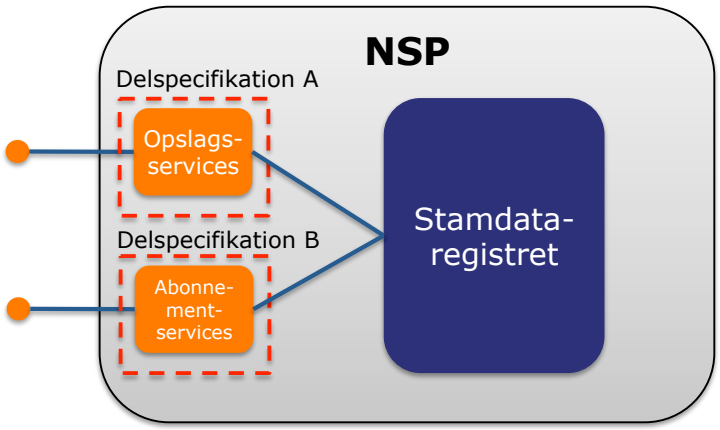
| | |
|---|---|
| **NSI Projektmodel**<br><br>**Kravspecifikation –CPR-services**<br><br>**Infrastrukturprogrammet fase 2 – NSPi projektet**<br><br>Dato: 10.08.2011<br>Version: 1.0<br>Udarbejdet af: NSI | NATIONAL SUNDHEDS-IT<br>NATIONAL BOARD OF E-HEALTH<br>www.nsi.dk<br><br>Islands Brygge 39<br>2300 København S |

# National Sundheds-it
# Program for infrastruktur og sikkerhed

Kravspecifikation: CPR-services (Stamdata Registret)



## Indholdsfortegnelse

# CPR-services under Stamdata registret

## Indledning

Stamdataregistret implementeret under NSPi projektet indeholder CPR stamdata. Den eksisterende kopiregisterservice, der giver mulighed for komplette samt løbende udtræk (”delta”) til en lokal kopi af registret ønskes suppleret med online services, foranlediget af P-VIT projektets behov.

Nærværende kravspecifikation er en formaliseret opsamling på P-VIT projektets servicespecifikation samt på Det Gode CPR-opslag (begge vedlagt). Kravspecifikationen specificerer funktionaliteten, der ønskes udviklet, dels hvordan projektet skal forløbe.

Udviklingen af CPR-services foregår som en udvidelse af det igangsatte SPOR 6 (”Stamdata services”), hvor den eksisterende projektmodel videreføres, og hvor de ønskede CPR-services bygges ovenpå det i SPOR 6 realiserede stamdata modul.

# Om kravspecifikationen

Dette afsnit forklarer kravenes form og hvordan kravene tænkes at tilgodese kundens forretningsmæssige mål.

## Kravenes form

Kravene er opdelt i kapitler efter deres art. I hvert kapitel er kravene opstillet i afsnit der vedrører en bestemt arbejdsopgave eller emne.

Kravene indeholder flg.:

- Kravnummer eller Optionsnummer
- Overskrift
- Beskrivelse
- (Info) Løsningsforslag
- (Info) Hyppighed
- (Info) Verificering
- (Info) Andre informationer (eksempel, kommentar …)

De første tre punkter er obligatoriske og udgør selve kravet. Foruden disse punkter kan kravet foreslå en løsning, redegøre for hyppighed, hvordan kunden har tænkt sig at verificere kravet samt andre oplysninger. Disse oplysninger er ikke en del af kravet, men nogle nyttige informationer til tilbudsgiver/leverandøren, der kan hjælpe eller guide mod den rigtige løsning.

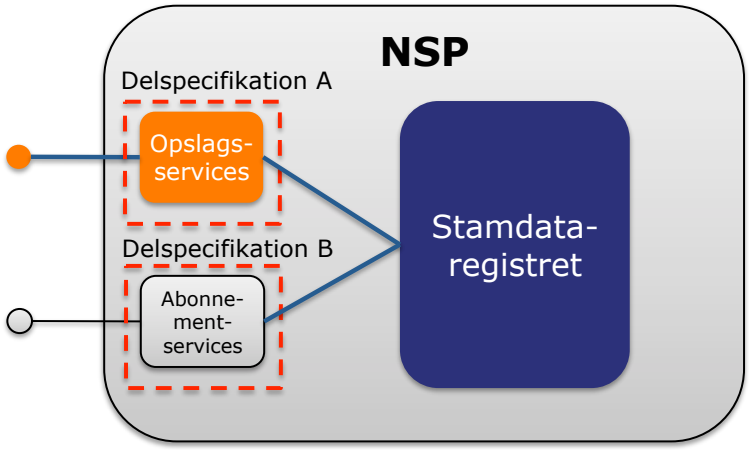
Kravene har fortløbende unikke numre og kan således utvetydigt refereres til med deres kravnummer, f.eks. Krav 1 eller K1.

## Forudsætninger

- De specificerede CPR-services bygger på det i SPOR 6 udviklede stamdata register

## Delspecifikation A: CPR opslagsservices

Der ønskes udstillet et antal opslagsservices på de enkelte NSP-instanser. Anvendelse af de enkelte services er identitetsbaseret og forudsætter en forudgående aftale med operatøren. Opslag vil blive benyttet af leverandører af fællesregionale systemer – og af de regionale CPR-komponenter, hvor regionen ikke i forvejen har cachet oplysninger for den pågældende person.




**Figur 1: CPR opslagsservices**

Krav 1. **Etablering af opslagsservice (”getPersonDetails”)**

P-VIT servicespecifikationen angiver fire varianter af ”getPersonDetails” (afsnit 4.1.1, 4.1.2, 4.1.3 og 4.1.4 i servicespecifikationen). Disse skal implementeres som standard identitetsbaserede DGWS-web services (jævnfør Krav 4 vedrørende adgangskontrol).

**Information:** Der henvises til [MEDCOM-CPROPSLAG] for specifikation af datastrukturer anvendt i input/output for de ønskede opslagsservices.

Krav 2. **Etablering af Det Gode CPR-opslag**

Specifikationen af Det Gode CPR-opslag (vedlagt) ønskes implementeret, dog med den afvigelse, at der stilles krav om et NIST niveau 3 STS-signeret IDkort (dvs. autentifikation på basis af OCES certifikater og ikke brugernavn+kodeord som angivet i den vedlagte specifikation).
Denne service må *ikke* returnere beskyttede data, og ved opslag, der indeholder beskyttede data i svaret, skal disse erstattes med en passende værdi (f.eks. ”ADRESSEBESKYTTET”).

**Information**: Servicen beskrevet i dette krav adskiller sig fra ”getPersonDetails”, idet adgangskontrollen er begrænset til krav om NIST niveau 3 STS-signeret IDkort, og idet denne service altid udelader beskyttede data.

Krav 3. **Dokumentation af opslagsservices**

De i Krav 1 og Krav 2 angivne opslagsservices skal dokumenteres, som minimum med angivelse af input og output, samt eventuelle særlige forhold.

Krav 4. **Adgangskontrol og beskyttede data for ”getPersonDetails”**

Anvendelse af de implementerede opslagsservices kræver STS-signerede IDkort. For beskyttede data i CPR-registret (på recordniveau) gælder specifikt, at kun offentlige myndigheder har adgang til disse. Dette ønskes styret ved hjælp af en CVR-baseret whitelist.
Andre interessenter end offentlige myndigheder (f.eks. privatpraktiserende læger) skal ved opslag, der indeholder beskyttede data i svaret, i stedet få et svar ”renset” for de beskyttede data (indholdet af de beskyttede felter skal erstattes med en passende tekst, f.eks. ”ADRESSEBESKYTTET”, eller blankes).

**Information**:
NSI må dele CPR data med alle interessenter i sundhedsvæsenet.
Kun offentlige myndigheder må se beskyttede informationer.
Det er på recordniveau markeret hvilke informationer der er beskyttede.

**Information**: Vedligehold af ovennævnte whitelist foregår på DoDi, og resultatet replikeres ud til samtlige NSP-instanser.

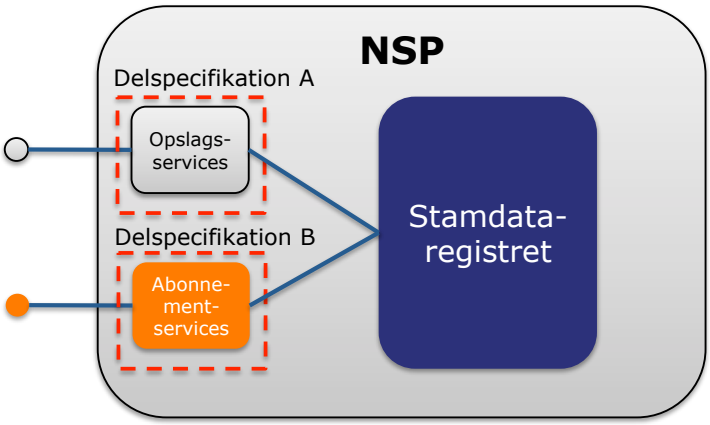
Krav 5. **Logning af brug af enkeltopslagsservices**

Der skal være logning på hvem, der har foretaget opslag, samt hvilke cpr-numre, svaret indeholder. Loggen skal indeholde tilstrækkelig information til at identificere den kaldende person, baseret på det medsendte SOSI IDkort.

**Information**: Der skal jf. persondataloven være logning af hvem, der har haft adgang til hvad (enkeltopslag).

## Delspecifikation B: Abonnementservices

Der ønskes et ”abonnementsmodul”, hvor et system kan til- og framelde cpr-numre en overvågningsliste, og efter behov forespørge på ændringer på listen siden sidste forespørgsel.




**Figur 2. Abonnementservices**

Krav 6. **Services til vedligeholdelse af abonnementsliste**

Som angivet i servicespecifikationen (afsnit 4.2.1 og 4.2.2) ønskes der en metode til at tilmelde et CPR-nummer (”subscribePersonDetails”) og en metode til at afmelde et CPR-nummer (”unsubscribePersonDetails”).

**Information:** Metoderne skal implementeres som DGWS identitetsbaserede webservices.

**Information:** Den i SPOR 2 udviklede opsamlingsservices ønskes anvendt til opsamling af til- og afmeldinger af CPR-numre.

Krav 7. **Services til forespørgsel på abonnementsliste**

Som angivet i servicespecifikationen (afsnit 4.2.3 og 4.2.4) ønskes der to metoder til forespørgsel på ændringer på cpr-numre tilknyttet en given abonnementsliste.

**Information:** Metoderne skal implementeres som DGWS identitetsbaserede webservices.

**Information:** Potentielt kan der være store datamængder i svaret, og der skal derfor tages højde for dette i implementeringen. Løsningsbeskrivelsen skal indeholde en beskrivelse af hvordan dette håndteres.

Krav 8. **Adgangskontrol for abonnementservices**

Anvendelse af de implementerede abonnementservices kræver STS-signerede IDkort. Adgangskontrollen ønskes implementeret ved hjælp af en CVR-baseret whitelist.

**Information**: Vedligehold af ovennævnte whitelist foregår på DoDi, og resultatet replikeres ud til samtlige NSP-instanser.

## Generelle krav

Krav 9. **Overholdelse af operatørkrav**

Kravene specificeret i [SDSD Operatør] skal overholdes eksplicit. Eventuelle fravigelser fra kravene på grund af manglende relevans eller sammenfald med krav i nærværende kravspecifikation skal begrundes.

Krav 10. **Overholdelse af krav til teknisk dokumentation**

Kravene specificeret i [SDSD Teknisk] skal overholdes eksplicit. Eventuelle fravigelser fra kravene på grund af manglende relevans eller sammenfald med krav i nærværende kravspecifikation skal begrundes.

Krav 11. **Performance**

Services, der udstilles på NSP som følge af Krav 2 og Krav 6 vil som udgangspunkt kaldes synkront fra f.eks. patientadministrative systemer. Løsningen skal derfor kunne håndtere 10 samtidige kald med en spredning i svartider som følger for opslagsservices og vedligehold af abonnementslister:

- Gennemsnit 100 ms
- 95% under 150 ms
- 99% under 500 ms

Proxyservices til ekstern funktionalitet må bidrage med tilsvarende svartider som beskrevet ovenfor, målt fra en request modtages til den bagvedliggende service er blevet kaldt.

Kald til abonnementslisten (ændringsliste) foregår som udgangspunkt som en del af en batchkørsel, og performancekravene er tilsvarende lave. Svartiderne vil afhænge dels af den pågældende listes størrelse, dels af hvor mange på listen, der er registrerede som ændrede i det angivne interval. Følgende krav stilles til performance for kald til abonnementslisten, hvor 10% af personerne på listen er ændrede:

- Liste med under 10000 personer:
  - Gennemsnit 1000 ms
  - 95% under 2000 ms
  - 99% under 3000 ms

Svartiderne må stige lineært med listens størrelse.

De leverede komponenter skal være robust over for en stigende belastning, således at svartiderne og den tidsmæssige spredning af svartiderne ikke forøges nævneværdigt ved stigende belastning (bemærk dog særlige vilkår for kald til abonnementslisten som beskrevet ovenfor).
Ved overbelastning skal komponenterne fortsat virke korrekt, hvilket betyder at de funktionelt fungerer, og ikke afleverer forkerte resultater.
Overholdelse af dette krav skal dokumenteres, eventuelt som en del af testrapporten der skal udarbejdes i Krav 18.

Krav 12. **Open Source JAVA komponenter**

Nærværende kravspecifikations komponenter skal udvikles i JAVA under open source licens i overensstemmelse med anbefalingerne i [SDSD OSS].

Krav 13. **Anvendelse af SOSI biblioteket**

Leverandøren skal benytte egnede SOSI-biblioteker i udviklingen af komponenterne. Såfremt leverandøren afviger fra dette skal der argumenteres herfor.

Krav 14. **Monitoreringssnitflade**

Til brug for driftsleverandøren af NSP skal leverandøren udstille en monitoreringssnitflade således, at status på alle dele af løsningen (opslagsservices, abonnementsservices og ) kan monitoreres. Monitoreringen skal udarbejdes i overensstemmelse med [SDSD Teknisk].

Krav 15. **Log**

Leverandøren skal som en del af løsningen logge på SLA (Service Level Agreement) niveau såvel som på audit niveau til den centrale log, som beskrevet i [SDSD Teknisk].

Krav 16. **Standarder**

Alle XML formater skal i videst muligt omfang følge de i ”Den Gode Webservice, version 1.0.1 ” beskrevne standarder (se [DGWS]), herunder SOAP 1.2, WS-Security, XML-signatur, SAML, osv. Sikkerhedsniveauet for webservices skal være niveau 4, dvs. digitalt signeret id-kort skal anvendes, med mindre lavere sikkerhedsniveauer eksplicit er nævnt i nærværende kravspecifikation.
Hvis leverandøren finder det nødvendigt at fravige fra dette, skal det eksplicit bemærkes og begrundes.

## Leverance og test

Krav til form og tidsplan for leverancen beskrives i det følgende.

Krav 17. **Test af CPR-services**

Leverandøren skal gennemføre en test af det samlede sæt af CPR-services, der demonstrerer, at det overholder kravene i nærværende kravspecifikation.
Der skal udarbejdes testplan, testsuites, testcases og testdata. Resultatet af testen skal ligeledes dokumenteres.
Der skal ydermere gennemføres kode test (unit testing) med minimum 80% coverage.

Krav 18. **Performancetest**

Der skal udføres en automatiseret performancetest, der indeholder flg.

- En skaleringstest der viser sammenhængen mellem svartider og stigende belastning indtil overbelastningspunktet nås. Endvidere skal skaleringstesten vise spredningen af svartiderne.
- En load/stresstest, der identificerer overbelastningspunktet og identificerer hvilke symptomer systemet udviser ved overbelastning og om eller hvornår systemet bryder sammen. Det skal påvises at systemet virker korrekt ved overbelastning, hvilket betyder at den funktionelt fungerer, og ikke afleverer forkerte resultater.
- Endurancetest der viser at systemet ikke har ressourcelækager (CPU, RAM) ved længerevarende jævn belastning.

Testen planlægges i en testplan og dokumenteres i en testrapport.
Den automatiserede test skal kunne afvikles i forbindelse med alle opdateringer af software og hardware.

Krav 19. **Tidsplan**

Tilbudsgiver skal vedlægge tidsplan, der i kalendertid angiver mulige starttidspunkter for projektet, varigheden af projektet, samt hvilke personressourcer, der tildeles.

Krav 20. **Afviklingsmiljøer**

De udviklede komponenter skal etableres i 3 miljøer.

- Et produktionsmiljø
- Præproduktionsmiljø
- Et testmiljø / udviklermiljø

Alle aspekter af komponenten skal kunne testes i præproduktionsmiljøet.

Krav 21. **Dokumentation**

Dokumentation leveres under samme forudsætninger som for det oprindelige SPOR 6.

Krav 22. **Løsningsbeskrivelse**

Tilbudsgiver skal i forbindelse med aflevering af løsningsbeskrivelse med prisoverslag også levere et estimat på forventet tidsforbrug specificeret på relevante funktionelle delelementer.

Krav 23. **Leverance**

Løsningen skal afleveres til NSP-operatøren, jævnfør de gældende retningslinier for produktleverancer (”KRAV TIL LEVERANCER TIL EN NSP RELEASE, version 2.0”). Specifikt henvises der til afsnit 5 i ovennævnte dokument.
Leverancen skal foreligge i en testet og godkendt version senest d. 15. september 2011 kl 12.

## Referencer

| | | |
|---|---|---|
| SDSD Teknisk | ”Note om teknisk dokumentation for arkitekturkomponenter – Operatørvurdering og prioritering” | http://arkitektur.sdsd.dk/twiki/bin/view/Servicedesk/Arkitekturkomponenter |
| SDSD OSS | Note on recommended Open Source Software licenses in Digital Health Denmark | http://arkitektur.sdsd.dk/twiki/bin/view/Operator/ArkitekturKompOSSLicens |
| PVIT-SERVICES | CPR Komponent Specifikation 0.3 | Vedlagt |
| DetGodeCPR | Det Gode CPR.doc | Vedlagt |

# Dokumenthistorik

## Dokumentplacering

Kilden til dette dokument vil blive placeret på www.nsi.dk.

## Revisionshistorik

| Revisionsnummer | Revisionsdato | Oversigt over rettelser | Rettet af | Rettelser markeret |
|---|---|---|---|---|
| 0.1 | 04/08-2011 | Første udkast | CHE | |