

BRUGERVEJLEDNING

Send filer med en SFTP-løsning i My File Transfer

AUGUST 2025



Indhold

Introduktion	1
1. Forbind til IP-adresse og port	2
2. Acceptér nyt fingerprint	7
3. Administrér postkassen	8
Sådan genererer du sikkerhedsnøgler	10
Få hjælp og svar på dine spørgsmål	17
Sikkerhed og rettigheder	17
Bilag.....	18
Krav til SFTP-klienten.....	18



Introduktion

Denne vejledning er til dig, der bruger en SFTP-løsning til at udveksle filer med Mastercard-produkterne Betalingsservice, Leverandørservice, Overførselsservice og Informationsservice via My File Transfer.

[Click here to find this guide in English](#)

Det kræver kendskab til både SFTP-løsningen og jeres tekniske setup at sætte jeres system op til My File Transfer. Hvis du ikke selv har dette kendskab, kan du med fordel dele denne vejledning med en kollega, systemleverandør eller IT-konsulent.

Sikkerheden i løsningen består i anvendelsen af RSA-sikkerhedsnøgler (private/offentlige nøgler), som skaber en sikker udveksling af filer mellem din virksomhed og Mastercards produkter.

Vejledningen guider dig til, hvordan du gennem tre trin sætter din virksomheds system op til at udveksle filer med en SFTP-løsning i My File Transfer. De tre trin er:

1. Forbind til IP-adresse og port
2. Acceptér nyt fingerprint
3. Administrér postkassen

Derefter følger et afsnit om, hvordan du genererer nye sikkerhedsnøgler, hvilket du kan gøre når som helst, efter behov. Vi anbefaler, at du udskifter dine sikkerhedsnøgler hvert tredje år.

Til sidst i denne vejledning finder du et afsnit om, hvordan du får hjælp, samt et afsnit om rettigheder og sikkerhed.

1. Forbind til IP-adresse og port

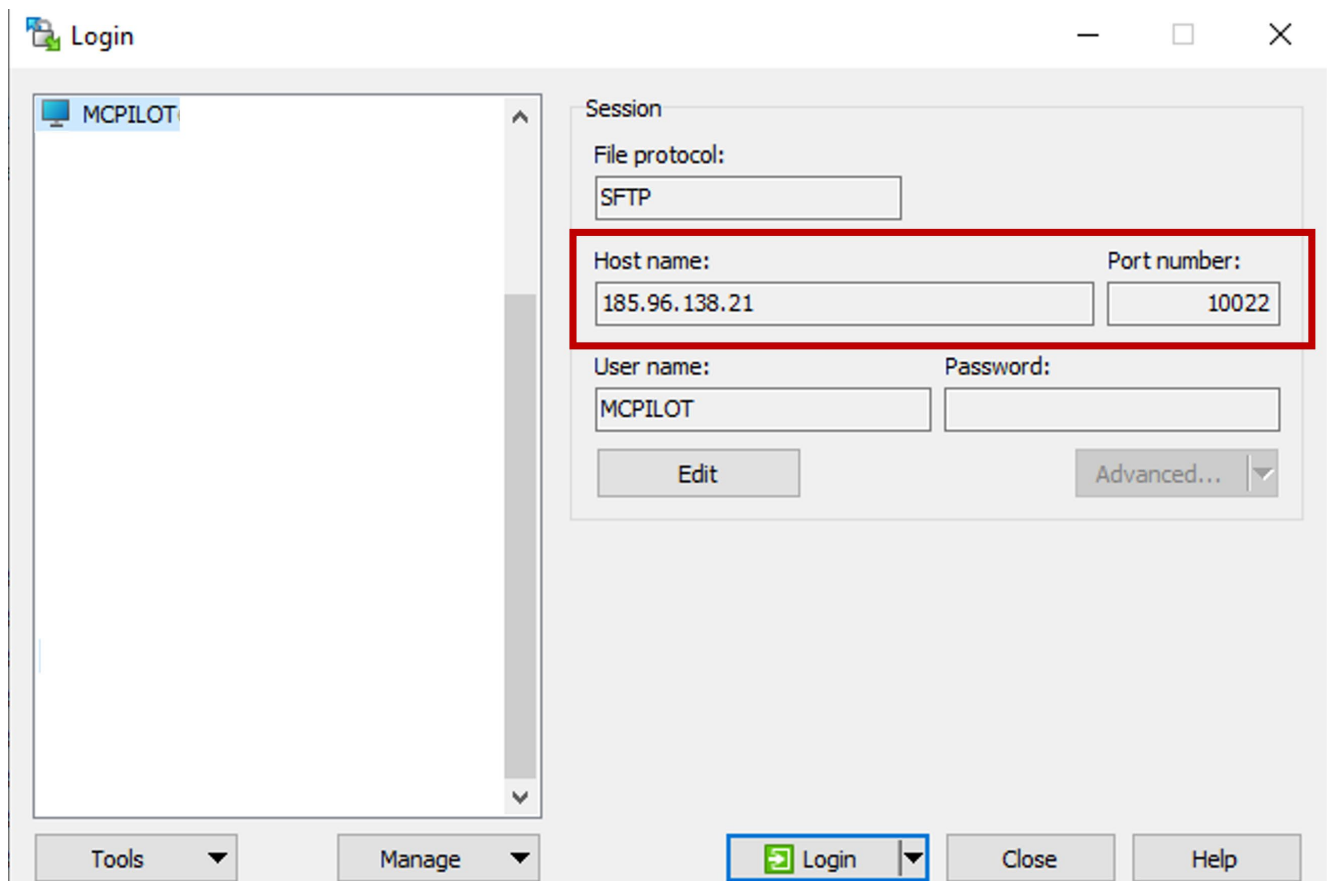
1.1 Åbn en moderne SFTP-klient. I denne vejledning anvender vi klienten WinSCP. Se bilaget i denne vejledning for kravspecifikationer til din SFTP-klient.



1.2 Forbind til IP-adressen 185.96.138.21 og portnummeret 10022. I eksemplet nedenfor forbinder vi til postkassen (UserID'et) 'MCPILOT'.

1.3 Klik på '**Login**'.

OBS! Husk at sikre, at IP-adressen er whitelistet i jeres system, og at alle relevante porte er åbne, inden du forbinder.

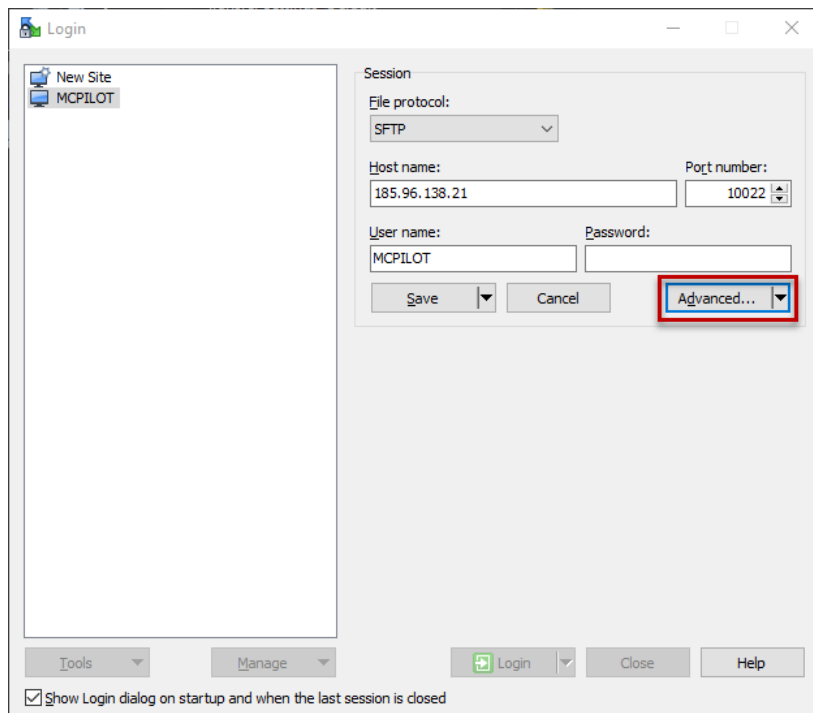


Hvis du ikke allerede har gjort det, skal du huske at indlæse din private nøgle, før du kan logge ind.

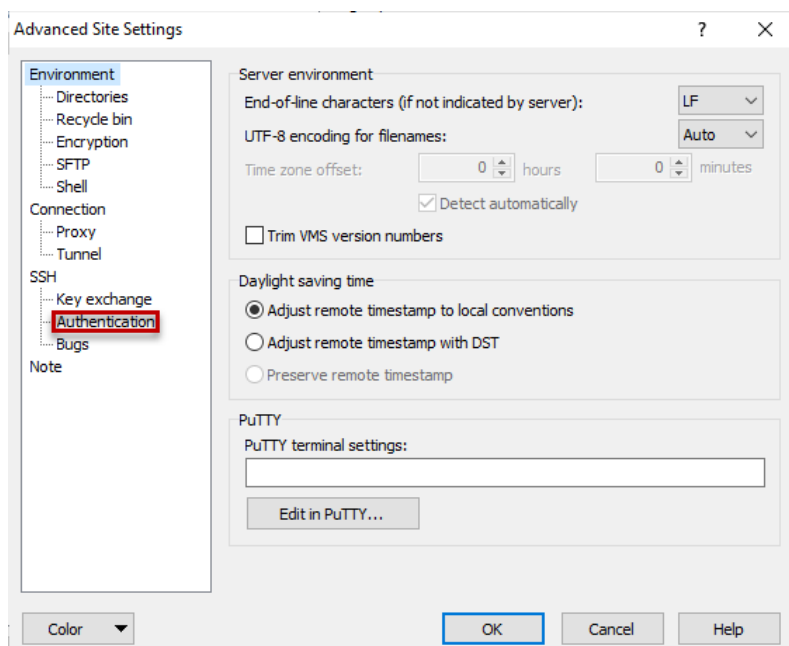
I de næste trin i denne sektion vises, hvordan du kan indlæse din private nøgle i SFTP-klienten. Vi anvender i eksemplet klienten WinSCP. Det er kun relevant for dig, som skal ændre din klient og sætte den nye klient op for første gang.

OBS! Hvis du ikke skal ændre din klient, er de næste trin altså ikke relevante for dig.

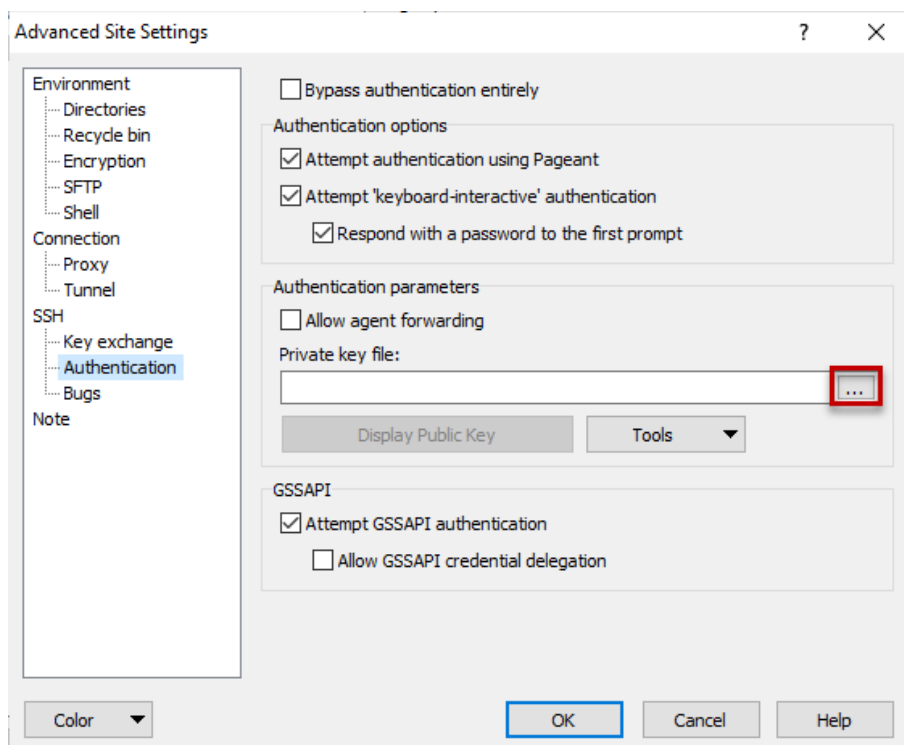
1.4 Klik på **'Advanced'**.



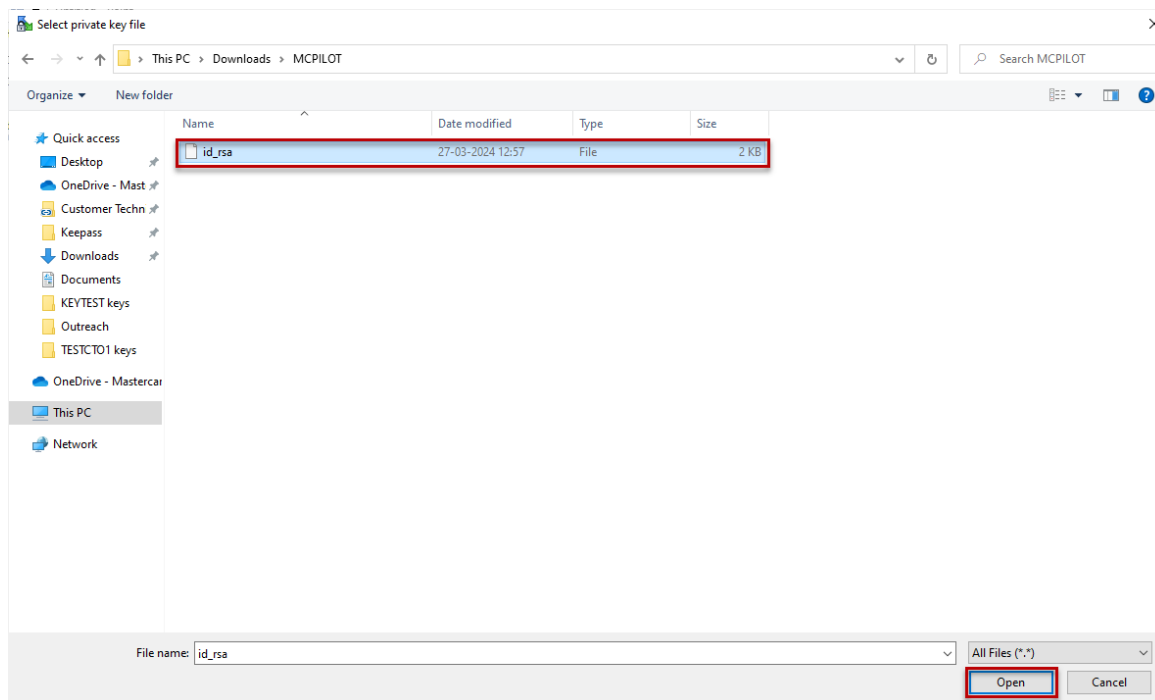
1.5 Klik på **'Authentication'** under **'SSH'**.



1.6 Klik på '...'



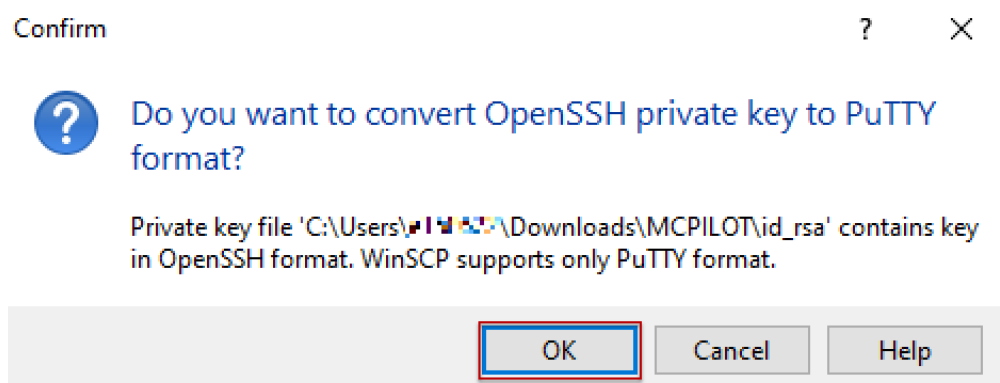
1.7 Find nu lokationen for din private nøgle og vælg denne. Klik på 'Open'.



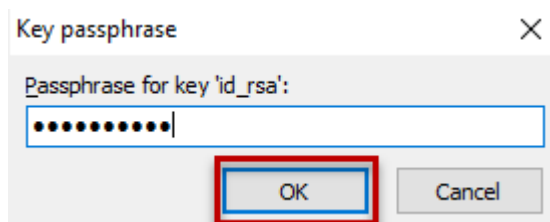
Husk at vælge '**Alle filer**' nede i højre hjørne af stifinderen for at se filen.



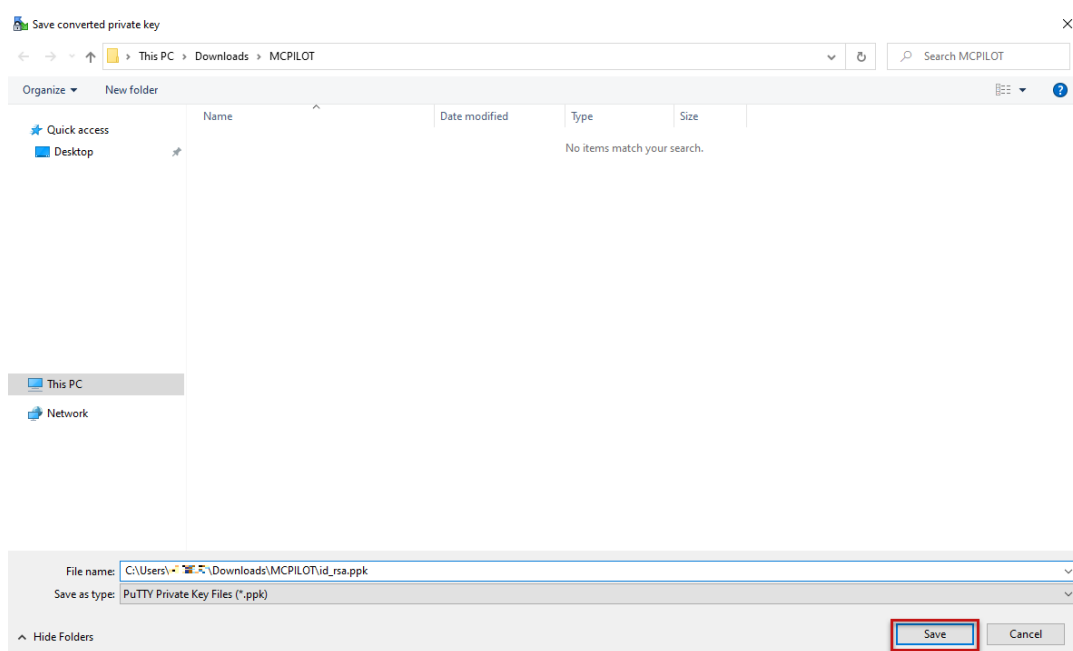
1.8 Nu bliver du spurgt, om du vil konvertere den private nøgle til PuTTY-format. Klik **'OK'**.



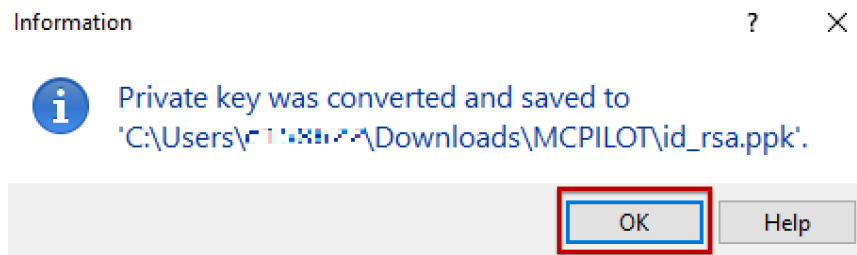
1.9 Indtast nu nøglens **passphrase** og klik **'OK'**.



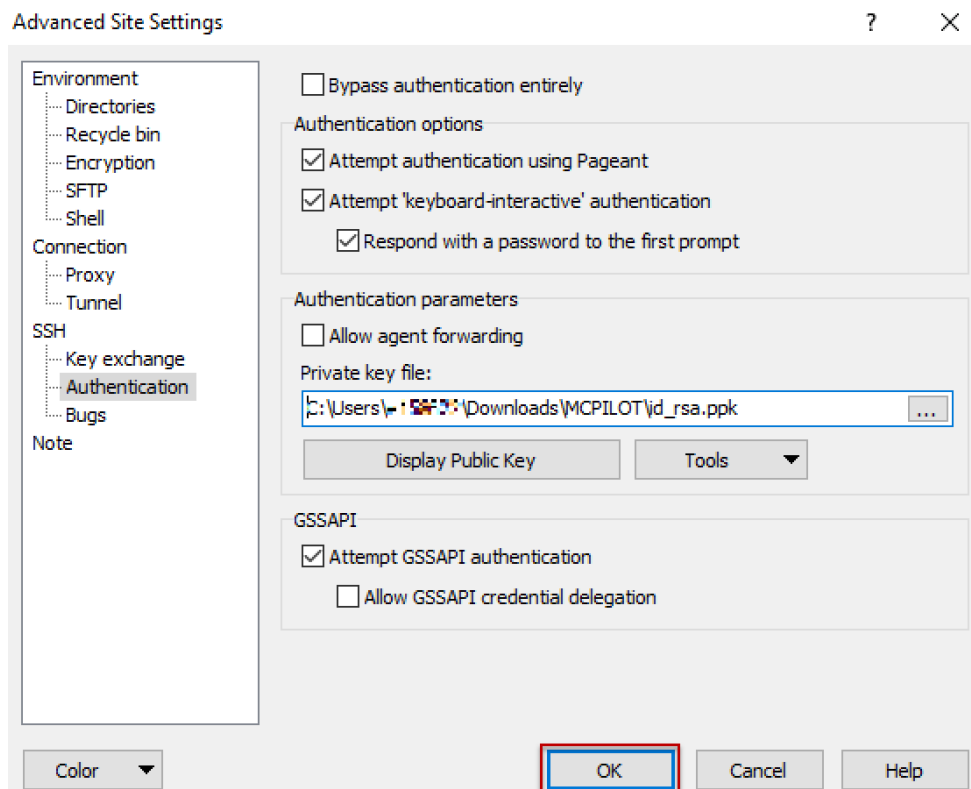
1.10 Nu skal du vælge, hvor du vil gemme den konverterede nøgle. Vi anbefaler at gemme den samme sted som den oprindelige nøgle. Vælg en lokation og klik **'Save'**.



1.11 Klik **'OK'**.



1.12 Klik **'OK'** igen for at lukke de avancerede indstillinger.



Nøglen er nu indlæst på postkassen, og du kan fortsætte med at logge ind.

2. Acceptér nyt fingerprint

Første gang, du forbinder til den nye IP-adresse, kan du blive bedt om at acceptere et nyt fingerprint.

2.1 Acceptér fingerprintet nedenfor ved at klikke på **'Yes'**.

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

Warning

? X



Continue connecting to an unknown server and add its host key to a cache?

The server's host key was not found in the cache. You have no guarantee that the server is the computer you think it is.

The server's RSA key details are:

Algorithm: ssh-rsa 2048
SHA-256: RHWE6QOfc5yc4VMmZVzWtEk3adFKEkVVen/nN+NZ2Ng
MD5: 66:e8:a9:9e:01:7f:cf:4b:70:da:cf:90:78:32:76:40

If you trust this host, press Yes. To connect without adding host key to the cache, press No. To abandon the connection press Cancel.

[Copy key fingerprints to clipboard](#)

Yes

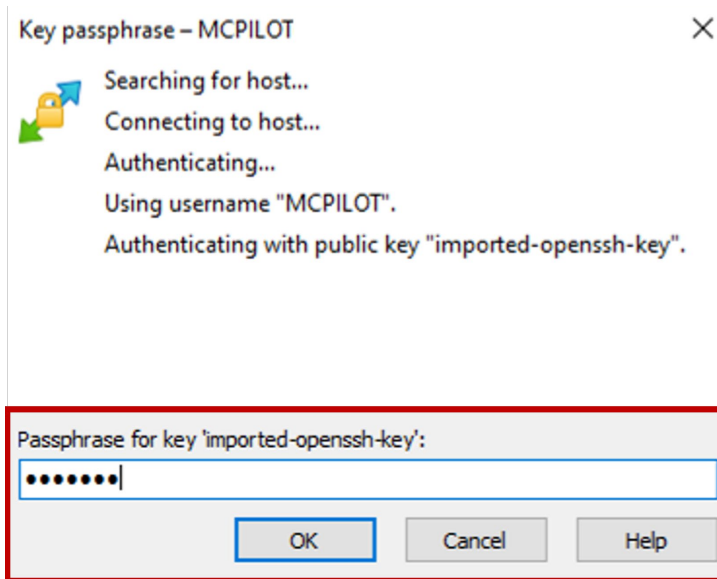
No

Cancel

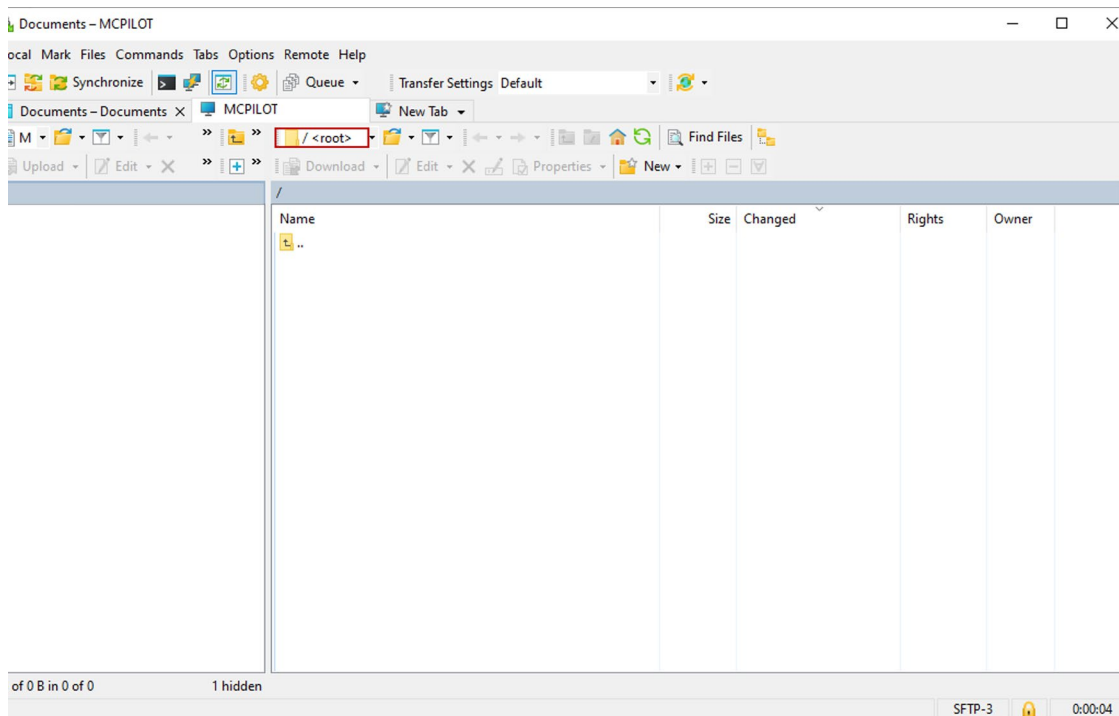
Help

3. Administrér postkassen

3.1 I nogle tilfælde vil du blive bedt om at skrive passphrasen til din private sikkerhedsnøgle (private key), som du fik sidste gang, du genererede ny sikkerhedsnøgle. Indtast denne og klik **'OK'**.

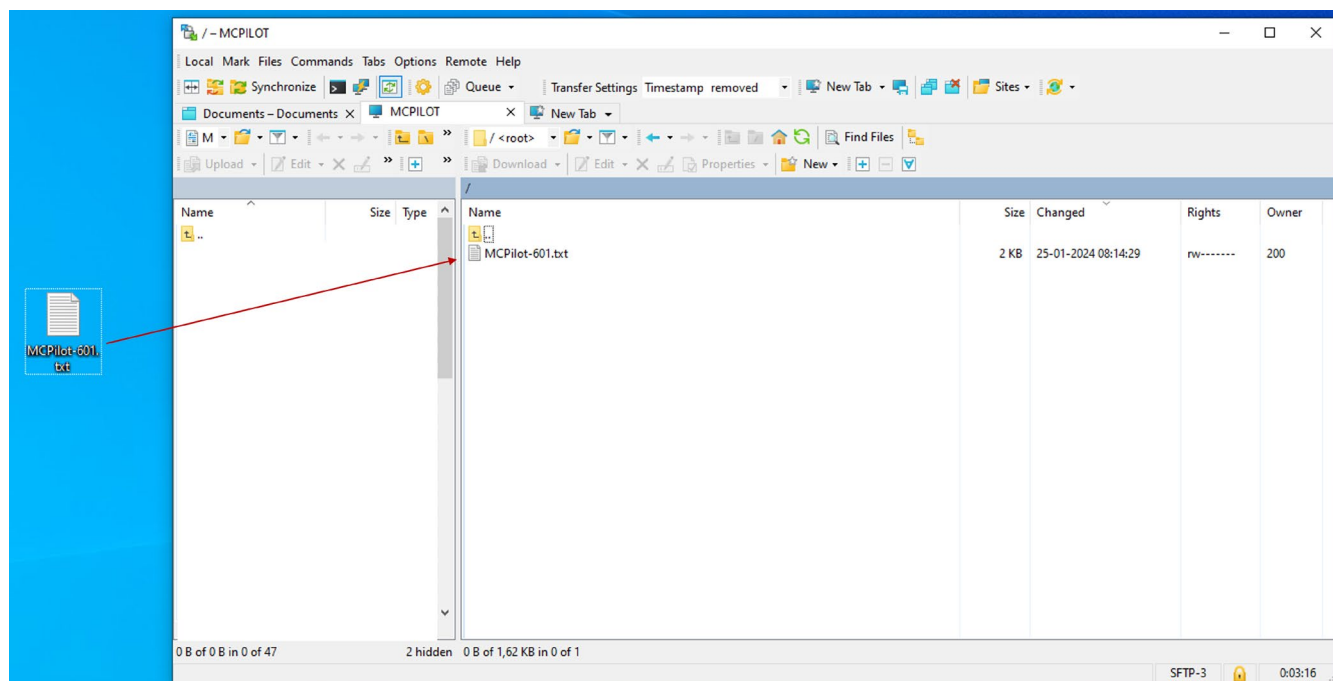


3.2 Du er nu logget ind i postkassen og kan sende og hente filer i folderen 'root'.

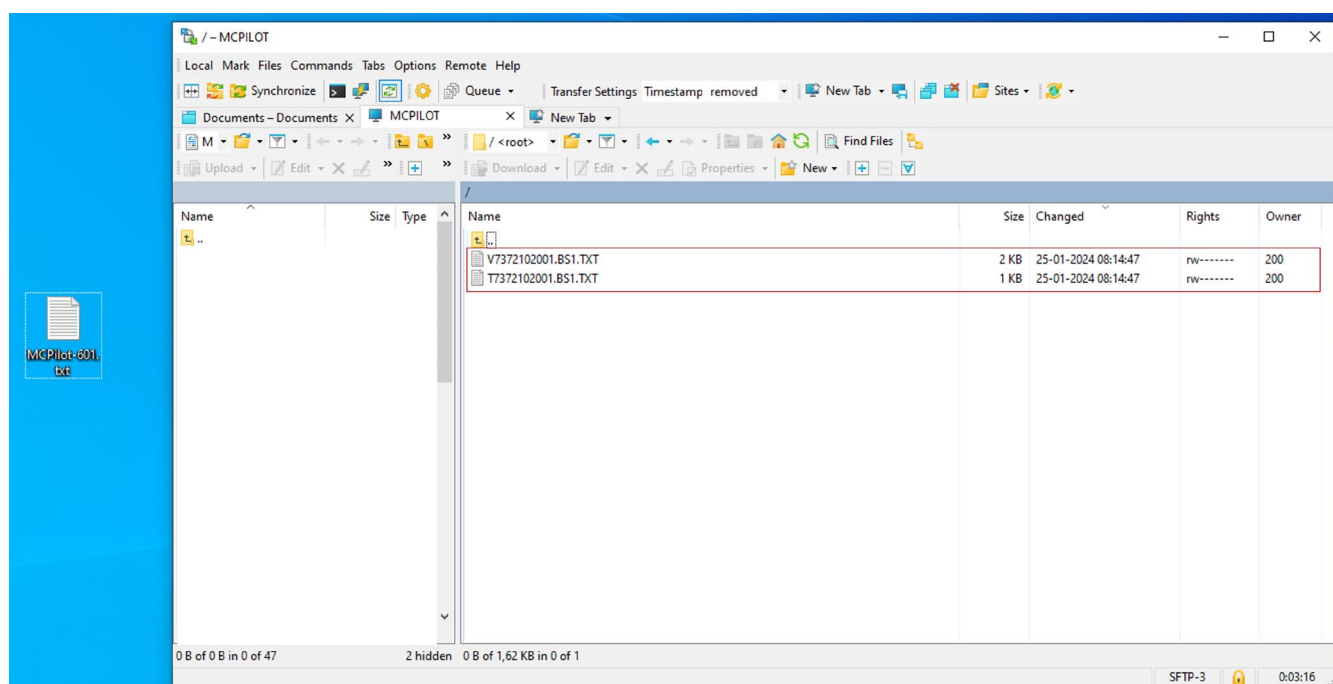


3.3 Når du vil sende en fil, finder du den ønskede fil, dér hvor du har gemt den på din PC. I dette tilfælde er filen gemt på PC'ens skrivebord.

Send nu filen ved at trække den fra skrivebordet (eller fra mappe, hvor du har gemt filen) på din PC til rodmappen i My File Transfer.



Kort efter kan du se dine kvitteringsfiler, som viser, at du har sendt filen. Hvis det ikke sker med det samme, kan du prøve at genindlæse siden.



Sådan genererer du sikkerhedsnøgler

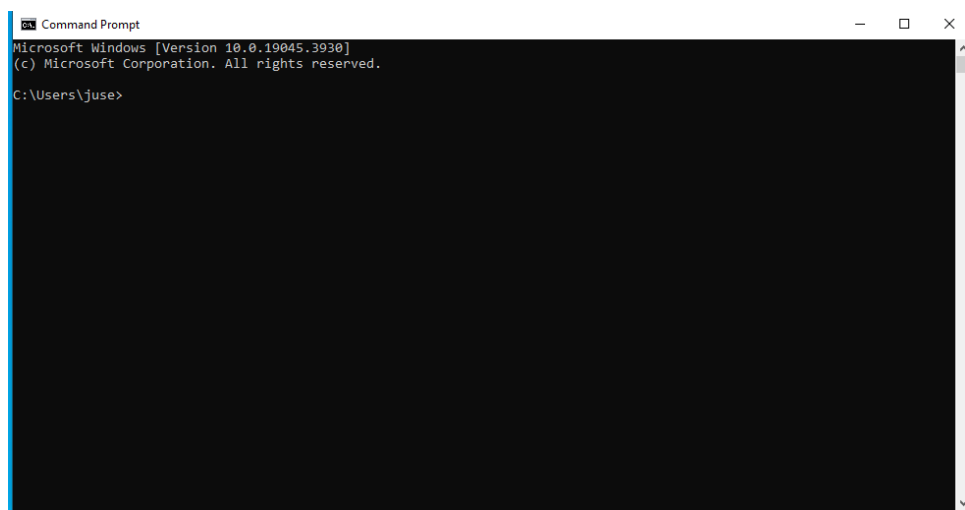
Når du ønsker at generere nye sikkerhedsnøgler, kan du følge trinene i dette afsnit. Du kan gøre det når som helst, efter behov. Vi anbefaler, at du udskifter dine sikkerhedsnøgler hvert tredje år.

For at sikre, at du kan kommunikere sikkert med Mastercard Payment Services' server gennem SFTP-løsningen, anvendes sikkerhedsnøgler. Sikkerhedsnøgler er et nøglepar, der består af en privat og en offentlig nøgle. Hver af din virksomheds postkasser i My File Transfer skal have sikkerhedsnøgler tilknyttet.

Den private nøgle tilhører din virksomhed og skal gemmes et sikkert sted på virksomhedens drev. Den offentlige sikkerhedsnøgle skal du overføre til den respektive postkasse i My File Transfer. Læs nedenfor, hvordan du gør dette.

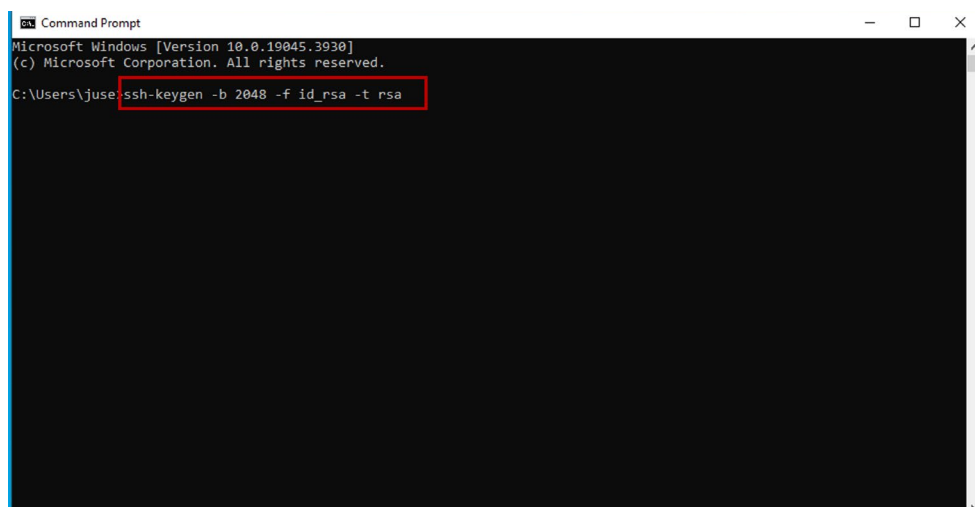
Nøglegenereringen udføres af dig selv med et kommandolinjeværktøj – en *command-line interpreter*.

1. Åbn **Command Prompt** eller et lignende værktøj, *command-line interpreter*. I eksemplet anvendes Command Prompt, og brugeren hedder 'juse'.



```
Microsoft Windows [Version 10.0.19045.3930]
(c) Microsoft Corporation. All rights reserved.
C:\Users\juse>
```

2. Skriv denne kommando for at generere nye RSA-sikkerhedsnøgler af længden 2048 bits*:
ssh-keygen -b 2048 -f id_rsa -t rsa

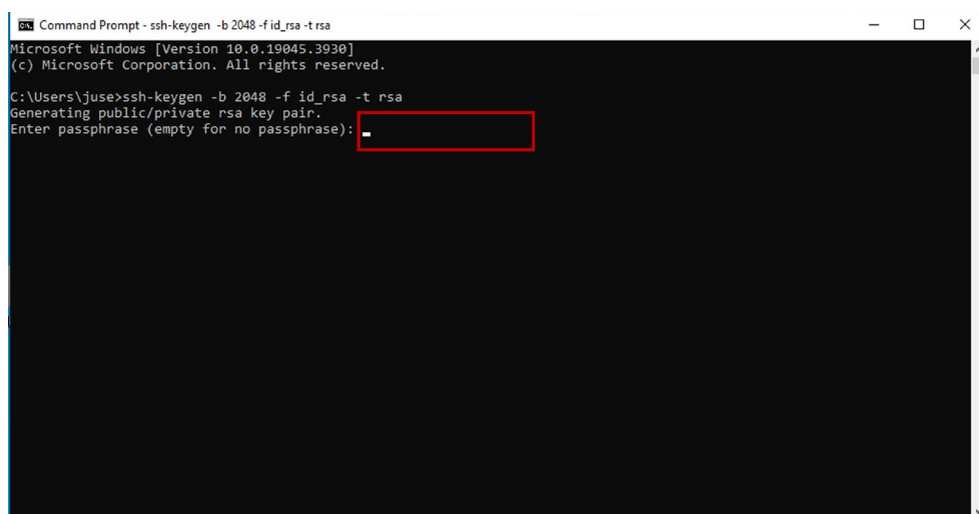


```
Microsoft Windows [Version 10.0.19045.3930]
(c) Microsoft Corporation. All rights reserved.
C:\Users\juse> ssh-keygen -b 2048 -f id_rsa -t rsa
```

*OBS! Sikkerhedsnøglerne skal være RSA-nøgler, og længden skal være 2048 bits.

3. Du vil nu blive bedt om at indtaste et selvvalgt kodeord, også kaldt passphrase.

Kodeordet skal bestå af minimum 5 karakterer, som må være tal og bogstaver. Kodeordet sikrer, at kun personer med kendskab til dette kan anvende den private sikkerhedsnøgle.

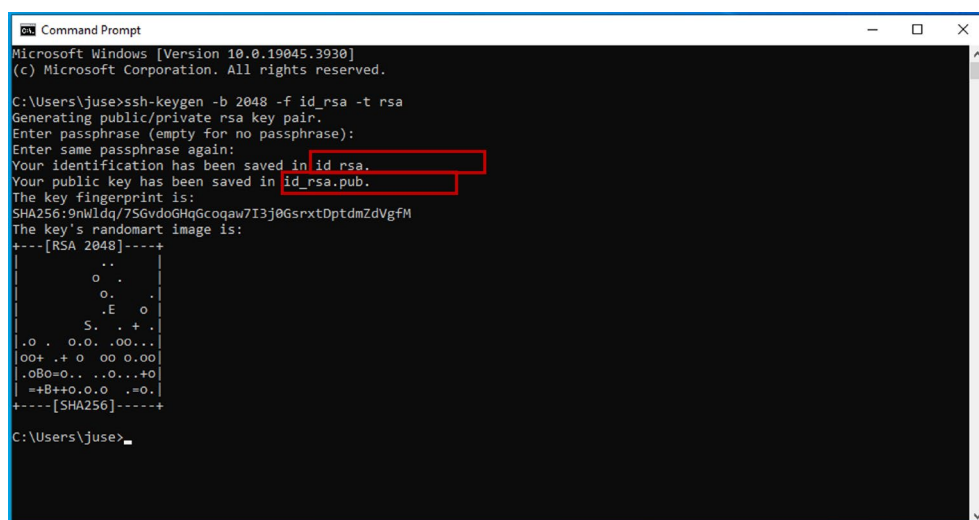


```
Command Prompt - ssh-keygen -b 2048 -f id_rsa -t rsa
Microsoft Windows [Version 10.0.19045.3930]
(c) Microsoft Corporation. All rights reserved.

C:\Users\juse>ssh-keygen -b 2048 -f id_rsa -t rsa
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
```

4. Kommandoen vil generere to nøglefiler:

- **id_rsa**, som er den private nøgle.
- **id_rsa.pub**, som er den offentlige nøgle.



```
Command Prompt
Microsoft Windows [Version 10.0.19045.3930]
(c) Microsoft Corporation. All rights reserved.

C:\Users\juse>ssh-keygen -b 2048 -f id_rsa -t rsa
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_rsa.
Your public key has been saved in id_rsa.pub.
The key fingerprint is:
SHA256:9nWldq/7SGvdoGhgGcoqaw7I3j0GsrxtDptdmZdVgfM
The key's randomart image is:
+---[RSA 2048]---+
  .o..
  o..
  .E o
  S. . +
  .o . o.o .oo..
  oo+ .+ o oo o.oo
  .oBo=o.. ..o..+o
  |=+B+o.o.o .o.
+---[SHA256]-----+

C:\Users\juse>
```

Du har nu genereret nye sikkerhedsnøgler. Den private nøgle skal du gemme et sikkert sted på din virksomheds drev, mens du skal overføre den offentlige nøgle til din postkasse i My File Transfer. Det gør du ved at følge de næste to trin.

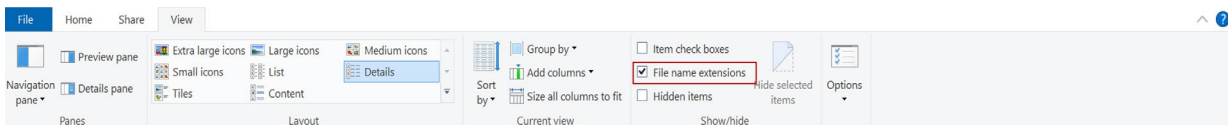
Har du mistet din sikkerhedsnøgle eller glemt dit passphrase, kan du anvende en HTTPS-løsning – læs mere i afsnittet "Få hjælp og svar på dine spørgsmål" på side 16 i denne vejledning.

5. Omdøb din offentlige nøgle

Tilgå nu den mappe, dine nøglefiler automatisk er blevet gemt i. I eksemplet ovenfor er der tale om mappen C:\Users\juse>.

Du skal nu omdøbe din offentlige nøgle og gemme den i formatet .txt. OBS! For at kunne gemme filen som en .txt skal du kunne se hele filnavnet.

Det kan du tilvælge i stifinder ved at klikke på **'View'** eller **'Vis'** og sætte et flueben i **'File name extensions'** eller **'Filtypernavne'**.



Filen skal navngives på følgende måde:

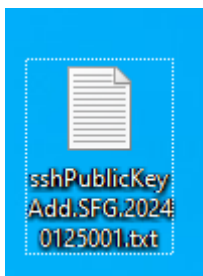
sshPublicKeyAdd.SFG.YYYYMMDDNNN.txt

YYYYMMDD henviser til dags dato skrevet på følgende måde: år, måned, dato.

NNN henviser til et selvvalgt nøglenummer, som skal bestå af tre tal som fx 001.

Til eksempel gemmes en fil, der sendes den 25. januar 2024 med nøglenummeret 001, derfor på følgende måde: **sshPublicKeyAdd.SFG.20240125001.txt**

Her er filen trukket ud af mappen og gemt på PC'ens skrivebord.



6a. Hvis du i dag anvender en HTTPS-løsning og nu også ønsker at benytte en SFTP-løsning, eller ikke længere kan skabe forbindelse med SFTP, skal du gøre følgende:

Log på postkassen, som du plejer, ved at indtaste **UserID** og **adgangskode**. Når du er logget ind i postkassen, står du automatisk på fanen **'Overfør filer'**.

Klik på pilen til højre for **'Postkassesti'** og vælg **'/'**.

The screenshot shows the 'My File Transfer' web application. At the top, there's a dark header with the Mastercard logo and the text 'My File Transfer'. Below this, a navigation bar contains two tabs: 'Overfør filer' (active) and 'Download filer'. In the top right corner of the header, there is a 'Log ud' link. The main content area is titled 'Overfør en fil' with the subtitle 'Angiv postkassefil og omdøbningsmønster'. It features a 'Postkassesti:' dropdown menu showing a path, a 'Fil:' input field with a 'Vælg filer' button and the text 'Der er ingen fil valgt', and an 'Omdøb fil som:' input field. An orange 'Send' button is located at the bottom left of the form. The footer of the page displays '© 2023 Mastercard'.

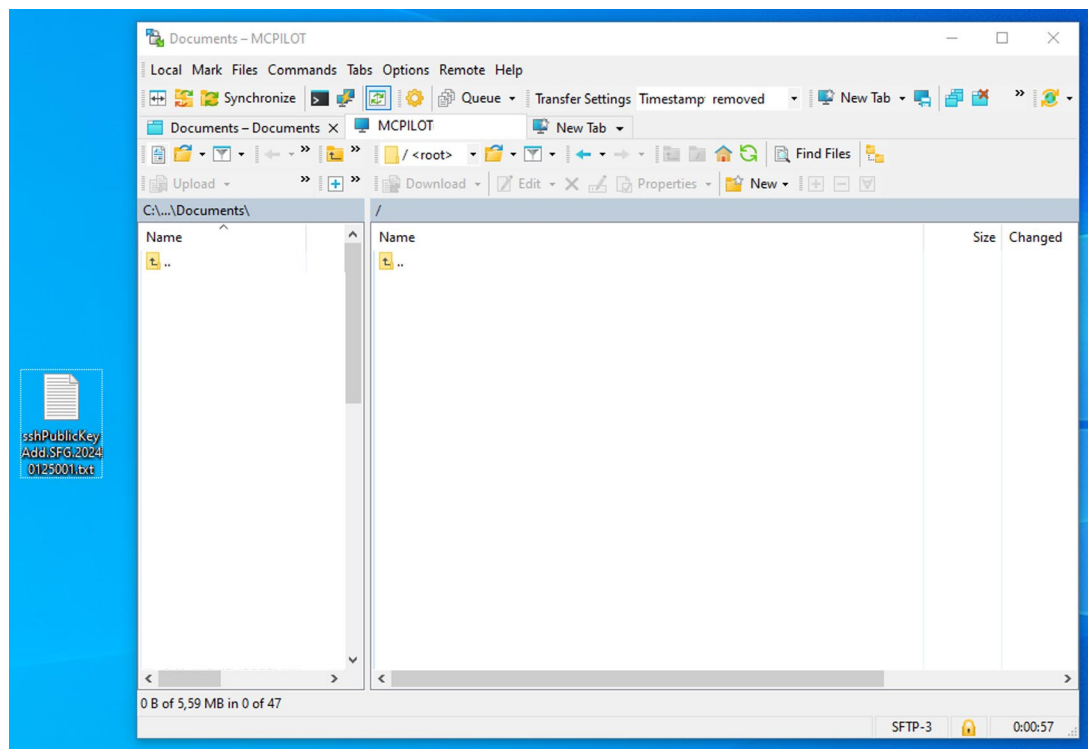
Klik på **'Vælg fil'** for at overføre den offentlige nøgle til postkassen og klik på **'Send'**.

Når din offentlige nøgle er overført til postkassen, kommer der en meddelelse frem, som fortæller, at filoverførslen er fuldført. Det er en god idé at sikre dig, at din nøgle er blevet overført og accepteret. Det gør du ved at gå ind under fanen 'Download filer', hvor du bl.a. kan finde kvitteringer. Der kan gå nogle minutter, før kvitteringen er klar.

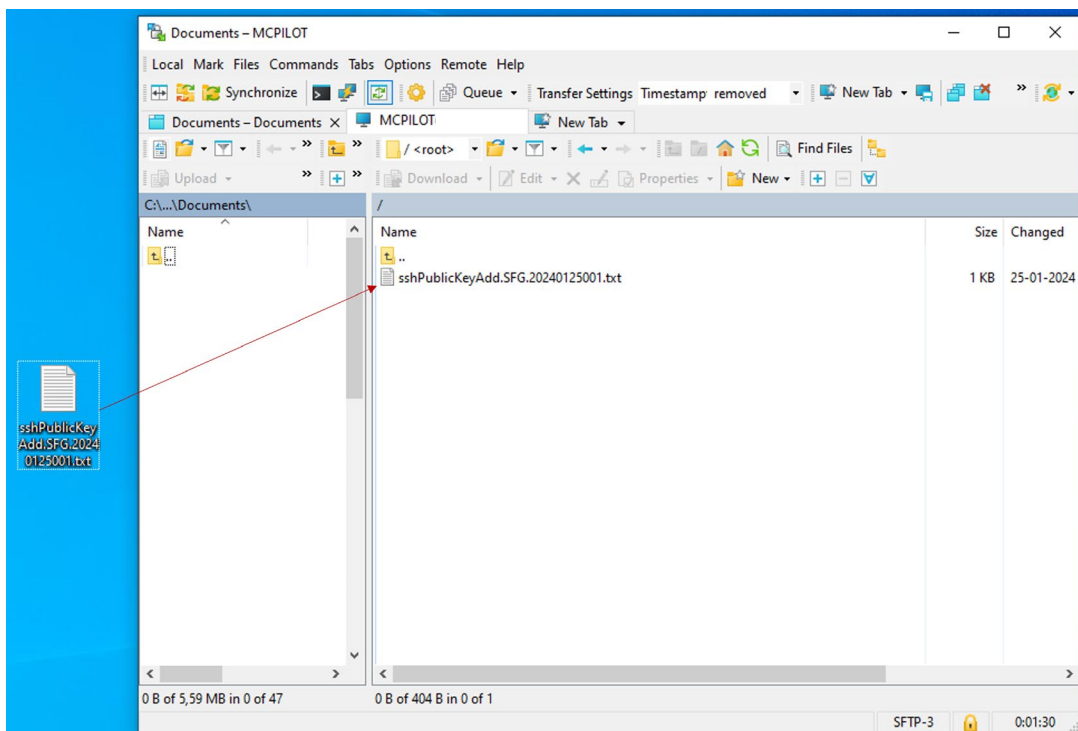
6b. Hvis du i dag anvender en SFTP-løsning og vil generere nye sikkerhedsnøgler, kan du uploade din offentlige nøgle til postkassen ved at gøre følgende (**OBS. Dette kræver, at du har et fungerende nøglepar og kan skabe forbindelse til postkassen i forvejen**):

Forbind din virksomheds postkasse i My File Transfer via en SFTP-klient (se afsnittet "Forbind til IP-adresse og port" i denne vejledning).

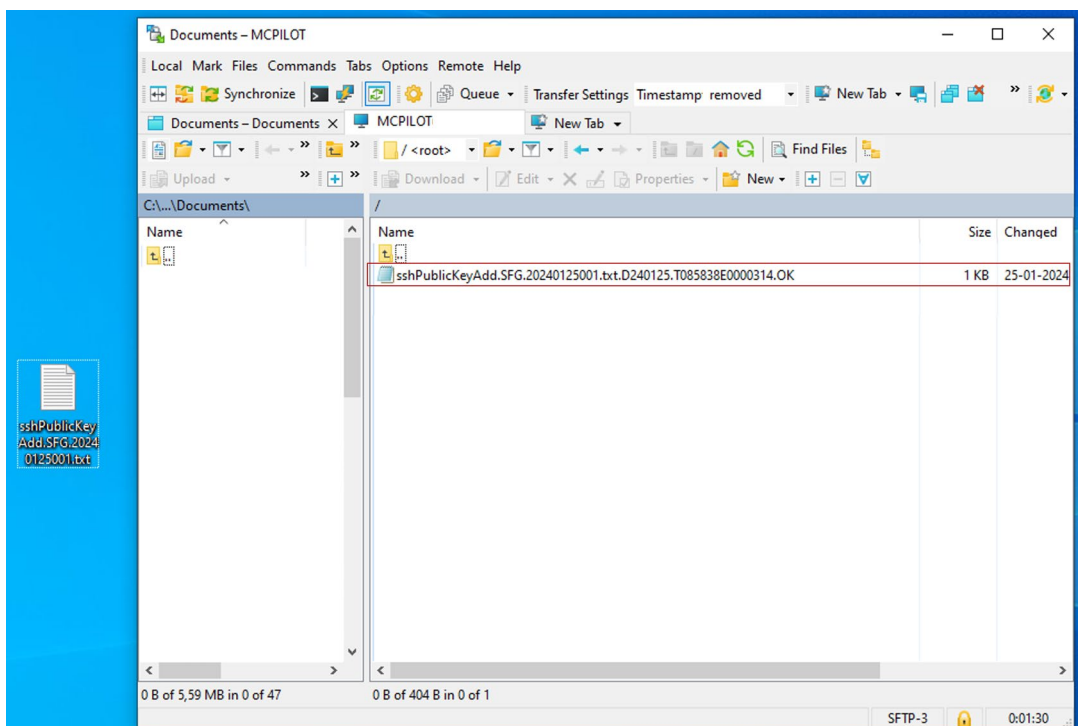
Find din offentlige nøgle. I dette tilfælde ligger den gemt på PC'ens skrivebord.



Din offentlige nøgle skal nu overføres til rodmappen i din postkasse i My File Transfer. Overfør din offentlige nøgle til rodmappen ved at trække filen fra PC'ens skrivebord (eller fra den mappe, hvor du har gemt filen) til postkassen i My File Transfer.



Du kan nu se din kvitteringsfil, som viser, at du har uploadet den offentlige nøgle.



Du har nu genereret og uploadet sikkerhedsnøgler til din postkasse i My File Transfer og kan lukke din SFTP-klient. Du kan udveksle filer med Mastercards produkter igen straks efter, at nøglerne er opdateret.

I syv dage efter, du har uploadet nye sikkerhedsnøgler, virker både dine nye og gamle nøgler. Efter de syv dage, er det kun de nye sikkerhedsnøgler, der virker. For at undgå forvirring, anbefaler vi derfor, at du begynder at anvende dine nye sikkerhedsnøgler lige efter, du har uploadet dem.

Få hjælp og svar på dine spørgsmål

På denne hjemmeside finder du mere information om SFTP-løsningen i My File Transfer:

<https://www.mastercardpaymentservices.com/denmark/my-file-transfer/sftp>

Her har vi også samlet svar på de mest stillede spørgsmål om systemet og løsningen.

Har du **mistet din sikkerhedsnøgle eller glemt dit passphrase**, er det muligt at bruge en HTTPS-løsning i stedet. Her skal du bruge dit UserID og adgangskode for at logge ind i My File Transfer. Du kan læse mere om, hvordan du bruger en HTTPS-løsning til at logge ind og sende og modtage filer her:

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

Sikkerhed og rettigheder

Ved overførsel af data er din forsendelse til Mastercard Payment Services identificeret ved hjælp af din private nøgle.

Inden dataudvekslingen finder sted udveksles der, sammen med den offentlige nøgle, en såkaldt sessionsnøgle, der anvendes til kryptering af dine data. Sessionsnøglen er unik for den enkelte dataudveksling og anvendes til kryptering af din leverance.

Løsningen giver sikkerhed for, at dataudvekslingen lever op til Momsbekendtgørelsens krav vedrørende elektronisk fakturering.

Den driftsmæssige sikkerhed kan etableres ved, at du opbygger SFTP-løsningen til at blive afviklet automatisk.

Dit MitID Erhverv kan samtidig anvendes som backup-løsning til en manuel dataudveksling ved hjælp af Mastercard Payment Services' HTTPS-løsning.

Mastercard Payment Services kan ikke drages til ansvar for konsekvensen af usikker opbevaring af de genererede sikkerhedsnøgler hos dig.

Mastercard Payment Services anbefaler, at du udskifter dine sikkerhedsnøgler med jævne mellemrum, gerne hvert tredje år. Du er selv ansvarlig for at kontrollere, om dette svarer til din virksomheds sikkerhedspolitik.

Hvis du har en fornemmelse af, at din private nøgle er blevet afluret eller af andre årsager ikke længere giver den nødvendige sikkerhed, skal du straks kontakte Mastercard Payment Services.

Alle rettigheder til denne vejledning og det tilhørende produkt tilhører Mastercard Payment Services A/S. Det er ikke tilladt at kopiere, videregive eller på anden måde gøre materialet eller dele heraf tilgængeligt for tredjepart uden tilladelse fra os.

Krav til SFTP-klienten

Du kan se, hvilke krav Mastercard stiller til din SFTP-klient nedenfor. Bemærk, at udtrykkene under 'Algoritmetype' ofte vil stå på engelsk i din klient.

Algoritmetype	Formål	Supporterede algoritmer/versioner
Host Key	Autentificering af server	- rsa-sha2-256 - rsa-sha2-512
Key Agreement / Key Exchange	Udledning af krypteringsnøgler, initialisering af vektorer, MAC-nøgler	- ecdh-sha2-nistp256 - ecdh-sha2-nistp384 - ecdh-sha2-nistp521 - curve25519-sha256@libssh.org
Message Authentication Codes (MACs)	Beskyttelse af dataintegritet og forebyggelse af replay angreb	- hmac-sha2-256 - hmac-sha2-512 - hmac-sha2-256-etm@openssh.com - hmac-sha2-512-etm@openssh.com
Ciphers	Kryptering af data i kanal	- aes256-ctr - aes192-ctr - aes128-ctr - aes256-gcm@openssh.com - aes128-gcm@openssh.com
Public Key Algorithms	Autentificering mellem klient og server	- rsa-sha2-256 - rsa-sha2-512

Hvilke SFTP-operationer er tilladt i MCEnett?

- MCEnett tillader GET-, PUT- og DELETE-operationer på filer.
- Brugere har ikke tilladelse til at oprette eller slette mapper i MCEnett.
- Under en GET-operation tillader MCEnett ikke yderligere operationer som f.eks. at kontrollere andre filattributter. For eksempel – hvis brugeren har igangsat en GET-operation og under denne proces forsøger at kontrollere filstørrelsen, vil de få en fejlmeddelelse, og sessionen vil blive afbrudt.

Nedenfor er nogle generelle retningslinjer, som MCEnett opfordrer brugerne til at følge for at holde systemet sundt:

- MCEnett anbefaler brugere at undlade at udføre kontinuerlige polling-checks på vores system. Dette betyder, at brugere ikke bør lave kontinuerlige forsøg på at oprette forbindelse for at kontrollere tilslutningen.
- MCEnett anbefaler, at brugerne afslutter sessionen straks eller inden for en rimelig tid (30 sekunder, hvis brugeren afventer en kvittering) efter filoperation.
- MCEnett anbefaler brugere at undlade at udføre nogen operation på filer efter vellykket upload til en postkasse. Brugere skal udføre alle operationer først og derefter uploade (foretage PUT-operationen). For eksempel, hvis en bruger har uploadet filen og derefter forsøger at omdøbe den, vil det resultere i en fejl, og operationen vil mislykkes.