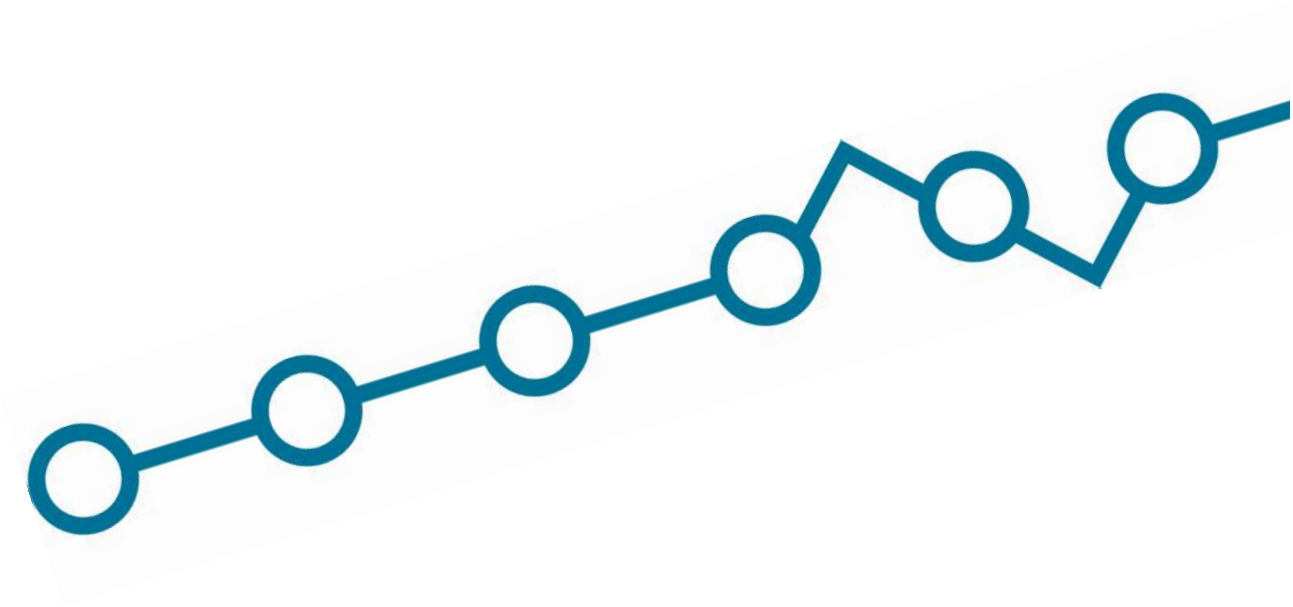
KOMBIT

Kommunernes it-fællesskab



Bilag 2.1.B Integrationer og snitflader

Samarbejdsplatformen

INSTRUKTION TIL TILBUDSGIVER

Nærværende bilag 2.1.B (Integrationer og snitflader) udgør et supplement til bilag 2 (Kravspecifikation). Bilaget indeholder dokumentation til snitflader, som Løsningen skal understøtte.

Tilbudsgiver skal ikke udfylde bilaget.

Tilbudsgivers eventuelle forbehold til bilag 2.1.B anføres i forbeholdslisten og skrives ind med track changes i selve bilaget i overensstemmelse med udbudsbetingelserne.

Det bemærkes, at Kontrakten (forstået som Kontrakten uden bilag) og Driftskontrakten (forstået som bilag 7.2, 7.3 og 7.4) er at betragte som minimumskrav, jf. udbudsbetingelserne. Tilbudsgiver skal derfor sikre, at eventuelle forbehold til bilag 2.1.B ikke udgør et forbehold overfor Kontrakten (forstået som Kontrakten uden bilag) og Driftskontrakten (forstået som bilag 7.2, 7.3 og 7.4).

Indholdsfortegnelse

1 Indledning

Nærværende bilag 2.1.B (Integrationer og snitflader) udgør et supplement til bilag 2 (Kravspecifikation). Bilaget indeholder dokumentation til snitflader, som Løsningen skal understøtte.

Bilaget indeholder tekniske beskrivelser af snitfladerne, der fungerer som kobling mellem bilag 2 (Kravspecifikation) og snitfladerne listet i afsnit 2.

1.1 Særligt om volumenangivelser

KOMBIT gør opmærksom på at de angivne volumenestimater i afsnit ”Volumen” er baseret på forventet brugsmønstre og derfor forbundet med en vis usikkerhed. Estimaterne skal forstås som en hjælp til Leverandøren, og KOMBIT kan ikke holdes ansvarlig, såfremt det faktiske brugsmønster viser sig anderledes.

2 Snitflade beskrivelser

ws15/wsaGRUPPE – Administration af projektgrupper (SAPL-01)

2.1.1 Snitfladens formål

I Løsningen er der behov for at der kan dannes Grupper som Brugere kan tilknyttes jf. afsnit 5.2.2.4 i bilag 2.1 Kravspecifikation. I UNI-Login understøttes det at Brugere kan være tilknyttet
2.1 Grupper, Grupperne indeholder en række stamdata, bl.a. et id, et navn og en type (se oversigt over stamdata i *Webservice beskrivelse af UNI-Login ifbm. BPI-bilag 2*). Disse Grupper kan dannes ad hoc i Løsningen og eksporteres til UNI-Login vha. ws15, på denne måde kan Grupper oprettet i Løsningen også benyttes af andre udbydere. Hvilke Brugere der er tilknyttet Grupperne gøres synligt for andre udbydere vha. ws16 (se afsnit 2.2).

2.1.2 Kilde- og Modtagersystem

Kildesystem: Løsningen

Modtagersystem: UNI-Login

2.1.3 Dataspecifikation

Det forventes at Løsningen skal eksportere samtlige informationer omkring Grupper fra snitfladen.

2.1.3.1 *Metoder* [1]

Metodenavn	Returnerer	Beskrivelse
opretProjektgruppe (wsBrugerid, wsPassword, ejernr, projektgruppekode, projektgruppenavn, fradato, tildato)	Svar	Opretter en projektgruppe. Projektgruppen skal være entydig for udbyderen
hentProjektgrupper (wsBrugerid, wsPassword, ejernr)	[Projektgruppe]	Returner liste over udbyderens projektgrupper
retProjektgruppe (wsBrugerid, wsPassword, ejernr, projektgruppekode, projektgruppenavn?, fradato?, tildato?)	Svar	Retter en eller flere attributter for en projektgruppe.
sletProjektgruppe (wsBrugerid, wsPassword, ejernr, projektgruppekode)	Svar	Sletter en projektgruppe. Fejler, hvis der er brugere tilknyttet projektgruppen.

[1] BPI - Snitfladebeskrivelser for UNI•Login til BPI: http://www.stil.dk/Projekter-og-initiativer/Brugerportal

foejBrugerTilProjektgruppe (wsBrugerid, wsPassword, ejernr, projektgruppekode, brugerid)	Svar	Tilføjer brugeren som medlem af projektgruppen. Brugeren arver dermed licens til de tjenester, som projektgruppen er tildelt.
fjernBrugerFraProjektgruppe (wsBrugerid, wsPassword, ejernr, projektgruppekode, brugerid)	Svar	Fjerner brugeren som medlem af projektgruppen. Brugeren mister dermed licens til de tjenester, som projektgruppen er tildelt.
hentBrugereIProjektgruppe (wsBrugerid, wsPassword, ejernr, projektgruppekode)	[Bruger]	Returnerer en liste af brugere, der er medlem ad den angivne projektgruppe.

2.1.4 Sikkerhed

Der henvises til afsnit 3 Sikkerhed.

2.1.5 Fejlhåndtering

Se Afsnit 4.1 Webservices (anvendes af Løsningen)

2.1.6 Volumen

Volumen på denne Snitflade er under afklaring

2.1.7 Dokumentation

Snitfladen ws15: UNI-Login

- UNI-Login dokumentation og begreber: http://www.stil.dk/It-og-administration/Brugere-og-adgangsstyring/Udbyder-UNILogin/Dokumentation
- Webservice beskrivelse af UNI-Login ifbm. BPI : http://www.stil.dk/Projekter-og-initiativer/Brugerportal

ws16/wsiUDBYDER - Information om projektgrupper, deres medlemmer og licenser (SAPL-02)

2.2.1 Snitfladens formål

Snitfladen er en udbyderrettet service der gør det muligt for udbydersystemer at se, hvilke Grupper og gruppemedlemmer end anden udbyder har. Løsningens informationer vedr. Grupper Eksporteres til UNI-Login via ws15 jf. afsnit 2.1.

2.2

WS16 er dermed relevant for både Løsningen og andre udbydere, da de via denne og efter aftale med hinanden kan hente informationer vedr. Grupper.

2.2.2 Kilde- og Modtagersystem

Kildesystem: STIL, via UNI-Login

Modtagersystem: Løsningen

2.2.3 Dataspecifikation

Det forventes at Løsningen skal hente samtlige informationer omkring Grupper fra snitfladen. De enkelte attributters navne i UNI-Logins outputstruktur matches med attributtens navn i Løsningens informationsmodel.

Metoder [2]

2.2.3.1

Metodenavn	Returnerer	Beskrivelse
hentProjektgrupper (wsBrugerid, wsPassword, ejernr)	[Projektgruppe]	Returnerer liste over udbyderens projektgrupper.
hentBrugereIProjektgruppe (wsBrugerid, wsPassword, ejernr, projektgruppekode)	[Bruger]	Returnerer en liste af brugere, der er medlem af den angivne projektgruppe. Brugertypen for brugeren fremgår.
hentProjektgruppersLicenser (wsBrugerid, wsPassword, ejernr)	[ProjektgruppeLicens]	Returnerer liste over de tjenester udbyderen har licens til, med angivelse af, hvilken projektgruppe licensen er givet til

2.2.4 Integrationsmønster

Snitflade	Teknologi	Synkron/asynkron

[2] BPI - Snitfladebeskrivelser for UNI•Login til BPI: http://www.stil.dk/Projekter-og-initiativer/Brugerportal

ws16/wsiUDBYDER	Webbaseret - http(s) og XML?	

2.2.5 Sikkerhed

Der henvises til afsnit 3 Sikkerhed.

2.2.6 Fejlhåndtering

Se Afsnit 4.1 Webservices (anvendes af Løsningen)

2.2.7 Volumen

Volumen på denne Snitflade er under afklaring

2.2.8 Dokumentation

Snitfladen ws16: UNI-Login

- UNI-Login dokumentation og begreber: http://www.stil.dk/It-og-administration/Brugere-og-adgangsstyring/Udbyder-UNILogin/Dokumentation
- Webservice beskrivelse af UNI-Login ifm. BPI: http://www.stil.dk/Projekter-og-initiativer/Brugerportal

2.3 ws17/wsiEKSPORT - Eksport af grupper, medlemmer og kontaktpersoner (SAPL-03)

2.3.1 Snitfladens formål

I Løsningen er der behov for at kende Brugernes Stamdata som er tilgængelig i UNI-Login, bl.a. hvilken Institution brugerne er tilknyttet, navn, id mm. Dette data er i dag tilgængelig fra UNI-Login webservicen ws17, som anvendes til at lave XML-udtræk af UNI-Login data. Løsningen har behov for at importere disse data og gøre relevante interessenter opmærksomme på, når der sker ændringer af Brugernes data, f.eks hvis et Barn skifter institution (se oversigt over Stamdata i *Webservice beskrivelse af UNI-Login ifm. BPI-bilag 2*).

UNI-Login modtager Brugernes Stamdata via ws10 i et XML-skema og data gøres tilgængelig i samme format via ws17. Løsningen har behov for jævnligt at importere disse data. Behovet for at importere jævnligt skyldes at Løsningen har behov for at registrere brugerændringer indenfor rimelig tid. Det kan f. eks. være hvis et Barn skifter institution, adresse el. lign. Webservicen tilbyder flere metoder til opslag, hvilket skal afdækkes og beskrives i afklaringsfasen.

2.3.2 Kilde- og Modtagersystem

Kildesystem: STIL, via UNI-Login

Modtagersystem: Løsningen

2.3.3 Dataspecifikation

Det forventes at Løsningen skal hente samtlige informationer vedr. Brugerne fra snitfladen. De enkelte attributters navne i UNI-Logins outputstruktur, matches med attributtens navn i Løsningens informationsmodel jf. bilag 2.1.A Begrebs- og Informationsmodel.

Metoder [3]

Metodenavn	Returnerer	Beskrivelse
eksporterXml (wsBrugerid, wsPassword, instnr)	XMLinst	Returnerer et XML dokument med data på tværs af institutionens importer
hentXmlSkema ()	XMLskema	Returnerer XML Schema for den aktuelle ws17-version.

2.3.3.1

2.3.4 Integrationsmønster

Snitflade	Teknologi	Synkron/asynkron
ws17/wsiEKSPORT	Webbaseret - http(s) og XML?	

2.3.5 Sikkerhed

Der henvises til afsnit 3 Sikkerhed.

2.3.6 Fejlhåndtering

Se Afsnit 4.1Webservices (anvendes af Løsningen)

2.3.7 Volumen

Volumen på denne Snitflade er under afklaring

2.3.8 Dokumentation

Snitfladen ws17: UNI-Login

- UNI-Login dokumentation og begreber: http://www.stil.dk/It-og-administration/Brugere-og-adgangsstyring/Udbyder-UNILogin/Dokumentation
- Webservice beskrivelse af UNI-Login ifbm. BPI: http://www.stil.dk/Projekter-og-initiativer/Brugerportal
- WSDL : https://ws17.infotjeneste.uni-c.dk/v1/?WSDL

[3] BPI - Snitfladebeskrivelser for UNI•Login til BPI: http://www.stil.dk/Projekter-og-initiativer/Brugerportal

Udveksling af skemaoplysninger og blokeret tid (SAPL-04)

2.4.1 Snitfladens formål

Institutionens skemaplanlægningssystem skal afsende skoleskemaer til Løsningen, som herefter anvender Skema i Kalendermodulet. Hver gang et Skema opdateres i Skemaplanlægningssystemet skal det igen sendes til Løsningen.

2.4

Fra Løsningen skal der afsendes information til Skemaplanlægningssystemet om tidsrum hvori det ikke kan skemalægge bestemte personer eller ressourcer (f. eks. hvis en Pædagogisk Personale har planlagt Skolehjem-samtaler, må et revideret Skema ikke kompromittere denne). Afsendelse af data fra Løsningen til skemalægningssystemerne eksisterer ikke i dag, men skal afdækkes i det videre arbejde.

Nedenstående beskrivelser er baseret på IST Tabulex, og vil blive uddybet med samme oplysninger for KMD Educa.

2.4.2 Kilde- og Modtagersystem

Kilde: Skemaplanlægningssystem (IST Tabulex eller KMD Educa)

Modtagersystem: Løsningen

2.4.3 Dataspecifikation

Følgende data modtages fra IST Tabulex omkring skema:

Felt	Navn	Maxtegn	Beskrivelse
1	Lærer	10	Lærer initialer
2	Hold	10	Holdbetegnelse
3	Klasse/klasser	50	Klasse eller klasser. Flere klasser deles med komma - og hver enkelt klassebetegnelse må max. være 10 tegn. Ex. 4A,4B,4C
4	Kort fag	10	Fagets korte betegnelse. Max. 10 tegn - bedst med 3 tegn.
5	Langt fag	50	En lang betegnelse for faget
6	Lokale/Lokaler	50	Lokalebetegnelse. Flere lokaler adskilles med komma. Hver lokalebetegnelse kan max. Være 10 tegn. Ex. MUS,HÅN,SLØ
7	Dag	1	Mandag = 1, tirsdag =2 osv.
8	Lektion	2	Lektionsnummer mellem 1 og 16
9	Startdato	8	Startdato for undervisningens begyndelse på formatet ååååmmdd.

10	Slutdato	8	Slutdato for undervisningens begyndelse på formatet ååååmmdd.

Ovenstående repræsenterer de data der i dag overføres, men listen vil eventuelt blive udvidet med flere data.

2.4.4 Integrationsmønster

Overførsel af skemadata sker ved Webservice kald, som en institution kan opsætte efter behov. Nogle institutioner kører med faste skemaer der kun sjældent opdateres, mens andre har behov for at overføre flere gange dagligt, eksempelvis såfremt vikardækning administreres i det brugeradministrative system hos IST.

2.4.5 Dokumentation

Se bilag 2.1.B.1 for IST dokumentation af Webservice.

2.5 Overførsel af profilbilleder (SAPL-05)

2.5.1 Snitfladens formål

De administrative systemer indeholder billeder af Elever og Medarbejdere, som kan overføres. I WS17/wsiEKSPORT overføres et felt med et ID til den pågældende brugers profilbillede. Ved at kalde det administrative system med dette ID, modtages selve billedfilen.

Nedenstående beskrivelser er baseret på IST Tabulex, og vil blive uddybet med samme oplysninger for KMD Educa.

2.5.2 Kilde- og Modtagersystem

Kildesystem: Kommunens administrative system

Modtagersystem: Løsningen

2.5.3 Dataspecifikation

Løsningen modtager Billeder med FotoID.

2.5.4 Integrationsmønster

Institutionen kalder det Brugeradministrative System, som leverer en liste med billeder der er ændret siden Institutionen sidst kaldte Webservicen.

2.5.5 Sikkerhed

Der henvises til afsnit 3 Sikkerhed.

Overførsel af data til LIS-systemer (SAPL-06)

Det er under afdækning hvilke informationer som det giver værdi at overføre fra Løsningen til Ledelsesinformationssystemer, det forventes bl.a. at være informationer omkring Børn og Elevers komme/gå tider. Yderligere områder afdækkes under Afklaringsfasen. Nedenstående skal derfor ses som et indledende udkast.

2.6 Udvikling af denne snitflade tager udgangspunkt den eksisterende snitflade SF1630 – Ledelsesinformation – Dataload, som forventes genbrugt i denne Løsning. Snitfladen vedlægges det endelige udbud

2.6.1 Snitfladens formål

Formålet med snitfladen er at kunne levere et dataudtræk til Serviceplatformen, så kommunerne kan udarbejde detaljeret ledelsesinformation på Skole og Dagtilbuds området. Løsningen skal således stille data til rådighed for den kommunale eller fælleskommunale ledelsesopfølgning gennem kommunens eget ledelsesinformationssystem (LIS) eller gennem det fælleskommunale ledelsesinformationssystem (FLIS).

Det konkrete dataudtræk kan være afgrænset tidsmæssigt og vil bestå af udvalgte entiteter fra Løsningens datamodel.

2.6.2 Kilde- og Modtagersystem

Kildesystem: Løsningen

Modtagersystem: Serviceplatformen som udstiller dataudtræk til kommunernes egne ledelsesinformationssystemer (LIS) samt det fælleskommunale ledelsesinformationssystem (FLIS).

Snitfladen gøres tilgængelige på Serviceplatformen af KOMBIT

2.6.3 Dataspecifikation

Der sendes et samlet dataudtræk baseret på Løsningens datamodel. Data der modtages af henholdsvis LIS og FLIS må ikke være personhenførbare (jf. CPR-nummer).

2.6.4 Integrationsmønster

Snitflade	**Teknologi**	**Synkron/asynkron**
SF 1630 Ledelsesinformation Dataload	SFTP	Asynkron

Løsningen skal levere et dataudtræk via sFTP-protokollen. Det vil være muligt at levere et dataudtræk til Serviceplatformens sFTP server (jf. *push*), hvilket kræver de fornødne rettigheder til efterfølgende at hente data (jf. *pull*). LIS og FLIS får adgang til Serviceplatformen via administrationsmodulet.

Det er Løsningens opgave at generere det korrekte dataudtræk til de forskellige modtagersystemer. Den konkrete fil overføres til et midlertidigt og unikt filnavn med endelsen ”tmp”; og omdøbes derefter til det endelige filnavn, når overførslen er slut.

2.6.5 Udvekslingsformat

Snitflade	Format	Bemærkninger
SF 1630 Ledelsesinformation Dataload	JSON, XML eller CSV	

Dataformatet *kan* være struktureret som enten JSON, XML (jf. OIO standarden) eller CSV i forlængelse af Løsningens datamodel.

2.6.6 Quality of Service

QoS ved upload af dataudtræk til sFTP Server er Exactly-Once.

2.6.7 Service invokation / Triggers

Løsningen leverer et tidsstyret dagligt dataudtræk.

2.6.8 Sikkerhed

Der henvises til afsnit 4 Sikkerhed.

2.6.9 Fejlhåndtering

Se afsnit 4 FTP (Løsningen pusher/uploader til SFTP server).

2.6.10 Volumen

Data vil blive uploadet udenfor normal arbejdstid.

2.6.11 Dokumentation

2.7

- Snitfladen SF-1630: FLIS/LIS – dataload
  - Batch eksport af sager - dette designes i forbindelse med udvikling af Løsningen

NemSMS (SAPL-07)

NemSMS anvendes til at sende SMS til de brugere som har valgt at få Notifikationer via SMS. Digitaliseringsstyrelsens NemSMS-løsning anvendes af Løsningen. Snitfladebeskrivelsen fra Digitaliseringsstyrelsen for NemSMS findes her: http://www.digst.dk/Loesninger-og-infrastruktur/Digital-Post/Vejledninger-Digital-Post/Om-digital-post-og-NemSMS

NemSMS løsningen anvendes også af andre af KOMBITs løsninger, f.eks. NemRefusion, det skal afdækkes om Snitfladen herfra evt. kan genbruges

2.7.1 Snitfladens formål

Formålet med snitflader er at give Løsningen mulighed for at sende SMS til de brugere som ønsker at modtage Nortifikationer på SMS.

2.7.2 Kilde- og Modtagersystem

Kildesystem: Løsningen

Modtagersystem: NemSMS

Data til hjemmeside (SAPL-08)

2.8 Skolerne og kommunerne er pligtige til at sikre at visse informationer udstilles på hver enkelt skoles hjemmeside. Nogle af disse informationer skal bl.a. hentes i nogle af STIL's databaser, f.eks. karaktergennemsnit for den enkelte skole.

Det er under afdækning, hvilke af disse informationer der skal stilles til rådighed for skolerne og kommunerne via Snitfladeintegrationer og hvilke informationer der skal stilles til rådighed for hjemmesiderne via widgets.

2.8.1 Snitfladens formål

Formålet med Snitfladen er at hjælpe skolerne og kommunerne med at løfte deres ansvar for udstilling af informationer som beskrevet i Loven om gennemsigtighed og åbenhed i uddannelserne.

2.8.2 Kilde- og Modtagersystem

Kildesystem: STIL's databaser

Modtagersystem: Løsningen

3 Sikkerhed i Integrationer

3.1 *Dette afsnit indeholder standard krav fra KOMBIT, og skal tilpasses når den overordnede sikkerhedsløsning er på plads.*

Indledning

Dette afsnit indeholder en fælles beskrivelse de sikkerhedsmodeller, der skal anvendes ved realisering af integrationer og hændelseskommunikation i nærværende bilag.

Den generelle model for servicegrænseflader er: "anvendersystem kalder service via snitfladen". Således anvendes følgende begreber:

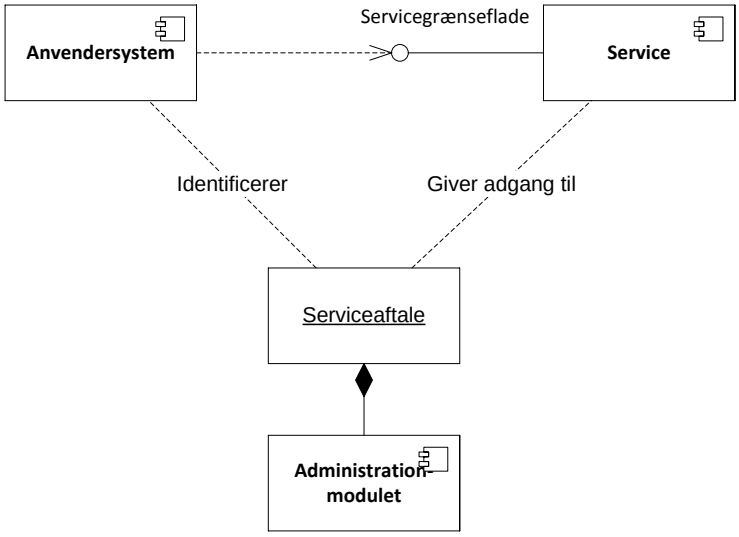
- en serviceudbyder er et it-system, der udstiller en service, som har en (eller flere) snitflade(r), og
- et anvendersystem er et it-system, der kalder snitflade.

Mange it-systemer vil således både optræde som anvendersystem og serviceudbyder, hvis de både udstiller services og anvender andre services.

Nedenstående Figur 1 illustrer den generelle model gældende for de enkelte sikkerhedsmodellerne, der er beskrevet i dette afsnit. Administrationen af hvilke anvendersystemer, der har adgang til hvilke snitflader foregår via de fælleskommunale støttesystemers Administrationsmodul. Anvendersystemer og services oprettes i Administrationsmodulet og adgang til en snitflade gives ved at indgå en serviceaftale.

Når anvendersystemet ønsker at tilgå en snitflade oprettes en sikker forbindelse med servicen og al kommunikation foregår via denne forbindelse. Det er efterfølgende servicens ansvar at håndhæve, at anvendersystemer kun får den adgang til funktionalitet og data hos servicen, som anvendersystemet er tildelt via serviceaftalen.

Løsningen skal understøtte, at Løsningen i en periode selv håndterer og administrerer OCES-certifikater, som er nødvendige for snitfladernes funktion.



3.2

Figur 1 Oversigt over den generelle sikkerhedsmodel for snitflader

Sikkerhedsmodeller

Ved servicekald i mellem systemer i den fælleskommunale rammearkitektur opereres der med tre forskellige typer af adgangsstyring, der tilgodeser forskellige behov. Adgangstyperne giver forskellige muligheder for detaljeringsgraden af de adgangsrettigheder, der kan håndhæves, når servicen kaldes, og understøttes på forskellig vis rent teknisk.

- **Simpel service:** Certifikatbaseret. Enten har anvendersystemet adgang til hele servicen eller også har det ikke adgang.
- **Simpel fælleskommunal service:** Certifikatbaseret. Et anvendersystem tilgår altid servicen på vegne af en given myndighed. Anvendersystemet har enten adgang til hele servicen (for den specifikke myndighed) eller også har det ikke adgang.
- **Fælleskommunal service:** Tokenbaseret. Et anvendersystem tilgår altid servicen på vegne af en given myndighed. Endvidere begrænses anvendersystemets brug af servicen ud fra systemroller, der tildeles anvendersystemet.

Oversigt over modeller for sikring af services

Nedenstående lister de sikkerhedsmodeller, der er understøttet i den fælleskommunale rammearkitektur, og er beskrevet ud fra varianter af adgangstyper og protokoller.

For at overholde den fælleskommunale rammearkitektur skal enhver service, der udstilles af en serviceudbyder indpasses til én af disse sikkerhedsmodeller.

3.3

Adgangstype	Protokol	Sikkerhedsmodeller, der understøttes i rammarkitekturen
Simpel service	Webservices	Se afsnit 3.5.1
	Filtransport	Se afsnit 3.5.2
	Andre protokoller	Se afsnit 3.5.3
Simpel fælleskommunal service	Webservices	Se afsnit 3.6.1
Fælleskommunal service	Webservices	Se afsnit 3.7.1
	Andre protokoller	Se afsnit 3.7.2
Simple callback services	Webservices	Se afsnit 3.8.1
	Andre protokoller	Se afsnit 3.8.2

Tabel 1 Sikkerhedsmodeller i r Rammearkitekturen

3.4

Gennemgang af sikkerhedsmodeller

I det afsnit gennemgås de enkelte snitflader. Der refereres i øvrigt til generelle vilkår i, ”bilag 2 (Sikkerhed), vers. 1.3 af 18. marts 2014” på https://share-komm.kombit.dk/P024/Delte%20dokumenter/Forms/Integrationsvilkr.aspx.

3.5

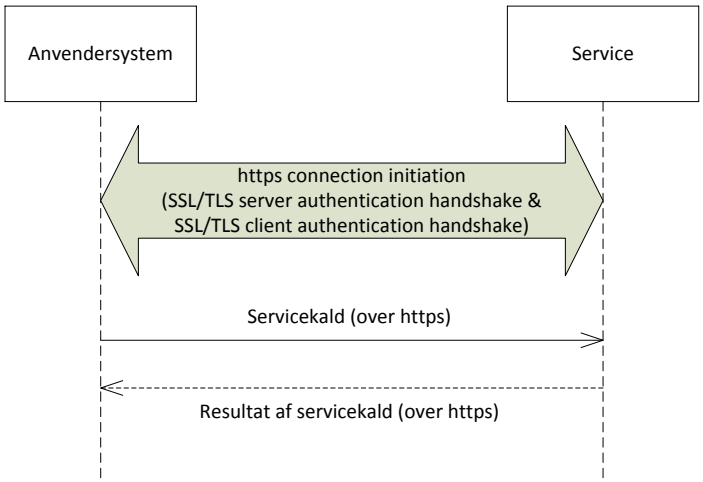
Det er serviceudbyder, som fastlægger sikkerhedsmodellen.

Simpel services

Adgangskontrollen for simple services karakteriseres ved, at der enten er adgang til servicen eller ej. Det vil sige, at der ikke granuleres yderligere i adgangskontrollen i forhold den funktionalitet og de data, der gives adgang til.

3.5.1 Simpel webservice

Adgangstype	Simpel service
Protokol	Webservice eller lignende over HTTPS
Adgangsstyring	Simpel. Enten er der adgang til alle operationer og data udstillet via servicen eller også er der slet ikke afgang.
Beskrivelse	

	Anvendersystemet kalder en webservice via HTTPS med client authentication via et klientcertifikat. Således foregår al kommunikation over en beskyttet SSL/TLS-forbindelse. 
Autentifikation af service	
	Anvendersystemet autentificerer servicen via et SSL/TLS-host/domæne certifikat. Anvendersystemet skal ved oprettelse af HTTPS-forbindelsen verificere at host/domænenavnet i serverudbyderens certifikatbesked er det samme som host/domænenavnet har brugt i servicekaldet (som det er standard for HTTPS).
Autentifikation af anvendersystem	
	Servicen autentificerer anvendersystemet via et SSL/TLS-klientcertifikat. Certifikatet er et OCES funktions- eller virksomhedscertifikat.
Fortrolighed og integritet	
	Beskyttet af SSL/TLS-forbindelsen. Servicen skal alene tilbyde SSL/TLS Cipher Suites, der understøtter stærk kryptering jævnfør retningslinjer fra Datatilsynet og NIST.

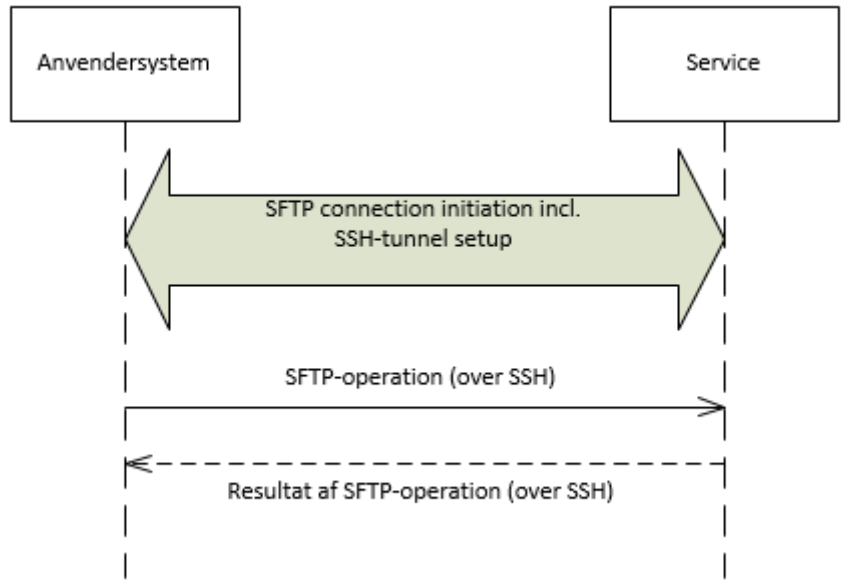
Tabel 3 Simpel webservice

3.5.2 Simpel filtransport service

Denne sikkerhedsmodel understøttes kun via Serviceplatformen. Her optræder Serviceplatformen altid som serviceudbyder, der tilbyder en SFTP-gateway service.

Adgangstype	Simpel service
Protokol	Filtransport over SFTP (SSH File Tranfer Protocol)[4]
Adgangsstyring	Hvert anvendersystem får begrænset adgang til relevante foldere, så det ikke uden videre kan læse eller overskrive andre anvendersystemers data.
Beskrivelse	
	Filtransport af store filer foregår via SFTP, hvor service og anvendersystem autentificeres på baggrund af SSH nøgler, der på forhånd er udvekslet. Således foregår al kommunikation over en beskyttet forbindelse.

[4] Denne skal ikke forveksles med Simple File Transport Protocol eller FTP over SSH.

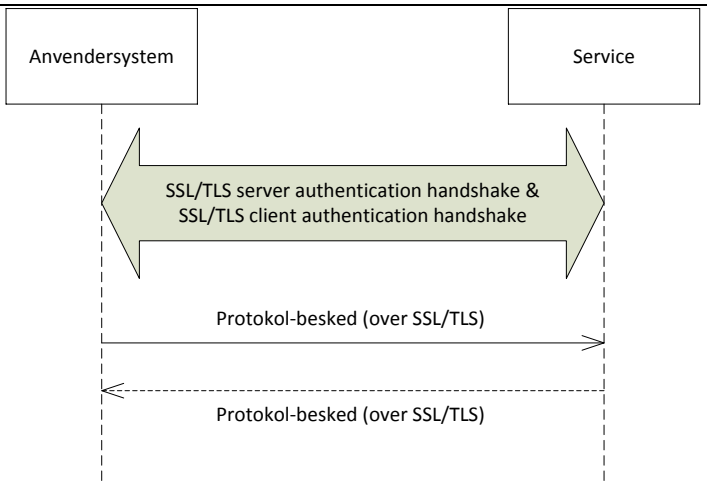


Autentifikation af service
Anvendersystemet (SFTP-klienten) autentificerer servicen (SFTP-serveren) ved brug servicens SSH nøgle, der på forhånd er udvekslet.
Autentifikation af anvendersystem
Servicen (SFTP-serveren) autentificerer anvendersystemet (SFTP-klienten) ved brug anvendersystemets SSH nøgle, der på forhånd er udvekslet.
Fortrolighed og integritet
Beskyttes via SSH-tunellen. Servicen skal alene tilbyde SSH Cipher Suites, der understøtter stærk kryptering jævnfør retningslinjer fra Datatilsynet og NIST.

Tabel 4 Simpel filtransport service

3.5.3 Anden simpel service

Adgangstype	Simpel service
Protokol	Der benyttes en protokol, som fungerer over internettet (dvs. kommunikation over TCP/IP eller UDP/IP). Der anvendes SSL/TLS med to-vejs-autentifikation til at beskytte kommunikationen.
Adgangsstyring	Simpel. Enten er der adgang til servicen ellers er der ikke.
Beskrivelse	
Der oprettes en SSL/TLS forbindelse og alle protokol-beskeder sendes over den.	



Autentifikation af service
Servicen autentificeres via sit SSL/TLS-servercertifikat, som er et OCES funktions- eller virksomhedscertifikat.
Autentifikation af anvendersystem
Anvendersystem autentificeres via sit SSL/TLS klientcertifikat, som er et OCES funktions- eller virksomhedscertifikat.
Fortrolighed og integritet
Beskyttes via SSL/TLS-forbindelsen. Servicen skal alene tilbyde SSL/TLS Cipher Suites, der understøtter stærk kryptering jævnfør retningslinjer fra Datatilsynet og NIST.

Tabel 5 Anden simpel service

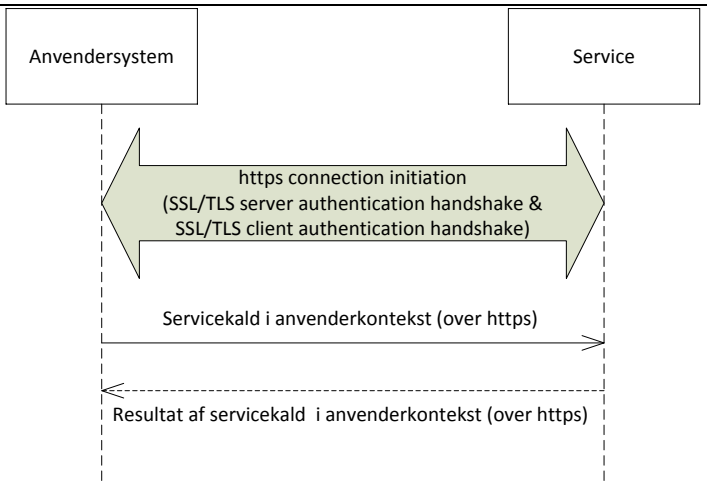
3.6

Simple fælleskommunale services

Simple fælleskommunale services karakteriseres ved, som for simple services, at der enten gives adgang til servicen eller ej. Dog afgrænses servicen til én specifik myndighed ved at der medsendes en anvenderkontekst.

3.6.1 Simpel fælleskommunal webservice

Adgangstype	Simpel fælleskommunal service
Protokol	Webservice eller lignende over HTTPS
Adgangsstyring	Simpel fælleskommunal. Adgang gives på vegne af specifik myndighed, men dataafgrænses ikke yderligere.
Beskrivelse	
Anvendersystemet kalder en webservice via HTTPS med client authentification via et klientcertifikat. Således foregår al kommunikation over en beskyttet SSL/TLS-forbindelse.	



Autentifikation af service
Anvendersystemet autentificerer servicen via et SSL/TLS-host/domæne certifikat. Anvendersystemet skal ved oprettelse af HTTPS-forbindelsen verificere at host/domænenavnet i serverudbyderens certifikatbesked er det samme som host/domænenavnet brugt i servicekaldet (som det er standard for HTTPS).
Autentifikation af anvendersystem
Service autentificerer anvendersystemet via et SSL/TLS klientcertifikat. Certifikatet er et OCES funktions- eller virksomhedscertifikat.
Fortrolighed og integritet
Foregår via SSL/TLS forbindelsen. Servicen skal alene tilbyde SSL/TLS Cipher Suites, der understøtter stærk kryptering jævnfør retningslinjer fra Datatilsynet og NIST.

Tabel 6 Simpel fælleskommunal webservice

3.7

Fælleskommunale services

Fælleskommunale services karakteriseres ved, at en service altid tilgås på vegne af en specifik myndighed. Endvidere begrænses anvendersystemet brug af servicen ud fra systemroller og tilhørende dataafgrænsninger.

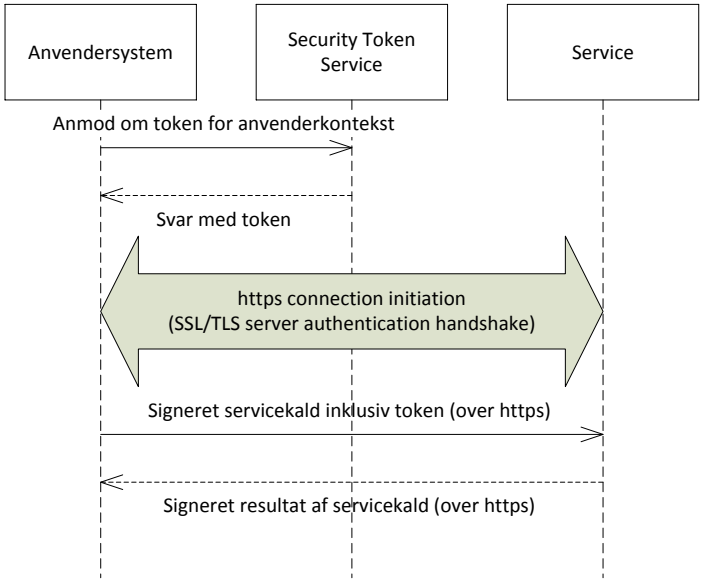
3.7.1 Fælleskommunal webservice

Adgangstype	Fælleskommunal service
Protokol	Webservice (fx SOAP eller REST) eller lignende over HTTPS
Adgangsstyring	Fælleskommunal. Adgang gives på vegne af en myndighed og specifikt tildelte rettigheder. Servicen håndhæver adgang på baggrund af de systemroller og tilhørende dataafgrænsninger, der er angivet i det medsendte security token.
Beskrivelse	
Anvendersystemet anmoder først Security Token Servicen om et security token på vegne af en given myndighed (en anvenderkontekst).	

Herefter kaldes servicens web service med det udstedte security token som parameter i kaldet.

Web service kaldet skal, for SOAP-baserede tjenester, ske i henhold til Liberty Basic SOAP Binding standarden [SOAP Binding], hvor servicekald og svar signeres, så de kan valideres i henhold til en nøgle, der er indeholdt i security tokenet. For REST-baserede og andre typer web services må hver service individuelt definere, hvorledes token og signatur indlejres i servicekaldet.

Begge kald sker over HTTPS med server autentifikation ud fra et SSL/TLS-host/domæne certifikat. (men uden brug af SSL/TLS klientcertifikat).



Autentifikation af service

Anvendersystemet autentificerer servicen via et SSL/TLS domæne certifikat.

Anvendersystemet skal ved oprettelse af HTTPS-forbindelsen verificere at host/domænenavnet i serverudbyderens certifikatbesked er det samme som host/domænenavnet brugt i servicekaldet (som det er standard for HTTPS).

Autentifikation af anvendersystem

Servicen autentificerer anvendersystemet dels via det modtagne security token, dels ved at tjekke at kaldet er signeret med et OCES certifikat, angivet i security tokenet (såkaldt holder-of-key). På den måde kan et security token kun præsenteres af det anvendersystem, der har den tilhørende private nøgle til OCES certifikatet.

Fortrolighed og integritet

Opnås via SSL/TLS forbindelsen. Servicen skal alene tilbyde SSL/TLS Cipher Suites, der understøtter stærk kryptering jævnfør retningslinjer fra Datatilsynet og NIST.

Tabel 7 Fælleskommunal webservice

3.7.2 Anden fælleskommunal service

Adgangstype	Fælleskommunal service
Protokol	Der benyttes en protokol, som fungerer på internettet (dvs. kommunikation over TCP/IP eller UDP/IP).

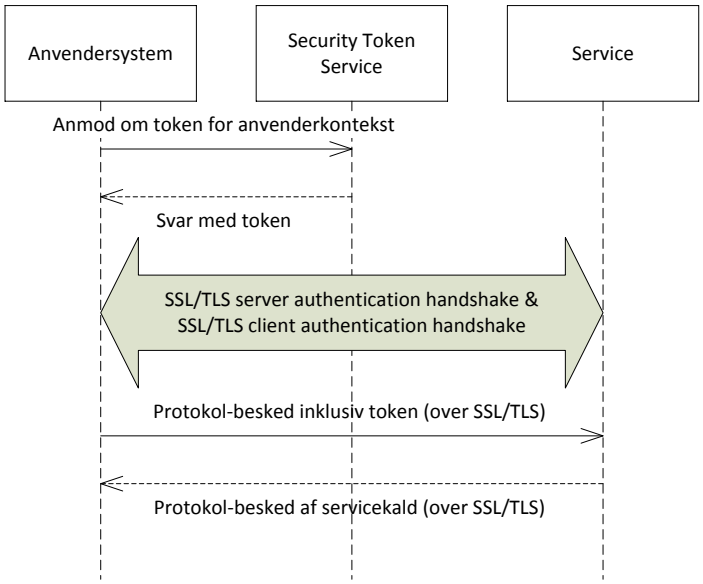
Adgangsstyring	Fælleskommunal. Adgang gives på vegne af en myndighed og specifikt tildelte rettigheder. Servicen håndhæver adgang på baggrund af de systemroller, der er angivet i det medsendte security token.

Beskrivelse

Anvendersystemet anmoder først Security Token Servicen i den fælleskommunale infrastruktur om et security token.

Herefter kaldes serviceudbyderens web service med det udstedte security token som parameter i kaldet.

Der anvendes SSL/TLS med to-vejs-autentifikation til at beskytte kommunikationen mellem anvendersystem og servicen.



Hver service må individuelt definere, hvorledes security tokens indlejres i servicekaldet.

Autentifikation af service

Servicen autentificeres via sit SSL/TLS server certifikat, som er et OCES funktions- eller virksomhedscertifikat.

Autentifikation af anvendersystem

Anvendersystem autentificeres via sit SSL/TLS klientcertifikat, som er et OCES funktions- eller virksomhedscertifikat.

3.8 **Fortrolighed og integritet**

Opnås via SSL/TLS forbindelsen. Servicen skal alene tilbyde SSL/TLS Cipher Suites, der understøtter stærk kryptering jævnfør retningslinjer fra Datatilsynet og NIST.

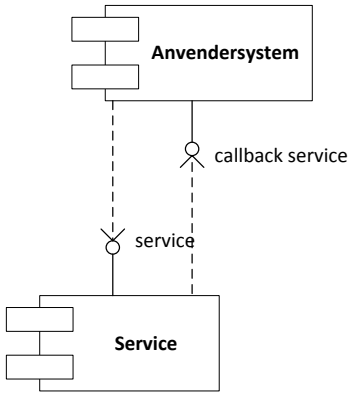
Simple callback services

Den sædvanlige model for services er, at en serviceudbyder udstiller en service, som et anvendersystem kan benytte. Modellen er endvidere udformet således, at det altid er servicen, der udstiller den servicegrænseflade, der skal kaldes for at anvende servicen. Der vil dog være scenarier, hvor servicekaldet teknisk set går den anden vej. Det kan eksempelvis være:

- Et push scenarie, hvor servicen udfører en handling, men ønsker at levere resultatet ved at kalde en grænseflade udstillet af anvendersystemet.
- Et polling scenarie, hvor servicen spørger anvendersystemet om det har nye data klar.

Det bemærkes, at det i disse scenarier stadig er serviceudbyderen, der udbyder en service, og at man derfor stadig ønsker anvendersystemet skal tildeles adgangsrettigheder til at gøre brug denne service. Det vil sige, at man når et anvendersystem vil indgå aftale med eksempelvis Beskedfordeler om at få leveret beskeder, så er det Anvendersystemet der initierer oprettelse af en serviceaftale med Beskedfordeler, og de enkelte Myndigheder der godkender, præcist som aftalemodellen for de øvrige service-typer.

For at håndtere scenarier, hvor kommunikationen rent teknisk går fra servicen til anvendersystemet introduceres begrebet callback service, der er en servicegrænseflade, der udstilles af anvendersystemet. Dette er illustreret på figuren nedenfor:



Figur 2 Komponenter og servicegrænseflader for callback service

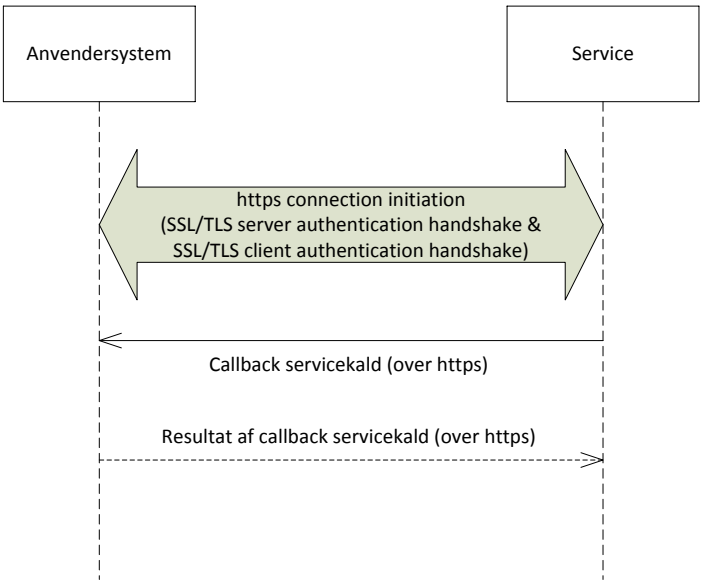
En callback service udstilles specifikt til brug for en given service, som serviceudbyderen tilbyder. En callback service vil således være en slags service, der altid anvendes i forbindelse med en anden service. Denne anden service vil skulle sikres ved brug af en af de sikkerhedsmodeller, der er beskrevet i afsnit 3.5 til 3.7 – dette gælder også i de scenarier hvor Anvendersystemet kalder en service, hvorefter servicen kalder tilbage via callback funktionaliteten.

Dette afsnit beskriver sikkerhedsmodellerne for hvordan selve callback servicen sikres.

3.8.1 Simpel callback-webservice

Denne sikkerhedsmodel for callback services svarer rent sikkerhedsmæssigt til, hvordan man sikrer en simpel webservice, som beskrevet i afsnit 3.5.1. Forskellen er dog den, at servicekaldet går den anden vej og, at adgang til callback servicen gives via den serviceaftale, der allerede indgås mellem anvendersystemet og servicen.

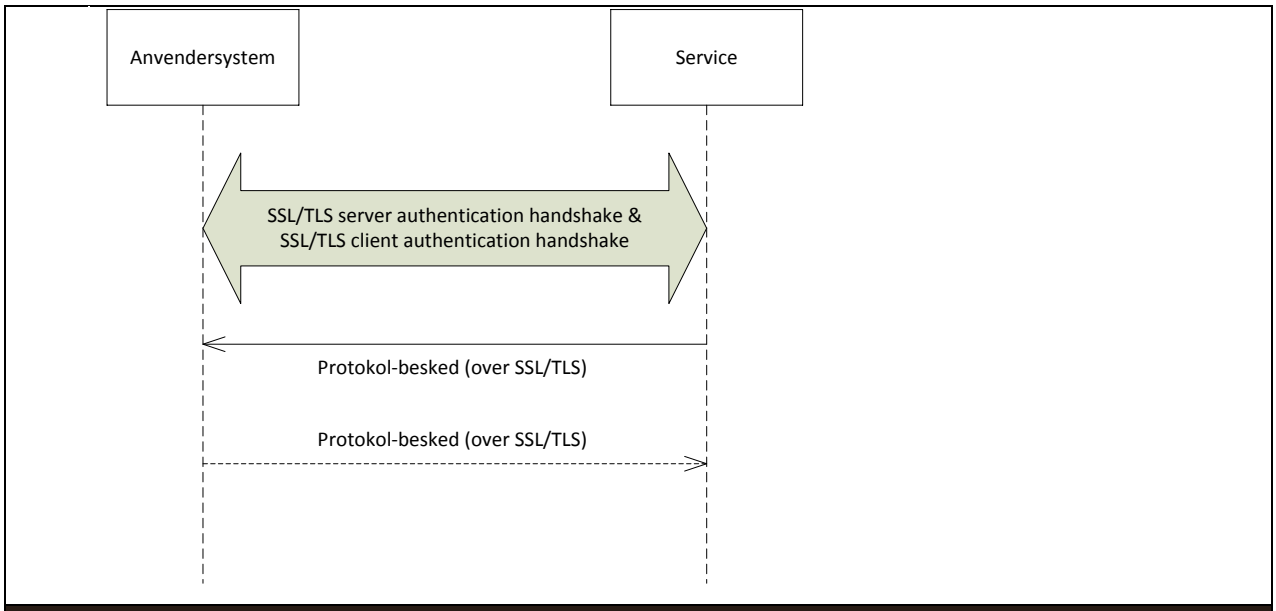
Adgangstype	Simpel callback service
Protokol	Webservice eller lignende over HTTPS
Adgangsstyring	Simpel. Enten er der adgang til callback-servicen ellers er der ikke.
Beskrivelse	

Servicen kalder en webservice via HTTPS med client authentication via et klientcertifikat. Således foregår al kommunikation over en beskyttet SSL/TLS-forbindelse. 
Autentifikation af service
Anvendersystemet autentificerer servicen via et SSL/TLS-klientcertifikat. Certifikatet er et OCES funktions- eller virksomhedscertifikat, der registres i Administrationsmodulet.
Autentifikation af anvendersystem
Servicen autentificerer anvendersystemet via et SSL/TLS-host/domæne certifikat. Servicen skal ved oprettelse af HTTPS-forbindelsen verificere at host/domænenavnet i anvendersystemets certifikat er det samme som host/domænenavnet har brugt i service-kaldet (som det er standard for HTTPS).
Fortrolighed og integritet
Beskyttet af SSL/TLS-forbindelsen. Anvendersystemet skal alene tilbyde SSL/TLS Cipher Suites, der understøtter stærk kryptering jævnfør retningslinjer fra Datatilsynet og NIST.

Tabel 9 Simpel callback-webservice

3.8.2 Anden simpel callback-service

Adgangstype	Simpel callback service
Protokol	Der benyttes en protokol, som fungerer over internettet (dvs. kommunikation over TCP/IP eller UDP/IP). Der anvendes SSL/TLS med to-vejs-autentifikation til at beskytte kommunikationen.
Adgangsstyring	Simpel. Enten er der adgang til callback-servicen ellers er der ikke.
Beskrivelse	
Der oprettes en SSL/TLS forbindelse og alle protokol-beskeder sendes over den.	



Autentifikation af service
Anvendersystemet autentificerer servicen via et SSL/TLS-klientcertifikat. Certifikatet er et OCES funktions- eller virksomhedscertifikat, der registres i Administrationsmodulet.
Autentifikation af anvendersystem
Servicen autentificerer anvendersystemet via et SSL/TLS-host/domæne certifikat. Servicen skal ved oprettelse af forbindelsen verificere at host/domænenavnet i anvendersystemets certifikat er det samme som host/domænenavnet har brugt i servicekaldet.
Fortrolighed og integritet
Beskyttes via SSL/TLS-forbindelsen. Servicen skal alene tilbyde SSL/TLS Cipher Suites, der understøtter stærk kryptering jævnfør retningslinjer fra Datatilsynet og NIST.

Tabel 10 Anden simpel callback-service

4 Fejltyper og håndteringer

Dette afsnit indeholder standard krav fra KOMBIT, og forventes tilpasset inden udbuddet udsendes.

Dette afsnit beskriver udvalgte teknisk relaterede fejlscenarier for integrationer, samt hvordan disse skal håndteres af Løsningen og/eller Leverandøren.

Generelt henvises til bilag 7 (Drift) samt bilag 2 (Kravspecifikation), Snitfladematrix, for retningslinjer for håndtering af integrationer.

Webservices (anvendes af Løsningen)

4.1

Navn:	**Kald (request) kan ikke valideres af modtager (XSD)**	**Fejltypekode:**	**WS-U-1**
Beskrivelse:	Løsningen kalder en WS, men WS'en returnerer fejl i valideringen af input parametre, ift. til fx XSD schema.		
Primær håndtering:	• Bruger notificeres på brugervenlig vis, med fejlkode, og • Bruger indmelder fejl til support, og • Fejlen logges (jf. underbilag 2.27).		
Alternativ håndtering:	• Driftovervågning behandler fejlen jf. procedure beskrevet i Driftskontrakten		
Bemærkning:	*Antager SOAP-baseret webservice*		

Navn:	**Svar (response) til løsning kan ikke valideres (XSD)**	**Fejltypekode:**	**WS-U-2**
Beskrivelse:	Løsningen kalder en WS, men WS'ens returnerede svar kan ikke valideres af Løsningen ift. fx XSD schema.		
Primær håndtering:	• Bruger notificeres på brugervenlig vis, med fejlkode, og • Bruger indmelder fejl til support, og • Fejlen logges (jf. underbilag 2.27).		
Alternativ håndtering:	• Driftovervågning behandler fejlen jf. procedure beskrevet i Driftskontrakten		
Bemærkning:	*Antager SOAP-baseret webservice*		

Navn:	**Serverfejl**	**Fejltypekode:**	**WS-U-3**

Beskrivelse:	Løsningen kalder en WS, men får returneret en serverfejl, fx HTTP-404
Primær håndtering:	• Bruger notificeres på brugervenlig vis, med fejlkode, og • Bruger indmelder fejl til support, og • Fejlen logges (jf. underbilag 2.27).
Alternativ håndtering:	• Driftovervågning behandler fejlen jf. procedure beskrevet i Driftskontrakten
Bemærkning:	

Navn:	**Connection/request timeout**	**Fejltypekode:**	**WS-U-4**
Beskrivelse:	Løsningen fejler i udveksling af webservice request og/eller response med en forbindelsestimeout.		

Primær håndtering:	• Løsningen implementerer max svartidsbegrænsning på et konfigurerbart antal sek., hvorefter request/response afbrydes af Løsningn, og
	• Løsningen forsøger kaldet igen et konfigurerbart antal gange
	• Såfremt gentagelsen også fejler:
	  ○ Bruger notificeres på brugervenlig vis, med fejlkode, og
	  ○ Bruger indmelder fejl til support, og
	  ○ Fejlen logges (jf. underbilag 2.27).		

Alternativ håndtering:	• Driftovervågning behandler fejlen jf. procedure beskrevet i Driftskontrakten		
Bemærkning:			

Navn:	**Sikkerhedsfejl (certifikat/token)**	**Fejltypekode:**	**WS-U-5**
Beskrivelse:	Løsningen kalder en WS, der afviser requestet med en sikkerhedsfejl relateret til det af Løsningen anvendte certifikat, sikkerheds-token, eller brugernavn/password.		
Primær håndtering:	• Bruger notificeres på brugervenlig vis, med fejlkode, og • Bruger indmelder fejl til support, og • Fejlen logges (jf. underbilag 2.27).		
Alternativ håndtering:	• Driftovervågning behandler fejlen jf. procedure beskrevet i Driftskontrakten		
Bemærkning:			

Navn:	Server ikke tilgængelig	Fejltypekode:	WS-U-6
Beskrivelse:	Løsningen forsøger at kalde en WS, der ikke er tilgængelig (endpoint kan ikke nås).		
Primær håndtering:	• Bruger notificeres på brugervenlig vis, med fejlkode, og • Bruger indmelder fejl til support, og • Fejlen logges (jf. underbilag 2.27).		
Alternativ håndtering:	• Driftovervågning behandler fejlen jf. procedure beskrevet i Driftskontrakten		
Bemærkning:			

Webservices (udstillet af Løsningen)

4.2

Navn:	Kald (request) kan ikke valideres af Løsningen (XSD)	Fejltypekode:	WS-I-1
Beskrivelse:	Løsningen modtager en request på en udstillet snitflade, hvor requestets input parametre ikke kan valideres ift. fx XSD schema.		
Primær håndtering:	• Løsningen returnerer en (SOAP) fejl til det kaldende system, og • Løsningen logger fejlen (jf. underbilag 2.27)		
Alternativ håndtering:	• Ingen		
Bemærkning:	*Antager SOAP-baseret webservice*		

Navn:	Svar (response) fra løsning kan ikke valideres (XSD)	Fejltypekode:	WS-I-2
Beskrivelse:	Det kaldende system kan ikke validere et svar (response) modtaget fra Løsningen ift. fx XSD schema.		
Primær håndtering:	• Afhængigt af kaldende systems fejlhåndteringsprocedurer. Fejlen meldes evt. til support (for Løsningen)		
Alternativ håndtering:	• Ingen		
Bemærkning:	*Antager SOAP-baseret webservice*		

Navn:	Sikkerhedsfejl (certifikat/token)	Fejltypekode:	WS-I-3

Beskrivelse:	Løsningen afviser et kald til en af Løsningens udstillede snitflader pga. af fejl i tjek af certifikat eller token anvendt i kaldet.
Primær håndtering:	• Afhængigt af kaldende systems fejlhåndteringsprocedurer. Fejlen meldes evt. til support (for Løsningen), og • Fejlen logges (jf. underbilag 2.27)
Alternativ håndtering:	• Driftovervågning behandler fejlen jf. procedure beskrevet i Driftskontrakten
Bemærkning:	

FTP (Løsningen pusher/uploader til SFTP server)

Navn:	**Server fejl**	**Fejltypekode:**	**FTP-U-1**
Beskrivelse:	Løsningen sender en fil til en SFTP server, men får returneret en serverfejl, fx '501 Syntax error in parameters or arguments.'		
Primær håndtering:	• Fejlen logges (jf. underbilag 2.27), og evt. • Administrator notificeres eksplicit.		
Alternativ håndtering:	• Driftovervågning behandler fejlen jf. procedure beskrevet i Driftskontrakten		
Bemærkning:	FTP (push/upload) integrationer er system-til-system, hvorfor der ikke er en bruger direkte involveret.		

4.3

Navn:	**Sikkerhedsfejl (certifikat/token)**	**Fejltypekode:**	**FTP-U-2**
Beskrivelse:	Løsningen vil sende en fil til en FTP, der afviser transaktionen med en sikkerhedsfejl i det af Løsningen anvendte certifikat, sikkerhedstoken, eller brugernavn/password.		
Primær håndtering:	• Fejlen logges (jf. underbilag 2.27), og evt. • Administrator notificeres eksplicit.		
Alternativ håndtering:	• Driftovervågning behandler fejlen jf. procedure beskrevet i Driftskontrakten		
Bemærkning:	FTP (push/upload) integrationer er system-til-system, hvorfor der ikke er en bruger direkte involveret.		

Navn:	**Server ikke tilgængelig**	**Fejltypekode:**	**FTP-U-3**

Beskrivelse:	Løsningen vil sende en fil til en FTP, men kan ikke etablere forbindelse til serveren.
Primær håndtering:	• Fejlen logges (jf. underbilag 2.27), og evt. at • Administrator notificeres eksplicit.
Alternativ håndtering:	• Driftovervågning behandler fejlen jf. procedure beskrevet i Driftskontrakten
Bemærkning:	FTP (push/upload) integrationer er system-til-system, hvorfor der ikke er en bruger direkte involveret.

Navn:	**Forbindelses-/overførselsfejl**	**Fejltypekode:**	**FTP-U-4**
Beskrivelse:	Løsningen vil sende en fil til en FTP, men der opstår en fejl under overførslen.		
Primær håndtering:	• Fejlen logges (jf. underbilag 2.27), og evt. at • Løsningen forsøger at gentage overførslen, og evt. at • Administrator notificeres eksplicit.		
Alternativ håndtering:	• Driftovervågning behandler fejlen jf. procedure beskrevet i Driftskontrakten		
Bemærkning:	FTP (push/upload) integrationer er system-til-system, hvorfor der ikke er en bruger direkte involveret.		

4.4

FTP (Løsningen puller/downloader fra FTP server)

Navn:	**Sikkerhedsfejl (certifikat/token)**	**Fejltypekode:**	**FTP-I-1**
Beskrivelse:	Løsningen vil hente en fil fra en FTP, der afviser transaktionen pga. en sikkerhedsfejl i det af Løsningen anvendte certifikat, sikkerhedstoken, eller brugernavn/password.		
Primær håndtering:	• Fejlen logges (jf. underbilag 2.27), og evt. at • Administrator notificeres eksplicit.		
Alternativ håndtering:	• Driftovervågning behandler fejlen jf. procedure beskrevet i Driftskontrakten		
Bemærkning:	FTP (pull/download) integrationer er system-til-system, hvorfor der ikke er en bruger direkte involveret.		

Navn:	Server ikke tilgængelig	Fejltypekode:	FTP-I-2
Beskrivelse:	Løsningen vil hente en fil fra en FTP, men kan ikke etablere forbindelse til serveren.		
Primær håndtering:	• Fejlen logges (jf. underbilag 2.27), og evt. at • Administrator notificeres eksplicit.		
Alternativ håndtering:	• Driftovervågning behandler fejlen jf. procedure beskrevet i Driftskontrakten		
Bemærkning:	FTP (pull/download) integrationer er system-til-system, hvorfor der ikke er en bruger direkte involveret.		

Navn:	Forbindelses-/overførselsfejl	Fejltypekode:	FTP-I-3
Beskrivelse:	Løsningen vil hente en fil fra en FTP, men der opstår en fejl under overførslen.		
Primær håndtering:	• Fejlen logges (jf. underbilag 2.27), og • Løsningen forsøger at gentage overførslen, og evt. at • Administrator notificeres eksplicit.		
Alternativ håndtering:	• Driftovervågning behandler fejlen jf. procedure beskrevet i Driftskontrakten		
Bemærkning:	FTP (pull/download) integrationer er system-til-system, hvorfor der ikke er en bruger direkte involveret.		

Navn:	Server fejl	Fejltypekode:	FTP-I-4
Beskrivelse:	Løsningen vil hente en fil fra en FTP, men får returneret en serverfejl, fx ’550 File not found.’		
Primær håndtering:	• Fejlen logges (jf. underbilag 2.27), og evt. at • Administrator notificeres eksplicit.		
Alternativ håndtering:	• Driftovervågning behandler fejlen jf. procedure beskrevet i Driftskontrakten		
Bemærkning:	FTP (push/upload) integrationer er system-til-system, hvorfor der ikke er en bruger direkte involveret.		