

Vejledning til anvendelse af Serviceplatformen SFTP Service

Udarbejdet for:

KOMBIT A/S

Halfdansgade 8

2300 København S

Revision

Nuværende revision: 1.66

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 DemoVirtual 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 "<RecipientIt-system>"
1.60	08.11.21 RouteSelectionValueDate funktionalitet tilføjet
1.61	10.11.21 Småkorrektioner ifbm. review
1.61_CR074_v0.1	30.06.22 CR074 - Småkorrektioner ifbm. Roller
1.61_CR074-073_v0.2	Konsolideret version CR074: Links tilrettet CR073: Opdateret begreber om it-system
1.61_CR074-073_v0.3	29.11.22: Mindre opdateringer ifbm. review
1.62 CR074 v0.4	09-12-22: Mindre opdatering i begreb om it-systemer
1.63 SREU16703936	28-09-23: Links til eksternt dokument rettet
1.64 CR242	12-02-24: Ruteregler
1.65	16-07-2024: Dokument overdraget fra KOMBIT, som har lavet småændringer for at forbereder kvaliteten af dokumentet til brugerne.
1.65 CR263v2	13-10-2025: Gyldighed af SSH-nøgler. Generering af nøglepar i browser.
1.66	Opdateringer ift. CR263 godkendt af Kombit. Dokument promoted til v. 1.66

Indhold

Contents

1	Formål med vejledning til Serviceplatformens SFTP Service.....	4
2	Begreber	4
3	SFTP Service beskrivelse	5
3.1	Simpel overførsel af filer	6
3.2	Styret overførsel af filer.....	6
3.3	Ruter	7
4	Oprettelse af adgang til SFTP servicen på Serviceplatformen.....	8
5	Teknisk dokumentation	9
5.1	Brug af SFTP serveren.....	9
5.1.1	Adgang til SFTP serveren	9
5.1.2	Mappestruktur	12
5.1.3	Upload af filer.....	12
5.1.4	Oprydning og monitorering på SFTP serveren.....	12
5.2	Information omkring SFTP server	14
5.3	Simpel overførsel af filer	14
5.3.1	Brugseksempel	14
5.4	Dynamisk routing	16
5.4.1	Oprettelse af dynamiske routingregler	17
5.4.2	Brugseksempel	21
5.5	Styret overførsel af filer.....	24
5.5.1	SFTP servicens webservice	24
5.5.2	It-systemets webservice beskrivelse	25
5.5.3	Brugseksempel	25
5.6	XML-Strukturer.....	29
5.6.1	Triggerobjekt	29
5.6.2	SFTPDynamicRoutingInfo.....	30
5.6.3	Teknisk kvittering.....	30
5.6.4	Fejlkode.....	32
5.6.5	Metadatafil.....	34
5.6.6	Forretningskvittering	34
5.7	Validering af triggerobjekter.....	36

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:

Afsender	Den forvaltningsansvarlige for afsendersystemet - typisk leverandøren
Afsendersystemet	Det it-system der vil overføre en fil til et modtagersystem.
Dataafgrænsning	Afgrænsning på en systemrolle, som indsnævrer systemrollens virkefelt.
EksPLICIT routing	Et begreb for routing, hvor destinationen (modtagersystemet) eksplicit er angivet i triggerfil og skal matche en route-konfiguration på Serviceplatformen.
Filservice	En udbudt virtuelle service fra Serviceplatformen serviceudbyder, hvor adgang administreres via Serviceaftaler
Forretningskvittering	En xml-struktur der bruges af et modtagersystem til at kvittere for modtagelsen af en fil.
InfRef	Information flow reference, mærker domænet (og versionen) af de data der skal overføres. Svarer til en entityID for WebServices.
InfRef	Information flow reference, mærker domænet (og versionen) af de data der skal overføres. Svarer til en entityID for WebServices.
It-system	Kommunens it-system, der benytter eller potentielt kan benytte services på Serviceplatformen. For at få adgang skal it-systemet identificere sig med et gyldigt OCES3 certifikat. For at bruge SFTP skal it-systemet være oprettet som bruger af Serviceplatformens SFTP Service
Metadata fil	En xml struktur der beskriver en given fil, der skal overføres fra et afsender- til et modtagersystem.
Modtager	Den forvaltningsansvarlige for modtagersystemet - typisk leverandøren
Modtagersystemet	Det it-system som et afsendersystem ønsker at sende en fil til.
Myndighed	Myndighed er i Administrationsmodulet den organisation, der godkender anvendelsen af services i forhold til et anvendersystem. En myndighed kan eksempelvis være kommuner, stat eller Udbetaling Danmark (UDK).
Serviceaftale	En serviceaftale er en aftale, der indgås mellem it-leverandøren og en myndighed, således at et anvendersystem kan tilgå myndighedens, data via en service. Service skal forstås i bred forstand, og dækker således både webservice og SFTP mf.

SFTP dynamisk routing	En betegnelse for routing af filer, hvor modtager findes med opslag pga. angivet parameter i triggerfilen og routekonfiguration på Serviceplatformen
SFTPDynamicRoutingInfo	En xml struktur der anvendes til at identificere modtagersystemet når dynamisk routing anvendes.
SFTP Rute (eller Rute I sammenhæng med dette document)	En SFTP rute angiver en mulig overførelse af en fil med en defineret dataspecifikation (InfRef) mellem en afsender og modtager.
SFTP webservice	En webservice der udstilles på Serviceplatformen som en del af SFTP-servicen.
Systemrolle	Gruppering af rettigheder, der definerer adgang og adgangsbegrænsninger til en given service
Triggerfil	En fil hvis indhold er et triggerobjekt.
Teknisk kvittering	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.
Triggerobjekt	En xml struktur der bruges til at specificere hvem modtageren af en given fil er.

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 3.1 og 6.3, 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 5.3.

Bemærk: Simple SFTP uden ruter må ikke anvendes til nye overførelser af andre typer data end der allerede eksistere. Eksisterende overførelser med Simple SFTP uden ruter, vil over den nærmeste tid blive migreret til SFTP med ruter.

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 5.5. Styret filoverførsel er i dag ikke anvendt, og vil på sigt blive udfaset.

3.3 Ruter

Dynamisk routing giver udvidede muligheder for at kontrollere overførslen af filer mellem afsender og modtager. Her overføres filer på baggrund af ekstra "routing info", der inkluderes i triggerfiler, og som sammenholdes med opsatte routingregler (ruter) på Serviceplatformen, angiver hvem modtageren skal være. Det ekstra data leveres i triggerfilen i xml strukturen SFTPDynamicRoutingInfo.

For at anvende dynamisk routing skal triggerfilen angive "routing motoren" som modtagersystemet – ganske som man vil angive et almindeligt modtagersystem. Derved sendes både data- og trigger-fil til "routing motoren", der forsøger at finde en matchende routingregel på baggrund af informationerne i triggerfilen. Hvis en sådan regel findes, sendes datafiler og genereret metadatafil til det modtagersystem, som reglen specificerer. I modsat fald afvises overførslen og afsenderen får besked om at der ikke kan findes en modtager. Ved dynamisk routing kræves det, at der på Serviceplatformen er opsat routingregler, der angiver hvilke systemer og myndigheder, der har tilladelse til at sende hvilke data til hinanden. Dette udgør den øgede sikkerhed i dynamisk routing, ved at det kun er systemer og myndigheder, som der er opsat prædefineret rute for, der har tilladelse til at sende til hinanden.

Hidtil er dynamiske routingregler blevet oprettet manuelt på baggrund bestillingsblanketter. Fremover bliver Routing-baseret filoverførsler understøttet af serviceaftaler, og Serviceplatformen vil automatisk oprette routingregler baseret på disse aftaler.

Der er ligeledes blevet tilføjet en ny GUI til at oprette og administrere bestillingerne på Serviceplatformen.

Endvidere udstilles en ny selvbetjeningsløsning, der muliggør efterfølgende administration af routingregler [USM0014 FilUdveksling GUI komponent]. Det skal bemærkes, at regler oprettet frem til marts 2024 betragtes som "legacy", og de vil fortsat fungere som hidtil.

Med den nye løsning skal IT-systemer, der ønsker at aflevere eller hente data via regelbaseret filudveksling, indgå serviceaftaler, der dækker udvekslingen. Serviceplatformen vil løbende undersøge, om nyligt godkendt serviceaftaler matcher eksisterende godkendte serviceaftaler, og den vil oprette nye routingregler i de tilfælde, hvor det er et match.

Overordnet fungerer matching-logikken således:

System A har en godkendt serviceaftale, der tillader at aflevere økonomiposteringer på vegne af en given kommune. System B har en godkendt serviceaftale, der tillader at deres system hente økonomiposteringer på vegne af samme kommune, så vil der være et match mellem aftalerne, og der oprettes en routingregel. Er der match mellem serviceaftalerne, oprettes der en routingregel. Typen (eksplicit eller implicit) af den oprettede ruteregul afhænger af InfRef valgt i Serviceaftalerne. InfRef registreres af KOMBIT administratorer, der definerer typen af regler, der er tilladt at oprette.

Afsnit 5.4.1 beskriver i flere detaljer, hvordan matching-logikken fungerer, samt hvordan aflever- og hent-serviceaftaler udfyldes.

Udover at danne grundlag for oprettelse af routingregler, benyttes serviceaftaler også i forbindelse med selve overførslen. Mere specifikt skal både det afsendende system og det modtagende system have

godkendte, relevante serviceaftaler på overførelstidspunktet. Dette valideres af Serviceplatformen, der sammenholder overførelsen med et lokalt replika af serviceaftaler.

Det er værd at bemærke, at trods routingregler oprettes på baggrund af matchende serviceaftaler, eksisterer reglerne efterfølgende delvis uafhængig af disse aftaler. Hvis en serviceaftale udløber, vil en routingregel således ikke straks blive nedlagt; derimod vil den fortsat eksistere i 3 måneder, og kun hvis der indenfor denne periode ikke godkendes en ny tilsvarende/matchende serviceaftale, nedlægges reglen. Hensigten med dette er at undgå, at routingregler nedlægges som følge af eksempelvis utilsigtede udløb af serviceaftaler.

Hovedparten af de fil-baseret integrationer og services i den fælleskommunale infrastruktur er efterhånden overgået til at benytte routingregler, men enkelte integrationer anvender stadig simpel overførelse uden regler. Disse vil i fremtiden blive udfaset - eller overgå til routingregler - men frem til det sker, vil disse fortsat fungere som beskrevet i afsnit [5.3 Simpel overførelse af filer], og der skal således ikke nye indgå serviceaftaler eller ændre på allerede eksisterende regler. Dermed også sagt at routingregel-baseret overførelser kun må benyttes for integrationer, der specifikt benytter denne type (dette vil fremgå af den relevante integrationsbeskrivelse).

Det generelle flow for en regel-baseret filoverførelse 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. I tilfælde af dynamisk rute (og ikke brug af de gamle ruteregler), valideres eksistensen af aktive Serviceaftaler for både afsender- og modtagersystemer.
4. Serviceplatformen genererer en teknisk kvittering på baggrund af valideringen af triggerfilen og uploader kvitteringen til afsendersystemets indkommende mappe.
5. Hvis valideringen er succesfuld overføres filen til modtagersystemets indkommende mappe, sammen med en genereret metadatafil.
6. 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 5.4.

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 serviceaftaler. 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 Fælleskommunale Administrationsmodul (se vejledning for dette i dokumentet: [Brugervejledning til Administrationsmodulet for leverandør](#), afsnit 5.4.3.).

Når først informationerne er indtastet i Fælleskommunalt Administrationsmodul vil disse informationer blive provisioneret til Serviceplatformens SFTP server.

5 Teknisk dokumentation

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

5.1 Brug af SFTP serveren

5.1.1 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. En SSH nøgle er asymmetrisk, dvs. den har en offentlig del og en privat del. Serviceplatformen skal kende den offentlige del af SSH nøglen i forbindelse med registrering af it-systemet og muligheden for anvendelse af SFTP. SFTP-klienten skal have adgang til den private del, som ikke deles med Serviceplatformen.

5.1.1.1 Gyldighed af SSH-nøgler

Administrationsmodulet og Serviceplatformen betragter en SSH-nøgle som gyldig i 2 år efter registreringen i Administrationsmodulet. 3 måneder før SSH-nøglen udløber, oprettes en opgave i Administrationsmodulet på at få nøglen udskiftet og samtidig udsendes en email-notifikation. Opgaven vil være synlig for alle brugere i rollen Leverandøradministrator fra systemejers organisation. Email-notifikationen udsendes til alle brugere fra systemejers organisation, der abonnerer på notifikationer af typen 'Udløb af SSH-nøgle'.

Fornyelse af nøglen sker ved at logge på Administrationsmodulet, fremsøge It-systemet og opdatere SSH-nøglen på Anvendersystem-fanebladet som beskrevet nedenfor.

Hvis en SSH-nøgle udløber, før den bliver udskiftet, bliver adgangen til den tilhørende SFTP-konto blokeret af Serviceplatformen. Adgangen åbnes igen, når nøglen bliver udskiftet.

5.1.1.2 Format for SSH nøgle

Formatet på SSH nøgle er som følger:

```
rsa-sha2-256
AAAAB3NzaC1yc2EAAAADAQABAAQDqINSRa97n8sagpvO8l6NcsHrc93M2CQT7hlsG0LAQ/m9LOSCAx
d5wmBt7LDWMLfpGLs/H64C6V1cUgDwbAnop2PgJPQ1caIkQyXPb9kqIw1WVTS+lgFmDm3AwHKAK4Ers3Q
ZQdVqPxyCb4yTM6xrtD65nev5gvUAWF4XXE5foPhplfUcHcoHFK33ImfX4VKOFbR/0ulpoOh2fq0sLyqBnAcD8H
O9oAGQZbjZ6z409fxiO/jZUV+jexowrm6cBEcl0rHR/AMn5X9hTLjGFZ5w+ol/pf8XWC6RqhHfZnHwoMHGLIbw
mYpeOfowVIYLuK5E6dyq5uxvWe4hZihCBpyobTdQSTNF9Wi+uaDlyZ1TUtVqO/V5u/1OLuFf3kJDp6oB9PVHtr
KsCgK/5BUKiAGQZybA2iEdZodYAijpyF8u15YmMrwPudSNQel+z/Lu56AWpk1+lr37b99fevB7JqLiNNZI3tzPPK
w5GeGDUs3cK6E4ji4k533i2S+pnGW+MUGu+Gru8TGEZOCzX4z4b6txB/TDDZ5zgA2Lgt6hW8zbZdTLZcjXS6
eBGvPeG9BqviCeYPJgHQtcBX/ulZ4wJuUS0bcQQRyRrrgboW++Oub2u0aq7saPWtzAxJFJESfPMYevlHmyhb
HQSAJmjvTThvyWY8X7UgtzoBrENh32t0GbpTQ==
```

I eksemplet anvendes den anbefalede protokol, rsa-sha2-256, og en RSA-nøglelængde på 4096.

SSH nøgle:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAvs5Wn8v
```

5.1.1.3 Generering af SSH-nøgler via Administrationsmodulets browserløsning

Administrationsmodulet giver mulighed for at generere både den offentlige og den private del af et nøglepar. Hvis man benytter sig af denne mulighed, bliver den offentlige del automatisk indsat i SSH Nøgle-feltet og overført til Serviceplatformen med angivelse af protokollen 'rsa-sha2-256', mens den private del skal kopieres og installeres i SFTP-klienten. Nøgleparret er af type RSA med bitlængde 4096. Den private del er ukrypteret og bliver hverken gemt i Administrationsmodulet eller overført til Serviceplatformen. Hvis den private nøgle mistes, skal man derfor generere et nyt nøglepar.

SFTP
?

SSH brugernavn:

?

[Klik her for at lade systemet foreslå et unikt brugernavn](#)

SSH nøgle:

[Klik her for at lade systemet generere et nøglepar](#)

Filudvekslingstype:

Vælg "Klik her for at lade systemet generere et nøglepar". Derved fremkommer følgende dialog:

SSH-nøglepar

Dette nøglepar må kun bruges til it-systemets SFTP-forbindelse. Du kan altid genere en ny nøgle.

Offentlig SSH-nøgle:

```
rsa-sha2-256
AAAAB3NzaC1yc2EAAAADAQABAAQCAQDt9NNsJAF8TQTV6onX
4D3D8HogWxENE3NCe8NWCFbTxgBPt/I4iRUb0TiJx6kZQPWWv
Fo7TWXI5rbkflQr5sZEP9pB+bnyl0L11UiDz0lpLhIRcEs9zcmxeWA
OQ4BVaXz6jw7LFuwzsGFkaztrkamibDGFRBZ/FQKKe+6G7YXhm
```

Privat SSH-nøgle

👁️ 📄

Den private nøgle skal opbevares sikkert og kan ikke vises eller kopieres igen, når dette vindue lukkes. For at fortsætte skal du acceptere disse betingelser. *

Anvend

Annuller

Den private del af nøglen er skjult men kan kopieres til udklipsholderen via kopierings-ikonet. Alternativt kan man få den vist ved at klikke på visnings-ikonet. Bemærk, at Anvend-knappen først bliver aktiv, når man har fået vist eller kopieret nøglen og accepteret betingelserne.

Den private del skal installeres i It-systemets SFTP-klient og bør håndteres og opbevares på sikker vis.

Det anbefales at lukke browseren ned, når denne funktion har været benyttet.

Det er også muligt at benytte et eksternt værktøj til at generere nøgleparret. I så fald skal man blot indsætte den offentlige del af parret i feltet "SSH nøgle" med angivelse af den ønskede protokol (anbefalet: rsa-sha2-256) og undlade at aktivere linket under dette felt i brugergrænsefladen.

5.1.2 Mappedstruktur

Når et it-system er registreret 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.

5.1.3 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 eller dynamisk ruting 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.

5.1.4 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, 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.

5.1.4.1 Oprettelse af filtre

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.

Filtre konfigureres gennem Serviceplatformen ved at sende en email til 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.

5.2 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: `sftpexttest.serviceplatformen.dk`

For begge miljøer skal der forbindes på port 22.

5.3 Simple overførsel af filer

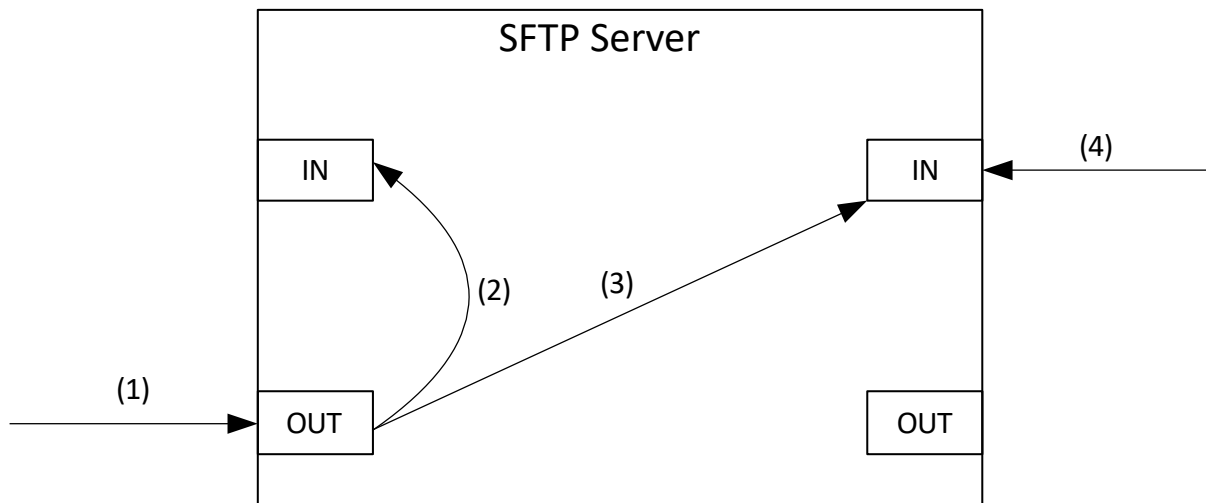
Ved simpel overførsel af filer sker udvekslingen af beskeder mellem modtagersystemet, afsendersystemet, og SFTP Servicen ved hjælp af filer på SFTP serveren.

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. Simple SFTP uden ruter må ikke anvendes til nye overførelser af andre type data end der allerede eksistere. Eksisterende overførelser med Simple SFTP uden ruter, vil over den nærmeste tid blive migreret til SFTP med router.

5.3.1 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>
</ns2:Trigger>
```

```

</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 "låsnings" ved, at afsendersystemets skriverettigheder 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.

5.4 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>
  <SenderIdt-system>40f6af96-db76-4570-91fa-068fa757582a</SenderIdt-system>
  <SenderAuthority>urn:oio:cvr-nr:64942212</SenderAuthority>
  <TransactionId>00000000-0000-0000-0000-000000000000</TransactionId>
  <SenderIdt-timestamp>2016-12-17T09:30:47Z</SenderIdt-timestamp>
  <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 5.6.2. 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	SenderIdt-System	RecipientAuthority	RecipientIt-system	SFTPUsername	ValidFrom	ValidTo
XXX	XXX	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 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 *SenderIdt-system*, *SenderAuthority*, *InfRef* og *RecipientAuthority* hentes ud af SFTPDynamicRoutingInfo strukturen.
- Der fremsøges en regel med værdierne: *SenderIdt-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 angivende *infref* værdi.
- SFTPDynamicRoutingInfo kan potentielt indeholde en valgfri struktur, *RouteParameterList*, med en liste af *RouteParameter* elementer. Hvis et felt *RouteSelectionValueDate* er angivet i *RouteParameter*, så bruges denne til processen for regelsøgning, og ellers bruges en nuværende server dato og tidspunkt.

- Hvis en routingregel kan fremsøges baseret på det givne data, vil den blive sendt til modtagersystemet med det fremsøgte SFTP brugernavn.

Ved *eksplicit* routing fremsøges routingregler på følgende måde:

- Værdierne fra felterne *SenderIt-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 den blive sendt til modtagersystemet med det fremsøgte SFTP brugernavn.
- Hvis feltet *RouteSelectionValueDate* er udfyldt i SFTPDynamicRoutingInfo / *RouteParameterList* strukturen, returneres en fejl i den tekniske kvittering, som indikerer at det udfyldte *InfRef*, bruger *eksplicit* routing. For *eksplicit* routing fremsøges reglen altid udelukkende baseret på det nuværende server tidspunkt.

5.4.1 Oprettelse af dynamiske routingregler

Som beskrevet i afsnit [5.4 Dynamisk routing] er routing-baseret filoverførsler understøttet af serviceaftaler, og Serviceplatformen er i stand til automatisk at oprette routingregler på baggrund af disse serviceaftaler.

Som anvender er det derfor nyttigt at forstå, hvordan Serviceplatformen opretter routingregler og i særdeleshed hvilken rolle, serviceaftaler spiller i den forbindelse. Dette gennemgås i nedenstående sektioner, der også beskriver de generelle mekanismer, der gør sig gældende på tværs af alle fil-baserede integrationer.

Forståelsen af den videre tekst forudsætter kendskab til serviceaftaler og dataafgrænsninger. Det beskrives i [Brugervejledning til Administrationsmodulerne for leverandører.pdf – USM0020].

Fokus i dette afsnit er på de serviceaftaler som afsender og modtager, hver især skal indgå. Endvidere beskrives dataafgrænsninger i serviceaftaler, og hvordan samspillet i dataafgrænsningerne er med til at danne grundlaget for den automatiske oprettelse af routingregler.

Serviceaftaler for afsender- og modtagersystemer er i stor udstrækning identiske, men der er små - men vigtige - forskelle. Derfor beskrives de individuelt nedenfor.

Afsender¹ skal anmode om serviceaftale af typen 'Uden videregivelse af data' og efterfølgende vælge det afsendende IT-system. Dernæst skal afsender vælge den myndighed, som serviceaftalen indgås med - i dette tilfælde den myndighed, som data afleveres på vegne af. Derefter skal afsender vælge servicen 'FilAflever', hvilket efterfølgende kræver opsætning af rolle og tilhørende parametre, også kaldet dataafgrænsningsværdier:

- **Rolle:** AfleverFil
- **InfRef:** Specificerer hvilke data, der udveksles. Navnet defineres af de enkelte services og kan findes i de pågældende integrationsbeskrivelser. Kun registrerede InfRefs vil fremgå af listen med mulige værdier, eks. UdvidetHelbredstillægAnsøgningBilag_1 og "SF0770_B_IF01".
- **Tilladte modtagermyndigheder:** Angiver de myndigheder, som data må sendes til. For langt de fleste integrationer udveksles data indenfor samme myndighed eks. kommune, og i de tilfælde vil tilladte modtagermyndighed(er) være identisk med den afsendende myndighed - dvs. den myndighed som

¹ Den forvaltningsansvarlige for afsendersystemet - typisk leverandøren

afsender er ved at indgå serviceaftale med. I få tilfælde udveksles data på tværs af myndigheder, eksempelvis fra en kommune til Udbetaling Danmark, og i de tilfælde vil tilladte modtagermyndighed(er) være forskellige fra den afsendende myndighed. Informationer om hvilke myndigheder, der udveksles data mellem, vil fremgå af de enkelte integrationsbeskrivelser.

- **Tilladte modtagersystemer:** Angiver hvilke IT-systemer, som data må sendes til. Generelt anbefales det at vælge "Alle" (*). Man bør kun vælge et specifikt modtagersystem, såfremt det fremgår af integrationsbeskrivelsen, og/eller man forstår betydningen af dette, herunder hvilke begrænsninger det medfører for automatisk oprettelse af routingregler.

Det er muligt at tilføje rolle "AfleverFil" flere gange i én serviceaftale, og hver instans vil have eget sæt af dataafgrænsninger. På den måde kan man for den afsendende myndighed lade flere filudvekslinger fremgå af samme serviceaftale.

Afslutningsvis sendes serviceaftalen til godkendelse hos den afsendende myndighed.

Modtager² skal anmode om serviceaftale af typen 'Uden videregivelse af data' og efterfølgende vælge det modtagende IT-system. Dernæst skal modtager vælge den myndighed, som serviceaftalen indgås med - i dette tilfælde den myndighed, som data modtages på vegne af. Derefter skal modtager vælge servicen 'FilHent', hvilket efterfølgende kræver opsætning rolle og tilhørende parametre, også kaldet dataafgrænsningsværdier:

- **Rolle:** HentFil
- **InfRef:** Specificerer hvilke data, der udveksles. Tekststreng, som unikt identificeret af de enkelte services og kan findes i de pågældende integrationsbeskrivelser.. Kun registrerede InfRefs vil fremgå af listen med mulige værdier, eks. "KommunalLedelseInformationOverfør_1" og "SF0770_B_IF01".
- **Tilladte afsendermyndigheder:** Angiver de myndigheder, som data må modtages fra. For langt de fleste integrationer udveksles data indenfor samme myndighed eks. kommune, og i de tilfælde vil tilladte afsendermyndighed(er) være identisk med den modtagende myndighed - dvs. den myndighed som modtager er ved at indgå serviceaftale med. I få tilfælde udveksles data på tværs af myndigheder, eksempelvis fra en kommune til Udbetaling Danmark, og i de tilfælde vil tilladte afsendermyndighed(er) være forskellige fra den modtagende myndighed. Informationer om hvilke myndigheder, der udveksles data mellem, vil fremgå af de enkelte integrationsbeskrivelser.
- **Tilladte afsendersystemer:** Angiver hvilke IT-systemer, som data må modtages fra. Generelt anbefales det at vælge "Alle" (*). Man bør kun vælge et specifikt afsendersystem, såfremt det fremgår af integrationsbeskrivelsen, og/eller man forstår betydningen af dette, herunder hvilke begrænsninger det medfører for automatisk oprettelse af routingregler.

Det er muligt at tilføje rollen "HentFil" flere gange i én serviceaftale, og hver instans vil have eget sæt af dataafgrænsninger. På den måde kan man for den modtagende myndighed lade flere filudvekslinger fremgå af samme serviceaftale.

Afslutningsvis sendes serviceaftalen til godkendelse hos den modtagende myndighed.

Den nye routingsregel kan kun oprettes i administreret tilstand ved at oprette et serviceaftalepar i ADM-modulet. Når begge rutedannende serviceaftaler er godkendt, oprettes den nye routingregel (hvis en sådan dynamisk regel ikke allerede eksisterer) – enten ved at overføre en eksisterende ældre-routingregel eller oprette en ny administreret routingregel.

² Den forvaltningsansvarlige for modtagersystemet - typisk leverandøren

Serviceaftalen er af typen 'Uden videregivelse af data' – der kun beskriver den ene side af overførslen – enten afsenderen eller modtageren. Anmoderen vælger den respektive sende/modtagende myndighed og det it-system, der er involveret i den pågældende side af overførslen. For korrekt at angive, om anmoderen udfylder serviceaftalen som afsender eller som modtagende part, skal de vælge passende service. Der er 2 'virtuelle' tjenester dedikeret til denne type serviceaftaler -'Fil Service Med Rutning Aflever' og 'Fil Service Med Rutning Hent', leveret af Serviceplatformen (kun én må vælges). Brugeren fortsætter derefter ved at vælge InfRef-navnet fra tilgængelig forudfyldt liste (InfRef-listen administreres af Kombit-administratorer, som kan oprette ny InfRef og beslutte, om typen er eksplicit eller implicit). Endelig kan brugeren i Serviceaftalens parametersektion begrænse, hvilke parter (myndigheder og it-systemer) der kan matches med denne serviceaftale for oprettelse af den dynamiske routingregel for at dynamisk routingoverførsel kan ske.

Eksempel på aflever-serviceaftale:

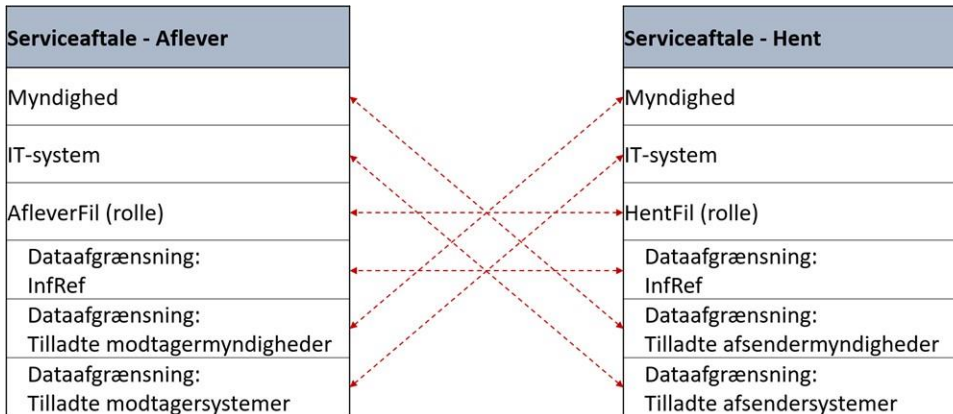
- Type: 'Uden videregivelse af data'
- Myndighed: Aarhus kommune
- ITSystem: KSD
- Service: 'FilAflever'
- Rolle: AfleverFil - Parametre:
 - InfRef: KommunalLedelseInformationOverfør_1
 - Tilladte modtagermyndigheder: Aarhus kommune
 - Tilladte modtagersystemer: *

Eksempel på hent-serviceaftale:

- Type: 'Uden videregivelse af data'
- Myndighed: Aarhus kommune
- ITSystem: Aarhus LIS
- Service: 'FilHent'
- Rolle: HentFil - Parametre:
 - InfRef: KommunalLedelseInformationOverfør_1
 - Tilladte afsendermyndigheder: Aarhus kommune
 - Tilladte afsendersystemer: *

Når en FilAflever-serviceaftale godkendes, undersøger Serviceplatformen, om den kan matches med en eller flere godkendte FilHent-serviceaftale, og i så fald oprettes de relevante routingregler. Tilsvarende gør sig gældende, når en FilHent-serviceaftale godkendes.

Matching-logikken forsøger at finde FilAflever- og FilHent-serviceaftaler, hvor dataafgrænsninger "spiller" sammen, eksempelvis at de vedrører samme datatype (InfRef). De specifikke sammenligninger fremgår af nedenstående figur:



Opsummeret gælder:

- Begge serviceaftaler skal vedrøre samme datatype (InfRef).
- FilHent-serviceaftalen skal være indgået med en myndighed, som fremgår af dataafgrænsningen "Tilladte modtagermyndigheder" i FilAflever-serviceaftalen.
- FilAflever-serviceaftalen skal være indgået med en myndighed, som fremgår af dataafgrænsningen "Tilladte afsendermyndigheder" i FilHent-serviceaftalen.
- FilHent-serviceaftalen skal være indgået med et IT-system, som fremgår af dataafgrænsningen "Tilladte modtagersystemer" i FilAflever-serviceaftalen.
- FilAflever-serviceaftalen skal være indgået med et IT-system, som fremgår af dataafgrænsningen "Tilladte afsendersystemer" i FilHent-serviceaftalen.

Det er værd at bemærke, at samtlige dataafgrænsninger i de to serviceaftaler skal stemme overens, før s - det er således ikke tilstrækkeligt, at blot ndelmængde gør, eks. InfRef.

Inden Serviceplatformens logik opretter en ny routingregel, undersøger den, om en tilsvarende eksisterer i forvejen, mere specifikt skal logikken undersøge og foretage et af følgende:

- Der eksisterer ikke en matchende routingregel: Der oprettes en ny routingregel.
- Der eksisterer en matchende "legacy" routingregel: Den eksisterende regel konverteres til den nye "non-legacy" type (dette har betydning for administrationsmulighederne på nye selvbetjeningsløsning - se evt. [USM0014 FilUdveksling GUI komponent]).

Der eksisterer en matchende "non-legacy" routingregel: Der er ikke behov for at oprette ny regel. Det er værd at bemærke, at afsender og modtager ikke nødvendigvis koordinerer oprettelse af serviceaftaler; man anmoder blot en serviceaftale, og såfremt der eksisterer en eller flere matchende serviceaftaler på den "anden" side, oprettes tilsvarende routingregler automatisk. Man vil som myndighed og leverandør kunne se routingregler (ruter) i den nye selvbetjeningsløsning ([USM0014: "Veiledning til Ruteadministration"](#)).

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

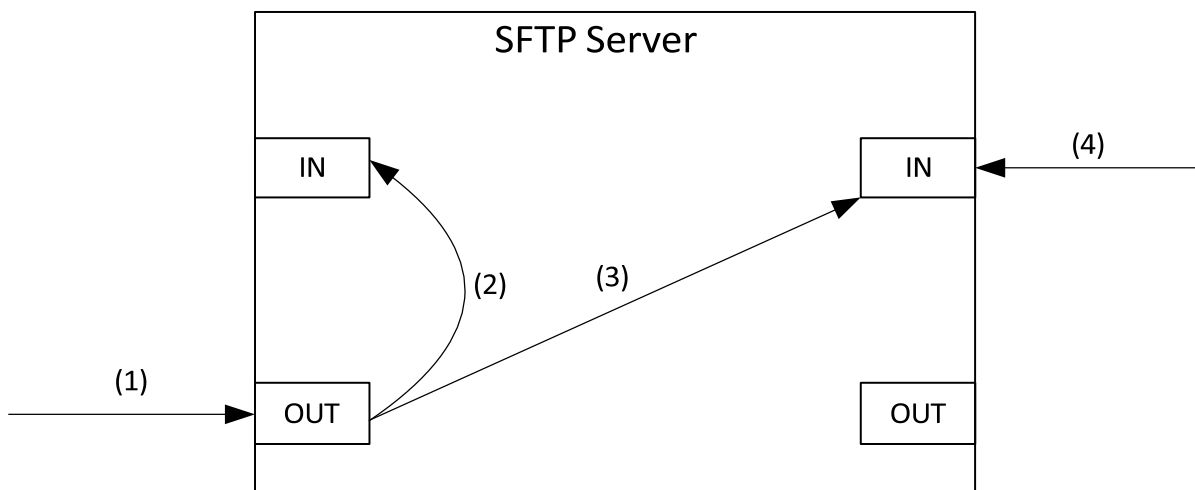
5.4.2 Brugseksempel

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	Recipient Authority	RecipientIt-system	SFTPUser name	ValidFrom	ValidTo
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. For at sende filen via dynamisk routing, skal rutekomponenten ("ROUTING_V1_0_0") angives i feltet Recipients.

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

```

    <RecipientAuthority>urn:oio:cvr-nr:64942212</RecipientAuthority>
    <RouteParameterList>
      <RouteParameter>
        < RouteSelectionValueDate>2016-06-20</ RouteSelectionValueDate>
      </RouteParameter>
    </RouteParameterList>
  </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/wsd/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/wsd/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/wsd/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>
      <TransactionId>ca02695f-497f-496d-86b1-4e9ecbd800a9</TransactionId>
      <SenderTimestamp>2016-06-27T06:48:00Z</SenderTimestamp>
      <RecipientAuthority>urn:oio:cvr-nr:64942212</RecipientAuthority>
      <RouteParameterList>
        <RouteParameter>

```

```

    < RouteSelectionValueDate>2016-06-20</ RouteSelectionValueDate>
  </RouteParameter>
</RouteParameterList>
</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*.

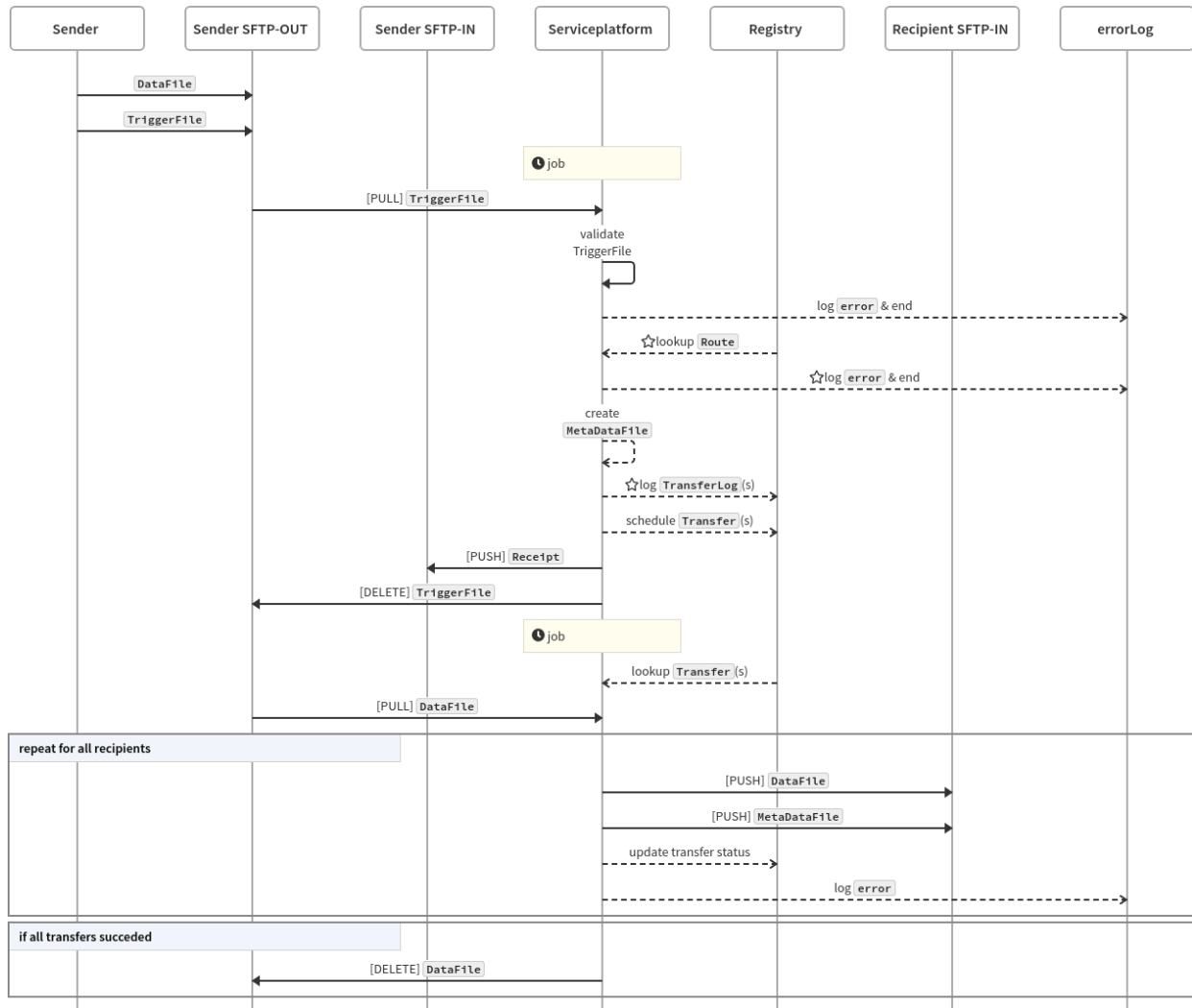
4. **Modtagersystemet tjekker dets IN-mappe og finder filen:** Modtagersystemet vil ved simpel overførsel af filer ikke modtage nogen notifikation om, at filen er blevet overført til dets IN-mappe. Det er derfor selv ansvarlig for at opdage, at en fil er blevet overført til det. Modtagersystemet kan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

5.4.3 *Bemærk at det anbefales at foretage oprydning i IN-mappen så snart filen er læst og håndteret af det pågældende system* *Process flow diagram*

Dette diagram beskriver (forenklet) trin for både den simple overførsel og den dynamiske rute. Trin markeret med et stjerne ikon er alene for den dynamiske rute.

Simple Overførsel / ☆Dynamisk Routing



5.5 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 SFTPServicenUser.wsdl. Serviceplatformen udstiller i forbindelse med SFTP servicen en webservice baseret på wsdl filen SFTPServicen.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 5.5.3.

5.5.1 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>

5.5.1.1 *TransferFile*

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

5.5.1.2 *DeliverBusinessReceipt*

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

5.5.2 *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.

5.5.2.1 *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.

5.5.2.2 *notifySender*

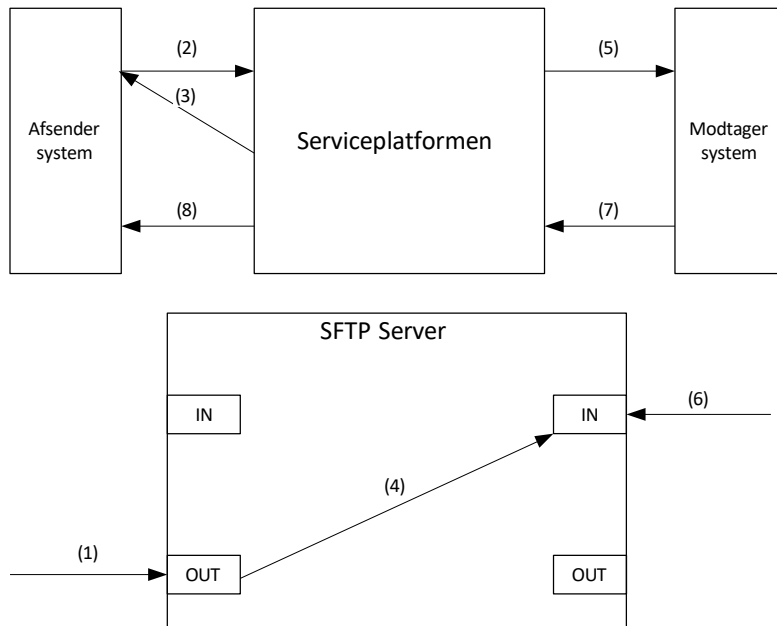
Kaldes af Serviceplatformen med en forretningskvitterings om at en fil er blevet overført til modtagersystemet, og modtagersystemet har kaldt ind med en forretningskvittering.

5.5.3 *Brugseksempel*

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

Forudsætningen ved rutebaseret filoverførelse er at myndigheden for afsendersystemet har godkendt en Serviceaftale med det relevante infref, og ligeså for modtagermyndigheds modtagersystem.

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



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

- 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/wSDL/soap11/SFTP/1/types"
xmlns:ns1="http://serviceplatformen.dk/xml/wSDL/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>
```

- Filen overføres til modtagersystemet:** Filen *info.txt* overføres fra afsendersystemets OUT-mappe til modtagersystemets IN-mappe.
- 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/wsdl/soap11/SFTP/1/types'
xmlns:ns4='http://serviceplatformen.dk/xml/wsdl/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>

```

5.6 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.

5.6.1 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://docs.kombit.dk/latest/0cfee71a>

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 5.3.1.

5.6.2 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://docs.kombit.dk/latest/0cfee71a>

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
- **SenderId-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:oio: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:XXXXXXXXX. Er en del af den routingregel som vil blive forsøgt fremsøgt.
- **RouteParameterList (o):** Skal udfyldes med en sekvens af RouteParameter elementer.

RouteParameter (o): Indeholder et element af typen 'any', hvilket skal være fra en liste a parametre, defineret af strukturen i RouteParameters.xsd, for eksempel RouteSelectionValueDate.

De tilladte elementer i RouteParameter strukturen er defineret i RouteParameters.xsd filen, som kan downloades via følgende link: <https://docs.kombit.dk/latest/0cfee71a>

5.6.3 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://docs.kombit.dk/latest/0cfee71a>

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 fejlkoder kan ses i afsnit 6.5.4 fejlkoder.
- **ErrorCodeDescription(o):** Navnet på fejlkoden
- **ErrorDescription(o):** En tekstbeskrivelse af fejlen relateret til fejlkoden

Et eksempel på en teknisk kvittering for en succesfuld validering kan ses i afsnit 5.3.1.

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

```
<ns2:TechnicalReceipt xmlns:ns2='http://serviceplatformen.dk/xml/wsdl/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>
```

5.6.4 Fejlkode

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

ErrorCode	ErrorCodeDescription	ErrorDescription
10	RejectedUnableToParseTrigger	<p>Incorrect trigger file /</p> <p>Unable to read file size /</p> <p>Unable to read name of input file /</p> <p>The file name contains unallowed characters.</p> <p>Unable to read number of recipients /</p> <p>No sender specified in the trigger</p>
11	RejectedUnknownUsername	<p>Sender's username <username> does not exist /</p> <p>Recipient <username> does not exist</p>
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: <SenderAuthority> => <RecipientAuthority> " with type <Infref> for SendingIt-system: <SenderIt-system>. /</p> <p>Could not load permission for transfer: <SenderAuthority> => <RecipientAuthority> " with type <Infref> for SendingIt-system: <SenderIt-system> => <RecipientIt-system></p> <p>Permission for transfer not allowed by any sending agreement</p> <p>Permission for transfer not allowed by any receiving agreement</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	RejectedInfrefRequiresRecipientItSystem	The RecipientIt-system field must be provided for the infref: <Infref>
62	RejectedInfrefRequiresNoRecipientItSystem	The RecipientIt-system field must not be provided for the infref: <Infref>
63	RejectedMultipleSFTPDynamicRoutingInfoFound	Multiple instances of SFTPDynamicRoutingInfo found. Only one is allowed.
64	RejectedInfrefCannotContainRouteSelectionValueDate	The RouteSelectionValueDate field must not be provided for the infref: <Infref>
65	RejectedUnableToParseParameter	Incorrect parameter in trigger file: <error details>

5.6.5 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://docs.kombit.dk/latest/0cfee71a>

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: 5.6.1. 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 5.6.1. Vil indeholde det samme som i det oprindelige triggerobjekt for filoverførslen.

Et eksempel på en metadatafil kan ses i afsnit 5.3.1.

5.6.6 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://docs.kombit.dk/latest/0cfee71a>

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>
```

5.7 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 5.6.1.

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.