USER GUIDE

Exchange files with an SFTP solution in My File Transfer

FEBRUARY 2025

Contents

Introduction

If you use an SFTP solution to exchange files with the Mastercard products Betalingsservice, Leverandørservice, Overførselsservice and Informationsservice, this user guide is for you.

The Nets system TeleService Internet (TSI) that you have previously used has been replaced by the Mastercard system My File Transfer.

Setting up your system for My File Transfer requires knowledge of both the SFTP solution and your company's technical setup. If you do not have this knowledge yourself, you can share this user guide with a colleague, systems vendor or IT consultant.

The security of the solution consists of the use of RSA security keys (private/public keys), which creates a secure exchange of files between your company and Mastercard's products.

If you have any questions or need help, please contact our support team on (+45) 8081 0679 on weekdays from 09:00 to 16:00. You can also find frequently asked questions and more information about My File Transfer and the SFTP solution on this website:
https://www.mastercardpaymentservices.com/denmark/my-file-transfer/sftp

The user guide will walk you through the following three steps to set up your company's system to exchange files with an SFTP solution in My File Transfer:

1. Connect to IP address and port
2. Accept new fingerprint
3. Manage your mailbox

This is followed by a section on how to generate new security keys, which you can do at any time, as needed. We recommend that you change your security keys every three years.

At the end of this user guide, you will find a section on how to get help and a section on rights and security.

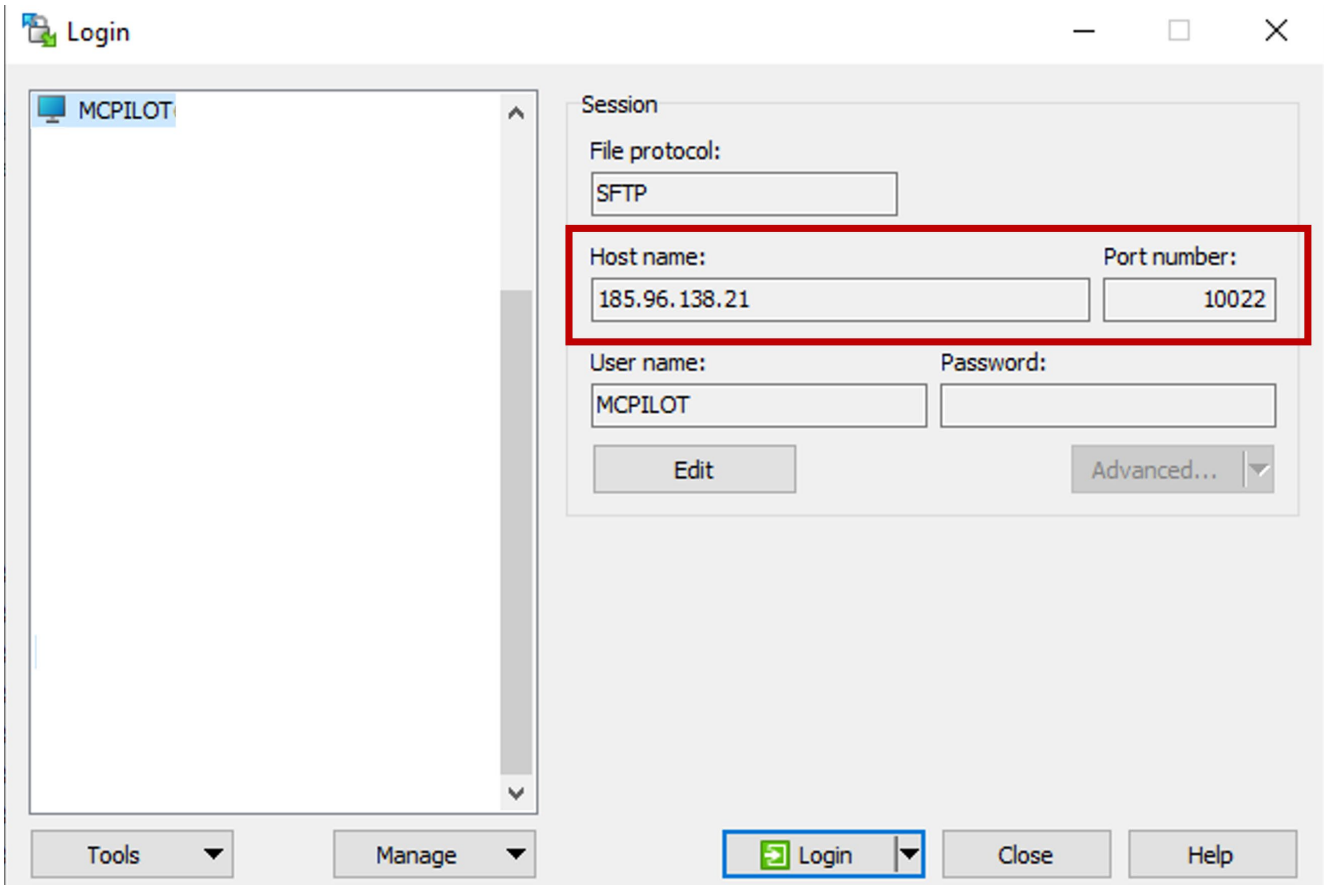
1. Connect to IP address and port

1.1 Open an SFTP client. In this user guide, we will use the WinSCP client. In the appendix of this user guide, you can see the requirements for the SFTP client.

1.2 Connect to IP address 185.96.138.21 on port number 10022. In the example below, we connect to the mailbox (UserID) "MCPILOT".

1.3 Click on '**Login**'.

Please note: Remember to ensure that the IP address is whitelisted in your system and that all relevant ports are open before connecting.

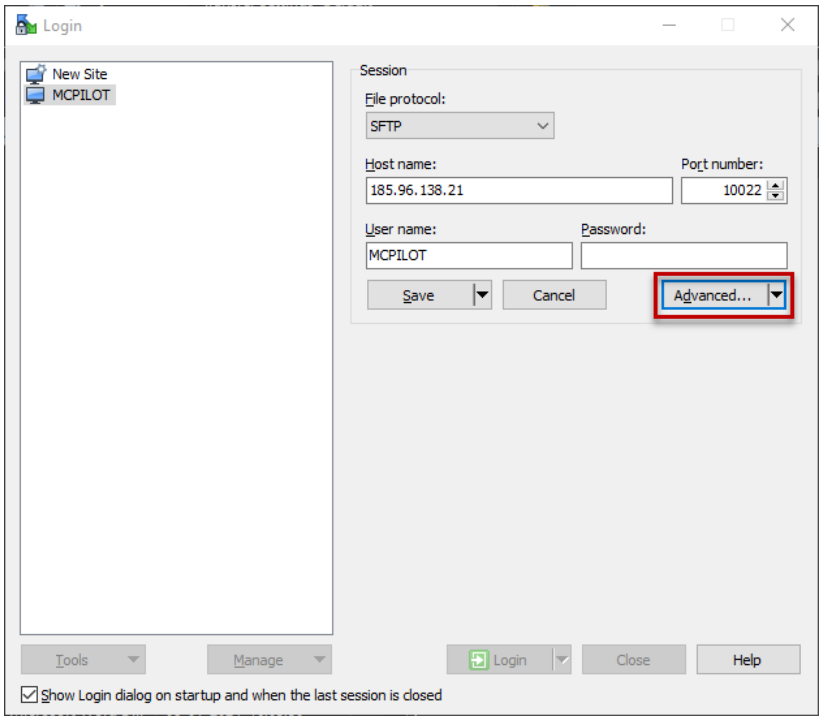


If you have not already done so, please remember to load your private key before you can log in.

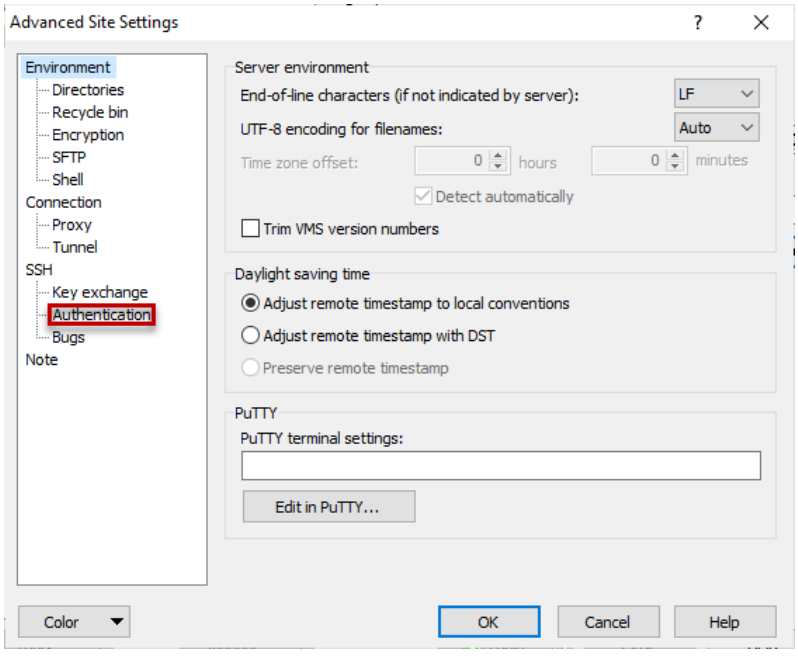
In the following steps within this section, you are guided on how to load your private key into the SFTP client. In the example below, we use the client WinSCP. This is only relevant for you who need to change your client and set up the new client for the first time.

Please note: If you are not going to change your client, then the next steps are not relevant for you.

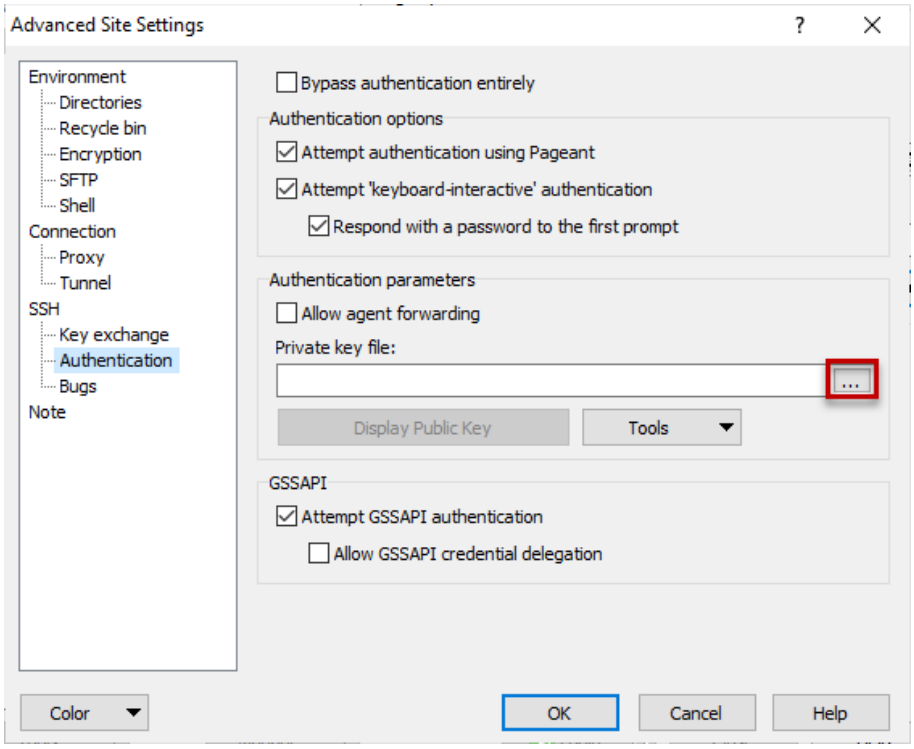
1.4 Click on **'Advanced'**.



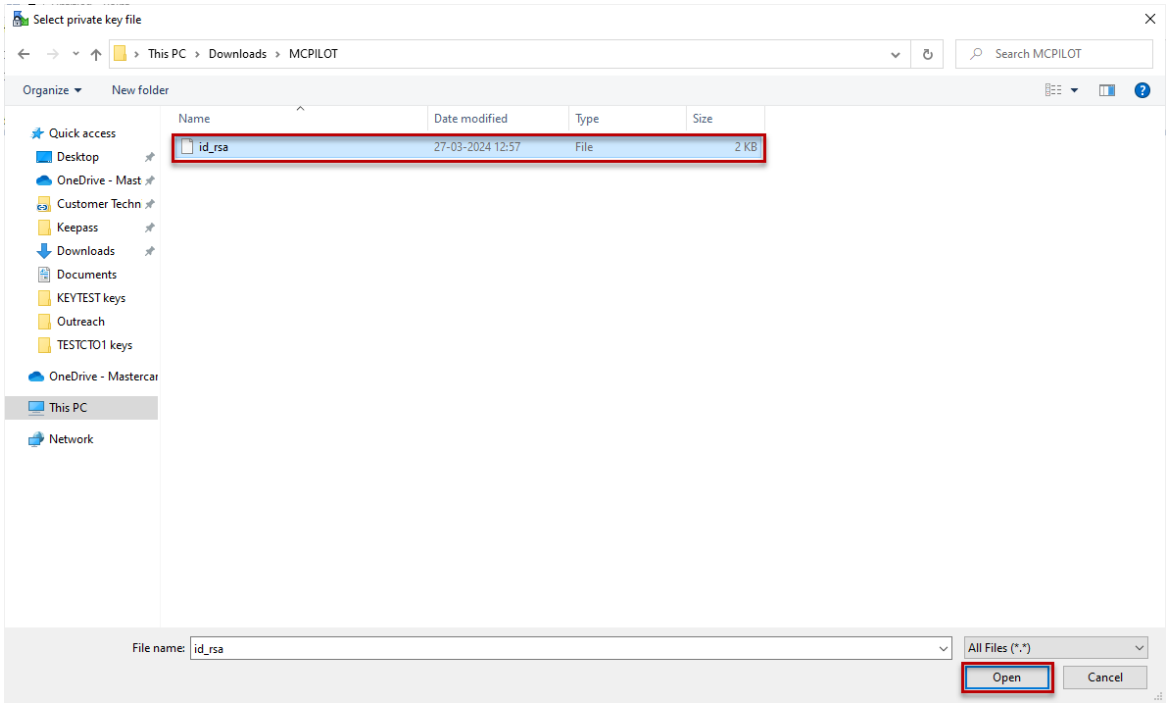
1.5 Click on **'Authentication'** under **'SSH'**.



1.6 Click on **'...'**

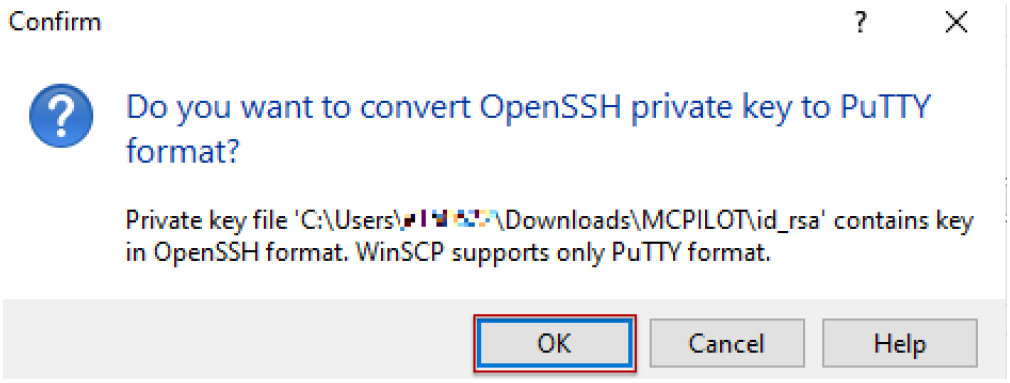


1.7 Now find the location of your private key and choose it. Click on **'Open'**.

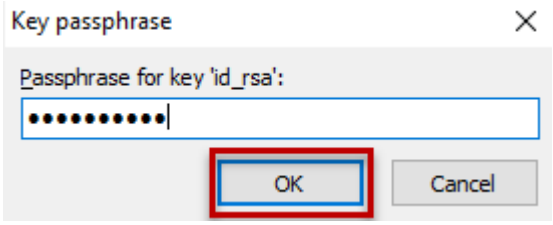


Remember to choose **'All files'** in the file explorer in the lower-right corner to see the file.

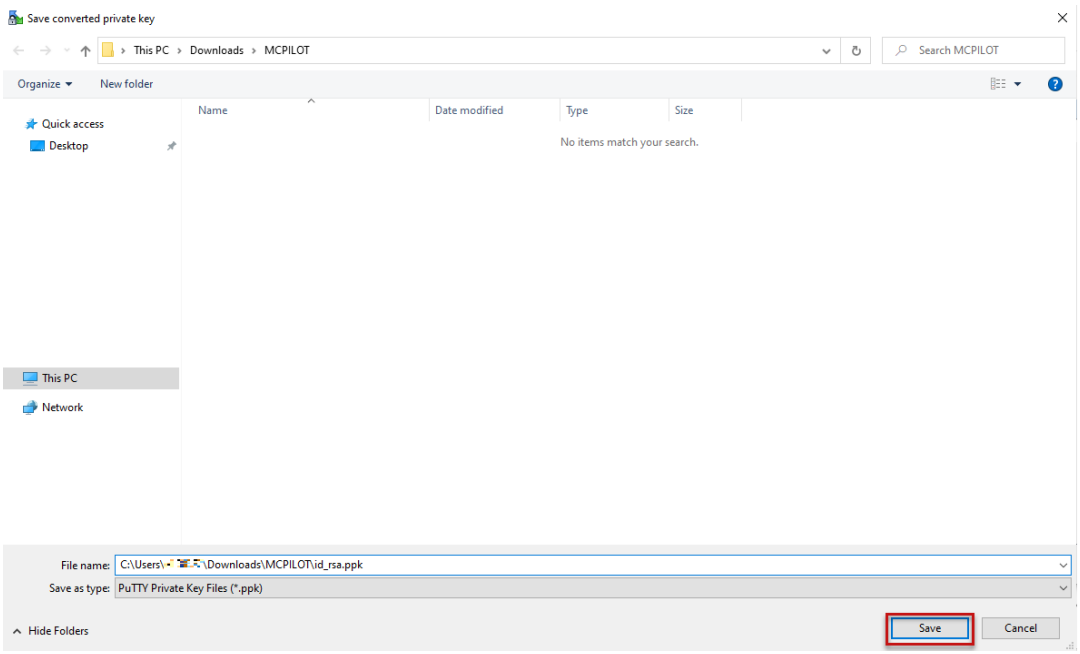
1.8 Now the prompt asks if you want to convert the private key to PuTTY-format. Click on **'OK'**.



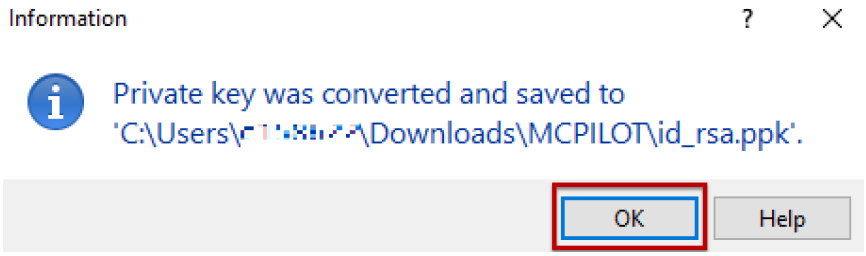
1.9 Enter the **passphrase** for the key and click on **'OK'**.



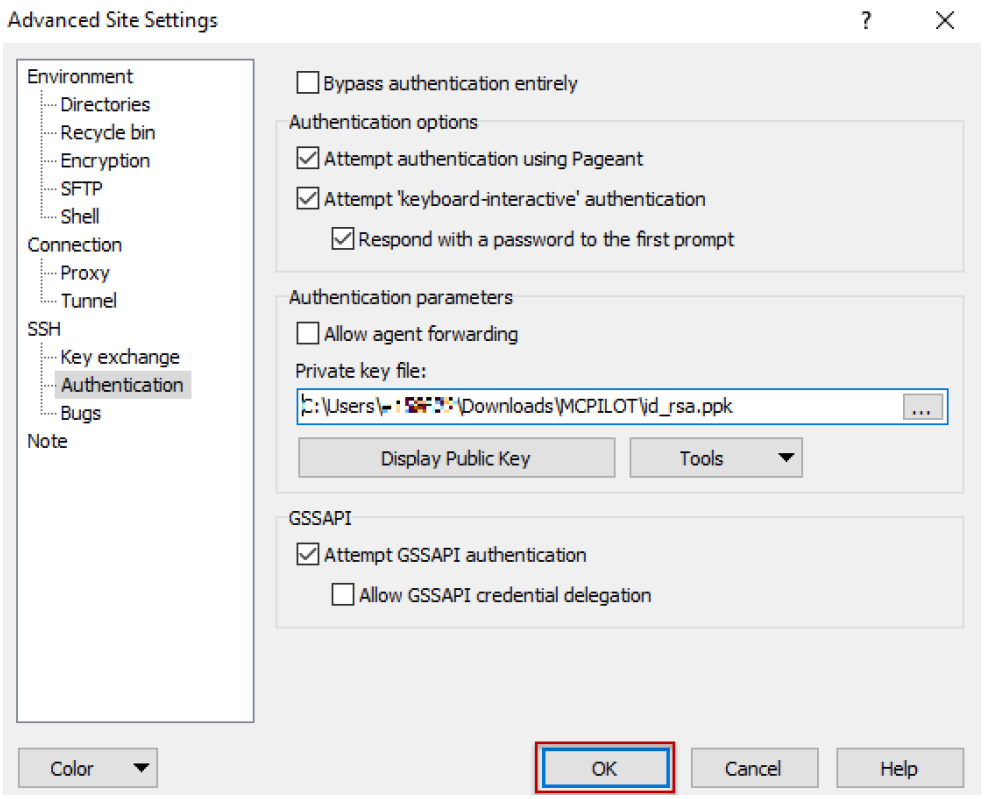
1.10 Now you choose where you want to save the converted key. We recommend saving it in the same location as the original key. Choose the location and click on **'Save'**.



1.11 Click on **'OK'**.



1.12 Click on **'OK'** again to close the advanced site settings.



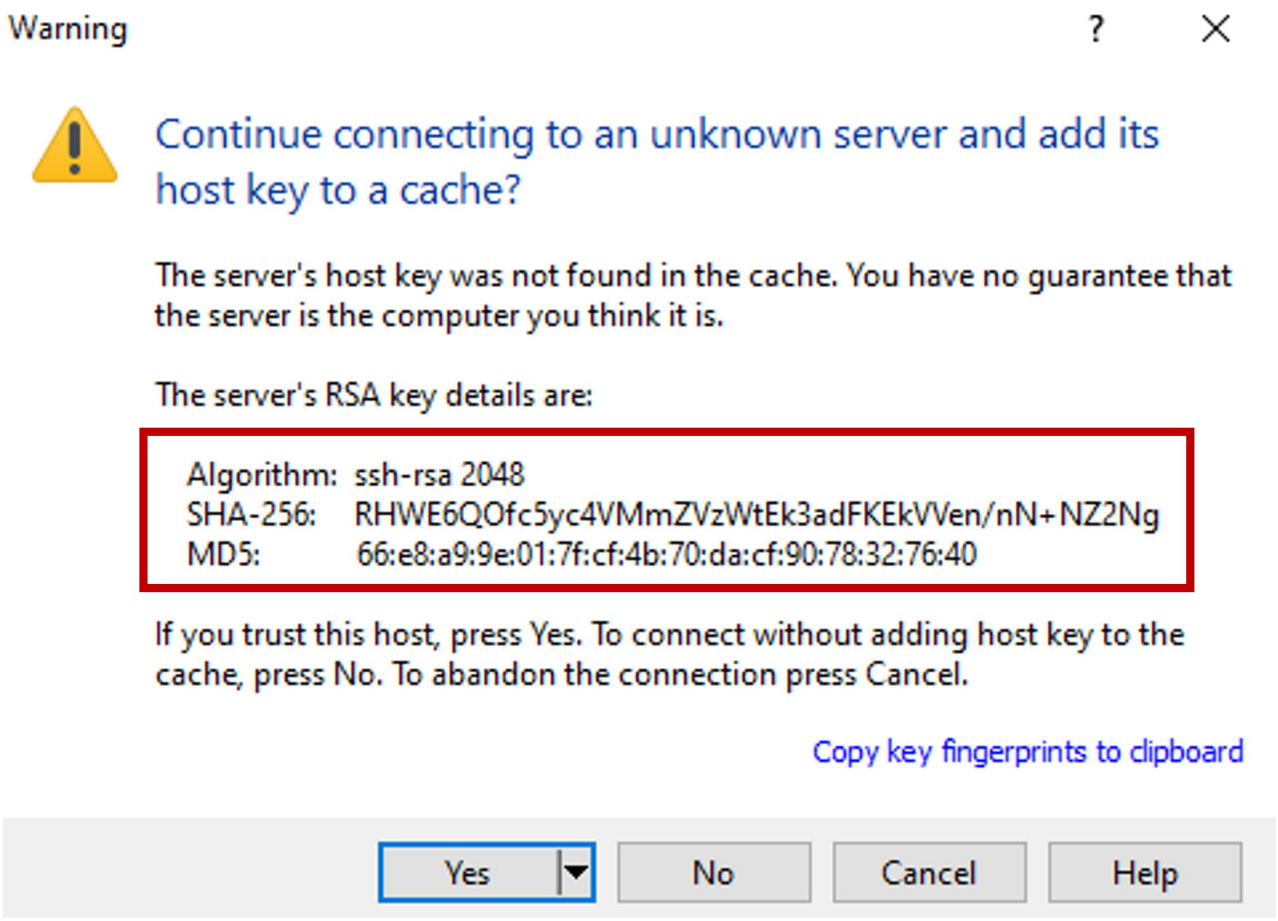
The key is now loaded into the mailbox and you can continue to log in.

2. Accept new fingerprint

The first time you connect to the new IP address, you may be asked to accept a new fingerprint.

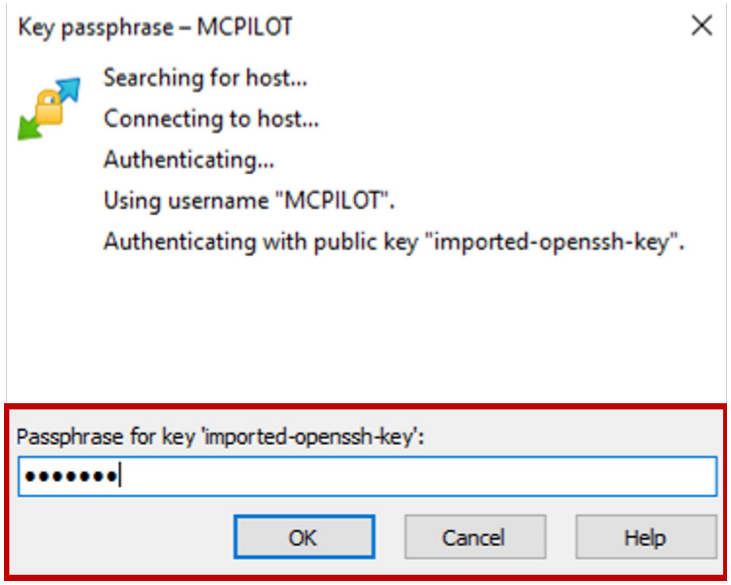
2.1 Accept the fingerprint below by clicking '**Yes**'.

- SHA256: RHWE6QOfc5yc4VMmZVzWtEk3adFKEkVVen/nN+NZ2Ng
- MD5: 66:e8:a9:9e:01:7f:cf:4b:70:da:cf:90:78:32:76:40

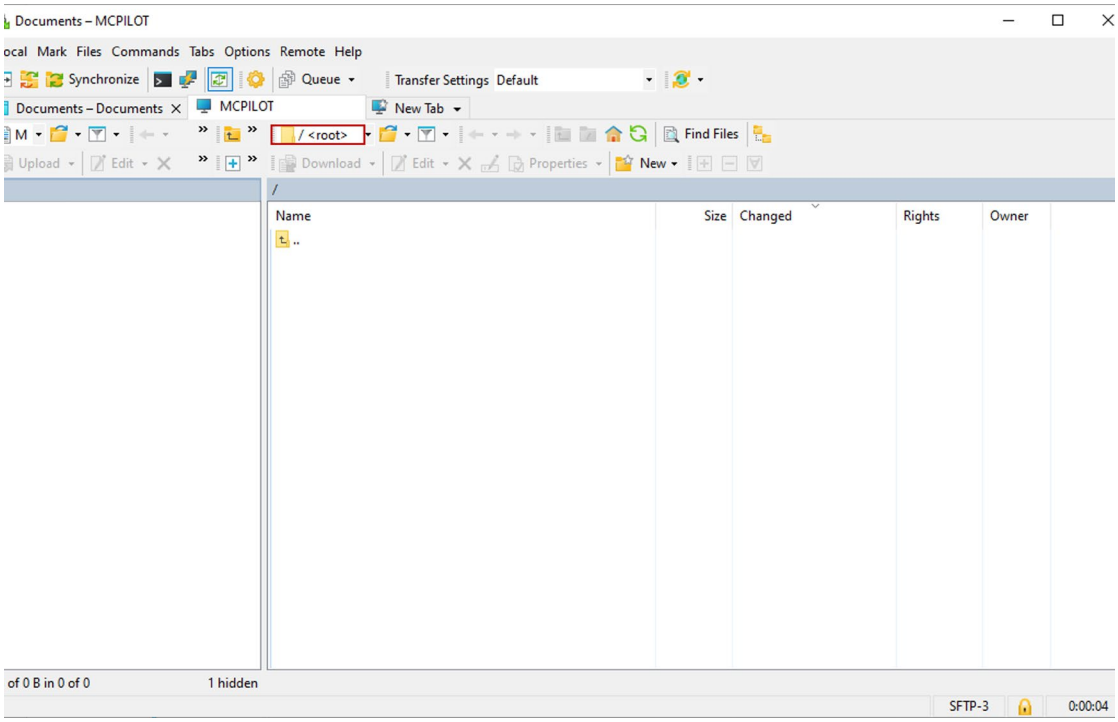


3. Manage your mailbox

3.1 In some cases, you will be asked to enter the passphrase for your private key, which you received the last time you generated a new security key. Enter passphrase and click '**OK**'.

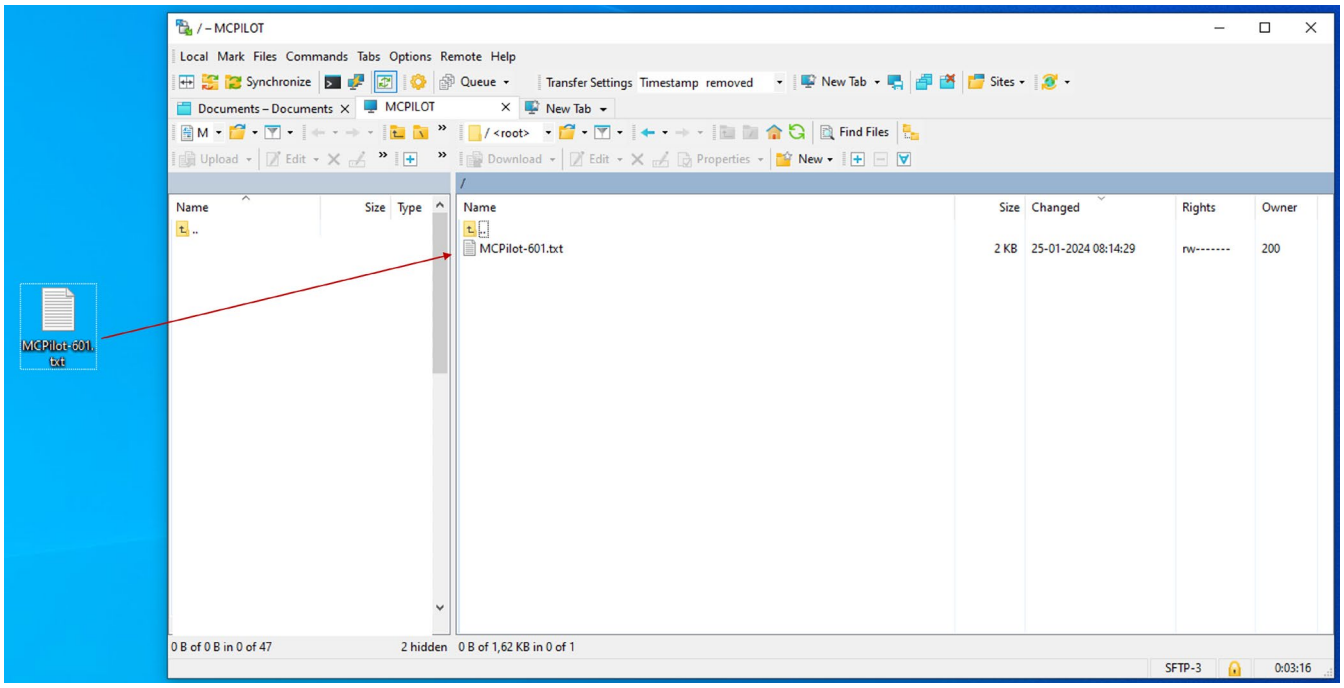


3.2 You are now logged into the mailbox and can send and retrieve files in the "root" folder.

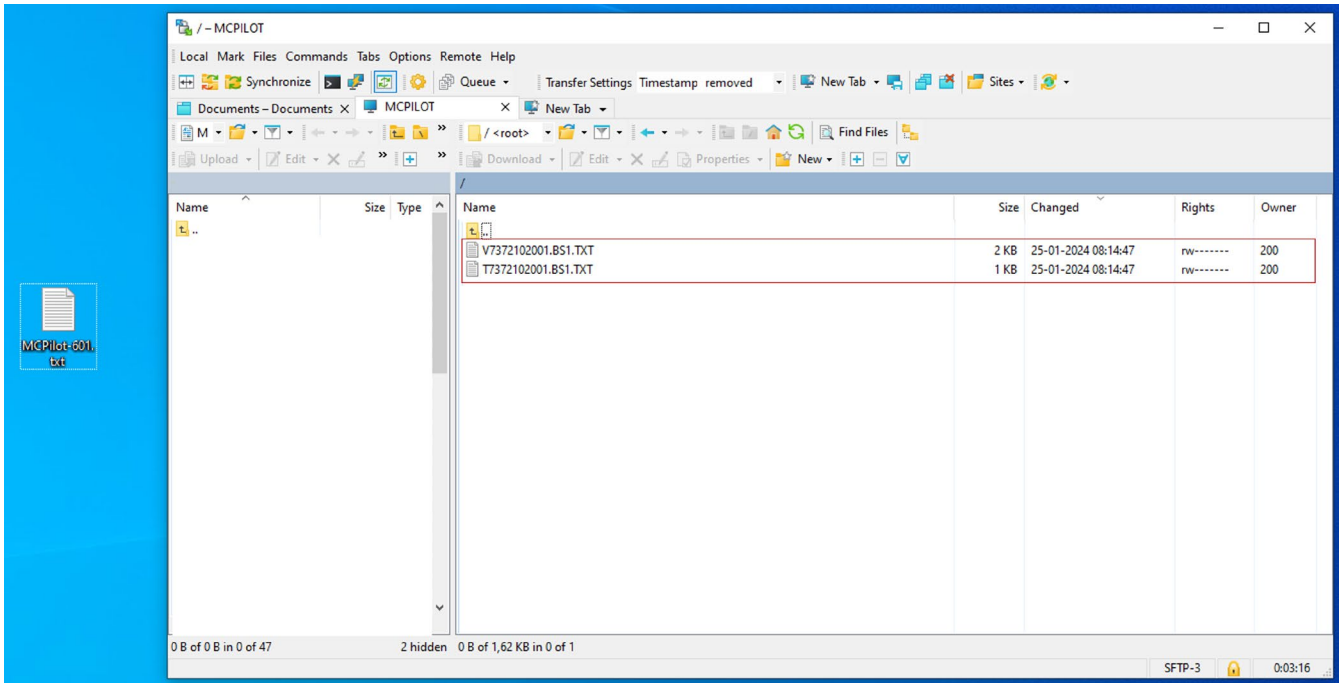


3.3 When you want to send a file, find the file where you have saved it on your PC. In this case, the file is saved on the desktop.

Now send the file by dragging it from the desktop (or from the folder where you have saved the file) on your PC to the root folder in My File Transfer.



Shortly after, you will see your receipt files showing that you have sent the file. If this does not happen right away, try reloading the page.



How to generate security keys

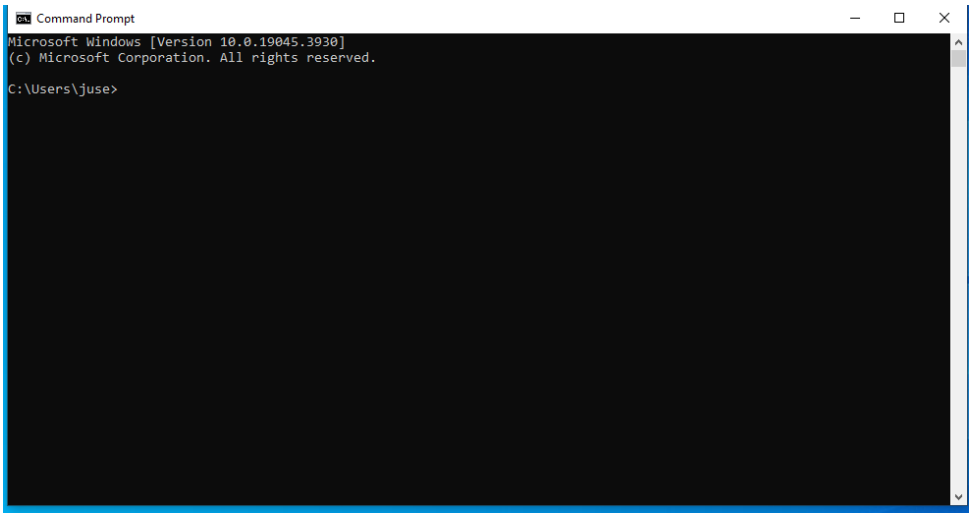
When you want to generate new security keys, follow the steps in this section. You can do this at any time, as needed. We recommend that you change your security keys every three years.

Security keys are used to ensure that you can communicate securely with Mastercard Payment Services' server via the SFTP solution. Security keys are a key pair consisting of a private and a public key. Each of your company's mailboxes in My File Transfer must have security keys associated with them.

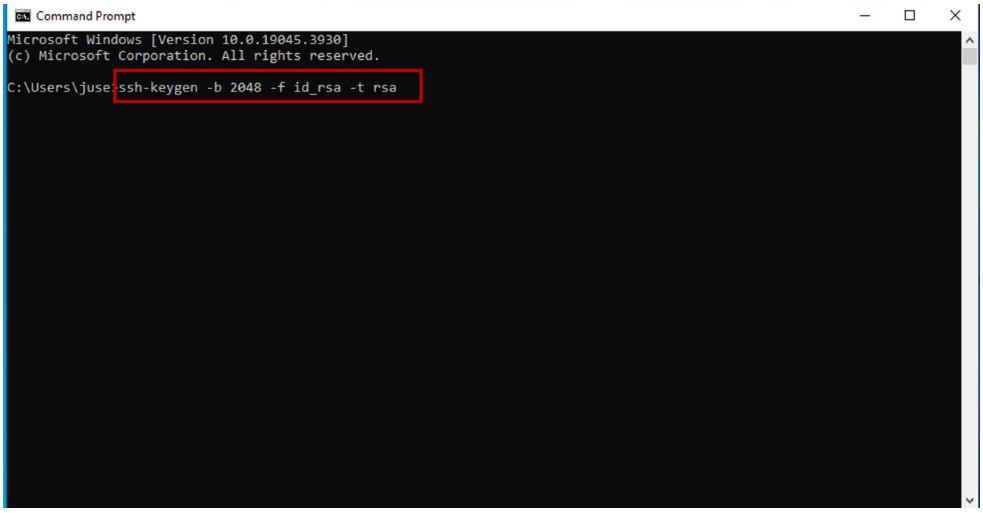
The private key belongs to your company and must be stored in a secure location on your company drive. The public security key must be transferred to the mailbox in question in My File Transfer. Read below how to do this.

You generate the key yourself using a command line tool – a *command line interpreter*.

1. Open **Command Prompt** or a similar tool – *the command line interpreter*. In this example, we use Command Prompt with the username "juse".



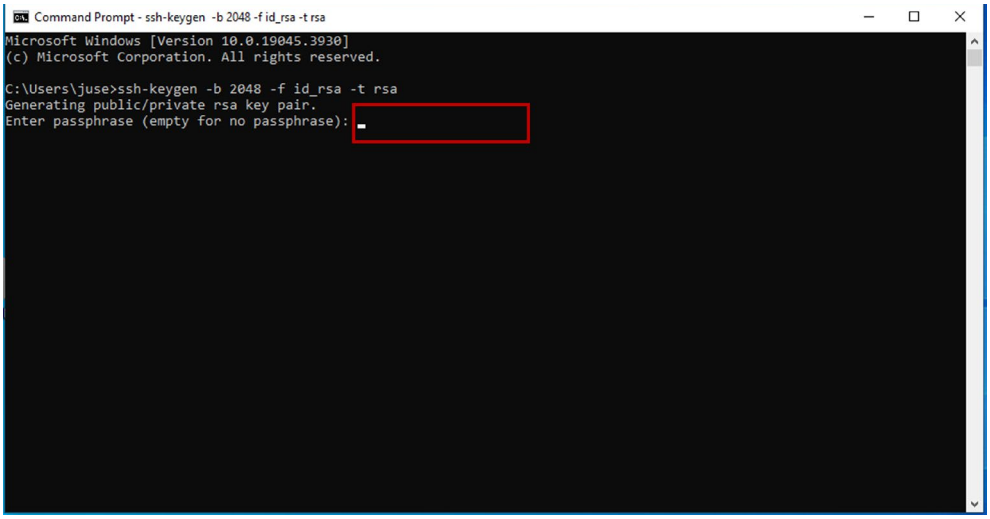
2. Type this command to generate new RSA security keys of length 2048 bits*:
ssh-keygen -b 2048 -f id_rsa -t rsa



*Please note: The security keys *must* be RSA keys, and the key length must be 2048 bits.

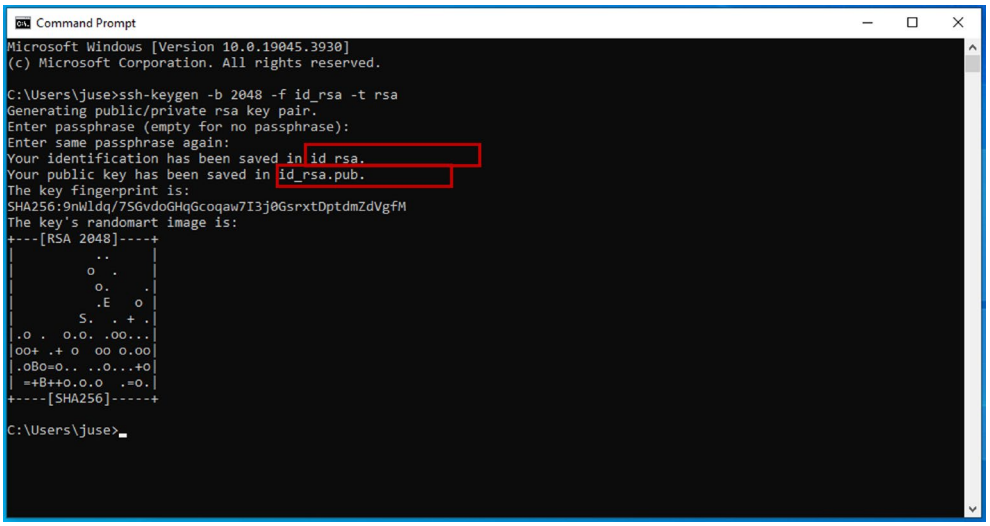
3. You will now be asked to enter a password of your choice, also known as a passphrase.

The passphrase must consist of a minimum of five characters, which must be a combination of letters and numbers. The passphrase ensures that only authorised people can use the private security key.



4. The command will generate two key files:

- **id_rsa**, which is the private key.
- **id_rsa.pub**, which is the public key.



You have now generated new security keys. You must store the private key in a secure location on your company drive, and the public key must be transferred to your mailbox in My File Transfer. To do this, follow the next two steps.

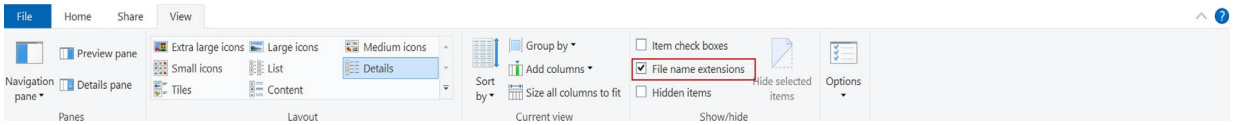
Have you lost your security key or forgotten your passphrase, you can use an HTTPS solution instead - read more in the section "Get help and answers to your questions" on page 16 of this guide.

5. Rename your public key

Access the folder where your key files have been automatically saved. In the example above, it is the folder: C:\Users\juse>.

You now need to rename your public key and save it in .txt format. Please note: In order to save the file in .txt format, you must be able to see the full file name.

You can select this in File Explorer by clicking '**View**' and ticking '**File name extensions**'.



The file should be named as follows:

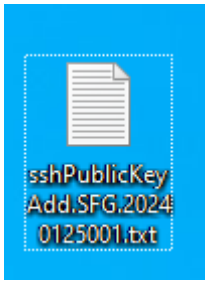
sshPublicKeyAdd.SFG.YYYYMMDDNNN.txt

YYYYYMMDD refers to today's date written as follows: year, month, date.

NNN refers to a key number that you have chosen yourself, which must consist of three numbers, e.g. 001.

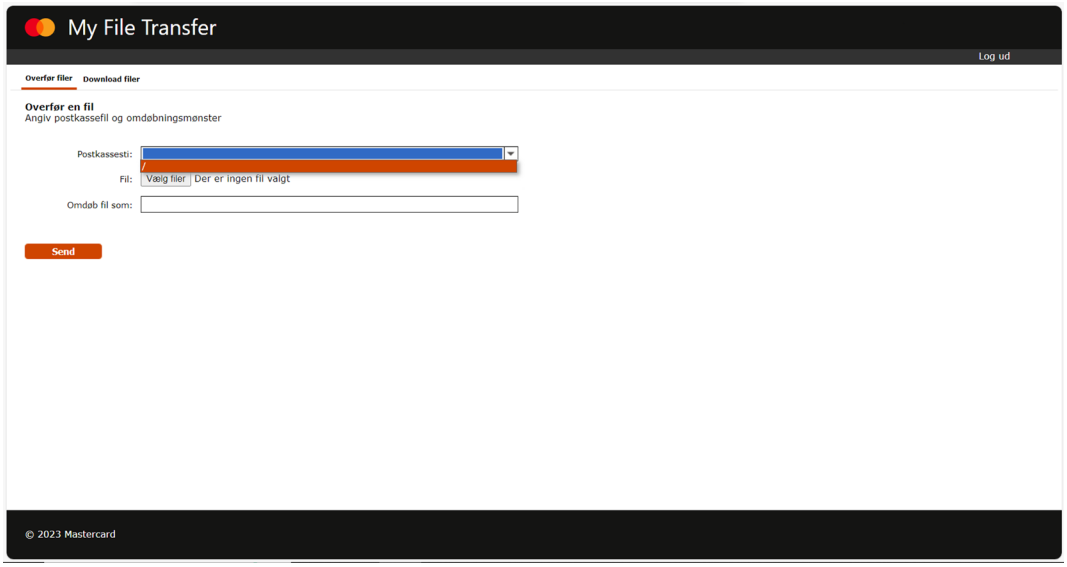
For example, a file sent on 25 January 2024 with key number 001 is saved as follows:
sshPublicKeyAdd.SFG.20240125001.txt

Here, the file is extracted from the folder and saved on the PC's desktop.



6a. If you are currently using an HTTPS solution and now also want to use a SFTP solution, or no longer can connect with your established SFTP solution, follow these instructions:

Log in to the mailbox as usual by entering **UserID** and **password**. When you are logged into the mailbox, you are automatically on the **'Overfør filer'** tab. Click on the arrow to the right of **'Postkassesti'** and select **'/'**.



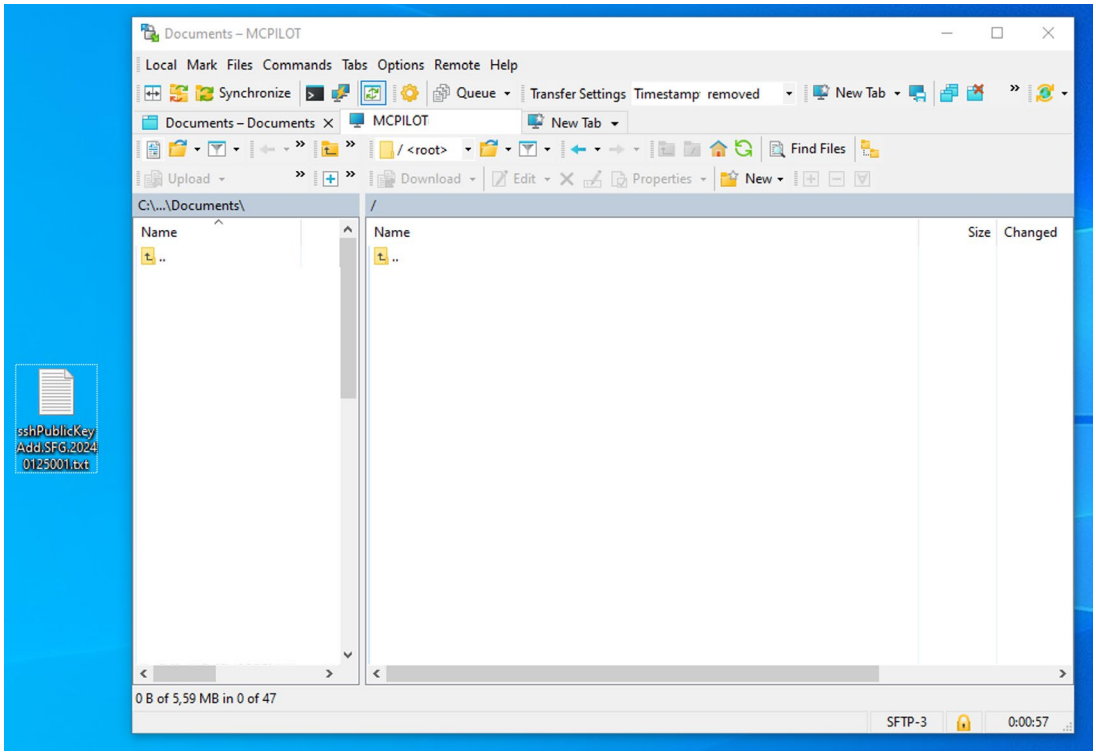
Click on **'Vælg filer'** to upload the public key to the mailbox and click on **'Send'**.

When your public key has been uploaded to the mailbox, a message will appear telling you that the file upload is complete. It is a good idea to make sure your key has indeed been uploaded and accepted. You do this on the **'Download filer'** tab, where you, among other things, can find receipts. It may take a few minutes before the receipt is ready.

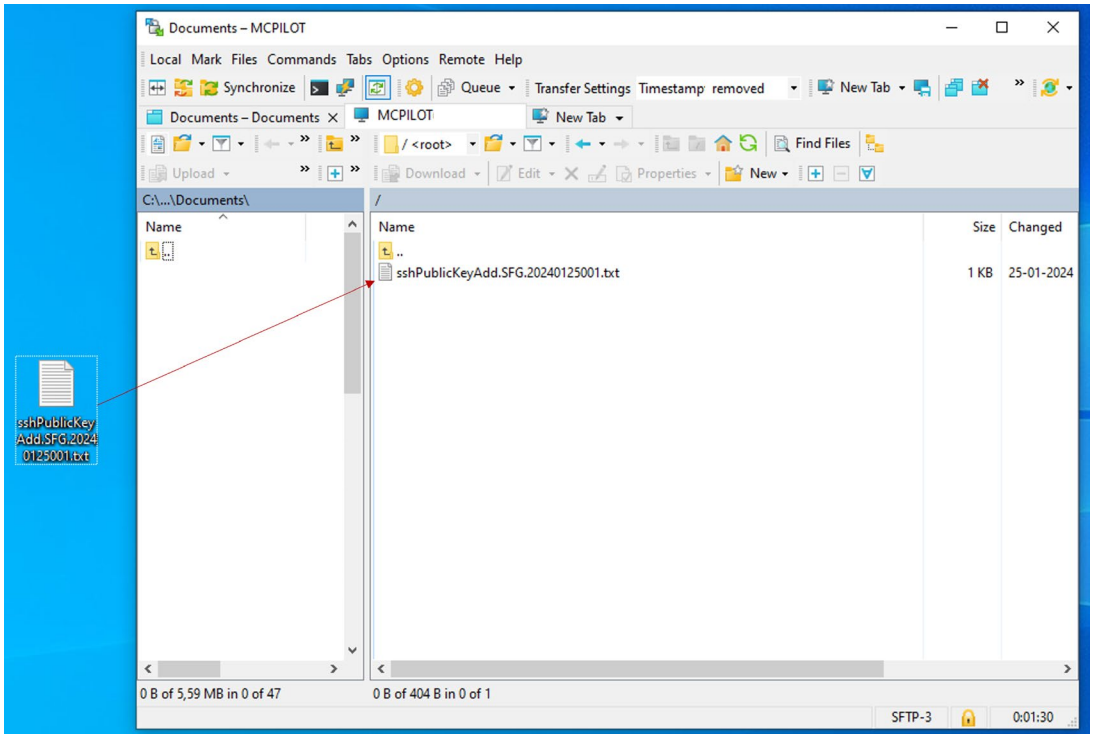
6b. If you are currently using a SFTP solution and need to generate a security key, you must upload your public key to the mailbox in My File Transfer (**ATT: This requires that you have a functioning key pair and are able to establish a connection already**):

Connect to your company mailbox in My File Transfer via an SFTP client (see the section "Connect to IP address and port" in this user guide).

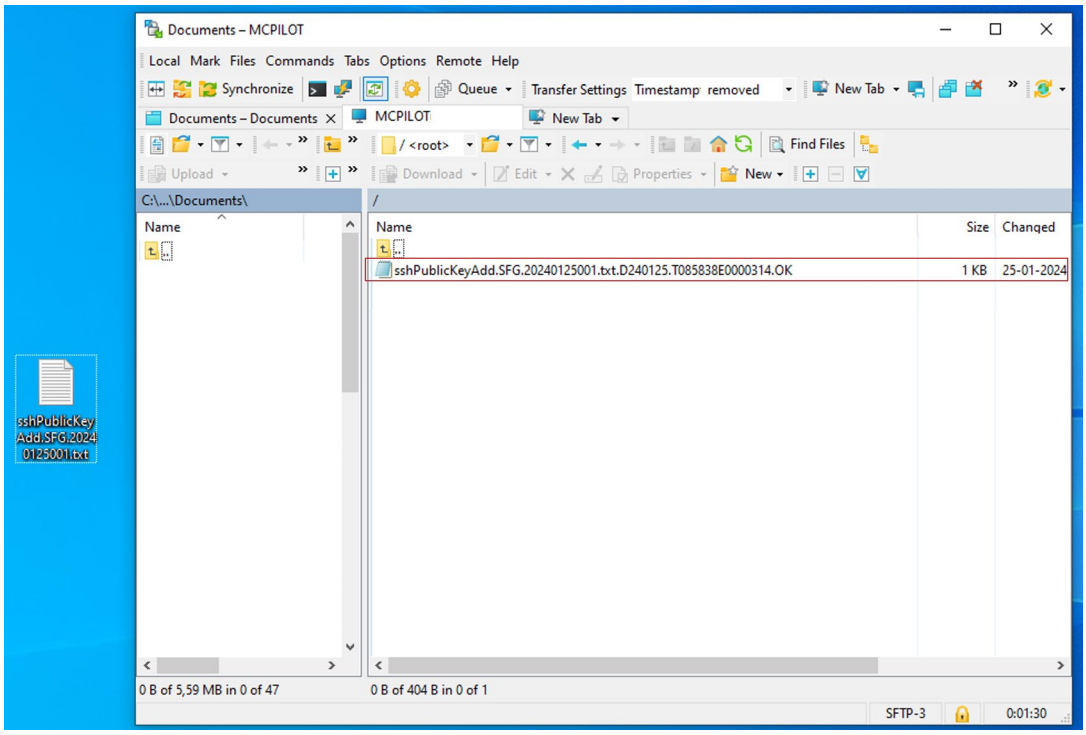
Find your public key. In this case, it is saved on your PC's desktop.



Your public key must now be transferred to the root folder in your mailbox in My File Transfer. Transfer your public key to the root folder by dragging the file from the desktop (or from the folder where you have saved the file) to the mailbox in My File Transfer.



You will now see your receipt file showing that you have uploaded the public key.



You have now generated security keys for your mailbox in My File Transfer and can close your SFTP client. You can exchange files with Mastercard products again immediately after the security keys have been updated.

Both your new and your old keys will work for seven days after generating new security keys. After the seven days, only the new security keys will work. To avoid confusion, we recommend that you start using your new security keys immediately after generating them.

Get help and answers to your questions

You can find more information about the SFTP solution in My File Transfer on this website: https://www.mastercardpaymentservices.com/denmark/my-file-transfer/sftp

Here, you can also find frequently asked questions about the system and the solution.

If you have **lost your security key or forgotten your passphrase**, it is possible to use an HTTPS solution instead. Here you must use your UserID and password to log in to My File Transfer. You can read more about how to use an HTTPS solution to log in and send and receive files here (in Danish):

https://www.mastercardpaymentservices.com/denmark_/Documents/Brugervejledning-Sadan-udveksler-du-filer-med-My-File-Transfer-HTTPS.pdf

If you have any further questions, you are always welcome to contact our support team on (+45) 8081 0679. We are available on weekdays from 09:00 to 16:00.

Security and rights

When transferring data, your shipment to Mastercard Payment Services is identified using your private key. Before the data exchange takes place, a so-called session key is exchanged, along with the public key, which is used to encrypt your data. The session key is unique for each data exchange and is used to encrypt your delivery.

The solution ensures that the data exchange complies with the requirements of the VAT Order regarding electronic invoicing.

Operational security can be established by setting up the SFTP solution to run automatically.

Your MitID Erhverv can also be used as a backup solution for manual data exchange using Mastercard Payment Services' HTTPS solution.

If the generated security keys are kept without the proper security, Mastercard Payment Services cannot be held liable for the consequences.

Mastercard Payment Services recommends that you change your security keys regularly, preferably every three years. You are responsible for checking that this is in accordance with your organisation's security policy.

If you suspect that your security keys have been compromised or, for any other reason, no longer provide the necessary security, you must contact Mastercard Payment Services immediately.

Appendix

Requirements for the SFTP client

You can read Mastercard's requirements for your SFTP client below.

Algorithm type	Purpose	Supported algorithms/versions
Host Key	Server authentication	• rsa-sha2-256 • rsa-sha2-512
Key Agreement / Key Exchange	Derive encryption keys, initialization vectors, MAC keys	• ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 • curve25519-sha256@libssh.org
Message Authentication Codes (MACs)	Protect data integrity and prevent replay attacks	• hmac-sha2-256 • hmac-sha2-512 • hmac-sha2-256-etm@openssh.com • hmac-sha2-512-etm@openssh.com
Ciphers	Encryption of data in channel	• aes256-ctr • aes192-ctr • aes128-ctr • aes256-gcm@openssh.com • aes128-gcm@openssh.com
Public Key Algorithms	Client authentication to server	• rsa-sha2-256 • rsa-sha2-512

What are the SFTP operations allowed in MCeNett?

- MCeNett allows GET, PUT and DELETE operations on files.
- Users are not allowed to create or delete directory at MCeNett.
- During the GET operation, MCeNett does not allow additional operation like checking any other attributes of the file. For example - If the User has initiated a GET operation and during this extraction, if they try to check the file size then they will get error, and the session will get abnormally terminated.

Below are some general guidelines which MCeNett encourage users to follow for keeping systems healthy

- MCeNett does not recommend users to perform continuous polling checks to our system. This means they should not make continuous connection to check the connectivity.
- MCeNett recommend users to close the session immediately or within some reasonable time (30 seconds if user is expecting some receipt) after file operation.
- MCeNett does not recommend users to perform any operation on the file after successful upload to their mailbox. The users must perform all the operations first and then upload (perform PUT operation.) For example, if a user has successfully uploaded the file and then try to rename it, it will result in error and operation will be failed.