

## **Vejledning til Serviceplatformens SFTP Service**

Udarbejdet for:

KOMBIT A/S

Halfdangsgade 8

2300 København S



## Revision

Nuværende revision: 1.59

### Revisionshistorik

Revision	Frigivelsesdato
1.0	22.05.15
1.1	24.11.15
1.2	28.07.16
1.3	Afventer Kombit godkendelse
1.40	25.01.17 godkendt af KOMBIT
1.41	Versionshistorik opdateret
1.42	Ændret afsnit ift. opsætning af SFTP på IT system idet dette nu håndteres på det fælles administrationsmodul (STS-Admin)
1.43	Diverse fejlrettelser
1.49	04.03.19 godkendt af KOMBIT
1.55	SenderTimestamp i Meta fil ændret til Zulu time format
1.56	Change DemoVirtuel to ROUTING_V1_0_0
1.57	Renset for kommentarer efter godkendelse.
1.58	Opdateret med info om SSH nøgle struktur (6.1.1.1)
1.59	18.08.21. Opdateret sektion 6.3 felt med dummy data efter KOMBITs ønske. "<RecipientIT-system>" ændret til "<Recipientlt-system>"

## Indhold

1	Formål med vejledning til Serviceplatformens SFTP Service .....	6
2	Begreber.....	6
3	SFTP Service beskrivelse .....	6
3.1	Simpel overførsel af filer .....	7
3.2	Styret overførsel af filer .....	7
3.3	Dynamisk Routing .....	8
4	Oprettelse af adgang til SFTP servicen på Serviceplatformen .....	9
5	Oversigt over it-systemers brugernavne.....	10
6	Teknisk dokumentation .....	11
6.1	Brug af SFTP serveren.....	11
6.1.1	Adgang til SFTP serveren.....	11
6.1.2	Mappestruktur .....	13
6.1.3	Upload af filer .....	13
6.1.4	Oprydning og monitorering på SFTP serveren .....	13
6.1.5	Information omkring SFTP server .....	15
	It-systemer skal tilgå Serviceplatformens SFTP server via dens offentlige hostnavn. ....	15
	For produktionsmiljøet er denne: <a href="https://sftp.serviceplatformen.dk">sftp.serviceplatformen.dk</a> .....	15
6.2	Simpel overførsel af filer .....	15
6.2.1	Brugseksempel.....	15
6.3	Dynamisk routing .....	17
6.3.1	Brugseksempel.....	18
6.4	Styret overførsel af filer .....	20
6.4.1	SFTP servicens webservice.....	20
6.4.2	It-systemets webservice beskrivelse.....	21
6.4.3	Brugseksempel.....	21
6.5	XML-Strukturer .....	24
6.5.1	Triggerobjekt.....	25
6.5.2	SFTPDynamicRoutingInfo.....	25
6.5.3	Teknisk kvittering .....	26
6.5.4	Fejlkode .....	28
6.5.5	Metadatafil .....	30
6.5.6	Forretningskvittering .....	30

6.6 Validering af triggerobjekter ..... 32

## 1 Formål med vejledning til Serviceplatformens SFTP Service

Dette dokument har til formål at vejlede it-leverandører i brug af Serviceplatformens SFTP service. Indledningsvis gives en kort overordnet introduktion til SFTP servicen. De følgende afsnit giver en vejledning til oprettelse af et it-system, som skal anvende SFTP servicen, og til anvendelse af Serviceplatformens SFTP server og selve SFTP servicen.

## 2 Begreber

Til dette dokument bruges følgende termer:

<b>Afsendersystemet</b>	Det it-system der vil overføre en fil til et modtagersystem.
<b>Modtagersystemet</b>	Det it-system som et afsendersystem ønsker at sende en fil til.
<b>It-system</b>	Kommunens it-system, der benytter eller potentielt kan benytte services på Serviceplatformen. For at få adgang skal it-systemet identificere sig med et gyldigt FOCES/VOCES certifikat. For at bruge SFTP skal it-systemet være oprettet som bruger af Serviceplatformens SFTP Service
<b>Triggerobjekt</b>	En xml struktur der bruges til at specificere hvem modtageren af en given fil er.
<b>Triggerfil</b>	En fil hvis indhold er et triggerobjekt.
<b>Teknisk kvittering</b>	En xml struktur der genereres af Serviceplatformen på basis af en validering af et triggerobjekt. Hvis triggerobjektet er validt eller indeholder fejl vil dette fremgå af den tekniske kvittering.
<b>Forretningskvittering</b>	En xml-struktur der bruges af et modtagersystem til at kvittere for modtagelsen af en fil.
<b>Metadata fil</b>	En xml struktur der beskriver en given fil, der skal overføres fra et afsender- til et modtagersystem.
<b>SFTPDynamicRoutingInfo</b>	En xml struktur der anvendes til at identificere modtagersystemet når dynamisk routing anvendes.
<b>SFTP webservice</b>	En webservice der udstilles på Serviceplatformen som en del af SFTP servicen.

## 3 SFTP Service beskrivelse

Serviceplatformens SFTP Service gør det muligt for it-systemer at udveksle filer med hinanden på en kontrolleret måde.

Udvekslingen af en fil sker ved at et afsendersystem uploader en fil til Serviceplatformens SFTP Server, hvorefter afsenderen leverer en besked til SFTP Servicen, om hvilket it-system filen skal sendes til. Adresseringen af en fil leveres i et såkaldt triggerobjekt. Et triggerobjekt er en xml struktur, hvori det er specificeret, hvem modtageren af en given fil er. Ved hjælp af triggerobjektet sørger Serviceplatformen for at overføre den specificerede fil til en mappe på SFTP Serveren, hvor modtagersystemet kan afhente den.

Serviceplatformen fungerer altså som bindeled mellem it-systemer, og gør det muligt for disse at udveksle filer på en kontrolleret måde.

Filudvekslingen mellem it-systemer sker på Serviceplatformens SFTP server. Hvert it-system har to private mapper på SFTP serveren, som kun it-systemet har adgang til. Den ene mappe er beregnet til

indkommende filer, mens den anden er beregnet til udgående filer. Overførslen af en fil mellem to it-systemer sker ved, at Serviceplatformen flytter filen fra afsendersystemets udgående mappe til modtagersystemets indkommende mappe på SFTP serveren.

Der er to typer af filudveksling som it-systemer der benytter SFTP Servicen kan anvende. Disse omtales som henholdsvis "simpel overførsel af filer" og "styret overførsel af filer" og er beskrevet i henholdsvis afsnit 3.1 og 3.2. Derudover er der ved "simpel overførsel af filer" mulighed for at anvende "dynamisk routing", som er en udvidet form for adressering af filer med ekstra sikkerhed. Dynamisk routing kan dog kun anvendes til services, hvor det er specificeret, at filudvekslingen skal ske via dynamisk routing på Serviceplatformens SFTP server. Dette skyldes, at dynamisk routing kræver, at der sættes ekstra konfiguration op på Serviceplatformen, for at det kan anvendes. Dynamisk routing er beskrevet i afsnit 3.3. Hvilken type et it-system vælger at bruge bestemmer bl.a., hvordan det skal levere triggerobjekter til SFTP servicen.

Pga. de forskellige typers virkemåde, er det kun muligt for it-systemer, der bruger samme type af filudveksling at udveksle filer.

SFTP servicen gør det også muligt for it-systemer at modtage opdateringsfiler med CPR-data ifm. brug af CPR Abonnement servicen. I den forbindelse skal it-systemet oprettes med filudvekslingstype "simpel". Det er kun nødvendigt at følge de trin som er beskrevet i afsnit 4, idet Serviceplatformen står for levering af opdateringsfilen.

## 3.1 Simpel overførsel af filer

Ved typen "simpel overførsel af filer", sker overførslen af filer mellem it-systemer ved følgende procedure.

1. Afsendersystemet uploader filen, det ønsker at sende, samt en triggerfil til dets udgående mappe på SFTP serveren.
2. Triggerfilen opdages og læses af Serviceplatformen og valideres.
3. Serviceplatformen genererer en teknisk kvittering på baggrund af valideringen af triggerfilen og uploader kvitteringen til afsendersystemets indkommende mappe.
4. Hvis valideringen er succesfuld overføres filen til modtagersystemets indkommende mappe, sammen med en metadatafil.
5. Modtagersystemet har til ansvar at opdage, at en fil er overført til dets indkommende mappe og for at hente den overførte fil inden for et begrænset tidsrum. Det er også modtagersystemets ansvar at fjerne filen samt metadata filen.

En mere detaljeret beskrivelse af typen "simpel overførsel af filer" findes i afsnit 6.2.

## 3.2 Styret overførsel af filer

I forbindelse med styret overførsel af filer udstiller Serviceplatformen en webservice i stil med eksisterende services på Serviceplatformen. It-systemer der ønsker at anvende denne type skal tillige udstille en webservice baseret på en wsdl fil leveret af Serviceplatformen.

Ved typen "styret overførsel af filer" sker overførslen af filer mellem it-systemer efter følgende procedure.

1. Afsendersystemet uploader filen, det ønsker at sende til dets udgående mappe på SFTP serveren.
2. Afsendersystemet foretager et webservice kald til SFTP webservicen med et triggerobjekt.

3. Triggerobjektet valideres af Serviceplatformen, og en teknisk kvittering returneres som svar på webservice kaldet.
4. Hvis triggerobjektet bliver succesfuldt valideret, overføres filen til modtagersystemets indkommende mappe.
5. Serviceplatformen foretager herefter et kald til en webservice udstillet af modtagersystemet, med en notifikation om at en fil er blevet overført til dets indkommende mappe.
6. Modtagersystemet henter filen fra dets indkommende mappe, og kalder SFTP webservicen med en forretningskvittering.
7. Serviceplatformen kalder herefter en webservice udstillet af afsendersystemet med forretningskvitteringen leveret af modtagersystemet.

En mere detaljeret beskrivelse af typen "styret overførsel af filer" findes i afsnit 6.4.

### 3.3 Dynamisk Routing

Dynamisk routing giver udvidede muligheder for at kontrollere overførslen af filer mellem anvendersystemer. Her overføres filen ikke til det modtagersystem, der er angivet i triggerfilen, men fremsøges i stedet baseret på ekstra data der medsendes i triggerfilen. Det ekstra data leveres i triggerfilen i xml strukturen SFTPDynamicRoutingInfo.

For at anvende dynamisk routing, skal der i triggerfilen angives et "virtuelt" system, som modtagersystemet. Et virtuelt system er en prædefineret værdi, der angives som modtagersystem i triggerfilen. Hvis et virtuelt system angives som modtagersystem i en triggerfil, vil filen blive sendt, hvis et modtagersystem kan fremsøges baseret på det data der er medsendt i SFTPDynamicRoutingInfo strukturen.

Ved dynamisk routing kræves det, at der på Serviceplatformen er opsat routingregler, der angiver hvilke systemer og myndigheder, der har tilladelse til at sende til hinanden. Dette udgør den øgede sikkerhed i dynamisk routing, ved at det kun er systemer og myndigheder, som der er opsat routingregler for, der har tilladelse til at sende til hinanden.

Dynamisk routing fungerer ved, at der laves et opslag i routingreglerne, baseret på data der medsendes i SFTPDynamicRoutingInfo strukturen. Hvis der findes en matchende routingregel, overføres filen til det i routingreglen specificerede modtagersystem.

Dynamisk routing kan kun anvendes af anvendersystemer, hvis det er specifikt angivet, at det skal anvendes for den service der integreres til via Serviceplatformens SFTP Service. Hvis det forsøges anvendt til andre services, vil anvendersystemet opleve fejl, da der ikke vil være konfigureret routingregler for disse services.

En overordnet beskrivelse af typen "simpel overførsel af filer", hvor der anvendes dynamisk routing, er som følger:

1. Afsendersystemet uploader filen, det ønsker at sende samt en triggerfil til dets udgående mappe på SFTP serveren. Triggerfilen angiver en "virtuel" bruger som modtager og indeholder SFTPDynamicRoutingInfo xml strukturen.
2. Triggerfilen opdages og læses af Serviceplatformen, valideres og der fremsøges en routing regel baseret på SFTPDynamicRoutingInfo hvis muligt.
3. Serviceplatformen genererer en teknisk kvittering på baggrund af valideringen af triggerfilen og uploader kvitteringen til afsendersystemets indkommende mappe.
4. Hvis valideringen er succesfuld overføres filen til modtagersystemets indkommende mappe, sammen med en metadatafil.



5. Modtagersystemet har til ansvar at opdage, at en fil er overført til dets indkommende mappe og for at hente den overførte fil inden for et begrænset tidsrum. Det er også modtagersystemets ansvar at fjerne filen samt metadata filen.

En mere detaljeret beskrivelse af dynamisk routing findes i afsnit 6.3.

## **4 Oprettelse af adgang til SFTP servicen på Serviceplatformen**

Processen for at blive oprettet som it-system, der kan benytte SFTP serveren og modtage og sende filer derfra, adskiller sig fra processen for at anvende andre services på Serviceplatformen. Eksempelvis får et it-system normalt adgang til en service via en af kommunen godkendt serviceaftale. For at it-systemet kan få adgang til SFTP serveren og muligheden for at sende og modtage filer, skal SFTP muligheden aktiveres for det enkelte it-system. Dette gøres under oprettelsen af it-systemet i det fælles administrationsmodul (se vejledning for dette i dokumentet: Vejledning til leverandørers brug af Administrationsmodulet).

Når først informationerne er indtastet i det fælles administrationsmodul vil disse informationer blive provisioneret til Serviceplatformens SFTP server.

## 5 Oversigt over it-systemers brugernavne

For at sende og modtage filer via SFTP serveren skal der gøres brug af it-systemernes SFTP brugernavn. Du kan finde en samlet oversigt over de registrerede it-systemer, der ønsker at benytte SFTP serveren i menupunktet "SFTP tilslutninger", efter at du er logget på selvbetjening på Serviceplatformen

For at se oversigten over it-systemers brugernavne skal du følge nedenstående trin:

**Brugeren:** Som leverandør-organisation skal du være logget på med rollen "bruger".

### Vejledning:

1. Klik på fanen SFTP Tilslutninger

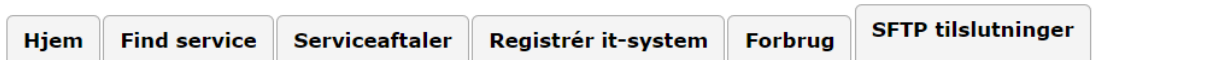
**Resultat:** En liste over it-systemer med SFTP tilknyttet vises. Fra denne liste kan det ses hvilken filudvekslingstype de registrerede it-systemer anvender.

Et eksempel på oversigten kan ses på nedenstående skærbillede. Bemærk at det også fremgår af listen om it-systemet er et konkret anvendersystem, eller et virtuelt system der skal anvendes til dynamisk routing.

### Serviceplatformen

[FAQ og kontakt](#) | [Log af](#)

Logget på som: Bruger



### Oversigt over SFTP tilslutninger

Her vises listen over alle it-systemer der har en SFTP tilslutning. Ved afsendelse af filer til en af disse it-systemer skal modtagerens brugernavn indsættes som recipient. For yderligere informationer om Serviceplatformens SFTP funktionalitet henvises til dokumentationen fundet [her](#).

Leverandør	it-system	SFTP-brugernavn	Filudvekslingstype	Brugertype
Systematic	SFTP Dynamic routing	VirtualUser2	Simpel	Virtuel
Systematic	SFTP Dynamic routing	VirtualUser1	Simpel	Virtuel
Brøndby Kommune	Testsystem	Testuser1	Styret	Anvendersystem

## 6 Teknisk dokumentation

Dette afsnit indeholder generel information om Serviceplatformens SFTP server, samt en beskrivelse af de to typer filudveksling.

### 6.1 Brug af SFTP serveren

#### 6.1.1 Adgang til SFTP serveren

Et it-system logger på SFTP serveren ved brug af it-systemets SSH nøgle. Denne SSH nøgle skal genereres, før et it-system kan blive registreret som it-system, der kan anvende SFTP serveren. Serviceplatformen skal kende den offentlige del af SSH nøglen i forbindelse med registrering af it-systemet og muligheden for anvendelse af SFTP.

##### 6.1.1.1 Format for SSH nøgle

Formatet på SSH nøgle er som følger:

ssh-rsa

```
AAAAB3NzaC1yc2EAAAABJQAAAQEAofzJMdwd87FmljVOYO6s4znOzEj7T7HQEzeG4+LHaNOsHvjKDam
5NrNePBLXAXrptG3PztNJuidWqooC+uy9S3yaFJ7Z0dldnmx8NTrpX7LZ9dZhVv5NuNu6ezLxY+nuZ17lCjx6
Sz/dFI4zDg1hfEiYDyBYD8UQi/yb0YJ5A2Ejv+1UBdtAbtpYfeHDOItA/i7Op6X/e6edZRIHUDnJW9V1/U1Feru
Xq7MiHREKxhd+AWMe6AKFgUWwLg3cPy1b4Finv657pk6dvy6KR/6n6DUID9mYyCihQjdNCbHQ3A3gSIQI
XZIKBDwaqXkYFBsDrMG0JkV68Rae2700m9BEQ==
```

Der skal således indsættes "ssh-rsa " foran den del af nøglen, der hentes ud af public key.

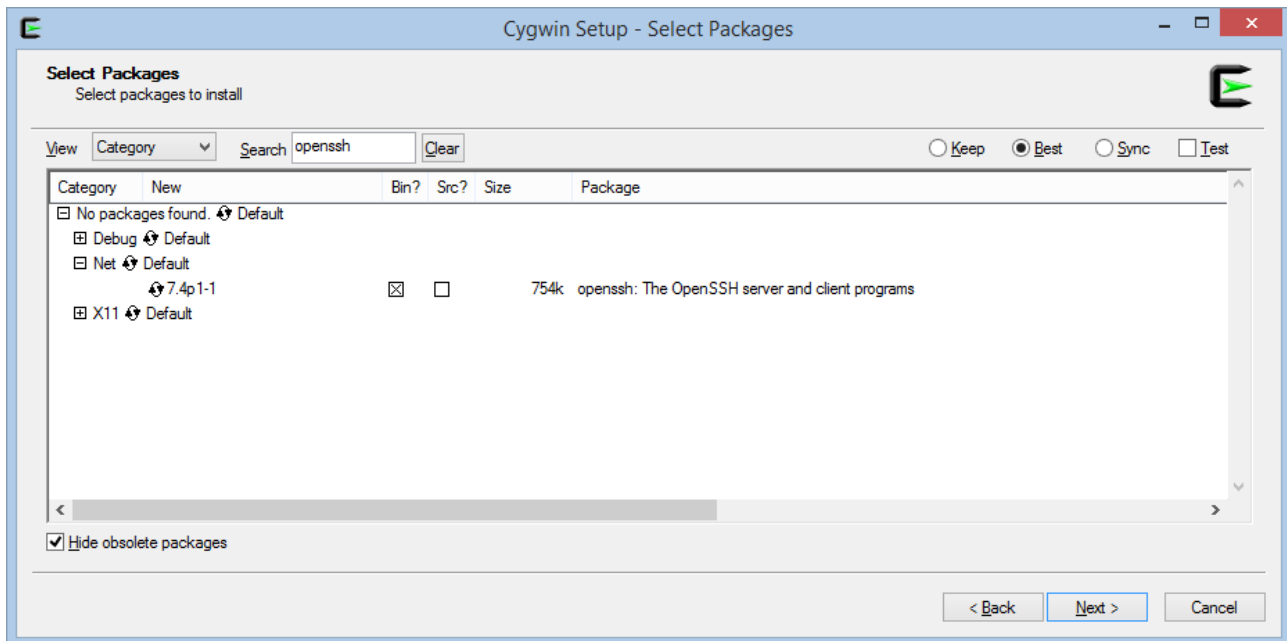
SSH nøgle:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAvs5Wn8v
```

##### 6.1.1.2 Generering af SSH nøgler

Der findes flere forskellige fremgangsmåder der kan bruges til at generere SSH nøgler. Serviceplatformens SFTP server kræver at SSH nøglerne er generet med OpenSSH. Den følgende metode kan bruges på både Windows, Linux og OSX, givet at OpenSSH er installeret på maskinen.

På Windows skal det bemærkes at OpenSSH ikke er en del af standard installationen. Dette kan dog tilføjes via programmet Cygwin, der kan findes på følgende hjemmeside: <http://cygwin.com/install.html>. Denne side beskriver også hvordan optionelle moduler kan installeres, med denne forklaring kan modulet openssh installeres. Nedenstående figur viser Cygwin installations GUI med tilvalgt OpenSSH modul:



OpenSSH suite består af følgende tools:

- Remote operations benytter ssh, scp og sftp
- Key management benytter ssh-add, ssh-keygen, ssh-keyscan og ssh-keygen.
- Service side består af sshd, sftp-server og ssh-agent.

ssh-keygen er værktøjet, beskrevet herunder.

1. Åben en terminal (Cygwin terminal på Windows maskiner) og indtast følgende kommando:  

```
ssh-keygen -t rsa -C "din_email@hostname.dk"
```
2. Du bliver bedt om at specificere hvor nøglen skal gemmes. Det anbefales blot at trykke enter og bruge den foreslåede placering:  

```
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/EPM/.ssh/id_rsa):
```
3. Du bliver bedt om at indtaste et passphrase, hvilket er en adgangskode. Indtast den ønskede passphrase (bemærk det er også muligt at indtaste en tom passphrase) og tryk enter:  

```
Enter passphrase (empty for no passphrase):
```
4. Herefter genereres SSH-nøglen og placeringen af den offentlige nøgle og private del af nøglen angives.  

```
Your identification has been saved in /home/EPM/.ssh/id_rsa.  
Your public key has been saved in /home/EPM/.ssh/id_rsa.pub.
```

Den offentlige del af nøglen som i dette eksempel ligger i filen `id_rsa.pub` i mappen `/home/EPM/.ssh/`, skal Serviceplatformen have i forbindelse med registrering af et it-system, der skal kunne benytte SFTP. Dette er beskrevet nærmere i afsnit 4. [openssh kan installeres som modul i cygwin via cygwin gui](#)

openssh inkluderer toolet <https://www.openssh.com/>

I eksemplet ovenfor findes den private del af nøglen i filen `id_rsa` i mappen `/home/EPM/.ssh/`.

### 6.1.2 Mappedstruktur

Når et it-system er registret og kan anvende SFTP har it-systemet adgang til to private mapper på SFTP serveren:

- **IN:** Den indkommende mappe, hvor it-systemet modtager filer sendt til it-systemet.
- **OUT:** Den udgående mappe, hvor it-systemet uploader de filer, det ønsker at sende til andre it-systemers mapper på SFTP serveren.

### 6.1.3 Upload af filer

Når dit it-system ønsker at sende filer til andre registrerede it-systemer på Serviceplatformen, er der følgende krav i forbindelse med upload af filer til SFTP serveren.

- **Hver fil skal have et unikt navn:** En fil kan kun overføres til modtagersystemets IN-mappe, hvis filnavnet er unikt. Filen afvises hvis der allerede findes en fil ved samme navn i IN-mappen hos modtagersystemet. Dette er for at undgå, at den nye fil overskriver en eksisterende fil i IN-mappen. For at undgå at få filoverførsler afvist grundet enslydende filnavne, anbefales det at definere en navnekonvention for filnavne, eksempelvis ved at præ- eller postfixe filnavne med en unik tekststreng. Et eksempel på dette kunne være, at it-systemet *Kombit* uploader filen med navnet *eksempel.txt* til SFTP serveren med navnet *Kombit\_eksempel.txt*.
- **Filer skal uploades til OUT-mappen:** Det er kun filer uploadet til OUT-mappen som bliver videresendt til andre it-systemers IN-mapper. Uploades filen fejlagtig til IN-mappen vil den ikke blive behandlet.
- **Triggerfil overføres efter endt filupload:** Alle filoverførsler hvor it-systemet anvender typen simpel overførsel af filer, skal forsynes med en triggerfil. Filen skal først være færdig uploadet i OUT-mappen før, der skal sendes en triggerfil for filoverførslen. Sendes triggerfilen før endt filupload kan overførslen risikere at blive afvist.

### 6.1.4 Oprydning og monitorering på SFTP serveren

It-systemer skal regelmæssigt rydde op i deres IN- og OUT-mapper på SFTP serveren. Det gøres ved at slette filer der er færdigbehandlede.

SFTP Servicen stiller følgende begrænsninger for et it-systems brug af SFTP serveren:

- Et it-system må højst have 10.000 filer i dets IN-mappe på SFTP serveren.
- På SFTP serveren findes en standard konfiguration for, hvordan Serviceplatformen rydder op i it-systemers IN- og OUT-mapper. Standard konfigurationen for nye, såvel som allerede eksisterende, it-systemer med SFTP server, er at Serviceplatformen dagligt rydder op på SFTP serverens IN- og OUT-foldere og sletter alle filer, der har ligget uændret på SFTP serveren i 40 dage.
- Oprydning på SFTP serveren er baseret på at filer har et tidsstempel, der siger hvornår de sidst er blevet ændret. Hvis en fil ikke er blevet ændret i 30 dage så notificeres it-systemet, der ejer filen om, at den vil blive slettet indenfor 10 dage. Notifikationen er til den email der er konfigureret under oprettelse af IT-systemets SFTP del. Hvis de 10 dage går og filen stadig ligger på serveren, vil den blive slettet.

Hvert it-system kan rekonfigurere deres SFTP brugersystem, således at der er selvbestemmelse over om den daglige oprydning kun skal foretages i IN- eller OUT-foldere eller ingen af dem.

For at ændre Serviceplatformens standardkonfiguration, for en given SFTP bruger, sendes en email til [helpdesk@serviceplatformen.dk](mailto:helpdesk@serviceplatformen.dk), for at få tilsendt blanketten: Oprydningskonfiguration til SFTP Server.

Heri vil følgende informationer blive efterspurgt:

- SFTP-brugernavn

- IN: sand/false – sand, angives hvis oprydning af SFTP serverens IN-folder skal foretages. Falsk, angives hvis oprydningen ikke skal foretages.
- OUT: sand/false – sand, angives hvis oprydning af SFTP serverens OUT-folder skal foretages. Falsk, angives hvis oprydningen ikke skal foretages.

Yderligere findes en mulighed for overvågning af filer, hvis det er vigtigt for et IT-system at blive notificeret om ikke behandlede filer inden de normale 30 dage eller hvis filer ikke må slettes.

Her monitorerer Serviceplatformen filer på en såkaldt "watchlist", hvor optrædende filer ikke bliver automatisk slettet af Serviceplatformen.

Et it-system har per default ingen filer på denne watchlist. Filer der er tilføjet til denne liste vil, som tidligere nævnt, ikke blive slettet af Serviceplatformen efter de 40 dage, som angivet i ovenstående standard konfiguration. 2 parametre er tilknyttet en watchlist; X ligmed antal dage hvorefter notifikationsmail sendes til it-systemet, Y ligmed antal dage hvorefter en medarbejder fra Serviceplatformen ønskes at kontakte it-systemet. Dvs. It-systemer der ejer filer på listen vil i stedet modtage en notifikationsmail, hvis filerne ikke er slettet efter X dage efter filen er flyttet til den specifikke mappe. Forbliver filerne stadig på SFTP serveren Y dage efter filen er flyttet til den specifikke mappe vil en medarbejder fra Serviceplatformen kontakte it-systemet. Intentionen er at it-system selv kan styre hvornår de ønsker en notifikation og selv er ansvarlige for at slette filer.

For at anvende SFTP serverens filovervågning skal der konfigureres filtre for hvert it-system, som er tilpasset de forskellige filer der ønskes monitoreret.

Filer som ønskes på SFTP serverens watchlist, skal således matche et af it-systemets filtre. Der er tre kriterier filtrene skal matche filerne på. Disse er:

- Om filen er i IN- eller OUT-folderen
- Filens XPath expression ( f.eks: /FileMetadata/FileTransferUUID )
- Filens Filemask, filtypen f.eks: %.txt. (Skal angives med % før filtypen)

Findes der flere filer tilhørende et it-system, der har været mere end X dage på SFTP serveren, vil det pågældende it-system altid kun modtage én notifikation om ældre filer fra Serviceplatformen.

#### 6.1.4.1 Oprettelse af filtre

Filtre konfigureres gennem Serviceplatformen ved at sende en email til [helpdesk@serviceplatformen.dk](mailto:helpdesk@serviceplatformen.dk), for at få tilsendt blanketten: Filovervågningskonfiguration til SFTP server.

I denne skal følgende detaljer om filtret fremgå:

- SFTP-brugernavn
- Navnet på folderen filtret skal fungere i. IN/OUT
- Hvilken XPath filen skal matche (skelner mellem store og små bogstaver).
- Hvilke filemask filen skal matche (skelner *ikke* mellem store og små bogstaver).
- Hvor mange dage X filen er på SFTP serveren før brugersystemet notificeres.
- Hvor mange dage Y filen er på SFTP serveren før en medarbejder fra Serviceplatformen kontakter it-systemet. ( Y bør være et større antal dage end X)
- Hvorvidt filens metafil skal inkluderes på listen, så den ligeledes overvåges.

## 6.1.5 Information omkring SFTP server

It-systemer skal tilgå Serviceplatformens SFTP server via dens offentlige hostnavn.

For produktionsmiljøet er denne: `sftp.serviceplatformen.dk`

For extttest er denne: `sftpextttest.serviceplatformen.dk`

For begge miljøer skal der forbindes på port 22.

## 6.2 Simpel overførsel af filer

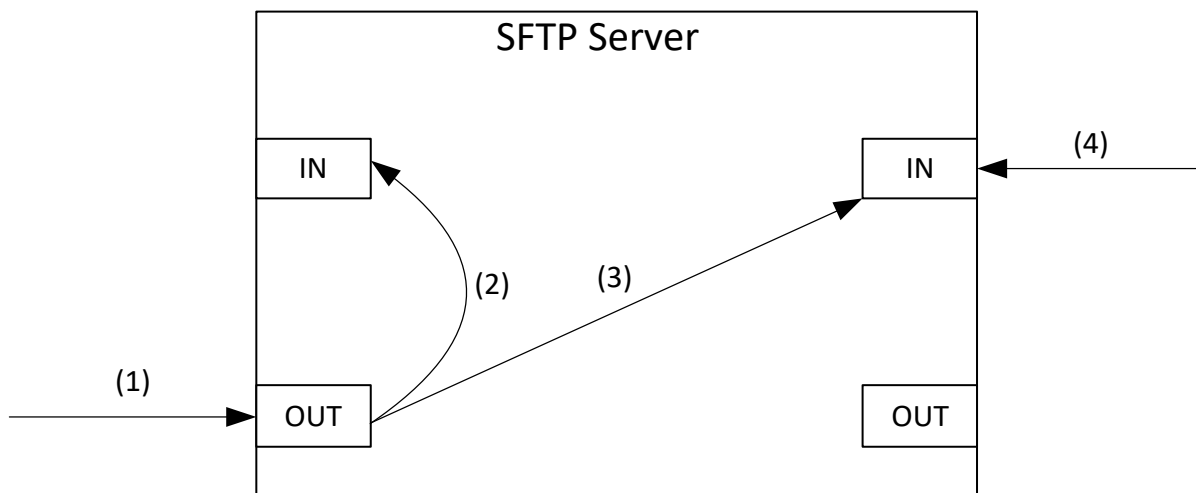
Ved simpel overførsel af filer sker udvekslingen af beskeder mellem modtagersystemet, afsendersystemet, og SFTP Servicen ved hjælp af filer på SFTP serveren.

For at give overblik over de forskellige trin, som indgår i udveksling af en fil ved typen simpel overførsel af fil, kan følgende brugseksempel konsulteres.

### 6.2.1 Brugseksempel

Dette brugseksempel dækker følgende scenarie: It-systemet med SFTP brugernavnet *DemoAfsender* ønsker at afsende filen *info.txt* til it-systemet *DemoModtager*.

Følgende figur viser de forskellige trin involveret ved simpel overførsel af filer.



- 1. Upload af fil samt triggerfil:** Afsendersystemet uploader filen *info.txt* til dets OUT-mappe på SFTP serveren sammen med triggerfilen *info.txt.trigger*, der har indholdet vist nedenfor. Bemærk at "Sender" feltet skal udfyldes med SFTP brugernavnet på afsendersystemet.

```
<ns2:Trigger xmlns:ns2="http://serviceplatformen.dk/xml/wsdl/soap11/SFTP/1/types">
  <FileDescriptor>
    <FileName>info.txt</FileName>
    <SizeInBytes>18</SizeInBytes>
    <Sender>DemoAfsender</Sender>
    <SendersFileId>67e072ec-2db2-4c38-aeb1-a71c135ce566</SendersFileId>
    <Recipients>DemoModtager</Recipients>
  </FileDescriptor>
  <FileContentDescriptor>
```

```
</FileContentDescriptor>
</ns2:Trigger>
```

2. **Teknisk kvittering uploades til afsendersystemet:** Triggerfilen valideres af Serviceplatformen og en teknisk kvittering uploades til afsendersystemets IN-mappe. Hvis triggerfilen er valid "låses" filen *info.txt* i afsendersystemets mappe, så den ikke kan ændres efter valideringen af triggerfilen er foretaget. I praksis sker "låsningsen" ved, at afsendersystemets skriverrettigheder til filen fjernes. Efter valideringen af triggerfilen slettes den fra afsendersystemets IN-mappe.

Den tekniske kvittering vil som udgangspunkt have filnavnet *info.txt.sftpreceipt*, altså filnavnet på filen, der sendes, postfixet med ".sftpreceipt". Det skal dog bemærkes at hvis en teknisk kvittering med dette navn allerede ligger i afsendersystemets IN-mappe vil den tekniske kvittering få navnet *info.txt.sftpreceipt<TIMESTAMP>*, hvor *<TIMESTAMP>* i praksis vil være erstattet af et timestamp i millisekunder for hvornår den tekniske kvittering er genereret. Dette vil f.eks. forekomme hvis man ikke har ryddet op i sin IN-mappe og sender en fil med samme navn igen.

I dette scenarie vil den tekniske kvittering have følgende indhold:

```
<ns2:TechnicalReceipt xmlns:ns2="http://serviceplatformen.dk/xml/wsd/soap11/SFTP/1/types">
  <FileTransferUUID>eb04e6e2-a4ae-468f-bdfd-8b676c720935</FileTransferUUID>
  <SendersFileId>67e072ec-2db2-4c38-aeb1-a71c135ce566</SendersFileId>
  <Receipt>
    <Message>SUCCESS</Message>
  </Receipt>
</ns2:TechnicalReceipt>
```

3. **Filen overføres til modtagersystemet sammen med en metadata fil:** Filen *info.txt* overføres fra afsendersystemets OUT-mappe til modtagersystemets IN-mappe. Ved samme proces uploades der en metadata fil til modtagersystemets IN-mappe. Metadata filen vil have filnavnet *info.txt.metadata* og have følgende indhold:

```
<ns2:FileMetadata xmlns:ns2="http://serviceplatformen.dk/xml/wsd/soap11/SFTP/1/types">
  <FileTransferUUID>eb04e6e2-a4ae-468f-bdfd-8b676c720935</FileTransferUUID>
  <FileDescriptor>
    <FileName>info.txt</FileName>
    <SizeInBytes>18</SizeInBytes>
    <Sender>DemoAfsender</Sender>
    <SendersFileId>67e072ec-2db2-4c38-aeb1-a71c135ce566</SendersFileId>
    <Recipients>DemoModtager</Recipients>
  </FileDescriptor>
  <FileContentDescriptor>
  </FileContentDescriptor>
</ns2:FileMetadata>
```

Det vil sige samme indhold som triggerfilen, men hvor FileTransferUUID er tilføjet.

4. **Modtagersystemet tjekker dets IN-mappe og finder filen:** Modtagersystemet vil ved simpel overførsel af filer ikke modtage nogen notifikation om, at filen er blevet overført til dets IN-mappe. Det er derfor selv ansvarlig for at opdage, at en fil er blevet overført til det. Modtagersystemet kan bl.a. gøre dette ved periodisk at downloade alle filer fra dets IN-mappe.

I det tilfælde at modtagersystemet sender en forretningskvittering tilbage til afsendersystemet, vil det samme gennemgåede flow foregå, men systemerne har byttet rolle så modtagersystemet ligger en datafil og triggerfil i OUT-mappen.



Bemærk at det anbefales at foretage oprydning i IN-mappen så snart filen er læst og håndteret af det pågældende system.

## 6.3 Dynamisk routing

Det overordnede flow for dynamisk routing er det samme som ved "simpel overførsel af filer". Forskellen ligger i hvordan modtagersystemet identificeres.

SFTPDynamicRoutingInfo strukturen, som skal medsendes, ser ud som herunder udfyldt med dummy data:

```
<SFTPDynamicRoutingInfo>
  <InfRef>SF1590_B_IF04</InfRef>
  <SenderId-system>40f6af96-db76-4570-91fa-068fa757582a</SenderId-system>
  <SenderAuthority>urn:oio:cvr-nr:64942212</SenderAuthority>
  <TransactionId>00000000-0000-0000-0000-000000000000</TransactionId>
  <SenderTimestamp>2016-12-17T09:30:47Z</SenderTimestamp>
  <RecipientIt-system>980a7e69-91f4-41ac-8a27-a5f9febd2602</RecipientIt-system>
  <RecipientAuthority>urn:oio:cvr-nr:64942212</RecipientAuthority>
</SFTPDynamicRoutingInfo>
```

Hvordan strukturen skal udfyldes er uddybet i afsnit 6.5.2. Hvilken service filen sendes i relation til er angivet i feltet *Infref*.

SFTPDynamicRoutingInfo strukturen skal medsendes i *FileContentDescriptor* elementet i triggerfilen.

Det er ud fra denne struktur at en routingregel fremsøges. En routingregel ser ud på følgende måde:

Infref	SenderAuthority	SenderId-System	RecipientAuthority	RecipientIt-system	SFTPUsername
XXX	XXX	XXX	XXX	XXX	XXX

Der findes to forskellige måder routingregler kan fremsøges på, der kaldes henholdsvis *implicit* og *eksplicit*. Det vil for hver service/infref værdi være konfigureret på Serviceplatformen om routingregler skal fremsøges henholdsvis *implicit* eller *eksplicit*. Det er kun muligt for en infref værdi at understøtte enten *implicit* eller *eksplicit* routing.

Ved *implicit* routing fremsøges routingregler på følgende måde:

- Værdierne fra felterne *SenderId-system*, *SenderAuthority*, *InfRef* og *RecipientAuthority* hentes ud af SFTPDynamicRoutingInfo strukturen.
- Der fremsøges en regel med værdierne: *SenderId-system*, *SenderAuthority*, *InfRef*, *RecipientAuthority* og med *RecipientIt-system=' '*
- Hvis værdien *RecipientIt-system* er medsendt returneres en fejl i den tekniske kvittering om, at feltet ikke må medsendes for den angivne *infref* værdi.
- Hvis en routingregel kan fremsøges baseret på det givne data, vil filen vil blive sendt til modtagersystemet med det fremsøgte SFTP brugernavn.

Ved *eksplicit* routing fremsøges routingregler på følgende måde:

- Værdierne fra felterne *SenderId-system*, *SenderAuthority*, *InfRef*, *RecipientAuthority* og *RecipientIt-system* hentes ud af SFTPDynamicRoutingInfo strukturen.

- Der fremsøges en regel med værdierne: *SenderIt-system*, *SenderAuthority*, *InfRef*, *RecipientAuthority* og *RecipientIt-system*
- Hvis værdien *RecipientIt-system* ikke er medsendt returneres en fejl i den tekniske kvittering om at feltet skal medsendes for den angivene *infref* værdi.
- Hvis en routingregel kan fremsøges baseret på det givne data, vil filen vil blive sendt til modtagersystemet med det fremsøgte SFTP brugernavn.

For at give overblik over de forskellige trin, som indgår i udveksling af en fil ved brug af dynamisk routing, kan følgende brugseksempel konsulteres.

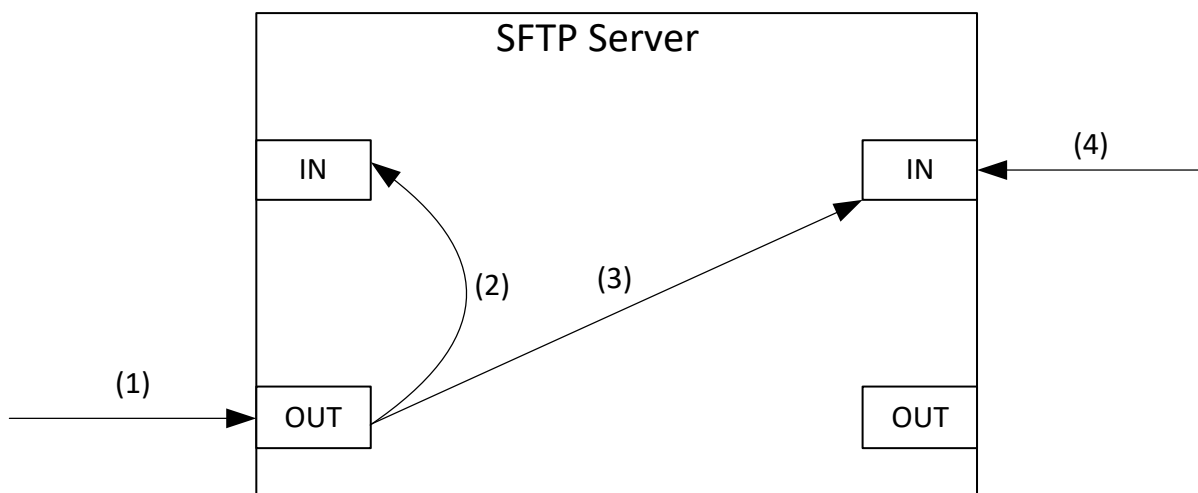
### 6.3.1 Brugseksempel

Dette brugseksempel dækker følgende scenarie: It-systemet med SFTP brugernavnet *DemoAfsender* ønsker at afsende filen *info.txt* til it-systemet *DemoModtager* ved brug af dynamisk routing. Der er på Serviceplatformen konfigureret en routingregel som herunder:

Infref	SenderAuthority	SenderIt-System	RecipientAuthority	RecipientIt-system	SFTPUsername
SF1590_A_IF02-03	urn:oio:cvr-nr:64942212	40f6af96-db76-4570-91fa-068fa757582a	urn:oio:cvr-nr:64942212		DemoModtager

Hvor det for SF1590\_A\_IF02-03 er konfigureret at routingregler skal fremsøges via *implicit* routing. Derudover findes der et virtuelt system der hedder *ROUTING\_V1\_0\_0* som filen skal adresseres til for at den sendes via dynamisk routing.

Følgende figur viser de forskellige trin involveret ved simpel overførsel af filer med dynamisk routing.



- 1. Upload af fil samt triggerfil:** Afsendersystemet uploader filen *info.txt* til dets OUT-mappe på SFTP serveren sammen med triggerfilen *info.txt.trigger*, der har indholdet vist nedenfor. Bemærk at "Sender" feltet skal udfyldes med SFTP brugernavnet på afsendersystemet og "Recipient" feltet skal udfyldes med en virtuel bruger, i dette tilfælde *ROUTING\_V1\_0\_0*.

```
<ns:Trigger xmlns:ns="http://serviceplatformen.dk/xml/wsd/soap11/SFTP/1/types">
  <FileDescriptor>
    <FileName>info.txt</FileName>
    <SizeInBytes>18</SizeInBytes>
    <Sender>DemoAfsender</Sender>
  </FileDescriptor>
</ns:Trigger>
```

```

<SendersFileId>67e072ec-2db2-4c38-aeb1-a71c135ce566</SendersFileId>
<Recipients>ROUTING_V1_0_0</Recipients>
</FileDescriptor>
<FileContentDescriptor>
  <SFTPDynamicRoutingInfo>
    <InfRef>SF1590_A_IF02-03</InfRef>
    <SenderId-system>40f6af96-db76-4570-91fa-068fa757582a</SenderId-system>
    <SenderAuthority>urn:oio:cvr-nr:64942212</SenderAuthority>
    <TransactionId>ca02695f-497f-496d-86b1-4e9ecbd800a9</TransactionId>
    <SenderTimestamp>2016-06-27T08:48:00+02:00</SenderTimestamp>
    <RecipientAuthority>urn:oio:cvr-nr:64942212</RecipientAuthority>
  </SFTPDynamicRoutingInfo>
</FileContentDescriptor>
</ns:Trigger>

```

2. **Teknisk kvittering uploades til afsendersystemet:** Triggerfilen valideres af Serviceplatformen og en teknisk kvittering uploades til afsendersystemets IN-mappe. Valideringen sker ved, at Serviceplatformen tjekker om den angivne modtager i triggerfilen er et virtuelt system. Hvis det er tilfældet laves der et opslag på om den Infref, der er angivet i SFTPDynamicRoutingInfo strukturen, skal behandles med henholdsvis *implicit* eller *eksplicit* routing. Hvis det er muligt at fremsøge en routingregel baseret på triggerfilens indhold, er triggerfilen valid, og der oprettes en opgave på Serviceplatformen med at overføre filen til det fremsøgte modtagersystem.

Hvis triggerfilen er valid foretages de samme trin som der foretages ved filudvekslingstypen "simpel overførsel af filer".

Den tekniske kvittering der genereres som et resultat af valideringen vil have følgende indhold:

```

<ns2:TechnicalReceipt xmlns:ns2="http://serviceplatformen.dk/xml/wsdl/soap11/SFTP/1/types">
  <FileTransferUUID>5c415adb-8dbc-40eb-a45c-dd2f40dcc4d5</FileTransferUUID>
  <SendersFileId>67e072ec-2db2-4c38-aeb1-a71c135ce566</SendersFileId>
  <Receipt>
    <Message>SUCCESS</Message>
  </Receipt>
</ns2:TechnicalReceipt>

```

3. **Filen overføres til modtagersystemet sammen med en metadata fil:** Filen *info.txt* overføres fra afsendersystemets OUT-mappe til modtagersystemets IN-mappe. Ved samme proces uploades der en metadata fil til modtagersystemets IN-mappe. Metadata filen vil have filnavnet *info.txt.metadata* og have følgende indhold:

```

<ns2:FileMetadata xmlns:ns2="http://serviceplatformen.dk/xml/wsdl/soap11/SFTP/1/types">
  <FileTransferUUID>5c415adb-8dbc-40eb-a45c-dd2f40dcc4d5</FileTransferUUID>
  <FileDescriptor>
    <FileName>info.txt</FileName>
    <SizeInBytes>18</SizeInBytes>
    <Sender>DemoAfsender</Sender>
    <SendersFileId>67e072ec-2db2-4c38-aeb1-a71c135ce566</SendersFileId>
    <Recipients>DemoModtager</Recipients>
  </FileDescriptor>
  <FileContentDescriptor>
    <SFTPDynamicRoutingInfo xmlns:ns="http://serviceplatformen.dk/xml/wsdl/soap11/SFTP/1/types">
      <InfRef>SF1590_A_IF02-03</InfRef>
      <SenderId-system>40f6af96-db76-4570-91fa-068fa757582a</SenderId-system>
      <SenderAuthority>urn:oio:cvr-nr:64942212</SenderAuthority>
    </SFTPDynamicRoutingInfo>
  </FileContentDescriptor>
</ns2:FileMetadata>

```

```
<TransactionId>ca02695f-497f-496d-86b1-4e9ecbd800a9</TransactionId>
<SenderTimestamp>2016-06-27T06:48:00Z</SenderTimestamp>
<RecipientAuthority>urn:oio:cvr-nr:64942212</RecipientAuthority>
</SFTPDynamicRoutingInfo>
</FileContentDescriptor>
</ns2:FileMetadata>
```

Det vil sige samme indhold som triggerfilen, men hvor FileTransferUUID er tilføjet, formatet for SenderTimestamp er ændret til "Zulu time", og modtager er sat til *DemoModtager* fremfor *ROUTING\_V1\_0\_0*.

- 4. Modtagersystemet tjekker dets IN-mappe og finder filen:** Modtagersystemet vil ved simpel overførsel af filer ikke modtage nogen notifikation om, at filen er blevet overført til dets IN-mappe. Det er derfor selv ansvarlig for at opdage, at en fil er blevet overført til det. Modtagersystemet kan bl.a. gøre dette ved periodisk at downloade alle filer fra dets IN-mappe.

I det tilfælde at modtagersystemet sender en forretningskvittering tilbage til afsendersystemet, vil det samme gennemgåede flow foregå, men systemerne har byttet rolle så modtagersystemet ligger en datafil og triggerfil i OUT-mappen.

Bemærk at det anbefales at foretage oprydning i IN-mappen så snart filen er læst og håndteret af det pågældende system.

## 6.4 Styret overførsel af filer

Ved styret overførsel af filer sker udvekslingen af beskeder mellem modtagersystemet, afsendersystemet, og SFTP Servicen ved hjælp af webservicekald. It-systemer der anvender typen styret overførsel af filer skal udstille en webservice baseret på WSDL filen SFTPSERVICEUser.wsdl. Serviceplatformen udstiller i forbindelse med SFTP servicen en webservice baseret på wsdl filen SFTPSERVICE.wsdl.

SFTP webservicen kaldes af it-systemer på samme måde som eksisterende webservices på Serviceplatformen, hvor en *invocationcontext* sendes med som en del af web requestet.

Typen styret overførsel af filer er forklaret ved brug af et eksempel i afsnit 6.4.3.

### 6.4.1 SFTP servicens webservice

Webservicen som udstilles i forbindelse med SFTP Servicen har to metoder: *TransferFile* og *DeliverBusinessReceipt*.

I testmiljøet ligger den på følgende endpoint:

<https://exttest.serviceplatformen.dk/service/SFTPSERVICE/SFTPSERVICE/1>

I produktionsmiljøet ligger den på følgende endpoint:

<https://prod.serviceplatformen.dk/service/SFTPSERVICE/SFTPSERVICE/1>

#### 6.4.1.1 TransferFile

Kaldes af afsendersystemet med et triggerobjekt. Som en del af kaldet skal en *invocationcontext* sendes med.

## 6.4.1.2 *DeliverBusinessReceipt*

Kaldes af modtagersystemet med en forretningskvittering. Som en del af kaldet skal en invocationcontext sendes med.

## 6.4.2 *It-systemets webservice beskrivelse*

Webservicen som skal udstilles af it-systemet har to metoder *notifySender* og *notifyRecipient*. SFTP serveren vil kalde webservicen og dens metoder med to-vejs TLS.

### 6.4.2.1 *notifyRecipient*

Kaldes af Serviceplatformen med en metadata xml struktur for at notificere modtagersystemet om at en fil er blevet overført deres IN-mappe på SFTP serveren.

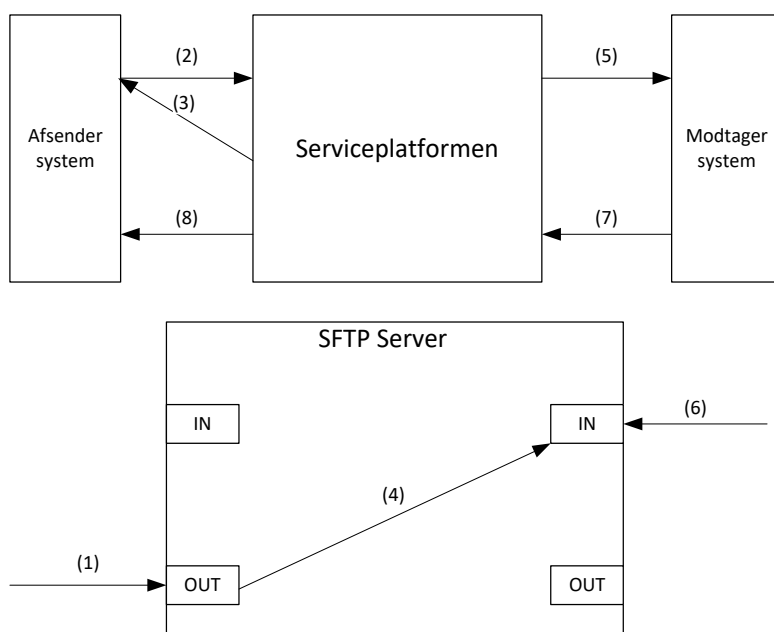
### 6.4.2.2 *notifySender*

Kaldes af Serviceplatformen med en forretningskvittering om at en fil er blevet overført til modtagersystemet, og modtagersystemet har kaldt ind med en forretningskvittering.

## 6.4.3 *Brugseksempel*

It-systemet med SFTP brugernavnet *DemoAfsender* ønsker at afsende filen *info.txt* til it-systemet *DemoModtager*.

Følgende figur viser de forskellige trin involveret ved styret overførsel af filer.



- 1. Upload af fil:** Afsendersystemet uploader filen *info.txt* til dets OUT-mappe på SFTP serveren.

2. **Kald af SFTP webservice:** Afsendersystemet kalder *TransferFile* metoden på SFTP webservicen med et triggerobjekt. Afsendersystemet vil kalde *TransferFile* metoden for overførsel af filen *info.txt* med følgende SOAP request:

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
<S:Body>
  <ns4:SFTPTransferFileRequest
xmlns:ns2="http://serviceplatformen.dk/xml/schemas/InvocationContext/1/"
xmlns:ns3="http://serviceplatformen.dk/xml/wsd/soap11/SFTP/1/types"
xmlns:ns4="http://serviceplatformen.dk/xml/wsd/soap11/SFTPService/1/">
  <ns2:InvocationContext>
    <ns2:ServiceAgreementUUID>752c91f2-aff3-4321-811a-2f3df7440a18</ns2:ServiceAgreementUUID>
    <ns2:UserSystemUUID>ba59aa63-a8a9-4a09-8a9a-a12daafd9fcb</ns2:UserSystemUUID>
    <ns2:UserUUID>d10ff51e-3abf-11e2-9724-d4bed98c63db</ns2:UserUUID>
    <ns2:OnBehalfOfUser>SFTPServicePort.test.uuid</ns2:OnBehalfOfUser>
    <ns2:ServiceUUID>d7ffb23b-49d3-4a22-877a-0ecd473a3d15</ns2:ServiceUUID>
  </ns2:InvocationContext>
  <ns3:Trigger>
    <ns3:FileDescriptor>
      <ns3:FileName>info.txt</ns3:FileName>
      <ns3:SizeInBytes>18</ns3:SizeInBytes>
      <ns3:Sender>DemoAfsender</ns3:Sender>
      <ns3:SendersFileId>67e072ec-2db2-4c38-aeb1-a71c135ce566</ns3:SendersFileId>
      <ns3:Recipients>DemoModtager</ns3:Recipients>
    </ns3:FileDescriptor>
    <ns3:FileContentDescriptor>
      </ns3:FileContentDescriptor>
    </ns3:Trigger>
  </ns4:SFTPTransferFileRequest>
</S:Body>
</S:Envelope>
```

3. **Teknisk kvittering returneres synkront:** SFTP servicen validerer triggerobjektet, der blev leveret gennem webservicekaldet, og en teknisk kvittering genereres. Den tekniske kvittering returneres som et synkront svar på det oprindelige webservicekald foretaget af afsendersystemet, hvor triggerobjektet blev leveret.

Den tekniske kvittering returneret som svar på webservicekaldet vil se ud på følgende måde:

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
<env:Header/>
<env:Body>
  <ns1:SFTPTransferFileResponse
xmlns:ns2="http://serviceplatformen.dk/xml/schemas/InvocationContext/1/"
xmlns:ns3="http://serviceplatformen.dk/xml/wsd/soap11/SFTP/1/types"
xmlns:ns1="http://serviceplatformen.dk/xml/wsd/soap11/SFTPService/1/">
    <ns3:TechnicalReceipt>
      <ns3:FileTransferUUID>9691d996-3284-4955-9cd7-cb469ac5d311</ns3:FileTransferUUID>
      <ns3:SendersFileId>67e072ec-2db2-4c38-aeb1-a71c135ce566</ns3:SendersFileId>
      <ns3:Receipt>
        <ns3:Message>SUCCESS</Message>
      </ns3:Receipt>
    </ns3:TechnicalReceipt>
  </ns1:SFTPTransferFileResponse>
```

```
</env:Body>
</env:Envelope>
```

- 4. Filen overføres til modtagersystemet:** Filen *info.txt* overføres fra afsendersystemets OUT-mappe til modtagersystemets IN-mappe.
- 5. Serviceplatformen notificerer modtagersystemet:** Serviceplatformen foretager et kald til webservicen udstillet af modtagersystemet på metoden *notifyRecipient*. Kaldet vil se ud på følgende måde:

```
<env:Envelope xmlns:env='http://schemas.xmlsoap.org/soap/envelope/'>
<env:Header/>
<env:Body>
  <ns1:RecipientNotificationRequest
xmlns:ns1='http://serviceplatformen.dk/xml/wsdl/soap11/SFTPService/1/'
xmlns:ns2='http://serviceplatformen.dk/xml/wsdl/soap11/SFTP/1/types'>
    <ns2:FileMetadata>
      <ns2:FileTransferUUID>5af1914e-b581-440a-ad00-0320a9f1143c</ns2:FileTransferUUID>
      <ns2:FileDescriptor>
        <ns2:FileName>info.txt</ns2:FileName>
        <ns2:SizeInBytes>18</ns2:SizeInBytes>
        <ns2:Sender>hKQp6fBvMg</ns2:Sender>
        <ns2:SendersFileId>sendersFileId</ns2:SendersFileId>
        <ns2:Recipients>DemoModtager</ns2:Recipients>
        <ns2:SendersFileId>67e072ec-2db2-4c38-aeb1-a71c135ce566</ns2:SendersFileId>
      </ns2:FileDescriptor>
      <ns2:FileContentDescriptor>
      </ns2:FileContentDescriptor>
    </ns2:FileMetadata>
  </ns1:RecipientNotificationRequest>
</env:Body>
</env:Envelope>
```

Serviceplatformen vil forvente at få et svar retur fra modtagersystemet, der ser ud på følgende måde:

```
<env:Envelope xmlns:env='http://schemas.xmlsoap.org/soap/envelope/'>
<env:Header/>
<env:Body>
  <ns1:BusinessReceiptResponse xmlns:ns1='http://serviceplatformen.dk/xml/wsdl/soap11/SFTPService/1/'
xmlns:ns2='http://serviceplatformen.dk/xml/schemas/InvocationContext/1/'
xmlns:ns3='http://serviceplatformen.dk/xml/wsdl/soap11/SFTP/1/types'>
    <ns3:BusinessResponse>
    </ns3:BusinessResponse>
  </ns1:BusinessReceiptResponse>
</env:Body>
</env:Envelope>
```

- 6. Modtagersystemet henter filen:** Efter at modtagersystemet er blevet informeret om at filen *info.txt* er blevet overført til det, henter det filen og verificerer, at det er en fil som det kan bruge.

7. **Modtagersystemet kalder Serviceplatformen med en forretningskvittering:** Modtagersystemet kalder ind på SFTP webservice med en forretningskvittering. I dette scenarie vil forretningskvitteringen se ud på følgende måde.

```
<S:Envelope xmlns:S='http://schemas.xmlsoap.org/soap/envelope/'>
<S:Body>
  <ns4:BusinessReceiptRequest xmlns:ns2='http://serviceplatformen.dk/xml/schemas/InvocationContext/1/'
xmlns:ns3='http://serviceplatformen.dk/xml/wsd/soap11/SFTP/1/types'
xmlns:ns4='http://serviceplatformen.dk/xml/wsd/soap11/SFTPService/1/'>
    <ns2:InvocationContext>
      <ns2:ServiceAgreementUUID>752c91f2-aff3-4321-811a-2f3df7440a18</ns2:ServiceAgreementUUID>
      <ns2:UserSystemUUID>ba59aa63-a8a9-4a09-8a9a-a12daafd9fcb</ns2:UserSystemUUID>
      <ns2:UserUUID>d10ff51e-3abf-11e2-9724-d4bed98c63db</ns2:UserUUID>
      <ns2:OnBehalfOfUser>SFTPServicePort.test.uuid</ns2:OnBehalfOfUser>
      <ns2:ServiceUUID>d7ffb23b-49d3-4a22-877a-0ecd473a3d15</ns2:ServiceUUID>
      <ns2:CallersServiceCallIdentifier>SFTPServicePort.test.uuid</ns2:CallersServiceCallIdentifier>
    </ns2:InvocationContext>
    <ns3:BusinessReceipt>
      <ns3:FileTransferUUID>5af1914e-b581-440a-ad00-0320a9f1143c</ns3:FileTransferUUID>
      <ns3:Filename>info.txt</ns3:Filename>
      <ns3:FileAcceptance>ACCEPTED</ns3:FileAcceptance>
      <ns3:Recipient>DemoModtager</ns3:Recipient>
    </ns3:BusinessReceipt>
  </ns4:BusinessReceiptRequest>
</S:Body>
</S:Envelope>
```

8. **Serviceplatformen kalder afsendersystemet med en forretningskvittering:** Serviceplatformen kalder afsendersystemet på webservice metoden *notifySender* med følgende forretningskvittering for at afslutte fil overførsels flowet.

```
<env:Envelope xmlns:env='http://schemas.xmlsoap.org/soap/envelope/'>
<env:Header/>
<env:Body>
  <ns1:SenderNotificationRequest xmlns:ns1='http://serviceplatformen.dk/xml/wsd/soap11/SFTPService/1/'
xmlns:ns2='http://serviceplatformen.dk/xml/wsd/soap11/SFTP/1/types'>
    <ns2:BusinessReceipt>
      <ns2:FileTransferUUID>5af1914e-b581-440a-ad00-0320a9f1143c </ns2:FileTransferUUID>
      <ns2:Filename>info.txt</ns2:Filename>
      <ns2:FileAcceptance>ACCEPTED</ns2:FileAcceptance>
    </ns2:BusinessReceipt>
    <ns2:Recipient>DemoModtager</ns2:Recipient>
  </ns1:SenderNotificationRequest>
</env:Body>
</env:Envelope>
```

## 6.5 XML-Strukturer

De beskeder der udveksles mellem Serviceplatformen og it-systemerne i forbindelse med SFTP servicen er i XML format. De følgende xml strukturer bruges i forbindelse med SFTP servicen.



De elementer som xml strukturerne består af, vil være markeret med enten **(o)** hvis det er et obligatorisk felt, **(v)** hvis det er et valgfrit felt og **(o\*)** betyder at kun et af felterne med **(o\*)** skal være udfyldt.

## 6.5.1 Triggerobjekt

It-systemer leverer adresseringen af en fil til Serviceplatformen i det der kaldes et triggerobjekt.

Indholdet af et triggerobjekt er xml. Det skal indeholde et *Trigger* xml element af typen *TriggerType* som den er defineret i *SFTPTypes.xsd* filen, der kan hentes på følgende link:

<https://www.serviceplatformen.dk/administration/contract-doc/contracts/ServiceContract-d7ffb23b-49d3-4a22-877a-0ecd473a3d15.zip>.

Typen *TriggerType* består af to elementer: *FileDescriptor* og *FileContentDescriptor*.

*FileDescriptor* kan indeholde elementer af 5 forskellige typer:

- **FileName(o)**: Filnavnet på filen der skal sendes. Skal inkludere fil type (file extension) på filen.
- **SizeInBytes(o)**: Filstørrelsen på den uploadede fil angivet i Bytes. Bruges til at validere at filen er færdigt uploadet inden en filoverførsel igangsættes.
- **Sender(o)**: SFTP brugernavnet på afsendersystemet. Skal sættes, da det viderekommunikeres til modtagersystemet, så det informeres om hvem afsenderen af en given fil er.
- **SendersFileId(v)**: Et felt afsendersystemet kan sætte til unik identifikation af filen. SFTP servicen bruger ikke dette felt, men det vil blive videregivet til modtagersystemet, og være at finde i den tekniske kvittering der generes på basis af triggerfilen.
- **Recipients(o)**: Indeholder SFTP brugernavnet på modtagersystemet. Der skal være et element af denne type tilstede for hver modtager der ønskes på filen.

*FileContentDescriptor*

- Indeholder et xml *any* element, hvilket vil sige at afsendersystemet kan udfylde dette felt med hvad det ønsker, så længe det er valid xml. Indholdet af dette felt videresendes til modtagersystemet.

Et eksempel på et triggerobjekt kan ses i afsnit 6.2.1.

## 6.5.2 SFTPDynamicRoutingInfo

Ved dynamisk routing leveres ekstra den routing information i xml strukturen *SFTPDynamicRoutingInfo*. Den indgår ikke i *xsd*'en for *Trigger* typen, og skal derfor medsendes i *FileContentDescriptor* feltet i triggerobjekter.

*SFTPDynamicRoutingInfo* strukturen er defineret i filen *SFTPDynamicRoutingInfo.xsd*, der kan hentes på følgende link: <https://www.serviceplatformen.dk/administration/contract-doc/contracts/ServiceContract-d7ffb23b-49d3-4a22-877a-0ecd473a3d15.zip>.

*SFTPDynamicRoutingInfo* består af følgende elementer som skal udfyldes på følgende måde:

- **Infref(o)**: Den service som filen, der skal afsendes, er relateret til vil typisk være på formen SFXXXX\_XX
- **SenderIt-system(o)**: UUID'et på det it-system på Serviceplatformen der er afsender af filen. Er en del af den routingregel som vil blive forsøgt fremsøgt.
- **SenderAuthority(o)**: Udfyldes med den myndighed som afsendersystemet sender filen på vegne af. Formatet er på formen: urn:io:cvr-nr:XXXXXXXXX. Er en del af den routingregel, som vil blive forsøgt fremsøgt.

- **TransactionId(o):** Udfyldes af afsendersystemet med et transaktionsId for den afsendte fil. Feltet anvendes ikke af Serviceplatformen, og sendes blot videre til modtagersystemet gennem metadata filen.
- **SenderTimestamp(o):** Udfyldes af afsendersystemet med et timestamp for filen der forsøges afsendt. Feltet anvendes ikke af Serviceplatformen, og sendes blot videre til modtagersystemet gennem metadata filen.
- **RecipientIt-system(v):** UUID'et på det it-system på Serviceplatformen der er den tiltænkte modtager af filen. Skal kun udfyldes hvis den angivne infref anvender *explicit* routing.
- **RecipientAuthority(o):** Udfyldes med den myndighed filen skal leveres til. Formatet er på formen: urn:oio:cvr-nr:XXXXXXXX. Er en del af den routingregel som vil blive forsøgt fremsøgt.

Et eksempel på en udfyldt SFTPDynamicRoutingInfo struktur kan ses i afsnit 6.3.1.

### 6.5.3 Teknisk kvittering

Som resultatet af en validering af et triggerobjekt leveret af et it-system, genererer Serviceplatformen en teknisk kvittering.

Indholdet af en teknisk kvittering er XML. En teknisk kvittering vil indeholde et *TechnicalReceipt* xml element af typen *TechnicalReceiptType*, som er defineret i *SFTPTypes.xsd* filen, der kan hentes på følgende link: <https://www.serviceplatformen.dk/administration/contract-doc/contracts/ServiceContract-d7ffb23b-49d3-4a22-877a-0ecd473a3d15.zip>.

*TechnicalReceiptType* indeholder:

- **Receipt(o\*):** Et element af typen *ReceiptType*.
- **ErrorMessage(o\*):** Et element af typen *ErrorMessage*. Vil kun være sat hvis der er valideringsfejl af triggerfilen.
- **FileTransferUUID(o):** UUID'et som SFTP servicen har tildelt filen. Filen vil på Serviceplatformen efter den tekniske kvittering er genereret blive refereret til ved dette UUID.
- **SendersFileId(v):** Et felt afsendersystemet kan sætte til unik identifikation af filen. SFTP servicen bruger ikke dette felt, men det vil blive videregivet til modtagersystemet.

Typen *ReceiptType* består af følgende elementer

- **Message(o):** En besked genereret af SFTP servicen der beskriver hvorvidt triggerfilen er blevet valideret til at være korrekt.

Typen *ErrorMessage* består af følgende elementer

- **ErrorCode(o):** En Fejlkode der bruges til at beskrive typen af fejlen. En komplet liste af fejkoder kan ses i afsnit 6.5.4 fejkoder.
- **ErrorCodeDescription(o):** Navnet på fejkoden
- **ErrorDescription(o):** En tekstbeskrivelse af fejlen relateret til fejkoden

Et eksempel på en teknisk kvittering for en succesfuld validering kan ses i afsnit 6.2.1.

Et eksempel på en teknisk kvittering for en validering med fejl kan ses nedenfor

```
<ns2:TechnicalReceipt xmlns:ns2='http://serviceplatformen.dk/xml/wsd/soap11/SFTP/1/types'>
  <FileTransferUUID>ca342b89-9c73-48e9-904a-1db31b32a60b</FileTransferUUID>
  <ErrorMessage>
    <ErrorCode>11</ns2:ErrorCode>
    <ErrorCodeDescription>RejectedUnknownUsername</ns2:ErrorCodeDescription>
    <ErrorDescription>Recipient Kombit does not exist</ns2:ErrorDescription>
  </ErrorMessage>
</ns2:TechnicalReceipt>
```

```
</ErrorMessage>  
</ns2:TechnicalReceipt>
```

## 6.5.4 Fejlkode

I forbindelse med valideringen af en triggerfil kan følgende fejlkode blive returneret i den tekniske kvittering.

ErrorCode	ErrorCodeDescription	ErrorDescription
10	RejectedUnableToParseTrigger	Incorrect trigger file / Unable to read file size / Unable to read name of input file / The file name contains unallowed characters. Unable to read number of recipients / No sender specified in the trigger
11	RejectedUnknownUsername	Sender's username <username> does not exist / Recipient <username> does not exist
12	RejectedFileNotFound	File <filename> does not exist
13	RejectedFileSizeDoesNotMatch	File size does not match. The file should have size <size1>, but it actually has size <size2>
14	RejectedFileAlreadyPresentAtRecipient	File already present at recipient.
15	RejectedRecipientHasTooManyFiles	Too many files are present in the recipient <username>'s IN folder.
16	RejectedMixOfUseCases	Trying to send to the recipient with username <username> but this recipient has a

		different use case than the sender.
17	RejectedFileSentByWrongUser	Mismatch between specified username and username in trigger file.
50	RejectedNoSFTPDynamicRoutingInfoFound	Could not find SFTPDynamicRoutingInfo structure.
51	RejectedFileSizeTooLarge	The provided file's size exceeds the maximum allowed.
52	RejectedNoInfRefFound	No InfRef in trigger file.
53	RejectedNoRecipientAuthorityFound	No RecipientAuthority in trigger file.
54	RejectedNoSenderAuthorityFound	No SenderAuthority in trigger file.
55	RejectedNoRoutingPermissionFound	<p>Could not load permission for transfer: &lt;SenderAuthority&gt; =&gt; &lt;RecipientAuthority&gt; " with type &lt;Infref&gt; for SendingIt-system: &lt;SenderIt-system&gt;. /</p> <p>Could not load permission for transfer: &lt;SenderAuthority&gt; =&gt; &lt;RecipientAuthority&gt; " with type &lt;Infref&gt; for SendingIt-system: &lt;SenderIt-system&gt; =&gt; &lt;RecipientIt-system&gt;</p>
56	RejectedMoreThanOneRecipient	Only one recipient is allowed when using sftp dynamic routing.
57	RejectedNoSenderItSystemFound	No SenderIt-system provided in the trigger file.
58	RejectedUnknownInfref	The provided Infref value is not supported by Serviceplatformen.
59	RejectedNoSFTPForRecipientItSystemFound	The RecipientIT-system <RecipientIt-system> has no SFTP.
60	RejectedUnknownRecipientItSystemFound	The RecipientIT-system <RecipientIt-system> could not be found.

61	RejectedInfrefRequiresRecipientSystem	The RecipientSystem field must be provided for the infref: <Infref>
62	RejectedInfrefRequiresNoRecipientSystem	The RecipientSystem field must not be provided for the infref: <Infref>
63	RejectedMultipleSFTPDynamicRoutingInfoFound	Multiple instances of SFTPDynamicRoutingInfo found. Only one is allowed.

## 6.5.5 Metadatafil

Indholdet af en metadatafil er xml. En metadatafil vil indeholde et *FileMetadata* xml element af typen *FileMetadataType* som er defineret i *SFTPTypes.xsd* filen der kan hentes på følgende link:

<https://www.serviceplatformen.dk/administration/contract-doc/contracts/ServiceContract-d7ffb23b-49d3-4a22-877a-0ecd473a3d15.zip>.

*FileMetadataType* indeholder:

- **FileTransferUUID(o):** Et UUID tildelt af Serviceplatformen til filoverførslen. Skal bruges af modtagersystemet ved brugsscenarioet styret overførsel af fil til at kvittere for filoverførslen.
- **FileDescriptor(o):** Et element af typen *FileDescriptorType* som er beskrevet i afsnit: 6.5.1. Vil indeholde det samme som i det oprindelige triggerobjekt for filoverførslen på nær, at kun modtagersystemet vil være listet som en af modtagerne.
- **FileContentDescriptor(o):** Et element af typen *FileContentDescriptorType* som er beskrevet i afsnit 6.5.1. Vil indeholde det samme som i det oprindelige triggerobjekt for filoverførslen.

Et eksempel på en metadatafil kan ses i afsnit 6.2.1.

## 6.5.6 Forretningskvittering

Leveres gennem et webservicekald. Forretningskvitteringen består af et *BusinessReceipt* xml element af typen *BusinessReceiptType* som er defineret i *SFTPTypes.xsd* filen der kan hentes på følgende link

<https://www.serviceplatformen.dk/administration/contract-doc/contracts/ServiceContract-d7ffb23b-49d3-4a22-877a-0ecd473a3d15.zip>.

*BusinessReceiptType* indeholder:

- **FileTransferUUID(o):** Et UUID tildelt af Serviceplatformen til filoverførslen.
- **Filename(o):** Filnavnet på filen der skal sendes. Skal inkludere filtypenavn på filen.
- **FileAcceptance(o):** Indikerer om modtagersystemet har accepteret eller afvist filen. Skal have en af værdierne "ACCEPTED", "REJECTED" eller "COULD\_NOT\_NOTIFY\_RECIPIENT". Sidstnævnte værdi benyttes ved styrede overførsler og vil kun returneres hvis modtagersystemet har modtaget filen, men ikke kunne notificeres.
- **Recipient(o):** SFTP brugernavnet på modtageren af filen.
- **Reason(v):** Indeholder en evt. begrundelse for at filen er blevet accepteret eller afvist.

```
<ns2:BusinessReceipt xmlns:ns2='http://serviceplatformen.dk/xml/wsd/soap11/SFTP/1/types>
```

```
<ns2:FileTransferUUID>1a958955-fb4a-421e-9f09-8ec0a97b39be</ns2:FileTransferUUID>  
<ns2:Filename>testfil.txt</ns2:Filename>  
<ns2:FileAcceptance>ACCEPTED</ns2:FileAcceptance>  
<ns2:Reason>Lige det vi manglede</ns2:Reason>  
<ns2:Recipient>Modtager</ns2:Recipient>  
</ns2:BusinessReceipt>
```

## 6.6 Validering af triggerobjekter

For at Serviceplatformen kan overføre en fil for et it-system, kræves det at it-systemet leverer et validt triggerobjekt til SFTP Servicen. For at et triggerobjekt regnes som validt skal følgende gælde:

Det valideres at triggerobjektet er korrekt xml i forhold til skemaet for triggerobjekt typen beskrevet i afsnit 6.5.1.

Det valideres, at det angivne afsendersystem i triggerobjektet eksisterer og stemmer overens med det it-system, der har leveret triggerobjektet.

Det valideres, at den angivne fil ligger i afsendersystemets OUT-mappe, og at den har den korrekte størrelse.

For hver angivne modtager gøres følgende:

- Det valideres at den angivne modtager eksisterer.
- Det valideres at den angivne modtager anvender samme filudvekslingstype som afsendersystemet.
- Det valideres at modtagersystemet ikke har en fil med samme navn i dets IN-mappe.
- Det valideres at modtagersystemet ikke har for mange filer i dets IN-mappe.