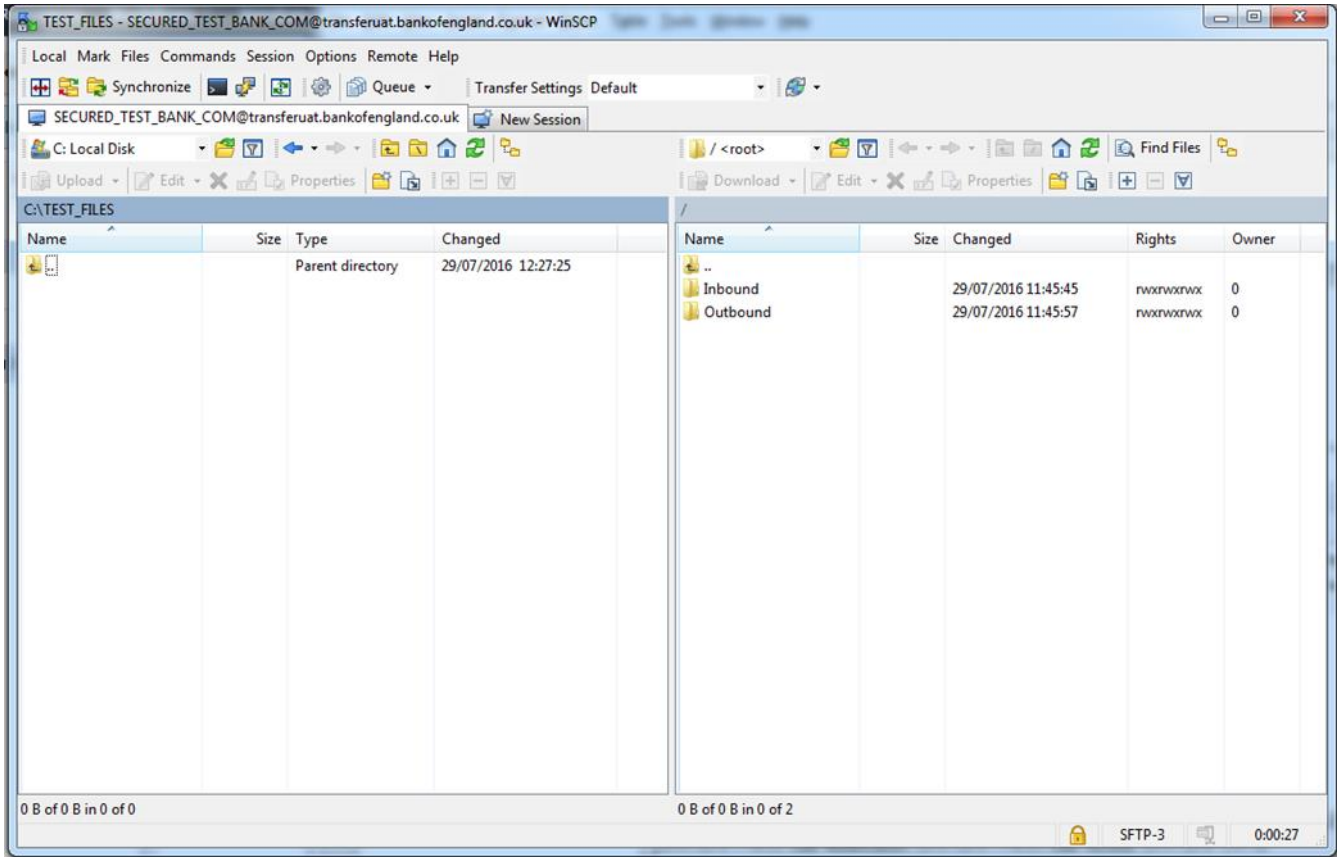
19. Click the **OK** button. For security reasons the Bank of England does not recommend setting the remember password for this session option.
20. You will now be prompted for a password.



21. Enter the password supplied to you for this account.

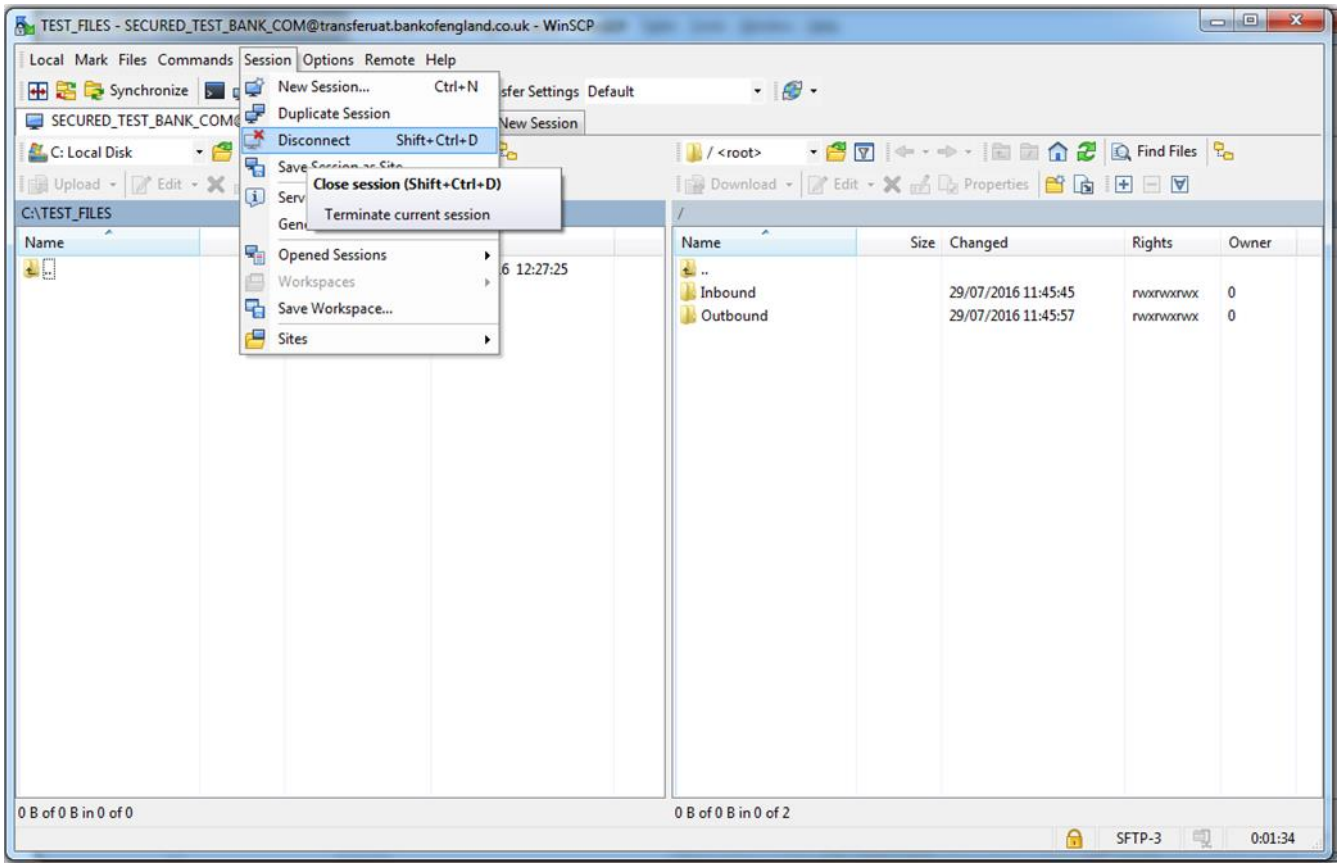


22. Click the **OK** button. For security reasons the Bank of England does not recommend setting the remember password for this session option.
23. If you have got all the credential information correct and the public key stored at the Bank of England pairs with your private key you will be logged in and presented with a GUI interface which works similar to windows explorer.



24. This explorer style window will allow you to drag files from your local resources to the folders on the right hand side located on the Bank of England MFT platform. Naming conventions, locations for files and the renaming process should be used as described earlier in the document.

25. Once you have finished you should log off from the Bank of England by going to **Session** on the top menu and choose **disconnect**.



Annex 1 Automated Submission Responses

An Excel spreadsheet is included within the zip file that compliments this document (http://www.bankofengland.co.uk/statistics/Documents/reporters/defs/instructions_smmd_combined.zip). The file sets out the various responses that are automatically generated by the Bank's internal systems. The name of the spreadsheet is NotificationsAndReponses.xlsx. Embedded within the Excel file are message files and CSV files containing examples of the responses.

Examples of the response files that will be supplied by the MFT platform are also available on the Bank of England website at:
http://www.bankofengland.co.uk/statistics/Documents/reporters/defs/instructions_smmd_combined.zip

Annex 2 MFT responses - file naming convention.

The Bank intend to embed metadata into the filenames of any response files in order for a reporting institute to easily identify what the file contains and which submission it refers to. The current naming convention is broken down into a number of components and is slightly different depending upon whether the submission is for secured or unsecured trades. Below is the pattern being used:

UnSecured_InstitutionDomainName_OriginalFileName_xml_**LoadFileSubmissionId_Checksum**.TXT
UnSecured_InstitutionDomainName_OriginalFileName_xml_**LoadFileSubmissionId_ValidationNotification**.TXT
UnSecured_InstitutionDomainName_OriginalFileName_xml_**LoadFileSubmissionId_ReportName**.CSV

Or

Secured_InstitutionDomainName_OriginalFileName_xml_**LoadFileSubmissionId_Checksum**.TXT
Secured_InstitutionDomainName_OriginalFileName_xml_**LoadFileSubmissionId_ValidationNotification**.TXT
Secured_InstitutionDomainName_OriginalFileName_xml_**LoadFileSubmissionId_ReportName**.CSV

In both cases *_ReportName can be of several variants

- **_XSD**
- **_Collateral.**
- **_Secured**
- **_Unsecured.**

Annex 3 MFT submissions – Recommended minimum test requirements.

The Bank of England proposes that each reporting institution carries out the following list of tests before self-certifying that they are ready to start sending SMM Daily submissions via the MFT platform.

The following tests should be carried out on the UAT platform:

A. Send 1 valid file of each type.
B. Send 1 invalid file of each type.
C. Ensure can pick up response files via email and MFT Outbound queue.
D. Check email route still works for them (e.g. switch between MFT / secure email…)

With the final test carried out against the LIVE platform:

A. Send a NOTX to live production environment

Annex 4 Errors and error handling

The table below gives description of the most common errors that may occur during an SFTP upload. It is expected that a firms submission system should be able to handle these errors and alert or recover in a clean manner.

Code	Name	Description	Comment
0	OK	Indicates successful completion of the operation.	
1	EOF	An attempt to read past the end-of-file was made; or, there are no more directory entries to return.	
2	No such file	A reference was made to a file which does not exist.	This may occur if an attempt to upload a malware infected file has occurred and the file has been deleted before a rename attempt
3	Permission denied	The user does not have sufficient permissions to perform the operation.	
4	Failure	An error occurred, but no specific error code exists to describe the failure. This error message should always have meaningful text in the the *error message* field.	
5	Bad message	A badly formatted packet or other SFTP protocol incompatibility was detected.	
6	No connection	There is no connection to the server. This error may be used locally, but must not be return by a server.	See note below on re-attempting uploads
7	Connection lost	The connection to the server was lost. This error may be used locally, but must not be return by a server.	See note below on re-attempting uploads
8	Operation unsupported	An attempted operation could not be completed by the server because the server does not support the operation. It may be returned by the server if the server does not implement an operation.	
9	Invalid handle	The handle value was invalid.	
10	No such path	The file path does not exist or is invalid.	This may occur if an attempt to upload a malware infected file has occurred and the file has been deleted before a rename attempt
11	File already exists	The file already exists.	

If a transmission fails and a firm needs to re-submit a partially uploaded file then the file will need to be re-submitted with a new filename. If this is not done then an error will be generated when the file overwrite is attempted.

Annex 5 Malware detection and removal

The Bank of England uses a number of malware detection and removal systems. In the event of detection of any form of malware content in a submission from an external party the entire file will be immediately quarantined for deletion. Furthermore alerts will be sent to the Bank of England security operations centre and the Chief data office informing them of the potential malware issue.

The Bank will act upon these alerts and contact the submitter regarding them. Repeated attempts to upload further malware will lead to the submitter account being disabled on the MFT platform.