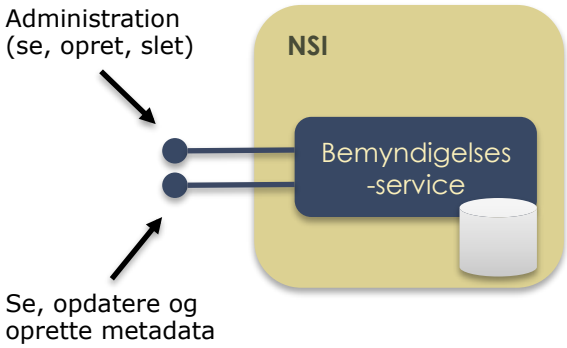
Fælles Bemyndigelsesservice - **Overordnet løsningsdesign** Dato: 13.02.2012 Version: 0.91 Udarbejdet af: NSI	National Sundheds-IT www.nsi.dk Islandsbrygge 39 2300 København S



Resumé

Nærværende notat beskriver det overordnede design af en fælles bemyndigelsesservice til brug for FMK og DDV og eventuelt andre nationale serviceudbydere. Formålet med servicen er at tilvejebringe teknisk understøttelse af delegerede rettigheder fra én sundhedsfaglig person til en anden. Ved at gøre dette i en fælles service opnås både simplere implementering i de services der arbejder med delegerede rettigheder, samt en fælles grænseflade for brugere, således at bemyndigelser kan registreres og administreres samme sted. Løsningen er fremkommet som et resultat af den organisatoriske sammenlægning af parterne bag hhv. FMK og DDV.

Version	Ansvarlig	Kommentar
0.9	CHE	Opdatering efter JRI og TSO review
0.91	CHE	Opdatering efter Trifork kommentarer.
0.92	CHE	Konsekvensrettelse som følge af ændring i placering af metadata

Indholdsfortegnelse

1 Indledning

FMK (Det Fælles Medicinkort) og DDV (Det Danske Vaccinationsregister) gør hver især brug af egenudviklede løsninger til håndtering af bemyndigelser imellem sundhedsfaglige personer. Da der er store fællestræk imellem løsningerne og de forretningsmæssige krav, er der både en driftsmæssig og en anvendelsesmæssig gevinst forbundet med anvendelse af en fælles løsning. I første omgang er bemyndigelsesservicen derfor en service, der opfylder konkrete og presserende behov for FMK og DDV i forhold til håndtering af bemyndigelser. Løsningen tager udgangspunkt i eksisterende funktionalitet i og forbedringsønsker for de to systemer.

Bemyndigelsesservicen registrerer uddelegerede rettigheder imellem personer til brug i it-systemer.

Behovet for it-understøttelse af bemyndigelse er ikke begrænset til FMK og DDV. Gevinsten forbundet med nærværende løsning kan derfor øges yderligere ved at etablere en fælles national bemyndigelsesservice, der kan anvendes af både FMK og DDV samt af andre services med behov for håndtering af digitale bemyndigelser indenfor sundheds-domænet nu og i fremtiden.

Bemyndigelsesservicen etableres derfor som en relativt generisk fælles service, der består af en database med registrerede bemyndigelser samt webservice snitflader, der giver mulighed for elektronisk administration af bemyndigelser, herunder oprettelse, nedlæggelse samt eventuel verificering af disse. Bemyndigelsesservicen udstiller derudover godkendte bemyndigelser på NSP som stamdata, således at services, der skal validere bemyndigelser, kan vælge at lave et internt replika af bemyndigelser for den pågældende service.[1]

Ved anvendelse af bemyndigelsesservicen opnås sikkerhed for, at bemyndigelser er udstedt af den bemyndigende part, idet godkendelsesproceduren for bemyndigelser forudsætter sikker autentifikation ved hjælp af OCES-certifikater.

Det er ikke muligt indenfor de givne økonomiske og tidsmæssige rammer at omlægge DDV og FMK til Sundhedsstyrelsens Elektroniske Brugerstyring (SEB), der i sin nuværende form ikke rummer bemyndigelsesbegrebet og derfor også skal udvides inden en migrering kan gennemføres. I designet af løsningen er der i videst muligt omfang taget højde for eventuel fremtidig understøttelse af bemyndigelser i SEB, hvor der pt. pågår tiltag omkring brugerstyring og arbejdsfunktioner.

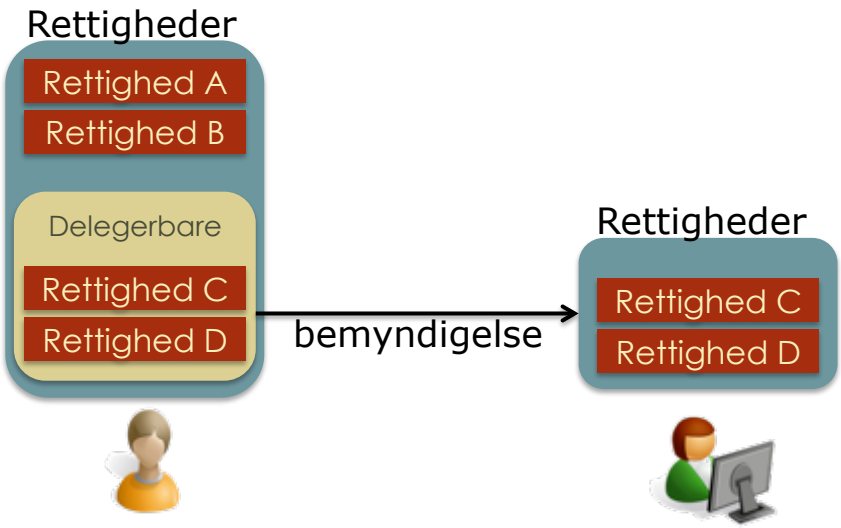
1.1 Formål og målgruppe

Notatet har til hensigt at give et overordnet billede af den konkrete løsningsarkitektur og design. Notatet indeholder relativt komplekse og tekniske elementer og henvender sig til læsere med erfaring inden for it-arkitektur og it-integration, f.eks. it-arkitekter, tekniske projektledere, systemdesignere, systemudviklere og driftsteknikere.

[1] Denne model anvendes i fase 1 og kan eventuelt suppleres med eller erstattes af en replikeringssnitflade udstillet af bemyndigelsesservicen.

1.2 Bemyndigelser og rettigheder

En bemyndigelse er i denne sammenhæng alene en delegering af (delegerbare) rettigheder i et it-system og er ikke begrænset til bemyndigelse imellem sundhedsfagligt personale, men kan også dække borger-til-borger fuldmagter. I praksis er en bemyndigelse derfor en fuldmagt til at udføre specifikke handlinger i et specifikt it-system på vegne af en anden, herunder at tilgå (og eventuelt videregive) potentielt personfølsomme informationer og oprette, slette og ændre oplysninger i it-systemer.



Figur 1 – Eksempel på en delegering af en rettighed i et it-system

En læge kan f.eks. bemyndige en medhjælp til at udføre visse arbejdsopgaver, som illustreret på Figur 1. En bemyndigelse giver dermed en bruger rettigheder til at udføre handlinger på vegne af den, der giver bemyndigelsen. Dette vil typisk være rettigheder brugeren normalt *ikke* har. Rettighederne er systemspecifikke, og skal fortsat valideres af det aktuelle system. Såfremt det ønskes, kan systemer, der anvender bemyndigelser som en del af rettighedstildelingen, åbne for at bemyndigelser kan begrænses til kun at omfatte et subsæt at de mulige delegerbare rettigheder.

På Figur 2 ses et eksempel på et sæt af systemspecifikke arbejdsfunktioner og tilhørende delegerbare rettigheder, som FMK har valgt at anvende. Arbejdsfunktionerne i eksemplet er specificeret med udgangspunkt i den bekendtgørelse, FMK arbejder under.

Bemærk at formålet med bemyndigelsesservicen alene er at registrere og formidle bemyndigelser til it-systemer. Bemyndigelser er ikke i sig selv adgangsgivende, men indgår i serviceudbyderens beslutningsgrundlag ved adgangskontrol og rettighedstildeling. Eventuelle forretningsregler og mapninger imellem systemspecifikke arbejdsfunktioner og delegerbare rettigheder er derfor fortsat er placeret hos den pågældende serviceudbyder. Da bemyndigelsesservicen kun registrerer og formidler bemyndigelser, er ansvaret for håndtering af følger ved ændringer i konfigurationen af et systems arbejdsfunktioner og delegerbare rettigheder placeret hos serviceudbyderen (f.eks. ved sletning af rettigheder, oprettelse af nye rettigheder eller opsplitning af en eksisterende rettighed i flere separate rettigheder).

Arbejdsfunktion	BorgerOpslag	SundhedsfagligOpslag	Recept	Lægemiddelordination	Effektuering	Privatmarkering	VisPrivatmarkeretVærdispring	VisPrivatmarkeretSamtykke	Suspendering	Afstemning	LøsRecept
Læge		x	x	x	x	x	x	x	x	x	x
Delegerbare rettigheder for læge		x		x	x	x	x	x	x	x	x
Tandlæge		x	x	x	x	x	x	x	x	x	x
Delegerbare rettigheder for tandlæge		x		x	x	x	x	x	x	x	x
Sygeplejerske		x			x		x	x	x		
Delegerbare rettigheder for sygeplejerske		x			x		x	x	x		

Figur 2 – Eksempel på rettigheder i et system [FMK-rettigheder], og en mapning mellem rettigheder og systemspecifikke arbejdsfunktioner.

Bemærk endvidere, at rettighederne for den bemyndigende person (de grønne rækker i tabellen) *ikke* indgår i metadata til bemyndigelsesservicen, men alene er inkluderet i eksemplet på Figur 2 for at illustrere, at der ikke nødvendigvis er sammenfald imellem en arbejdsfunktions rettigheder og de tilhørende delegerbare rettigheder (de røde rækker i tabellen).

1.3 Afgrænsninger

Bemyndigelsesservicen er en webservice, der registrerer bemyndigelser og giver mulighed for vedligehold af disse. Bemyndigelsesservicen

- er **ikke adgangsgivende i sig selv**, men bidrager alene med beslutningsgrundlag for adgang og rettighedstildeling for den bemyndigede person
- er **ikke et administrativt system med en visuel grænseflade**, men udstiller alene en webservice grænseflade til integration i klientsystemer og browserbaserede systemer

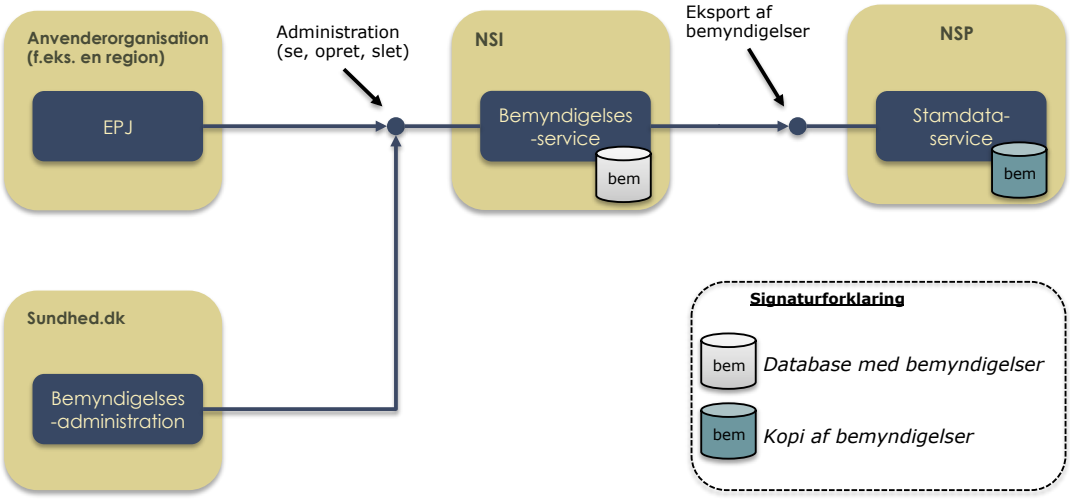
- er **ikke billetudstedende i første fase**, dvs. klientsystemer kan ikke erhverve signerede billetter til medsendelse ved forespørgsler til serviceudbydere (dette er en option der kan tilføjes)
- **tilbyder ikke mulighed for online verifikation** af bemyndigelser.
- **understøtter kun borger-til-borger bemyndigelser** hvis dette er implementeret i services og klienter

1.4 Forkortelser og definitioner

Term / Forkortelse	Definition
Bemyndigende person	Den person, der videregiver rettigheder til den bemyndigede.
Bemyndigede person	Den person, der får tildelt rettigheder af den bemyndigende.
System	System-attributen angiver i hvilket system, den pågældende bemyndigelse gælder.
Arbejdsfunktion	Den systemspecifikke arbejdsfunktion i hvilken den bemyndigende delegerer rettigheder. Begrebet gør det muligt for en person at delegere rettigheder i forskellige arbejdsfunktioner, f.eks. hvis den bemyndigende har flere autorisationer.
Delegerede rettigheder	En liste af systemspecifikke delegerede rettigheder.

2 Overordnet design

Bemyndigelsesservicen er en webservice baseret på de nationale retningslinjer for identitetsbaserede services, der tilbyder dels elektronisk registrering og administration af bemyndigelser, dels rekvirering af bemyndigelsesdata. Klientsystemer kan f.eks. være administrative systemer i en region eller lægepraksissystemer, der integrerer bemyndigelsesservicen, eller det kan være browserbaserede systemer, der tilbyder mulighed for administration af bemyndigelser uafhængigt af lokale fagsystemer, f.eks. som en udvidelse af Sundhed.dk. Bemyndigelsesservicens administrationssnitflade er illustreret på Figur 3.

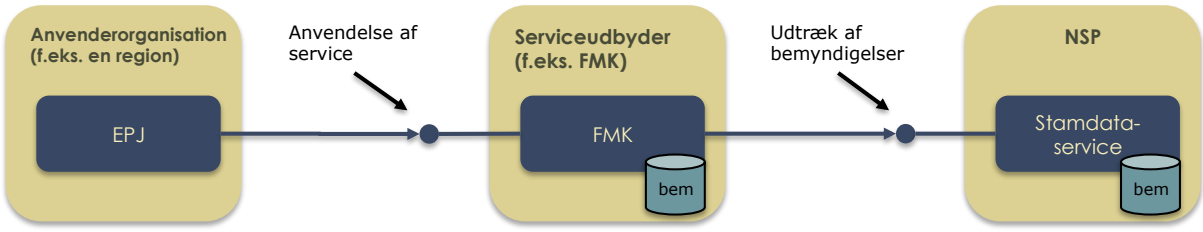


Figur 3 – Skitse med administrationssnitfladen til bemyndigelsesservicen

Bemyndigelserne udstilles til serviceudbydere gennem den nationale stamdataservice på NSP. Serviceudbydere får dermed mulighed for at have en ajourført lokal kopi af det centrale bemyndigelsesregister til brug i adgangskontrol og privilegietildeling[2].

Bemærk at stamdataservicen på NSP er valgt som en bekvem mekanisme til replikering af data på tværs af indbyrdes uafhængige aktører. Hvis det giver anledning til problemer vil det være muligt at udstille replikeringsfunktionalitet direkte på bemyndigelsesservicen.

Designet er skitseret på Figur 4.



Figur 4 – skitse af designet og brugen af bemyndigelsesservicen

[2] Bemærk at adgangskontrollen og tildelingen af priveligier foregår hos serviceudbyderen, *ikke* hos bemyndigelsesservicen.

Da bemyndigelsesservicen er en selvstændig, databærende service, skal der etableres en passende ramme for driften af servicen. Det bemærkes, at bemyndigelsesdata udstilles gennem NSP, mens ansvaret for persistering af data fastholdes af driftorganisationen, der driver bemyndigelsesservicen.

2.1 Indholdet af en bemyndigelse

En bemyndigelse er en elektronisk registrering, der indeholder følgende overordnede informationer:

Information	Forklaring og kommentarer
Bemyndigende person	Den bemyndigende persons identitet, der består af et obligatorisk CPR-nummer.
Bemyndigede person	Den bemyndigede persons identitet, der består af et obligatorisk CPR-nummer samt et optionelt CVR-nummer. Angivelses et CVR-nummer låses bemyndigelsen til et ansættelsesforhold i den pågældende virksomhed, mens en bemyndigelse uden angivet CVR-nummer gælder personen uanset ansættelsesforhold.
System	System-attributen angiver i hvilket system, den pågældende bemyndigelse gælder.
Arbejdsfunktion	Den systemspecifikke arbejdsfunktion i hvilken den bemyndigende delegerer rettigheder.
Delegerede rettigheder	En liste af delegerede rettigheder til det givne system. En bemyndigelse uden eksplicit angivelse af rettigheder dækker alle rettigheder, den bemyndigende kan delegere i den angivne arbejdsfunktion.
Status	En bemyndigelse kan have følgende statusser: - ”Bestilt” - ”Godkendt” Kun bemyndigelser godkendt af den bemyndigende videregives til serviceudbydere.

2.2 Administrationssnitflade

Administrationssnitfladen udstillet af bemyndigelsesservicen er en DGWS identitetsbaseret webservice, der forudsætter SOSI niveau 3 IDkort eller højere[3]. Der udstilles en række operationer, der tilsammen giver mulighed for fyldestgørende administration af bemyndigelser foretaget af dels den bemyndigende, den bemyndigede og brugeradministratorer for klientsystemer.

[3] De nøjagtige krav bør fastlægges ud fra en konkret sikkerhedsvurdering.

I regi af Digitaliseringsstyrelsen og Styregruppen for NemLog-in er der udarbejdet et notat, der beskriver handlinger, et administrativt system for fuldmagter som udgangspunkt bør understøtte [BEHOV-LØSN]. I tabellen nedenfor er disse handlinger opsummeret, og eventuel understøttelse af handlingerne i bemyndigelsesservicen er angivet i en kolonne for sig.

Da administrationssnitfladen er webservicebaseret og er fælles for mange klientsystemer og flere serviceudbydere vil flere af handlingerne ikke skulle understøttes i bemyndigelsesservicen, men i stedet i klientsystemerne og hos serviceudbyderne.

Handling	Forklaring og kommentarer	Understøttelse af handling i bemyndigelsesservicen
Udstede bemyndigelse (samt ændre og tilbagekalde)	Den bemyndigende kan udstede en bemyndigelse digitalt ved udfyldelse af en formular. Den bemyndigende kan ændre eller tilbagekalde en bemyndigelse.	Der udstilles operationer, der giver mulighed for oprettelse, ændring og tilbagekaldelse af bemyndigelser.
Udpege bemyndigede	Klinikeren skal angive den bemyndigede præcist og sikkert. Det kan ske ved at vælge fra en liste eller ved at indtaste entydig identifikation som CPR-nummer	Bemyndigelsesservicen forholder sig ikke til lister og indbyrdes forhold imellem bemyndigende og bemyndigede. Funktionalitet, der understøtter arbejdsgangen med f.eks. opslag i relevante lister og validering af CPR-numre skal implementeres i klientsystemerne hvis det skønnes påkrævet.
Signere bemyndigelse	Den bemyndigende skal afgive digital signatur ved godkendelse af en bemyndigelse så der opnås juridisk sikkerhed for den bemyndigendes handling.	Der kræves enten IDkort niveau 4 eller digitalt signerede forespørgsler ved den bemyndigendes godkendelse af en bemyndigelse.
Se oversigt over bemyndigelser	En oversigt over de bemyndigelser, klinikeren har afgivet, samt en oversigt over hvilke bemyndigelser, der er givet til klinikeren.	Der udstilles en operation, der returnerer en liste af bemyndigelser givet **af** et CPR-nummer. Der udstilles endvidere en operation, der returnerer en liste af bemyndigelser givet **til** et CPR-nummer.

Handling	Forklaring og kommentarer	Understøttelse af handling i bemyndigelsesservicen
Anmode om bemyndigelse	En kliniker, der ønsker en given bemyndigelse, kan oprette en ”bemyndigelseskladde”, der efterfølgende kan fremfindes og godkendes af den bemyndigende.	Der udstilles en operation, der giver mulighed for at oprette (og slette) en ønsket bemyndigelse dvs. en bemyndigelse med status ”Bestilt af bemyndigede” eller ”Bestilt af tredjepart”. Bemyndigelsen kan ikke anvendes før den er godkendt.
Kontrollere bemyndigelse	Det skal være muligt for det system, overfor hvilket en bemyndigelse anvendes, at foretage en kontrol af bemyndigelsen (i den situation hvor bemyndigelse medsendes som en ”billet”).	Dette understøttes **ikke** i første fase, hvor serviceudbyderne alene tilgår bemyndigelser gennem udtræk fra stamdataservicen. Det vil være relativt simpelt at udvide bemyndigelsesservicen til at kunne udstede bemyndigelsesbilletter.
Registrere bemyndigelse	Bemyndigelsen skal registreres, så den kan anvendes i myndighedens it-system. Registreringen kan ske i myndighedens eget it-system eller i et ”fuldmagtssystem” og derfra overføres, nå det skal bruges.	Bemyndigelsen registreres og godkendes i bemyndigelsesservicens regi. Godkendte bemyndigelser overføres til serviceudbyderen ved anvendelse af stamdataservicen på NSP.
Besked til den bemyndigede	Den bemyndigede skal eventuelt have besked om bemyndigelse, så vedkommende kan udføre de opgaver, som den indebærer.	Dette understøttes **ikke** i første fase.
Kvittering fra den bemyndigede	Afhængigt af bemyndigelsens indhold kan der være behov for, at bemyndigende får besked om, at bemyndigede har accepteret opgaven og vil udføre de aftalte handlinger.	Dette understøttes **ikke** af bemyndigelsesservicen.

Handling	Forklaring og kommentarer	Understøttelse af handling i bemyndigelsesservicen
Accept af vilkår for fuldmagt	Afhængigt af domænet vil der være behov for, at der er vilkår for bemyndigedes opgaver og forpligtelser, og at bemyndigende informeres om disse vilkår. Myndigheden har forpligtelsen til at sikre de fornødne vilkår og eventuelt sikre, at bemyndigede signerer dem.	Dette understøttes **ikke** af bemyndigelsesservicen.

2.3 Servicespecifikke metadata

Bemyndigelsesservicen udstiller en snitflade med mulighed for inddatering af servicespecifikke metadata i form af en konfiguration af arbejdsfunktioner, rettigheder og den tilhørende mapning af delegerbare rettigheder. Formålet med disse metadata er udelukkende at hjælpe klienter, der skal lave GUI til administration af bemyndigelser.

Som beskrevet i afsnit 1.2 specificerer serviceudbyderen denne konfiguration af arbejdsfunktioner og delegerbare rettigheder. Den systemspecifikke konfiguration vedligeholdes af serviceudbyderen[4], og konfigurationen inddateres af serviceudbyderen til bemyndigelsesservicen. Disse metadata udstilles af bemyndigelsesservicen til klientsystemer gennem bemyndigelsesservicens snitflade.

Da bemyndigelsesservicen som beskrevet ovenfor ikke udstiller en administrationssnitflade til vedligehold af metadata men alene opbevarer en kopi af de respektive serviceudbyderes konfigurationer, foretages opdatering af metadata som komplette inddateringer af en given konfiguration. En serviceudbyder, der f.eks. tilføjer en ny delegerbar rettighed eller justerer på hvilke rettigheder der er delegerbare for en given arbejdsfunktion, skal derfor afslutte opdateringen af konfigurationen ved at sende den komplette konfiguration til bemyndigelsesservicen.[5]

2.4 Kontrol af bemyndigelser hos serviceudbydere

Bemyndigelsesservicen udstiller i første fase godkendte bemyndigelser til brug hos serviceudbydere gennem stamdataservicen på NSP. Det er dermed muligt for serviceudbydere at opbevare (næsten) tidstro kopier af de relevante bemyndigelser i deres egne databaser, og foretage passende optimeringer i forhold til svartider og lagring.

2.4.1 Alternative muligheder for kontrol af bemyndigelser

I første fase anvendes som beskrevet ovenfor stamdataservicen. Der eksisterer følgende alternative muligheder, der eventuelt kan understøttes i senere faser:

[4] Dette sker afkoblet fra bemyndigelsesservicen, f.eks. i de enkelte serviceudbyderes administrationssystemer og med udgangspunkt i fælles klassifikationer, givet sådanne findes.

[5] Justeringer af konfigurationen for en serviceudbyder forventes at forekomme meget sjældent, idet konfigurationerne vil være udformet som resultat af relevante bekendtgørelser og andet lovgrundlag.

Signerede billetter

Bemyndigelsesservicen kan udstede bemyndigelsesbilletter, der er selvindeholdte udsagn om en (sekvens af) bemyndigelse(r). Billetterne er digitalt signerede, enten af bemyndigelsesservicen selv eller af en betroet tredjepart (SOSI STS).

Online validering af bemyndigelse

Bemyndigelsesservicen udstiller en snitflade, hvor en serviceudbyder kan forespørge på en given bemyndigelse.

Replikering af bemyndigelser

Bemyndigelsesservicen udstiller en snitflade, hvor serviceudbydere kan ajourføre lokale kopier af relevante bemyndigelser (dette adskiller sig fra fase 1 tilgangen, hvor replikeringen foregår gennem stamdataservicen på NSP)

3 Funktionalitet hos de involverede parter

Anvendelse af bemyndigelsesservicen kræver forskellig funktionalitet hos de involverede parter. Den nødvendige funktionalitet og eventuelle særlige forhold for de enkelte parter er beskrevet i de følgende afsnit.

3.1.1 Bemyndigelsesservicen

Bemyndigelsesservicen integrerer med stamdataservicen og udstiller funktionalitet til administration af bemyndigelser. Af hensyn til de juridiske aspekter ved anvendelse af bemyndigelser i forhold til videregivelse af rettigheder i it-systemer i sundhedsdomænet indgår validering og sikring af data som en væsentlig faktor i implementeringen af bemyndigelsesservicen.

Følgende funktionalitet er implementeret i bemyndigelsesservicen:

- En administrationswebservice, der kan anvendes af bemyndigere, bemyndigede og administrative systemer
- Variabel autenticitetssikring af brugere afhængigt af anvendelse af bemyndigelsesservicen
- En webservice til inddatering af metadata for de tilknyttede serviceudbydere
- Integration med stamdataservicen på NSP i forhold til godkendte bemyndigelser (data eksporteres til stamdataservicen)
- En webservice til download af metadata (klassifikationer af arbejdsfunktioner og rettigheder) for de enkelte serviceudbydere

3.1.2 Klientsystem (f.eks. fagsystem eller andet it-system)

Klientsystemer skal enten implementere en passende administrationsklient, der gør brug af bemyndigelsesservicen, eller viderestille brugerne til det browserbaserede administrationssystem på f.eks. Sundhed.dk eller Medicin-IT.

Følgende funktionalitet skal implementeres i klientsystemerne:

- En administrationsklient, der gør brug af bemyndigelsesservicen (alternativt kan brugerne hos klientsystemet henvises til det browserbaserede administrationssystem)
- Ved kald til serviceudbydere, hvor kaldet er baseret på en bemyndigelse, skal klientsystemet angive den bemyndigende person på passende vis

3.1.3 Serviceudbyderen

Serviceudbydere der tillader anvendelse af bemyndigelser skal kontrollere bemyndigelsernes gyldighed og på passende vis lade de relevante bemyndigelser indgå i adgangskontrol og rettighedstildeling. I første fase opnår serviceudbydere adgang til bemyndigelserne gennem udtræk fra stamdataservicens bemyndigelsesregister. Serviceudbydere skal derudover udarbejde og vedligeholde en klassifikation af rettigheder, der kan indgå i bemyndigelser.

Følgende funktionalitet skal implementeres hos serviceudbydere:

- Løbende kald til stamdataservicen (udtræk af godkendte bemyndigelser).
- Opslag i lokal kopi af bemyndigelsesregistret til verifikation af bemyndigelser angivet i kald til serviceudbyderen
- Passende adgangskontrol og tildeling af rettigheder hvor bemyndigelsen indgår i forretningslogikken

- Udveksling af metadata med bemyndigelsesservicen omkring mulige bemyndigelser (klassifikation)

3.1.4 Stamdataservicen

Stamdataservicen på NSP udvides med et bemyndigelsesregister, der importeres fra bemyndigelsesservicen. Registret indgår i stamdataservicens portefølje af registre, med standardfunktionalitet udstillet af stamdataservicen, herunder udtræksmuligheder og adgangsbeskyttelse af personfølsomme data.

Følgende funktionalitet skal implementeres i stamdataservicen:

- import af bemyndigelsesregistret
- udtræk af bemyndigelsesregistret
- Adgangskontrol (whitelist) for bemyndigelsesregistret

3.1.5 Browserbaseret administrationssystem

Et browserbaseret administrationssystem[6] skal implementere en passende snitflade, der gør brug af de operationer, bemyndigelsesservicens administrationssnitflade udstiller. Brugere skal kunne se og administrere egne bemyndigelser og kunne "bestille" bemyndigelser.

For browserbaserede administrationssystemer til bemyndigelser gælder det særlige forhold, at de skal godkendes til brug af bemyndigelsesservicen.

Følgende funktionalitet implementeres i browserbaserede administrationssystemer:

- Administrationssnitflade, hvor brugere kan se og administrere egne bemyndigelser, herunder oprette, godkende og slette bemyndigelser
- Administrationssnitflade, hvor brugere kan "bestille" bemyndigelser (dvs. anmode om en bemyndigelse gældende en specifik serviceudbyder hos en specifik bemyndiger)

[6] Som beskrevet i afsnit 2 forventes det at sundhed.dk og/eller Medicin-IT vil implementere et browserbaseret administrationssystem som beskrevet her.

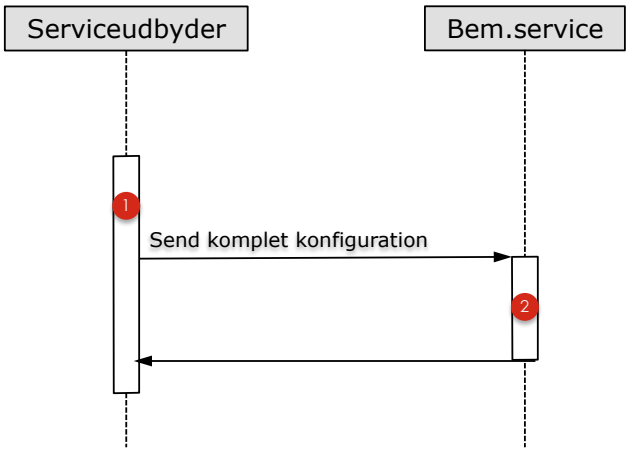
4 Sekvensdiagrammer ved brug af bemyndigelsesservicen

I dette afsnit gennemgås den tekniske arbejdsgang ift. bemyndigelsesservicen for udvalgte scenarier. Notationen er UML sekvensdiagrammer, og hvert diagram gennemgås ganske kort.

Bemyndigelsesservicen gør alene brug af infrastrukturkomponenter (såsom NSP, STS, DCC og SOSI-GW) på standardiseret vis, og disse er derfor ikke beskrevet eksplicit i arbejdsgangene nedenfor. Endvidere forudsættes det, at klientsystemer har ajourført eventuelle kopier af metadata forud for gennemførsel af arbejdsgangene beskrevet nedenfor.

4.1 Opdatering af metadata

En serviceudbyder vedligeholder den systemspecifikke konfiguration af roller, rettigheder og delegerbare rettigheder for de enkelte roller. Administrationen foregår hos serviceudbyderen. Når konfigurationen er som ønsket opdateres bemyndigelsesservicen med den samlede konfiguration.



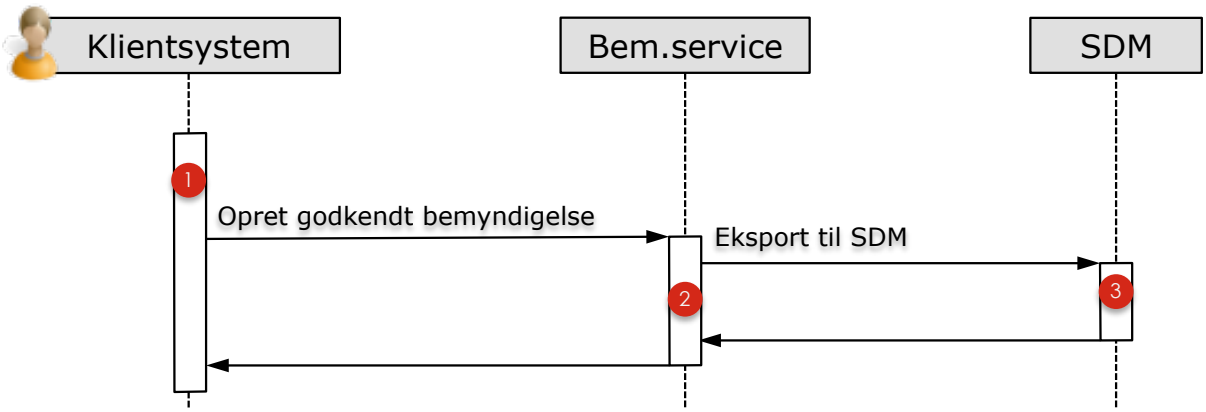
Sekvensdiagram 1 – Opdatering af metadata

1. Serviceudbyderen opdaterer roller, rettigheder og delegerbare rettigheder. Opdateringen afsluttes med en inddatering af den komplette konfiguration til bemyndigelsesservicen
2. Bemyndigelsesservicen modtager den komplette konfiguration fra serviceudbyderen. En eventuel eksisterende konfiguration erstattes med den nye udgave.

4.2 Oprettelse af en godkendt bemyndigelse fra et klientsystem

En læge bemyndiger en assistent til at udføre arbejdsgange på vegne af lægen ved brug af en serviceudbyder, f.eks. FMK. Lægen fremfinder assistenten i klientsystemets brugergrænseflade, markerer de ønskede rettigheder, og godkender bemyndigelsen.

Forudsætninger: Lægen har forud for disse arbejdsgange erhvervet sig et SOSI IDkort, enten i klientsystemet eller på anden vis.



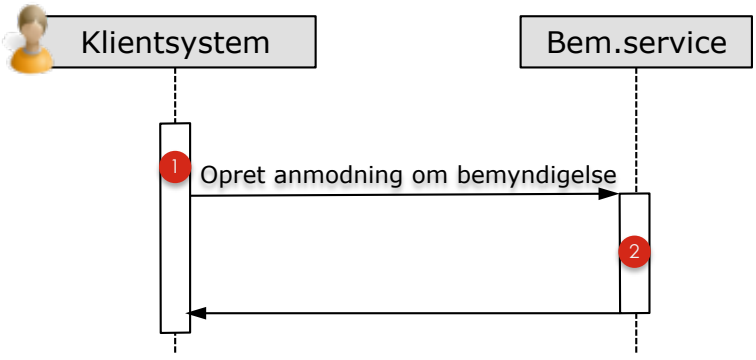
Sekvensdiagram 2 – Oprettelse af godkendt bemyndigelse

1. Den bemyndigende anvender klientsystemet til at oprette en godkendt bemyndigelse.
2. Den bemyndigende delegerer de ønskede rettigheder til den ønskede bemyndigede, og klientsystemet kalder bemyndigelsesservicens administrationssnitflade (i den bemyndigendes navn, dvs. med brugerens SOSI IDkort).
3. Bemyndigelsesservicen modtager kaldet og opdaterer stamdataservicen med den godkendte bemyndigelse.

Den godkendte bemyndigelse er nu tilgængelig i stamdataservicens bemyndigelsesregister for den pågældende serviceudbyder.

4.3 Oprettelse af anmodning om bemyndigelse

En bruger af et klientsystem opretter en anmodning om bemyndigelse hos en specifik bemyndigende. Bemyndigelsen har status ”Bestilt” og eksporteres ikke til stamdataservicen. Dette scenarie beskriver kun oprettelsen af anmodningen, for beskrivelse af godkendelse af bestilte bemyndigelser henvises til scenariet beskrevet i afsnit 4.4.



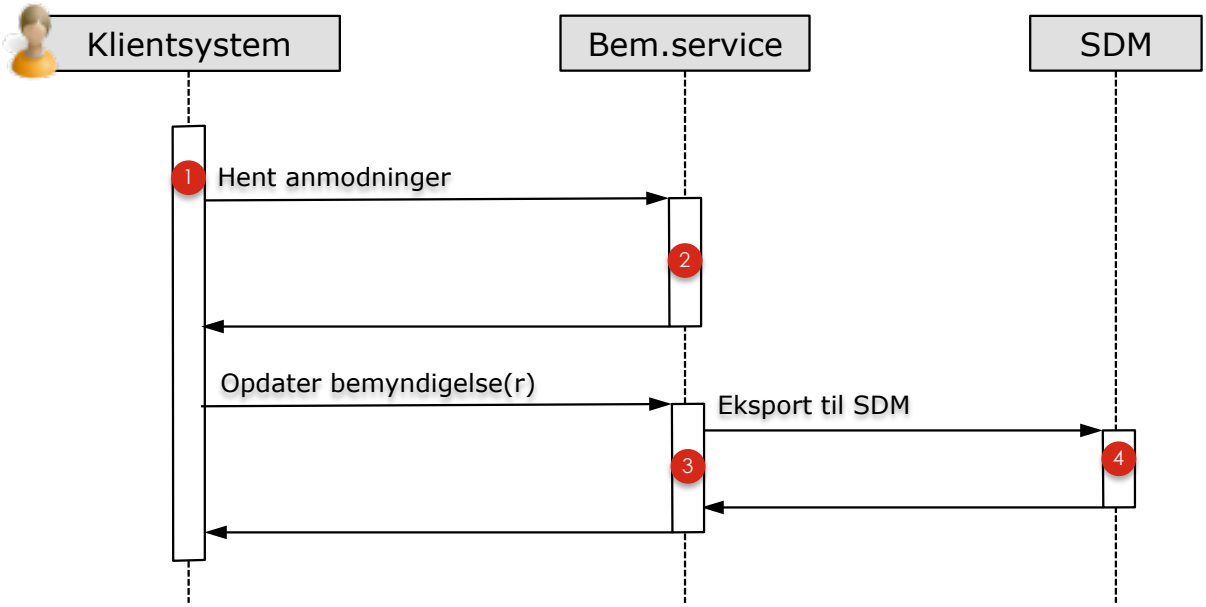
Sekvensdiagram 3 – anmodning om bemyndigelse

1. Brugeren anvender klientsystemet til at anmode en specifik bemyndigende om en bemyndigelse.
2. Brugeren vælger de ønskede rettigheder, og sender anmodningen til bemyndigelsesservicen.

Anmodningen er nu registreret i bemyndigelsesservicen, men eksporteres ikke til stamdataservicen, da kun godkendte bemyndigelser udstilles.

4.4 Godkendelse af bestilte bemyndigelser

En bruger i et klientsystem bliver adviseret om at vedkommende har en eller flere anmodninger liggende til godkendelse.[7] Brugeren får listen af anmodninger og har mulighed for at godkende eller afvise bemyndigelserne.



Sekvensdiagram 4 – godkendelse af bemyndigelse(r)

1. Brugeren anvender klientsystemet til at godkende og/eller afvise anmodninger om bemyndigelser.
2. Klientsystemet henter udestående anmodninger (dvs. anmodninger, der ikke er blevet godkendt eller afvist) for brugeren.
3. Brugeren gennemgår anmodningerne og godkender/afviser hver enkelt. Dette trin kan gentages af brugeren til der ikke er flere udestående anmodninger, eller der kan gennemføres en opdatering af anmodningerne på én gang (begge dele er understøtet af bemyndigelsesservicen).
4. For hver opdatering bemyndigelsesservicen modtager registreres bemyndigelsens status, og bemyndigelsen eksporteres til stamdataservicen hvis den er godkendt eller afvist.

[7] En sådan advisering forudsætter at klientsystemet har implementeret en passende adviseringsmekanisme og gør brug af muligheden for at hente "egne" bemyndigelser gennem bemyndigelsesservicen.

5 Referencer

Krydshenvisning	Kilde
BEMYN	”*Bemyndigelsesservice – Løsningsbeskrivelse*”, Digital Sundhed, 3. november 2008.
BEHOV-LØSN	”*FULDMAGT,PARTSREPRÆSENTATION OG SAMTYKKE BEHOV OG LØSNINGSMULIGHEDER*”, Digitaliseringsstyrelsen; Styregruppen for NemLog-in, januar 2012.
FMK-rettigheder	”*Ændringer til rettigheder*”, FMK, januar 2012.