Fælles bemyndigelsesservice - **Overordnet løsningsdesign** Dato: 13.02.2012 Version: 0.1 Udarbejdet af: NSI	National Sundheds-IT www.nsi.dk Islandsbrygge 39 2300 København S

Snitfladebeskrivelse krav for den fælles bemyndigelsesservice

Version	Ansvarlig	Kommentar
0.1	CHE	Første udkast, indarbejdet kommentarer fra TSO

Indholdsfortegnelse

1 Indledning

1.1 Formål og målgruppe

Formålet med denne snitfladebeskrivelse er at uddybe løsningsbeskrivelsen med en mere konkret beskrivelse af de services, der skal være tilgængelige på bemyndigelsesservicen.

Snitfladebeskrivelsen indeholder 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.

Kapitel 3 vedrører administrationssnitfladen, der er målrettet klientsystemer, f.eks. administrative systemer i en region eller et nationalt browserbaseret system som sundhed.dk, der administrerer bemyndigelser.

Kapitel 4 vedrører systemspecifikke metadata, der er målrettet serviceudbydere, der anvender digitale bemyndigelser.

1.2 Navngivning og standarder

Bemyndigelsesservicen er en identitetsbaseret webservice, der overholder Den Gode Web-Service (DGWS) 1.0.1.

Feltnavne og regler for indhold følger så vidt muligt relevante OIO-specifikationer, f.eks. CPR-numre og CVR-numre.

2 Datastruktur

Bemyndigelsesservicen registrerer og opbevarer digitale bemyndigelser. Derudover registreres metadata for de systemer, der anvender bemyndigelsesservicen.

Nedenfor ses en uformel specifikation af datastrukturen for disse elementer.

2.1 Digital bemyndigelse

En digital bemyndigelse består af en simpel datastruktur, der indeholder følgende felter:

Felt	Type	Særlige forhold
Bemyndigelseskode	Tekst	Unik identifier for bemyndigelser.
Bemyndigende	cpr:PersonCivilRegistration IdentifierType	CPR-nummer for den person, der videregiver rettigheder til den bemyndigede.Der anvendes *ikke* bindestreg.
Bemyndigede	cpr:PersonCivilRegistration IdentifierType	CPR-nummer for den person, der bemyndiges. Der anvendes *ikke* bindestreg.
BemyndigedeCVR	cvr:CVRnumberIdentifierType	CVR-nummer for den person, der bemyndiges. **Valgfrit felt**. Angivelsen af et CVR-nummer låser bemyndigelsen til et ansættelsesforhold i den pågældende virksomhed, mens en bemyndigelse uden angivelse af CVR-nummer for den bemyndigede gælder personen uanset ansættelsesforhold.
System	Tekst	Systemet, for hvilket bemyndigelsen gælder. Systemnavn aftales imellem serviceudbyder og driftleverandøren af bemyndigelsesservicen.
Arbejdsfunktion	Tekst	Den bemyndigendes arbejdsfunktion i systemet. Mulige værdier findes i metadata for det pågældende system (Arbejdsfunktioner).

Felt	Type	Særlige forhold
Rettighedskode	Tekst	Den delegerede rettighed. Mulige værdier findes i metadata for det pågældende system (Rettigheder). **NB!** Angivelse af værdien "" i dette felt indikerer at samtlige delegarbare rettigheder for den pågældende arbejdsfunktion er delegeret i bemyndigelsen.
Status	TEKST	Status for bemyndigelsen. **Mulige værdier**: "Bestilt" – oprettet af enten den bemyndigede eller en tredjepart. "Godkendt" – godkendt af den bemyndigende.
Godkendelsesdato	DatoTid	Starttidspunkt for bemyndigelsens gyldighed. **Valgfrit felt,** dog obligatorisk hvis bemyndigelsen har status "Godkendt".

2.2 Metadata – systemspecifikke informationer

It-systemer, der tillader anvendelse af digitale bemyndigelser, skal publicere en konfiguration af arbejdsfunktioner, rettigheder og delegerbare rettigheder for de enkelte arbejdsfunktioner. Bemyndigelsesservicen opbevarer en kopi af konfigurationerne og stiller disse informationer til rådighed for klientsystemer gennem stamdataservicen på NSP.

En konfiguration er specificeret som følger:

Arbejdsfunktion

Felt	Type	Særlige forhold
Domæne	Tekst	Myndigheden, der står bag det udstillede system. Værdien skal være globalt unik.
System	Tekst	System, til hvilket arbejdsfunktionenn er knyttet. Værdien skal være globalt unik.
Arbejdsfunktion	Tekst	Unik identifier. Bemærk: Kun krav om unikhed for arbejdsfunktionen indenfor hvert enkelt system.
Tekst til arbejdsfunktion	Tekst	Tekst, der beskriver arbejdsfunktionen (f.eks. ”Læge” eller ”Tandlæge”).

Rettighed

Felt	Type	Særlige forhold
Domæne	Tekst	Myndigheden, der står bag det udstillede system. Værdien skal være globalt unik.
System	Tekst	System, til hvilket rettigheden er knyttet. Værdien skal være globalt unik.
Rettighedskode	Tekst	Unik identifier. Bemærk: Kun krav om unikhed for rettighedskoden indenfor hvert enkelt system.
Rettighedstekst	Tekst	Kort tekst (f.eks. ”Dispensering”) der beskriver rettigheden.

Delegerbar rettighed

Felt	Type	Særlige forhold
Domæne	Tekst	Myndigheden, der står bag det udstillede system. Værdien skal være globalt unik.
System	Tekst	System, til hvilket rettigheden er knyttet. Værdien skal være globalt unik.
Arbejdsfunktion	Tekst	Reference til arbejdsfunktionen.
Rettighedskode	Tekst	Reference til rettighed.

3 Metoder – administrationssnitflade

Administrationssnitfladen udstillet af bemyndigelsesservicen er en DGWS identitetsbaseret webservice, der forudsætter SOSI niveau 3 IDkort eller højere[1]. Der udstilles en række metoder, der tilsammen giver mulighed for fyldestgørende administration af bemyndigelser foretaget af dels den bemyndigende, den bemyndigede og brugeradministratorer for klientsystemer. Metoderne er opsummeret i tabellen nedenfor, og er beskrevet i detaljer i de følgende afsnit.

Metode	Beskrivelse
Hent bemyndigelser	Returnerer alle bemyndigelser for et givet CPR-nummer. En parameter i kaldet afgør om det er bemyndigelser hvor CPR-nummeret er hhv. bemyndiget eller bemyndigende. Metoden anvendes af klientsystemer til at give brugeren et overblik over bemyndigelser.
Bestil bemyndigelse	Opretter en ønsket bemyndigelse (status ”Bestilt”).
Opret godkendt bemyndigelse	Opretter en godkendt bemyndigelse.
Godkend bemyndigelse	Godkender bemyndigelse oprettet af bemyndigede eller tredjepart (f.eks. en brugeradministrator). Kun den bemyndigende kan godkende en bemyndigelse.
Slet bemyndigelse	Sletter en bemyndigelse. Anvendes af bemyndigende og whitelistede systemer på både godkendte og ønskede bemyndigelser, og af bemyndigede på ønskede bemyndigelser.

3.1 Hent bemyndigelser

Metoden returnerer alle bemyndigelser for et givet CPR-nummer. Det er muligt at angive CPR-nummer for hhv. bemyndigende og bemyndigede.

Metoden anvendes af klientsystemer til at give brugeren et overblik over relevante bemyndigelser, både i betydningen ”Hvem har jeg bemyndiget”, og ”Hvem har bemyndiget mig”.

3.1.1 Forespørgsel

Felt	Type
Bemyndigende	cpr:PersonCivilRegistrationIdentifierType
Bemyndigede	cpr:PersonCivilRegistrationIdentifierType

[1] Godkendelse af en bemyndigelse kræver niveau 4, mens det er tilstrækkeligt med niveau 3 for de resterende operationer.

3.1.2 Svar

Der returneres en liste af bemyndigelser indeholdende samtlige felter som specificeret i afsnit 2.1. Der kan returneres 0, 1 eller flere bemyndigelser.

3.1.3 Særlige forhold

Brugere kan kun fremfinde egne bemyndigelser, dvs. bemyndigelser hvor enten bemyndigede eller bemyndigende har brugerens CPR-nummer angivet. Kontrollen baseres på sammenligning af CPR-nummer i SOSI IDkort med CPR-nummer for bemyndiget hhv. bemyndigende.

Denne begrænsning gælder ikke for whitelistede systemer.

3.1.4 Fejl

Ingen særlige fejlsituationer.

3.2 Bestil bemyndigelse

Opretter en ønsket bemyndigelse. Metoden anvendes af assistenter eller brugeradministratorer til at bestille en bemyndigelse hos en specifik bemyndigende, f.eks. en læge på en afdeling. Bemyndigelsen får status ”Bestilt” og er først gyldig når den godkendes af angivne bemyndigende, jvf. afsnit **Error! Reference source not found.** ”**Error! Reference source not found.**”.

3.2.1 Forespørgsel

Felt	Type
Bemyndigende	cpr:PersonCivilRegistrationIdentifierType
Bemyndigede	cpr:PersonCivilRegistrationIdentifierType
BemyndigedeCVR	cvr:CVRnumberIdentifierType
System	Tekst
Arbejdsfunktion	Tekst
Rettighedskode	Tekst

3.2.2 Svar

Der returneres ”ok” hvis oprettelsen kan gennemføres.

3.2.3 Særlige forhold

Brugere kan kun bestille bemyndigelser hvor de selv fremgår som bemyndigede. Kontrollen baseres på sammenligning af CPR-nummer i SOSI IDkort med CPR-nummer for bemyndiget.

Denne begrænsning gælder ikke for whitelistede systemer.

3.2.4 Fejl

Der returneres en fejl hvis en bruger i et ikke-whitelistet klientsystem forsøger at oprette en bemyndigelse på vegne af tredjepart.

3.3 Opret godkendt bemyndigelse

Opretter en godkendt bemyndigelse. Denne metode anvendes når den bemyndigende opretter og godkender bemyndigelser i samme arbejdsgang. Metoden kan tage en liste af bemyndigelser som input og opretter og godkender alle bemyndigelserne på listen.

3.3.1 Forespørgsel

Felt	Type
Bemyndigende	cpr:PersonCivilRegistrationIdentifierType
Bemyndigede	cpr:PersonCivilRegistrationIdentifierType
BemyndigedeCVR	cvr:CVRnumberIdentifierType
System	Tekst
Arbejdsfunktion	Tekst
Rettighedskode	Tekst

3.3.2 Svar

Der returneres en bemyndigelseskode for hver af de oprettede bemyndigelser.

3.3.3 Særlige forhold

Brugere kan kun oprette godkendte bemyndigelser hvor de selv fremgår som bemyndigende. Kontrollen baseres på sammenligning af CPR-nummer i SOSI IDkort med CPR-nummer for bemyndiget.

Denne begrænsning gælder ikke for whitelistede systemer.

Bemærk: Der udestår en afklaring af hvordan dette håndteres for browserbaserede systemer der administrerer bemyndigelser.

3.3.4 Fejl

Metoden returnerer en fejl, hvis der forsøges oprettet en bemyndigelse hvor brugeren ikke selv er bemyndigende part (eller anvender et whitelistet system).

3.4 Godkend bemyndigelse

Godkender bemyndigelse oprettet af bemyndigede eller tredjepart (f.eks. en brugeradministrator). Metoden tager både enkelte bemyndigelser og en liste af bemyndigelser som input.

3.4.1 Forespørgsel

Felt	Type
Bemyndigelseskode	Tekst

3.4.2 Svar

Der returneres bemyndigelseskoder for de bemyndigelser, der nu er godkendte.

3.4.3 Særlige forhold

Brugere kan kun godkende bemyndigelser hvor de selv fremgår som bemyndigende. Kontrollen baseres på sammenligning af CPR-nummer i SOSI IDkort med CPR-nummer for bemyndigende.

Denne begrænsning gælder ikke for whitelistede systemer.

Bemærk: Der udestår en afklaring af hvordan dette håndteres for browserbaserede systemer der administrerer bemyndigelser.

3.4.4 Fejl

Metoden returnerer en fejl, hvis der forsøges godkendt en bemyndigelse hvor brugeren ikke selv er bemyndigende part (eller anvender et whitelistet system).

3.5 Slet bemyndigelse

Sletter en bemyndigelse. Anvendes af bemyndigende og whitelistede systemer på både godkendte og ønskede bemyndigelser, samt af bemyndigede på ønskede bemyndigelser. Metoden tager både enkelte og lister af bemyndigelser som input.

3.5.1 Forespørgsel

Felt	Type
Bemyndigelseskode	Tekst

3.5.2 Svar

Der returneres en liste af bemyndigelseskoder for de bemyndigelser, der blev slettet.

3.5.3 Særlige forhold

Brugere kan kun afvise bemyndigelser hvor de selv fremgår som bemyndigende. Kontrollen baseres på sammenligning af CPR-nummer i SOSI IDkort med CPR-nummer for bemyndigende.

Denne begrænsning gælder ikke for whitelistede systemer.

Bemærk: Der udestår en afklaring af hvordan dette håndteres for browserbaserede systemer der administrerer bemyndigelser.

3.5.4 Fejl

Metoden returnerer en fejl, hvis der forsøges afvist en bemyndigelse hvor brugeren ikke selv er bemyndigende part (eller anvender et whitelistet system).

4 Metoder - Servicespecifikke metadata

Metode	Beskrivelse
setMetadata	Inddater en komplet konfiguration for et system
getMetadata	Returnerer en komplet konfiguration for et system

4.1 setMetadata

Inddater en komplet konfiguration for et system. Kaldet består af tre lister: Arbejdsfunktion, Rettighed og Delegerbar Rettighed.

4.1.1 Forespørgsel

Liste	Felt	Type
Arbejdsfunktion	Domæne	Tekst
	System	Tekst
	Arbejdsfunktion	Tekst
	Beskrivende tekst	Tekst
Rettighed	Domæne	Tekst
	System	Tekst
	Rettighedskode	Tekst
	Beskrivende tekst	Tekst
Delegerbar Rettighed	Domæne	Tekst
	System	Tekst
	Arbejdsfunktion	Tekst
	Rettighedskode	Tekst

4.1.2 Svar

Der returneres ”ok” hvis inddateringen kan gennemføres.

4.1.3 Særlige forhold

Kun whitelistede systemer kan uploade konfigurationer.

4.1.4 Fejl

Metoden returnerer en fejl, hvis systemet ikke er whitelistet.

4.2 getMetadata

Returnerer en komplet konfiguration for et system. Svaret består af tre lister: Arbejdsfunktion, Rettighed og Delegerbar Rettighed.

4.2.1 Forespørgsel

Felt	Type
Domæne	Tekst
System	Tekst

4.2.2 Svar

Liste	Felt	Type
Arbejdsfunktion	Domæne	Tekst
	System	Tekst
	Arbejdsfunktion	Tekst
	Beskrivende tekst	Tekst
Rettighed	Domæne	Tekst
	System	Tekst
	Rettighedskode	Tekst
	Beskrivende tekst	Tekst
Delegerbar Rettighed	Domæne	Tekst
	System	Tekst
	Arbejdsfunktion	Tekst
	Rettighedskode	Tekst

4.2.3 Særlige forhold

Ingen særlige forhold.

4.2.4 Fejl

Metoden returnerer en fejl, hvis kombinationen af domæne og system ikke findes.

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.
OIOSAML-BPP	”*OIOSAML Basic Privilege Profile Version 1.0.1*”, Digitaliseringsstyrelsen, december 2011.