



Brugervejledning

**SÅDAN GENERERER DU NYE
SIKKERHEDSNØGLER I ENETT2**

Opdateret marts 2023

Indhold

Indhold	2
Introduktion	3
1 Generér nye sikkerhedsnøgler	4
2 Omdøb din offentlige nøgle	6
3 Upload din offentlige nøgle i eNett2	7
Har du spørgsmål eller brug for hjælp?	9
Rettigheder og sikkerhed	9

Introduktion

Denne brugervejledning er for dig, der anvender en SFTP-forbindelse i systemet eNett2 til at udveksle filer med produkter hos Mastercard Payment Services (tidligere Nets).

Vejledningen guider dig igennem tre trin til at opdatere dine sikkerhedsnøgler i eNett2 ved brug af en SFTP-klient.

Sikkerhedsnøgler er et nøglepar bestående af en privat og en offentlig nøgle. De har til formål at skabe en sikker forbindelse, når du via eNett2 udveksler filer med Mastercard Payment Services. Den private nøgle skal være gemt et sikkert sted på din virksomheds drev, mens den offentlige nøgle skal være tilknyttet din postkasse i eNett2.

Du skal generere nye sikkerhedsnøgler for hver af din virksomheds postkasser i eNett2. De nye sikkerhedsnøgler skal være RSA-nøgler, der består af 2048 bits.

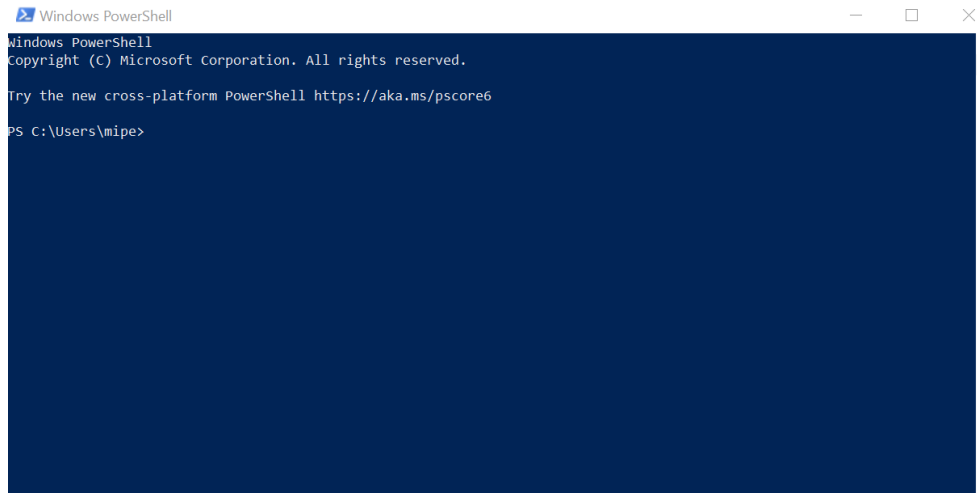
Det kræver kendskab til jeres SFTP-forbindelse i eNett2 at opdatere sikkerhedsnøgler. Hvis ikke du selv har dette kendskab, kan du kan med fordel dele denne vejledning med en kollega, systemleverandør eller IT-konsulent, der kan hjælpe dig med at opdatere nøglerne.

Nedenfor følger en gennemgang af de tre trin, du skal igennem for at opdatere sikkerhedsnøgler for en postkasse i eNett2.

1 Generér nye sikkerhedsnøgler

Åbn Windows PowerShell eller et lignende værktøj, *command-line interpreter*.

I eksemplet anvendes Windows Powershell, og brugeren hedder 'mipe'.



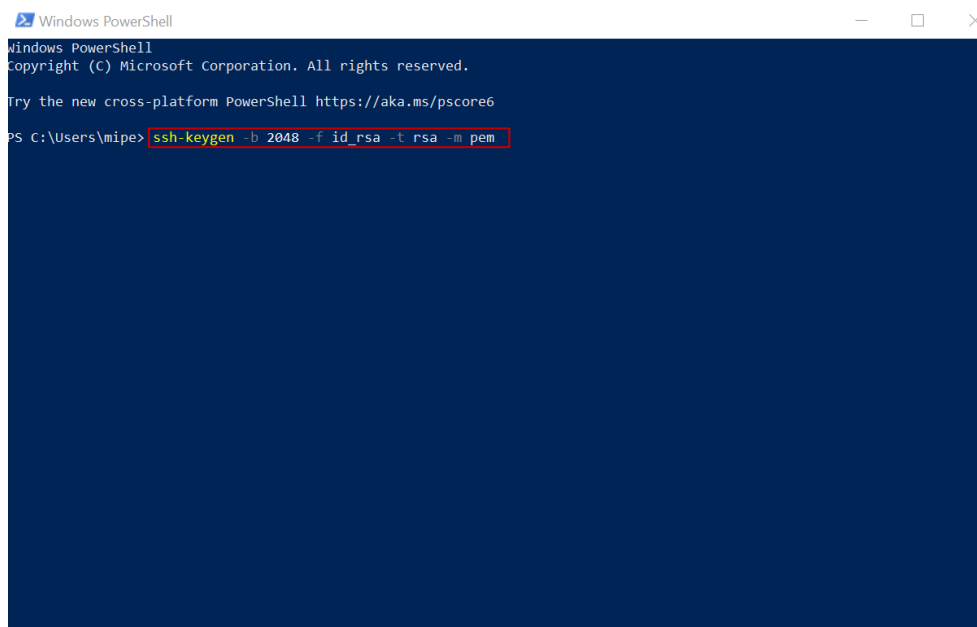
```
Windows PowerShell
Copyright (c) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\mipe>
```

Skriv denne commando for at generere nye RSA-sikkerhedsnøgler af længden 2048 bits*:

ssh-keygen -b 2048 -f id_rsa -t rsa



```
Windows PowerShell
Copyright (c) Microsoft Corporation. All rights reserved.

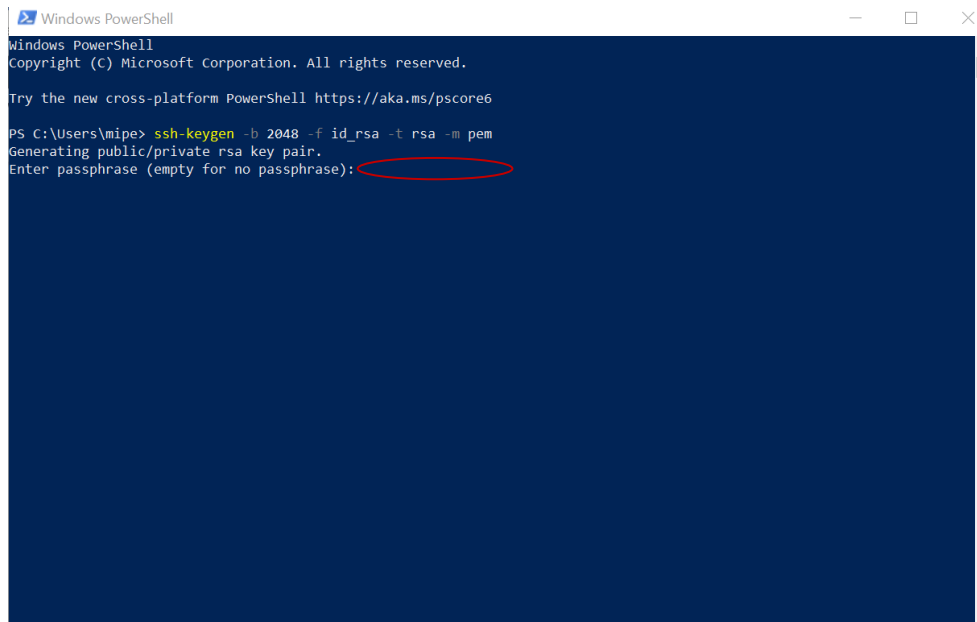
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\mipe> ssh-keygen -b 2048 -f id_rsa -t rsa -m pem
```

*NB! Sikkerhedsnøglerne *skal* være RSA-nøgler og længden skal være 2048 bits for at kunne benyttes fremadrettet.

Du vil nu blive bedt om at indtaste en selvvalgt kodeord eller **passphrase**.

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



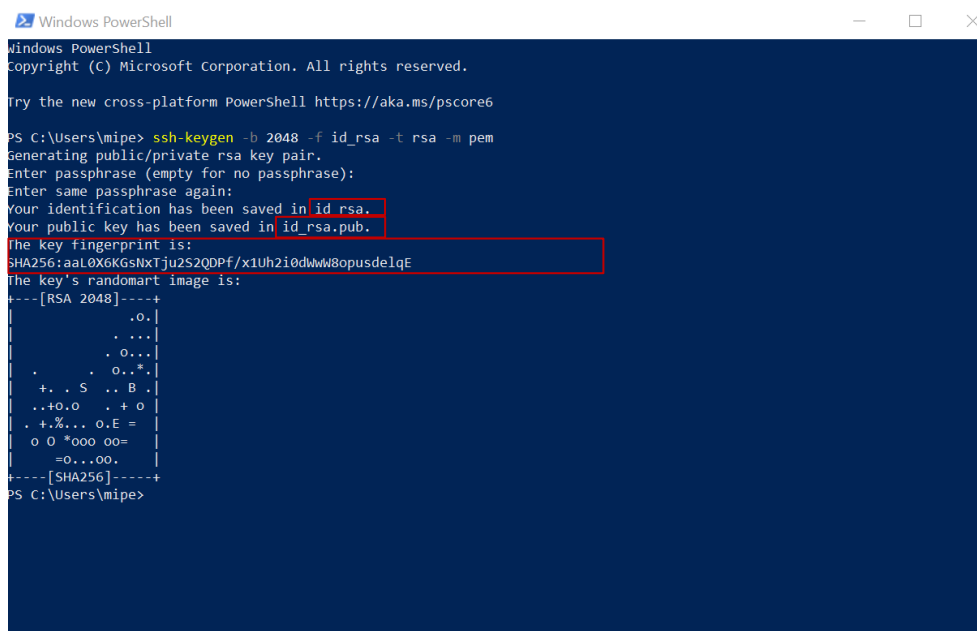
```
Windows PowerShell
Copyright (c) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

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

Kommandoen vil generere to nøglefiler:

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



```
Windows PowerShell
Copyright (c) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\mipe> ssh-keygen -b 2048 -f id_rsa -t rsa -m pem
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:aaL0X6KGSNXTju2S2QDPf/x1Uh2i0dww8opusdelqE
The key's randomart image is:
+---[RSA 2048]-----+
|
|  .o. |
| +. +. |
|  o.. |
| +. o.. |
|  .S..B |
| ..+o.o .+o |
| .+%. .o.E = |
| o 0 *000 00= |
| =0...00. |
+---[SHA256]-----+
PS C:\Users\mipe>
```

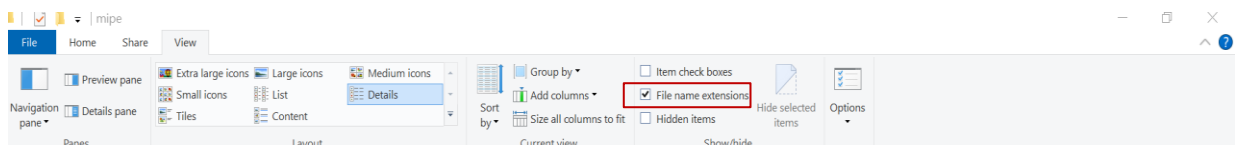
Du har nu generet nye sikkerhedsnøgler. Den private nøgle skal du gemme et sikkert sted på din virksomheds drev, mens du skal overføre den offentlige nøgle til din postkasse i eNett2. Det gør du ved at følge de to følgende step.

2 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\mipe>.

Du skal nu omdøbe din offentlige nøgle og gemme den i formatet .txt. **NB!** 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 **'Filtypenavne'**.



Filen skal navngives på følgende måde:

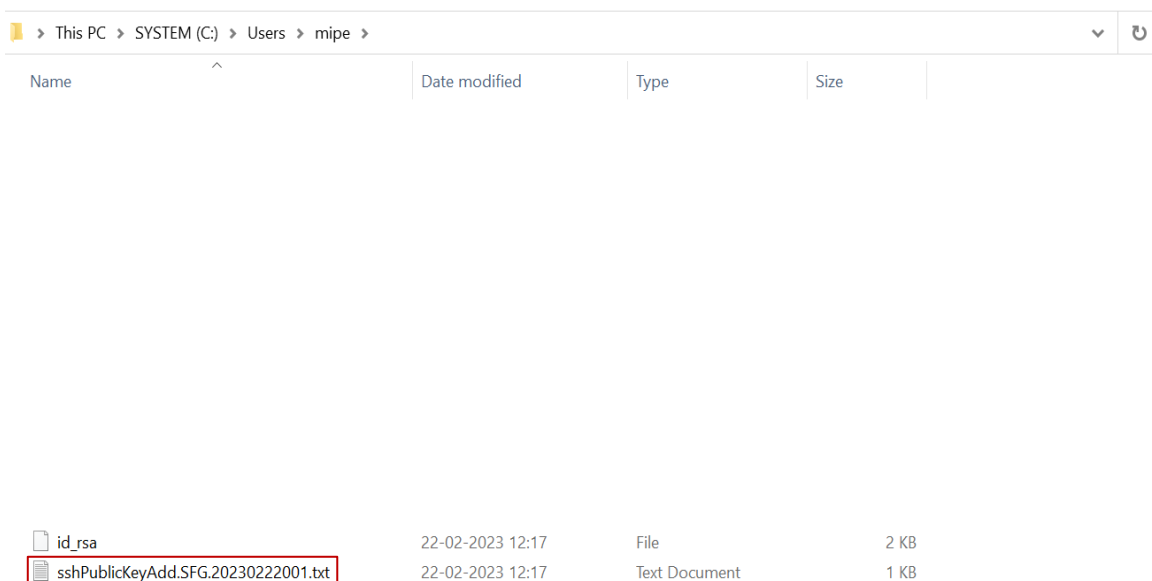
sshPublicKeyAdd.SFG.yyyymmddnnn.txt

yyymmdd 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 22. februar 2023 med nøglenummeret 001 derfor på følgende måde*:

sshPublicKeyAdd.SFG.20230222001.txt

A screenshot of the Windows File Explorer interface showing a file list. The file 'sshPublicKeyAdd.SFG.20230222001.txt' is highlighted with a red rectangle. The file list has columns for Name, Date modified, Type, and Size.

Name	Date modified	Type	Size
id_rsa	22-02-2023 12:17	File	2 KB
sshPublicKeyAdd.SFG.20230222001.txt	22-02-2023 12:17	Text Document	1 KB

3 Upload din offentlige nøgle i eNett2

Forbind nu til din virksomheds postkasse i eNett2 via en SFTP-klient. I eksemplet neden for anvendes Filezilla, og vi tilgår en testbruger kaldet TMAFILE1 i et testmiljø.

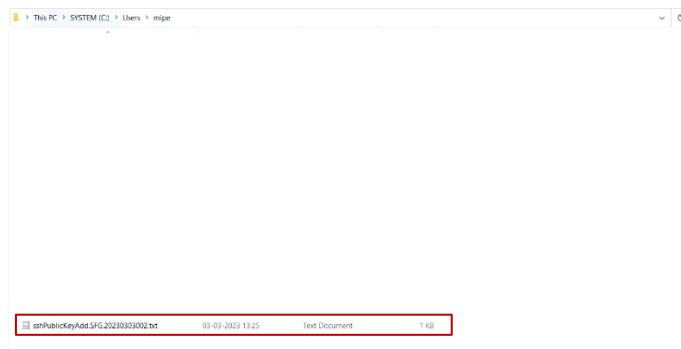
Anvend følgende host for at tilgå via en SFTP-forbindelse: **sftp://ft.nets.eu**

Anvend følgende port: **10222**

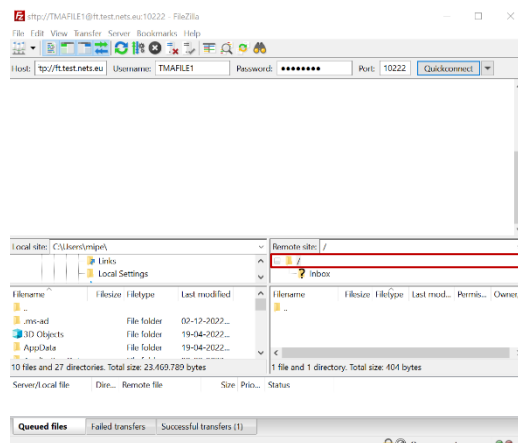
Klik nu på **'Quickconnect'**.



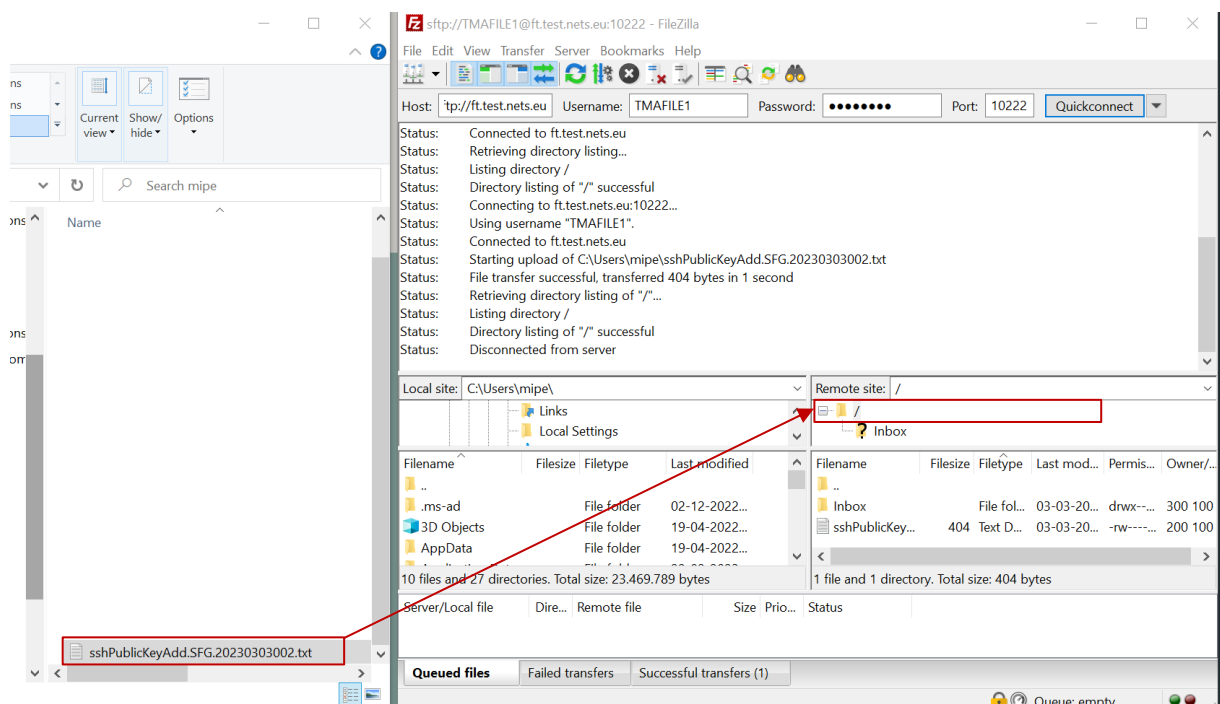
Find nu din offentlige nøgle. I dette tilfælde ligger den i **This PC → System (C) → Users → mipe**.



Din offentlige nøgle skal nu overføres til **rodmappen i din postkasse** i eNett2.



Overfør nu din offentlige nøgle til rodmappen i din postkasse ved at trække filen fra mappen på din PC til postkassen i eNett2.



Du har nu opdateret dine sikkerhedsnøgler til din postkasse i eNett2 og kan lukke din SFTP-klient. Du kan udveksle filer med Mastercards produkter igen straks efter, nøglerne er opdateret.

I syv dage efter, du har genereret 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, du begynder at anvende dine nye sikkerhedsnøgler lige efter, du har genereret dem.

Har du spørgsmål eller brug for hjælp?

Besøg dette site og få mere information om, hvorfor det er nødvendigt at hente nye offentlige og private nøgler: <https://www.mastercardpaymentservices.com/denmark/my-file-transfer>.

Du er også altid velkommen til at ringe til vores datasupport på (+45) 8081 0679, hvis du har yderligere spørgsmål. De kan træffes alle hverdage mellem 09:00-16:00.

Rettigheder og sikkerhed

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

Mastercard Payment Services anbefaler, at du udskifter dine sikkerhedsnøgler med jævne mellemrum. 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.



©2021 Mastercard. Mastercard is a registered trademark, and the circles design is a trademark of Mastercard International Incorporated.