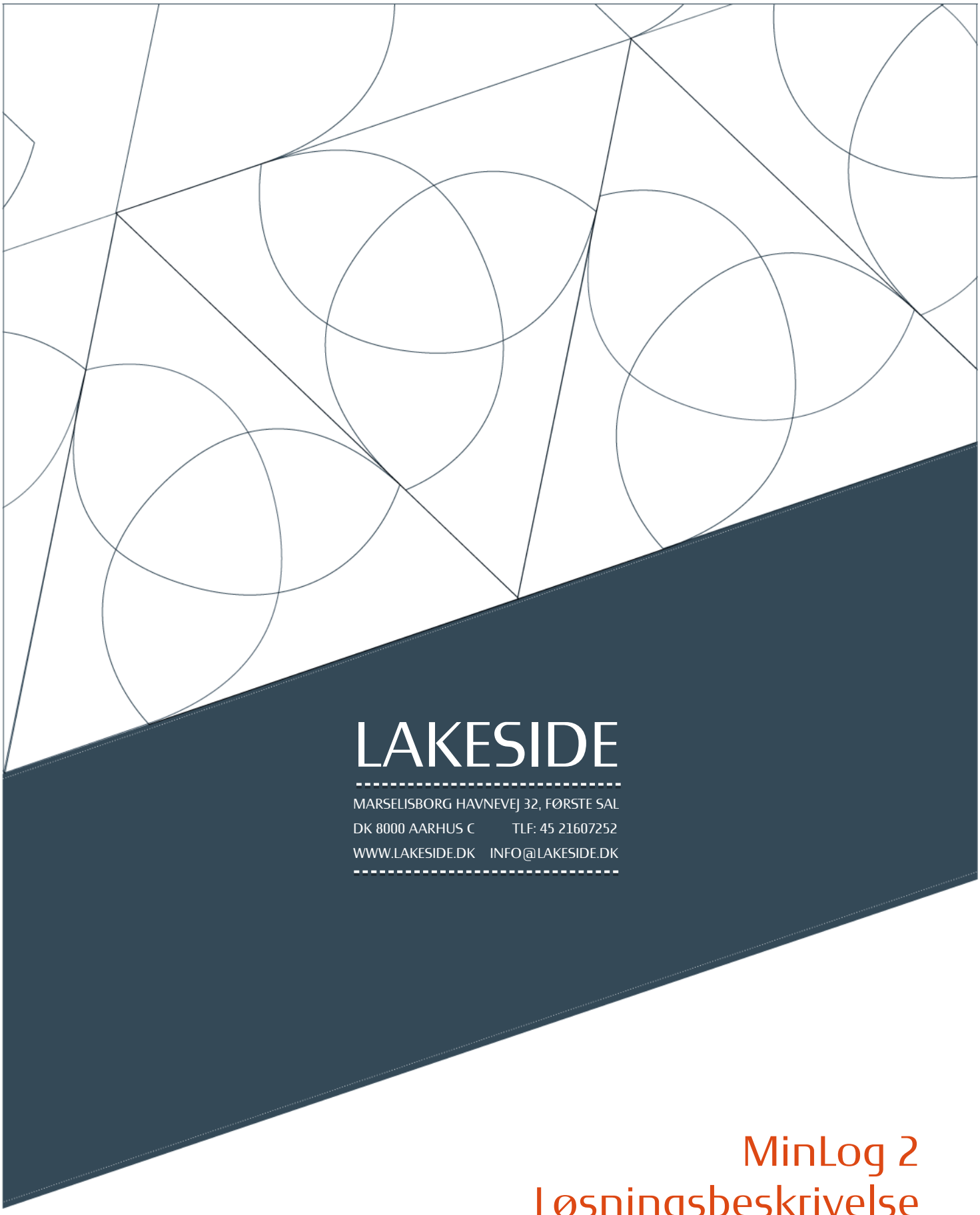


LAKESIDE

MARSELISBORG HAVNEVEJ 32, FØRSTE SAL
DK 8000 AARHUS C TLF: 45 21607252
WWW.LAKESIDE.DK INFO@LAKESIDE.DK

MinLog 2
Løsningsbeskrivelse

Dokumenthistorik

Version	Dato	Ansvarlig	Beskrivelse
0.1	2015-11-13	TKN	Udkast til snitfladespecifikation
0.2	2015-12-16	ANNI	Tilføjelser af ny grafik, leverancekrav, svartider og datamængder
0.3	2016-01-12	TKN	Opdateret med kommentarer fra TSO
0.4	2016-03-04	TKN	Opdateret med performancetal og datamængder
0.5	2016-03-17	ANNI	Opdateret sikkerhedsafsnit
0.9	2016-05-10	TKN	Opdateret efter høring. ”Audience” flag ændret til ”Filter” og beskrivelse udvidet. Privatmarkering, samtykke og værdispring ændret og udvidet. EventDateTime ændret til DateTime eller From- og ToDateTime. Ændret tal for databasestørrelse. Mindre ændringer og præciseringer.
1.0	2016-05-20	TKN	Tilføjet præcisering omkring anonymisering i borgeropslag og note omkring afklaring af hvorvidt alle former for værger findes i CPR-registret.
1.1	2016-05-30	TKN	Erstatte forældre-rolle med forældre-myndighedsindehaver. Præciseret værge-rolle. Udvidet filter for prævention. Fjernet eksempler for filtrering/sammenkædning, tekst skal stå i vejledningsdokument.
1.2	2016-09-01	TKN	Opdateret med funktionalitet til: • Gruppering på dato, aktører og organisation • Tal for antal logninger indeholdt i gruppe i svar (NumberOf-LogDataEntries) • Filtrering på privatmarkering, værdispring og samtykke i opslag Ændringer fra 1.1 til 1.2 er i denne version markeret med blå skrift.
1.3	2016-09-09	TKN	Opdateret med: • Note omkring beskyttelse af sundhedspersoners identitet og format af PersonIdentifier og OnBehalfOfPersonIdentifier Ændringer fra 1.1 til 1.2 eller 1.3 er i denne version markeret med blå skrift.

1.4	2016-10-14	TKN	Opdateret med slettejob, afsnit 7.
1.5	2017-01-31	TKN	Rettet datamængder og kaldmængder afsnit 11 på baggrund af tal fra Netic, ændringer markeret med grøn skrift.
1.6	2017-03-24	TKN	Se ændringslog 12.1 Ændringer til version 1.6, 2016-03-24
1.7	2017-05-09	TKN	Reason-felt tilføjet, se 12.2 Ændringer til version 1.7, 2017-05-09

Indholdsfortegnelse

1 Indledning

I forbindelse med et tidligere projekt i NSI og i forbindelse med den igangværende konsolidering af PEM og FMK, er der blevet etableret en national it-service til opsamling af log-data på NSP. Hensigten er at skabe et samlet sted, hvor log-data kan afleveres og hentes af relevante systemer.

Servicen er i forbindelse med PEM-konsolideringen blevet trykprøvet og FMK, DDV, Recept-modulet og CTR har taget komponenten i anvendelse. Samtidig har Sundhed.dk omlagt deres nuværende præsentationsløsning, så log-data fra FMK, Vaccinationsregistret og Tilskuds-ansøgningsservicen alle rekvireres i den centrale service.

Da hensigten er at udbrede denne løsning til den resterende del af sundhedsvæsenet, kan den nuværende implementering betragtes som en “pilotafprøvning”.

MinLog har bl.a. vist, at der er behov for at få revideret løsningen, så den bliver mere brugervenlig, og både for borger og sundhedsfaglige kan understøtte gruppering af log-data med folde-ud muligheder etc. Der er med den nuværende løsning problemer med forældremyndighedsindehaveres og værgers adgang til loggen. Her ud over bør opslag fra disse (og borgeren selv) også logges, så misbrug og identitetstyveri kan opdages.

Log-data anvendes i forskellige sammenhænge:

- Borgerrettet i ”MinLog”, til at borgeren kan se hvilke opslag der er foretaget på borgerens sundhedsdata, evt. også såfremt borgeren optræder som forældremyndighedsindehaver, fuldmagtshaver eller værge.
- Og i medhjælpsloggen til at autoriserede sundhedspersoner kan se hvad deres evt. medhjælpere slår op på deres vegne.
- Eventuelt (som option), at samtlige aktører kan se hvad der er logget omkring aktørens opslag, dvs. til ”register-indsigt”.

Enkelte dele af teksten er markeret med grå, hvor teksten omhandler optioner.

2 Introduktion

Dokumentet her er udgør en løsningsbeskrivelse for MinLog 2, den udgave af MinLog der aktuelt er i drift betegnes i dette dokument ”MinLog 1” for at tydeliggøre forskellen. På baggrund af en endelig løsningsbeskrivelse udarbejdes der en egentlig snitfladespecifikation, samt et dokument med vejledninger og retningslinjer. Samlet udgør de snitfladespecifikation og ”vejledninger og retningslinjer” en specifikation af anvendelse af MinLog 2.

Løsningsbeskrivelsen har hovedvægt på at beskrive den tekniske funktionalitet, herunder snitflader på et overordnet niveau, samt virkemåder for MinLog 2.

Dokumentet er ikke en komplet snitfladebeskrivelse. Der vil være en række felter, hvor indhold fastlægges ved implementering, f.eks. XML-skemabeskrivelser, eller beskrives i vejledninger og retningslinjer.

Læserne forventes bekendt med de overordnede tekniske forudsætninger for services NSP'en, herunder NSP'ens husregler.

2.1 Termer

Værdispring: Defineret i sundhedslovens §42a stk 5: ”...hvis indhentningen er nødvendig til berettiget varetagelse af en åbenbar almen interesse eller af væsentlige hensyn til patienten, herunder en patient, der ikke kan varetage sine interesser, sundhedspersonen eller andre patienter.”

2.2 Referencer

- MinLog 1:
  https://svn.nspop.dk/public/components/minlog-reg/latest/doc/
  https://svn.nspop.dk/public/components/minlog-ws/latest/doc/
- Den gode webservice (anvendte version er 1.0.1):
  http://www.medcom.dk/wm110731
- NSP husregler (aktuelle version på tidspunket dette dokument skrives er 1.7):
  https://www.nspop.dk/display/web/Husregler
- Sundhedsloven:
  https://www.retsinformation.dk/Forms/R0710.aspx?id=152710

2.3 Afgrænsninger

2.3.1 MinLogRegistrationClient

Til MinLog 1 er der lavet et ”MinLogRegistrationClient” API til Java-klienter. Dette API udgør den offentlige snitflade, frem for en WSDL. I MinLog 2 vil der ikke blive lavet et tilsvarende API, men den offentlige snitflade vil være WSDL'en.

2.3.2 Transport-funktionalitet

MinLog 2 projektet omfatter udvidelse af services, som beskrevet i afsnit 4 Registreringsservice og 6 Opslagsservice, herunder flere felter i log-data, mere fleksible opslagsmuligheder og en udvidet sikkerhedsløsning. Som konsekvens deraf vil der skulle foretages mindre ændringer i den Splunk-funktionalitet, der transporterer log-data.

En grundlæggende ændring af transportfunktionaliteten til andet end Splunk er ikke omfattet af den her beskrevne løsning, og transportfunktionaliteten er kun overordnet gennemgået i afsnit 3.2 Transportfunktionalitet.

Bemærk at transportfunktionalitet her ikke er det samme som transportlaget i OSI 7-lags-modellen.

2.3.3 Vejledninger og retningslinjer

Som supplement, til den tekniske funktionalitet beskrevet i dette dokument, vil der blive udarbejdet et separat dokument med ”Vejledninger og retningslinjer” for logning. Herunder hvad der skal logges i forskellige typer af systemer såfremt MinLog 2 anvendes, hvordan data afleveres osv.

Krav til logning, eller vejledninger og retningslinjer, findes ikke i dette dokument, ud over hvad der er nødvendigt for at beskrive funktionaliteten.

2.3.4 Beskyttelse af sundhedspersoners identitet

Et af formålene med MinLog 2 er at sikre beskyttelse af sundhedspersoners identitet. Der foregår en afklaring omkring privacy-forhold omkring beskyttelse af sundhedspersonens identitet, hvis handlinger udstilles i MinLog og medhjælpsloggen. Der skal findes et passende kompromis mellem behov for indhold i opslag i MinLog og medhjælpsloggen og beskyttelse af oplysninger omkring sundhedspersonen.

Forhold omkring beskyttelse af sundhedspersoners identitet er ikke beskrevet i dokumentet her, men services skal være tilstrækkeligt fleksible til at kunne håndtere at al data returneres (f.eks. i det sundhedsfaglige opslag) og at der kun returneres overordnet information (f.eks. i borgeropslaget).

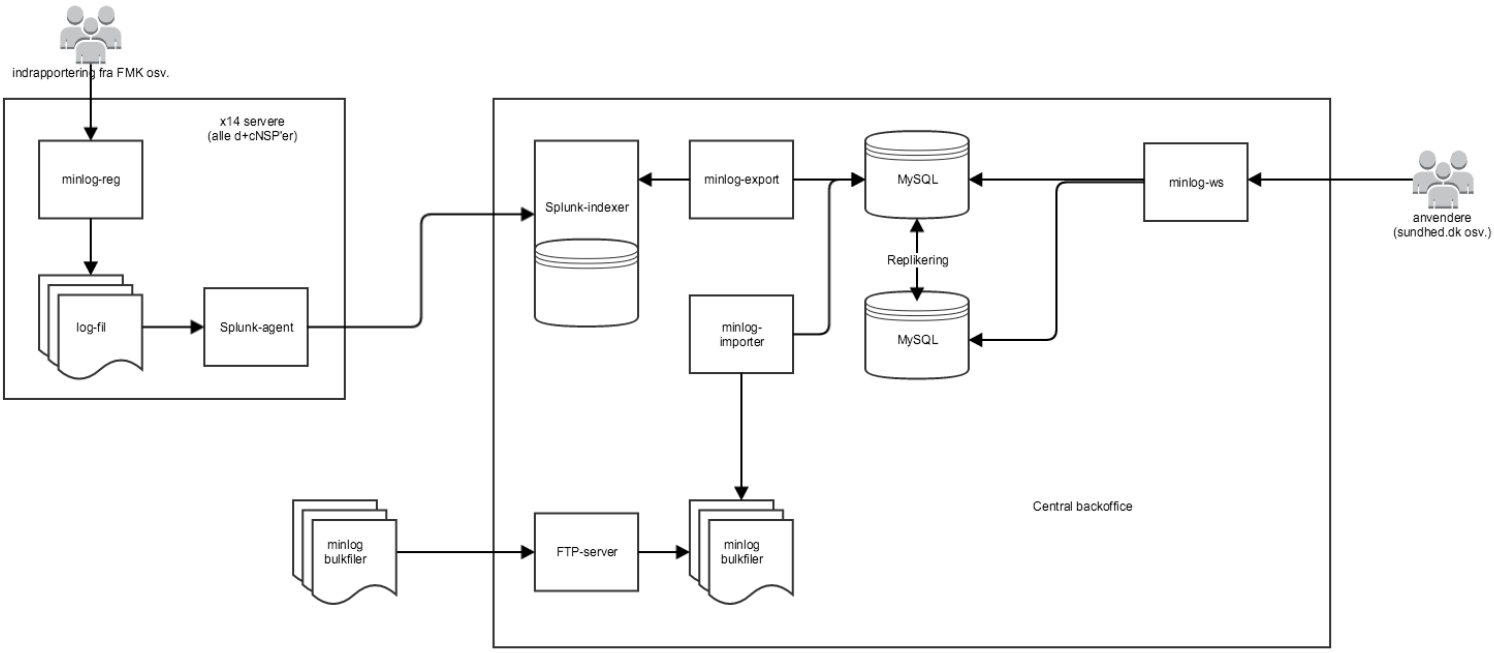
2.3.5 Fuldmagtshåndtering

Der kan på et senere tidspunkt overvejes at skabe integration til en fællesoffentlige fuldmagts-service i forbindelse med opslagsservicen. Aktuelt er processen omkring en fællesoffentlig fuldmagtsservice dog ikke tilstrækkeligt fremskreden til at integration hertil kan tilføjes som krav eller option.

3 Kontekst

3.1 Systemer

Figuren herunder viser det eksisterende systemkontekst som de aktuelle services, registreringsservicen og de to opslagsservices, udstilles i.



Figur 1: Systemkontekst som registreringsservicen og de to opslagsservices udstilles i, som det ser ud for MinLog 1. Registreringsservicen findes hvor der på figuren er vist "Indrapportering fra FMK osv, og opslagsservices hvor der på figuren er vist "anvendere".

Registreringsservicens eksisterende version anvendes af FMK, receptmodulet, DDV og TAS. Aktuelt er den yderligere ved at blive taget i brug af CTR. Det er tanken at en ny registreringsservice fremover skal anvendes af flere både interne og eksterne systemer.

Opslagsservices anvendes af Sundhed.dk og FMK-online. I Sundhed.dk vises udelukkende data fra MinLog2 opslagsservices, indeholdende data omkring sundhedsfagliges opslag på borger-data. I FMK-online vises yderligere opslag foretaget af en medhjælp for en autoriseret sundhedsperson.

Log-data bliver pushet asynkront fra de decentrale NSP'er samt cNSP'en til NSP backoffice. Der kan ikke gives garanti på frekvensen af opsamlingerne af MinLog data fra de decentrale platforme. Dog vil der erfaringsmæssigt gå maksimalt et minut før data fra decentrale miljøer er tilgængelig.

3.2 Transportfunktionalitet

Som beskrevet i afsnit 2.3 Afgrænsninger er grundlæggende ændring af transportfunktionaliteten ikke omfattet af den her beskrevne løsning. Væsentligt er dog at datasættet udvides, hvorved format for logfil m.v. også skal udvides.

Transportfunktionalitet består af en Splunk-agent og en Splunk-indexer, sammenhængen fremgår på Figur 1 side 8. Strengen der omhandler importen af bulkfiler vil udgå, idet formålet med denne er at importere fra PEM, og denne import nu er lukket.

Transportfunktionalitet skal ikke beskrives yderligere i denne sammenhæng.

3.3 Aktører

3.3.1 Autoriseret sundhedsperson

En autoriseret sundhedsperson er f.eks. en læge, sygeplejerske, tandlæge m.v. Autoriserede sundhedspersoner har adgang til at anvende medhjælpere, men har også en forpligtigelse til at sikre at medhjælpere kun udfører handlinger i overensstemmelse med de anvisninger medhjælpen har fået.

En autoriseret sundhedsperson skal have følgende muligheder for opslag:

- Opslag i medhjælpsloggen, hvor en autoriseret sundhedsperson kan se, hvad hver enkelt medhjælp har udført af handlinger på vegne af den autoriserede sundhedsperson.
- (Option) Den autoriserede sundhedsperson skal have mulighed for at slå op for at se hvilke log-data der er registreret i MinLog 2 at vedkommende har set, oprettet eller opdateret. Dvs. opslag hvor både en sundhedsperson og en medhjælp kan se, hvad der er registreret omkring denne.

3.3.2 (Option) Medhjælp

Medhjælpen er kun en aktør i MinLog 2-sammenhæng såfremt opslaget beskrevet i Eksempel 3: Opslag for ”register-indsigt” implementeres.

Medhjælpere agerer på vegne af en autoriseret sundhedsperson. Medhjælpen kan selv være en autoriseret sundhedsperson, men kan også være uden autorisation.

Medhjælpere skal have følgende muligheder for at slå op:

- Medhjælpen skal have mulighed for at slå op for at se hvilke log-data der er registreret at vedkommende har set, oprettet eller opdateret. Herunder hvilken autoriseret sundhedsperson opslaget er sket under ansvar af.

Hvis f.eks. en sygeplejerske har en medhjælp vil sygeplejersken selv i den sammenhæng ikke optræde som medhjælp. Dvs. at medhjælpere til medhjælpere skal ikke understøttes.

3.3.3 Borger

Borgeren (eller patienten) optræder i MinLog 2-sammenhæng hovedsageligt som personen, hvis data der slås op på.

- Borgeren skal have mulighed for at slå op i MinLog for at se, hvilke aktører der har set, oprettet eller opdateret borgerens sundhedsdata.
- Borgeren kan desuden optræde som forældremyndighedsindehaver, værge eller fuldmagtshaver, og skal derfor desuden have mulighed for at slå op på hvilke opslag borgeren evt. selv har foretaget som forældremyndighedsindehaver, værge eller fuldmagtshaver.

3.3.4 Forældremyndighedsindehaver

Forældremyndighedsindehaver er en borger, og kan slå op på MinLog for en anden borger (barn), såfremt der findes stamdata i CPR-registret, der viser en forældremyndighedsrelation.

Stamdata i CPR-registret indeholder forældremyndighedsrelationer for børn født maj 2004 og senere. Børn født tidligere findes der kun undtagelsesvist en registreret en forældremyndigheds-relation for i CPR-registret.

De gældende regler for aldersgrænser for hvornår forældremyndighedsindehaver må se deres barns sundhedsdata, er fra barnets fødsel, hvor barnets CPR-nummer også oprettes, til barnet fylder 15 år. Fra den unge er mellem 15 år og 18 år, er det muligt at få udstede et særligt "ung under 18"-NemID som kan benyttes til login. Forældremyndighedsindehaver kan ikke se den unges sundhedsdata efter de er fyldt 15 år.

Forældremyndighedsindehavere (samt værger) må ikke se deres børns præventionsmidler, informationer relateret til aborter, evt. blodtransfusioner m.v, heller ikke selv om barnet er under 15 år. Logdata der omhandler præventionsmidler m.v. skal filtreres fra i data returneret når forældremyndighedsindehaver slår op på Min Log 2. Hertil anvendes en markering som beskrevet under 4.2.3 Filter flag – for data ikke i forældremyndighedsindehaver-opslag.

3.3.5 Værge

En borger kan være værge for personer, der har fået frataget retlig handleevne. Der findes andre typer af værgemål, I MinLog 2-sammenhæng er det udelukkende værger for personer der har fået frataget retlig handleevne der er relevant. I dette dokument vil det alle steder være denne type værge der menes, når værge omtales.

I MinLog 2 kan værger for personer, der har fået frataget retlig handleevne slå op i MinLog 2 for denne personen som denne er værge for.

Oplysninger om relationen findes i CPR-registret, som er tilgængeligt via stamdata på NSP.

Der gælder samme forhold omkring børns præventionsmidler m.v. for værge som beskrevet under Forældremyndighedsindehaver.

3.3.6 (Option) Fuldmagtshaver

Som option kan MinLog evt. udvides med funktionalitet omkring fuldmagtshaver. Hertil anvendes fuldmagtsservicen udstillet af Digitaliseringsstyrelsen. Fuldmagtshaver er selv en borger og kan slå op i MinLog 2 for en anden borger.

Børn under 15 skal ikke kunne registrere fuldmagtshaver, forhold omkring børns præventionsmidler (flaget "Ikke forældremyndighedsindehaver") m.v. er derfor ikke relevante i denne sammenhæng.

4 Registreringsservice

Registreringsservicen kaldes af systemer for at foretage registrering af opslag på borgerens sundhedsdata. Der udstilles kun en enkelt service, der kan anvendes både til registrering af enkelte opslag og til registrering af en samlet række opslag. Der er ingen restriktioner på, at opslag skal være foretaget på samme borgers CPR-nummer, af samme bruger m.v.

4.1.1 Sikkerhedsmodel

Registreringsservices kræver anvendelse af virksomheds-, funktions- eller medarbejdercertifikat. Servicen overholder Den Gode Web Service 1.0.1, og kræver:

- At enten det kaldende system er autentificeret af STS'en (sikkerhedsniveau 3) eller at den kaldende bruger er autentificeret af STS'en (sikkerhedsniveau 4)
- At den kaldende organisation er autoriseret, hvilket kontrolleres vha. en whiteliste på CVR-niveau

Servicekald efter Den Gode Webservice 1.0.1 består af en sikkerhedsheader med indlejret STS-signeret sikkerhedstoken (SOSI idkort), en MedCom-header og et body element.

Indholdet i MedCom-headeren er specificeret i Den Gode Webservice. For det i sikkerhedsheaderen medsendte STS-signerede SOSI idkort valideres signatur, trust, tidsmæssig gyldighed og autentifikationsniveau.

4.2 Registreringskald

Der udstilles en service til at foretage registrering af opslag. Servicen skal anvendes af FMK, receptmodulet, DDV, TAS og CTR. Registreringsservicen kan fremover også blive anvendt af flere både interne og eksterne systemer.

I kaldet til servicen indeholder rodelementet LogDataAddRequest et eller flere LogDataEntry-elementer med log-data for en handling. Hvert LogDataEntry-element indeholder først et Source- og et Destination-element.

4.2.1 Source- og destination-systemer

Source-elementet indeholder information omkring systemet der har kaldt servicen. Destination-elementet indeholder information omkring systemet der udstiller servicen og som har kaldt MinLog-registreringsservicen, samt information der er dannet af dette system.

Det er det system der "ejer" data, der er ansvarlig for at logge. Dvs. kalder et EPJ-system FMK er det FMK's ansvar at logge, og EPJ-systemet skal ikke foretage en logning. Tilsvarende hvis der slås op i data i EPJ-systemet alene, og EPJ-systemet afleverer log-data til MinLog 2, skal denne handling logges af EPJ-systemet.

Source-systemet, der kalder servicen, kan igen være kaldt af et andet system. For at understøtte at services (nu eller i fremtiden) kan få overført metadata omkring kæden af services, er det muligt at et Source-element igen kan indeholde et Source-element. Registreringsservicen kan dermed kaldes med information der muliggør at sammenkæde handlinger i en kæde af systemer, hvordan er beskrevet i afsnittet 5.2 Sammenkædning af log-data. Eventuelt kan Source-elementet være udeladt, f.eks. for systemer der anvendes direkte af brugeren og ikke kaldes af et andet system.

4.2.2 Filter flag – for data ikke relevant i borgeropslag

Der kan forekomme typer af opslag der ikke er relevante i borgeropslag, men skal returneres i sundhedsfaglige opslag. Eksempelvis er apotekets opslag på en liste af "adresserede" recepter

relevante i medhjælpsloggen, men ikke for borgeren, idet det apoteket ikke har set væsentlig følsom information, og opslaget vil være ”støj” i borgerens opslag.

At data ikke er relevant i borgeropslaget angives i Filter-element som:

```
<Filter>Ikke borger</Filter>
```

Det er muligt at angive mere end et filter-element.

4.2.3 Filter flag – for data ikke i forældremyndighedsindehaver-opslag

Som tidligere nævn under 3.3.4 Forældremyndighedsindehaver er det et krav, at når forældre-myndighedsindehaver slår på log data for deres børn under 15 år, skal eventuelle logdata der omhandler prævention, aborter, blodtransfusioner m.v. filtreres fra.

MinLog 2 har ikke mulighed for at vurdere om der ud fra lægemidlet eller evt. ud fra organisationen (f.eks. ”Sexologisk Klinik”), kan udledes at data indeholder data omkring prævention m.v, det ikke skal vises for forældremyndighedsindehaver. Ansvaret for at flage dette kan derfor kun placeres hos systemet der afleverer logdata. Se evt. afsnit 5.4.1 Filter ”Ikke forældremyndighedsindehaver”

”Ikke forældremyndighedsindehaver”-flaget angives i et filter-element som:

```
<Filter>Ikke forældremyndighedsindehaver</Filter>
```

Det er muligt at angive mere end et filter-element.

4.2.4 Kritikalitet og "tilføjelse" – for eksplicit samtykke, opslag på privat-markerede data mm.

Privatmarkerede data angives med et flag for niveau af kritikalitet som ”Privatmarket”. Flaget er optionelt, og er værdien ikke angivet svarer dette til at der ikke er privatmarkerede data.

Registreringen af opslag på privatmarkerede data sker som en kombination af kritikalitet og en tilføjelse omkring samtykke eller værdispring.

Eksempelvis angives opslag på privatmarkerede data med samtykke som:

```
<Criticality>Privatmarkeret</Criticality>
<Addition>Samtykke</Addition>
```

Begge felter er optionelle, og kombinationen af de to felter fortolkes på følgende måde:

Criticality	**Addition**	**Fortolkning**	**Eksempel**
Ingen angivelse	Ingen angivelse	Opslag på ikke privatmarkerede data som aktøren normalt vil anvende ud fra sin autorisation eller arbejdssituation. Borgerens samtykke er ikke nødvendigt.	En læge slår op på FMK på et medicinkort hvor der ikke findes privatmarkerede data. En læge slår op på FMK på et medicinkort hvor der findes privatmarkerede data, men lægen vælger ikke at se de privat-markerede data (lægen vurdere at dette er forsvarligt i situationen).

			Læges medhjælp der på samme måde slår op. Farmakonom eller farmaceut på apotek, der slår op på recept-data for at foretage en udlevering.
Ingen angivelse	Samtykke	Opslag på ikke privatmarkerede data som aktøren normalt ikke vil anvende ud fra sin autorisation eller arbejdssituation. Borgeren har givet sit eksplicitte samtykke, se afsnit	En farmaceut på apotek der efter aftale med borgeren laver en medicingennemgang ud fra data på FMK. Dvs. at farmaceuten slår op på alle aktuelle lægemiddelordinationer på FMK. Derved foretages et bredere opslag, i modsætning til apotekets normale opslag på data der aktuelt skal anvendes til at udlevere et eller flere lægemidler.
Ingen angivelse	Værdispring	Opslag på ikke privatmarkerede data som aktøren normalt ikke vil anvende ud fra sin autorisation eller arbejdssituation. Opslaget er sket med værdispring.	Kombinationen bør aktuelt ikke anvendes. Aktører bør i kraft af deres autorisation eller arbejdssituation ikke have behov for værdispring på normale data.
Privat-markeret	Ingen angivelse	Opslag på privatmarkerede data. Borgeren har ikke givet samtykke, og værdispringsreglen er ikke anvendt	Aktøren har slået op på privatmarkerede data, uden at indhente borgerens samtykke eller at markere værdispring. Opslaget må derfor indtil andet er vist betraget som et regelbrud!
Privat-markeret	Samtykke	Opslag på privatmarkerede data. Borgerens har givet sit eksplicitte samtykke hertil.	En læge slår op på FMK på et medicinkort hvor der findes privatmarkerede data, og lægen vælger at se de privatmarkerede data, efter at borgeren har givet sit eksplicitte samtykke hertil.
Privat-markeret	Værdispring	Opslag på privatmarkerede data.	En læge slår op på FMK på et medicinkort hvor der findes privatmarkerede data, og lægen vælger at se de privatmarkerede data, på trods af at patienten er

			bevidstløs og ikke kan give sit samtykke, idet lægen vurderer dette er væsentligt af hensyn til patienten. Lægen anvender værdispringsreglen.

4.2.5 Eksempler

Eksemplerne herunder viser indholdet af et forespørgsels-dokument, hvor header-elementer og namespaces er udeladt.

Navngivningen af elementerne er generelt tilpasset FMK's praksis, dvs. noget kortere end de tidligere OIO-navne i MinLog 1. Indhold og rækkefølge svarer ellers til MinLog 1, dog er der strammet op i skemadefinitionen, således at systemet, der kalder servicen, selv kan validere, at formatet er korrekt.

4.2.6 Eksempel 1: Logning af direkte opslag

Herunder ses et eksempel på et direkte opslag, f.eks. hvor en bruger har slået op i et EPJ-system, og EPJ-systemet logger dette til MinLog.

```
<LogDataAddRequest>
     <LogDataEntry>
          <Destination>
               <SystemName>COSMIC</SystemName>
               <Activity>Medicinoversigt</Activity>
               <DateTime>2015-11-13T13:14:15Z</DateTime>
               <OrganisationId source="SOR">240971000016006</OrganisationId>
               <OrganisationName>Sygehus Sønderjylland</OrganisationName>
               <PersonIdentifier source="CPR">1111111118</PersonIdentifier>
               <SequenceNumber>1</SequenceNumber>
               <CorrelationId>07f59cdb-28f5-4bab-ac18-fd618235d386</CorrelationId>
               <UserPersonIdentifier source="CPR">0101014444</UserPersonIdentif...
               <OnBehalfOfPersonIdentifier source="CPR">1212128888</OnBehalfOfP...
               <Filter>Ikke borger</Filter>
          </Destination>
     <LogDataEntry>
<LogDataAddRequest>
```

4.2.7 Eksempel 2: Logning af opslag fra andet system

Eksempel på kald hvor source-systemet kalder destination-systemet FMK, dvs. hvor der er en simpel kæde af kun to systemer. Kaldet fra source-systemet har her indeholdt et CorrelationId, der genbruges af destination-systemet.

```
<LogDataAddRequest>
     <LogDataEntry>
          <Source>
               <SystemName>COSMIC</SystemName>
               <CorrelationId>07f59cdb-28f5-4bab-ac18-fd618235d386</CorrelationId>
          </Source>
          <Destination>
               <SystemName>FMK</SystemName>
               <Activity>Hent medicinkort</Activity>
               <Criticality>Privatmarkeret</Criticality>
```

```
                <Addition>Samtykke</Addition>
                <FromDateTime>2015-11-13T13:14:15Z</FromDateTime>
                <ToDateTime>2015-11-13T13:21:41Z</ToDateTime>
                <OrganisationId source="SOR">240971000016006</OrganisationId>
                <OrganisationName>Sygehus Sønderjylland</OrganisationName>
                <PersonIdentifier source="CPR">1111111118</PersonIdentifier>
                <SequenceNumber>1</SequenceNumber>
                <CorrelationId>07f59cdb-28f5-4bab-ac18-fd618235d386</CorrelationId>
                <UserPersonIdentifier source="CPR">0101014444</UserPersonIdenti...
                <OnBehalfOfPersonIdentifier source="CPR">1212128888</OnBehalfOf...
          </Destination>
     <LogDataEntry>
<LogDataAddRequest>
```

4.2.8 Eksempel 3: Logning af opslag hvor tre systemer er involveret

Endeligt ses her et eksempel hvor tre systemer er involveret: En mobil løsning til et EPJ-system har kaldt EPJ-systemet, der igen kalder FMK. Det viste eksempel viser hvorledes FMK kan foretage logningen, med information omkring kæden af systemet. Kaldet har her indeholdt et CorrelationId, der genbruges af destination-systemet.

```
<LogDataAddRequest>
     <LogDataEntry>
          <Source>
               <Source>
                    <SystemName>Mobil-X</SystemName>
                    <CorrelationId>07f59cdb-28f5-4bab-ac18-fd618235d386</CorrelationId>
               </Source>
               <SystemName>Cosmic</SystemName>
               <CorrelationId>07f59cdb-28f5-4bab-ac18-fd618235d386</CorrelationId>
          </Source>
          <Destination>
               <SystemName>FMK</SystemName>
               <Activity>Hent medicinkort</Activity>
               <DateTime>2015-11-13T13:14:17Z</DateTime>
               <OrganisationId source="SOR">240971000016006</OrganisationId>
               <OrganisationName>Sygehus Sønderjylland</OrganisationName>
               <PersonIdentifier source="CPR">1111111118</PersonIdentifier>
               <CorrelationId>07f59cdb-28f5-4bab-ac18-fd618235d386</CorrelationId>
               <SequenceNumber>1</SequenceNumber>
               <UserPersonIdentifier source="CPR">0101014444</UserPersonIdentif...
          <LogDataEntry>
     </Destination>
<LogDataAddRequest>
```

4.2.9 Indhold i kald-dokumentet

Følgende elementer anvendes i registreringen:

Navn	**Beskrivelse**	**Definition**	**Kardinalitet**
LogDataAdd-Request	Rod-element for forespørgslen. Indeholder 1 eller flere LogDataEntry-elementer		1
LogDataEntry	Indeholder data til registrering af en handling.		1-*

Source	Element der indeholder information omkring det kaldende system, kilde systemet. Kildesystemet kan udelades i de tilfælde en bruger slår direkte op på systemet.		0-1
Source/Source[/...]	Source-elementet kan igen indeholde et source-element. Dette anvendes såfremt kildesystemet igen er kaldt af et andet system, som vist i 4.2.8 Eksempel 3: Logning af opslag hvor tre systemer er involveret		0-1
Source/ SystemName	Navn, evt. forkortet, for det anvendte kilde-system	Streng med max længde på 25 tegn	1
Source/ CorrelationId	Et teknisk id, medsendt fra kildessytemetet. Værdien anvendes til at identificere den sammenhæng som handlingen er gennemført i, eksempelvis et id for behandlingen eller indlæggelsen (EPJ) eller kontakten (LPS). Se afsnit 5.3 Gruppering af log-data. Systemet skal være unikt for det anvendte system.	Streng med max længde på 46 tegn.	0-1
Destination	Element der indeholder information omkring og fra det kaldte system, destinations-systemet, dvs. det system der foretager logningen.		1
Destination/ SystemName	Navn, evt. forkortet, for det anvendte system, f.eks. ”FMK”.	Streng med max længde på 25 tegn	1
Destination/ Activity	Tekst der beskriver den handling, som brugeren har udført eller forsøgt udført på kildesystemet. Eksempelvis ”hent medicinkort” på FMK. Datasættet fastlægges endeligt i forbindelse med udarbejdelse af vejledninger og retningslinjer.	Streng, max længde på 75 tegn	1

Destination/ Reason	Optionel tekst der beskriver årsagen til den handling, som brugeren har udført eller forsøgt udført på kildesystemet. Teksten anvendes kun i særlige tilfælde, hvor borgeren ikke har direkte kontakt til brugeren, eksempelvis ved support, fejlsøgning og tilskudsansøgninger. Teksten udfyldes af systemet, som en eller få forud-definerede tekster, og må ikke være en fritekst udfyldt af brugeren.	Streng, max længde på 50 tegn	0-1
Destination/ Criticality	Niveau for kritikalitet, aktuelt kun ”Privatmarkeret” Se 4.2.4 Kritikalitet og ”tilføjelse” – for eksplicit samtykke, opslag på privatmarkerede data mm.	Streng, defineret som en union af en enumeration af niveau for kritikalitet, og en Streng med max længde 50 tegn	0-1
Destination/ Addition	Angivelse af type af opslag som tilføjelse til kritikalitet, aktuelt ”Samtykke” eller ”Værdispring”	Streng, defineret som en union af en enumeration, og en Streng med max længde 50 tegn	0-1
Destination/ DateTime	DateTime-elementet indeholder en tids-angivelse for opslag på eller forsøg på handling på borgerens data. Dato og tid skal angives i zulu tid / UTC. I praksis gøres dette ved at tilføje Z efter tidsangivelsen, som vist i eksemplet, samt at korrigere for de 1-2 timers forskel (henholdsvis vinter- og sommertid) der er mellem dansk tid og UTC. Tiden angives med en præcision i sekunder.	DateTime med pattern der sikrer anvendelse af zulu-tid	0-1 Enten skal DateTime eller (FromDateTime og ToDateTime) forekomme. Dette skal modelleres i XML-skemaet.
Destination/ FromDateTime	Som alternativ til DateTime herover kan der være foretaget en gruppering af f.eks. FMK inden data er afleveret til MinLog 2. I så fald kan FromDateTime og ToDate-Time angive det interval hvor hændelserne er sket.	DateTime med pattern der sikrer anvendelse af zulu-tid	0-1 Enten skal DateTime eller (FromDateTime og ToDateTime) forekomme.

	FMK kan gruppere samme type service-kald foretaget inden for et tidsrum på samme borger og af samme aktør m.v.		Dette skal modelleres i XML-skemaet.
Destination/ ToDateTime	Se FromDateTime herover.	DateTime med pattern der sikrer anvendelse af zulu-tid	0-1 Enten skal DateTime eller (FromDateTime og ToDateTime) forekomme. Dette skal modelleres i XML-skemaet.
Destination/ OrganisationId	ID for brugerens organisation. Elementet skal forekomme for alt andet end private borgeres opslag.	Streng på max 200 tegn	0-1
Destination/ OrganisationId attribut source	Kilde til ID for brugerens organisation, defineret som en attribut på OrganisationId-elementet.	Streng, defineret som en union af en enumeration af SOR, SKS, Yder, CVR-P, CVR, Kommunekode og en Streng med max længde 200	1 (attributten er obligatorisk på elementet OrganisationId, når elementet forekommer)
Destination/ OrganisationName	Navn på brugens organisation , Elementet skal forekomme for alt andet end private borgeres opslag.	Streng med max længde 200	0-1
Destination/ PersonIdentifier	CPR-nummer eller evt. erstatnings-CPR-nummer på borgeren. Se 4.4 Valideringsregler	Streng af længde 50	1
Destination/ PersonIdentifier attribut source	Kilde til ID for borgerens CPR-nummer eller erstatnings-CPR-nummer. F.eks. ”CPR” for almindelige CPR-numre i CPR-registret. Se 4.4 Valideringsregler	Streng, defineret som en union af en enumeration af CPR, E-CPR, ... og en Streng med max længde 200	1 (attributten er obligatorisk på elementet PersonIdentifier, når elementet forekommer)

Destination/ PersonName	Borgerens navn. Optionelt men krævet af anvendersystemet hvor source ikke er CPR.	Streng med max længde 147 tegn (max 4*36 tegn + 2 skilletegn jf. CPR snitflader)	0
Destination/ CorrelationId	Et teknisk id, medsendt fra kildessytemetet. Værdien anvendes til at identificere den sammenhæng som handlingen er gennemført i, eksempelvis et id for behandlingen eller indlæggelsen (EPJ) eller kontakten (LPS). Se afsnit 5.3 Gruppering af log-data. Værdien skal være unik for det anvendte system.	Streng med max længde på 46 tegn.	0-1
Destination/ SequenceNumber	Et teknisk sekvens-nummer, angivet af afsender, der anvendes i forbindelse med fejlhåndtering. F.eks. et fortløbende nummer eller et uuid. Værdien skal være unikt i kaldet.	Streng med max længde på 36 tegn (svarende til at feltet evt. kan indeholde en uuid)	1
Destination/ UserPerson-Identifier	CPR-nummer eller evt. erstatnings-CPR-nummer på brugeren der har udført handlingen. En forekomst af CPR-nummer eller erstatnings-CPR-nummer er som udgangspunkt obligatorisk og valideres af registreringsservicen. Det kan være nødvendigt at supplere med yderligere id'er for personen. Eksempelvis et autorisationsnummer hvis aktøren har mere end én autorisation. Se 4.4 Valideringsregler	Streng af længde 50	1-*
Destination/ UserPerson-Identifier attribut source	Kilde til UserPersonIndentifier. F.eks. ”CPR” for almindelige CPR-numre i CPR-registret. Se 4.4 Valideringsregler	Streng, defineret som en union af en enumeration af CPR, eCPR, ... og en Streng med max længde 200	1 (attributten er obligatorisk på elementet UserPerson-Identifier, når elementet forekommer)
Destination/ UserPersonName	Brugerens navn. Optionelt men krævet af anvendersystemet hvor source ikke er CPR,	Streng med max længde 147 tegn	0

	Autorisation m.v.		
Destination/ UserRole	Brugerens rolle. Der vil være en sammenhæng til et evt. angivet autorisationsnummer, det er op til systemet der kalder registreringsservicen at sikre sammenhængen er korrekt.	Streng af længde 200 (svarende til FMK's RequestedRole)	0-1
Destination/ OnBehalfOf-PersonIdentifier	CPR-nummer eller evt. erstatnings-CPR-nummer på brugeren handlingen er udført på vegne af. Se 4.4 Valideringsregler	Streng med max længde 50	0-*
Destination/ OnBehalfOf-PersonIdentifier attribut source	Kilde til OnBehalfOfPersonIdentifier. F.eks. ”CPR” for almindelige CPR-numre i CPR-registret. Se 4.4 Valideringsregler	Streng, defineret som en union af en enumeration af CPR, eCPR, ... og en Streng med max længde 200	1 (attributten er obligatorisk på elementet OnBehalfOf-PersonIdentifier, når elementet forekommer)
Destination/ OnBehalfOf-PersonName	Navn svarende til ”på vegne af”. Optionelt men krævet af anvendersystemet hvor source ikke er CPR, Autorisation m.v.	Streng med max længde 147 tegn	0
Destination/ Filter	Et eller flere felter der anvendes til angivelse af hvilken målgruppe logningen skal filtreres fra for. Udelades feltet er der underforstået at logningen er relevant for alle. Eksempelvis er apotekets opslag på en liste af ”adresserede” recepter relevante i medhjælpsloggen, men ikke for borgeren, idet det apoteket ikke har set væsentlig følsom information, og opslaget vil være ”støj” i borgerens opslag.	Streng, aktuelt defineret som en union af en enumeration aktuelt indeholdende ” Ikke borger” , ”Ikke forældre-myndigheds-indehaver” og en Streng med max længde 50 tegn.	0-*

4.3 Svar

I svaret returneres der kun en værdi for antal LogDataEntry-elementer der er registreret. Eksempel på svar hvor alle LogDataEntry-elementer er registreret korrekt:

```
<LogDataAddResponse>
      <NumberAdded>12</NumberAdded>
```

```
<LogDataAddResponse>
```

I tilfælde af at en eller flere elementer er fejlet returneres yderligere information herom. I eksemplet herunder er et LogDataEntry-elementer registreret korrekt og et er fejlet:

```
<LogDataAddResponse>
      <NumberAdded>1</NumberAdded>
      <NumberFailed>1</NumberFailed>
      <FailedLogDataEntry>
            <SequenceNumber>42</SequenceNumber>
            <FaultCode>10012002</FaultCode>
            <Message>Ydernummer "23928392193" har ikke et korrekt format</Message>
      <FailedLogDataEntry>
<LogDataAddResponse>
```

Er der tale om at der er sket en generel fejl, f.eks. en skemavalideringsfejl, returneres der i stedet en fejlbesked efter ”Den Gode Webservice”-profileringen.

Følgende elementer returneres i svaret:

Navn	**Beskrivelse**	**Definition**	**Kardinalitet**
LogDataAdd-Response	Rod-element for svaret.		1
NumberAdded	Antal LogDataEntry registreret med succes	Integer	1
NumberFailed	Antal LogDataEntry registreret med med fejl	Integer	0-1
FailedLogData-Entry	Såfremt en registrering er fejlet indeholder elementet information herom		0-*
SequenceNumber	Svarer til teknisk sekvens-nummer, angivet af afsender.	Streng med max længde på 36 tegn (svarende til at feltet evt. kan indeholde en uuid)	1
FaultCode	Fejlkode. En endelig liste vil skulle udarbejdes og dokumenteres når servicen implementeres.	...	1
FaultText	Fejltekst. En endelig liste vil skulle udarbejdes og dokumenteres når servicen implementeres.	...	1

4.4 Valideringsregler

4.4.1 Validering af …PersonIdentifier-felter

Felterne PersonIdentifier, UserPersonIdentifier og OnBehalfOfPersonIdentifier anvendelse alle til at identificere en person, enten aktør eller borger/patient. Feltet er sammensat på den måde at attributten source definerer hvilken type af person-id feltet indeholder. F.eks:

```
<PersonIdentifier source="CPR">1111111118</PersonIdentifier>

<PersonIdentifier source="eCPR">1303171AA1</PersonIdentifier>

<PersonIdentifier source="Initaler">ÅA</PersonIdentifier>

<PersonIdentifier source="Autorisation">0BS3P</PersonIdentifier>
```

Ud fra source-attributten defineres indholdet, og dermed hvorledes værdien kan valideres:

CPR: `((((0[1-9]|1[0-9]|2[0-9]|3[0-1])(01|03|05|07|08|10|12))|((0[1-9]|1[0-9]|2[0-9]|30)(04|06|09|11))|((0[1-9]|1[0-9]|2[0-9])(02)))[0-9]{6})`

eCPR: `([0-9]|[A-Z]){10}`

Autorisation: `([0-9]|(B|C|D|F|G|H|J|K|L|M|N|P|Q|R|S|T|V|W|X|Y|Z)){5}`

Initialer: `\p{L}{2,10}` (2 til 10 bogstaver i UTF-8 tegnsættet, men ikke tal)

Udtrykket for CPR og autorisation svarer til hvad der anvendes i bl.a FMK.

5 Intern funktionalitet

I afsnit 4 Registreringsservice er der beskrevet hvorledes logdata afleveres. Tilsvarende vil der senere i afsnit 6 Opslagsservice blive beskrevet hvorledes data udstilles til FMK og sundhed.dk. På et sted herimellem skal der være intern funktionalitet til at berige og gruppere data. Hvor og hvorledes dette implementeres skal ikke fastlægges her, men afgøres ved implementeringen.

5.1 Håndtering af dubletter

Servicen vil kunne håndtere at et system sender samme log-data mere end en enkelt gang.

Præcist hvorledes dette foretages afgøres ved implementeringen. Eventuelt kan samme algoritme som for den eksisterende MinLog 1 løsning anvendes:

I den eksisterende MinLog 1 løsning anvendes en algoritme, hvor der indledningsvist udregnes en hash-værdi af data, og at der ved sammenfald af hash-værdier kontrolleres om data findes i databasen i forvejen. Såfremt data findes i forvejen skrives ikke et nyt datasæt.

I Den Gode Webservice er der specificeret at MessageID bruges til at identificere dubletter ved genfremsendelse. Idet MinLog 2 vil identificere dubletter ud fra logningens indhold ignoreres MessageId i denne forbindelse, dvs. at der antages at der kan forekomme dubletter også selvom MessageId ikke er genbrugt.

5.2 Sammenkædning af log-data

En af formålene med MinLog 2 er at flere forskellige systemer kan aflevere logdata. Eksempelvis afleverer FMK og Receptmodulet i dag log-data, og fremover kan eksterne systemer som f.eks. EPJ-systemer også aflevere logdata. Det vil derfor kunne opstå situationer hvor f.eks. et EPJ-system, FMK og Receptmodulet logger opslag relateret til samme behandling eller forløb. Det vil derfor være af stor værdi at MinLog kan afgøre at disse opslag naturligt hænger sammen, og kan sammenkædes.

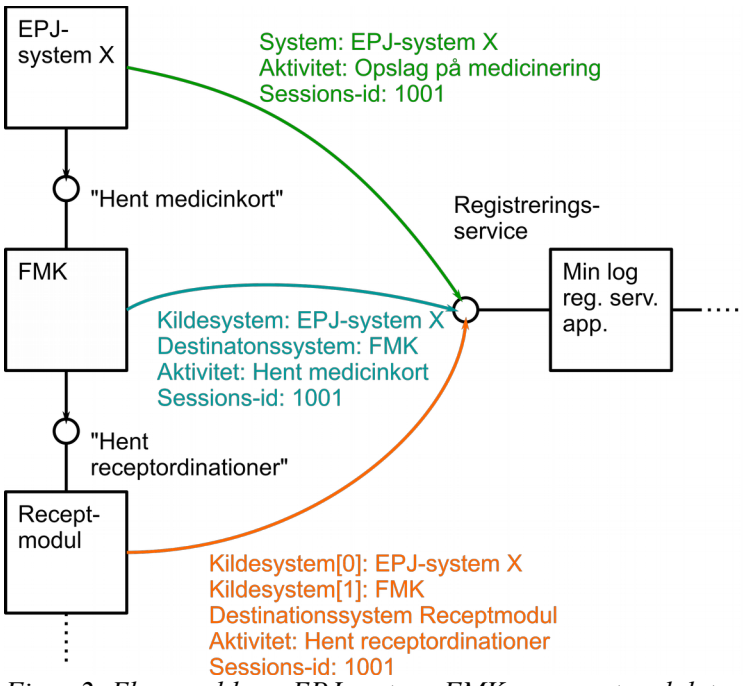
Problemstilling omkring sammenkædning af log-data ligner meget en problemstilling der opstår allerede i MinLog 1, hvor der er ønske om at kunne gruppere en række opslag f.eks. opstået ved en borgers besøg hos lægen, ambulant behandling, receptudlevering mm. Det sidste er behandlet i afsnit 5.3 Gruppering af log-data.

5.2.1 Sammenkædning ud fra CorrelationId

Den simpleste situation for MinLog 2 opnås hvis systemet hvor brugeren initierer kæden af kald danner et CorrelationId, og dette sCorrelationId kan sendes med igennem kæden af samtlige servicekald. Dette forudsætter naturligvis at samtlige services understøtter dette (hvilket ikke er tilfældet i dag).

Hertil kan evt. komme en liste af navne m.v. på systemer der tidligere optræde i kæden. Som minimum skal navnet på det kildesystem der kalder servicen være kendt, og naturligvis navnet på destinationssystemet der kaldes. En liste af navne m.v. for kildesystemer længere tilbage i kæden kan understøttes, men er dog ikke strengt nødvendigt.

Ud fra CorrelationId og navne på systemer kan MinLog 2 afgøre at to eller flere kald relaterer til samme opslag, og derfor at log-data kan grupperes.

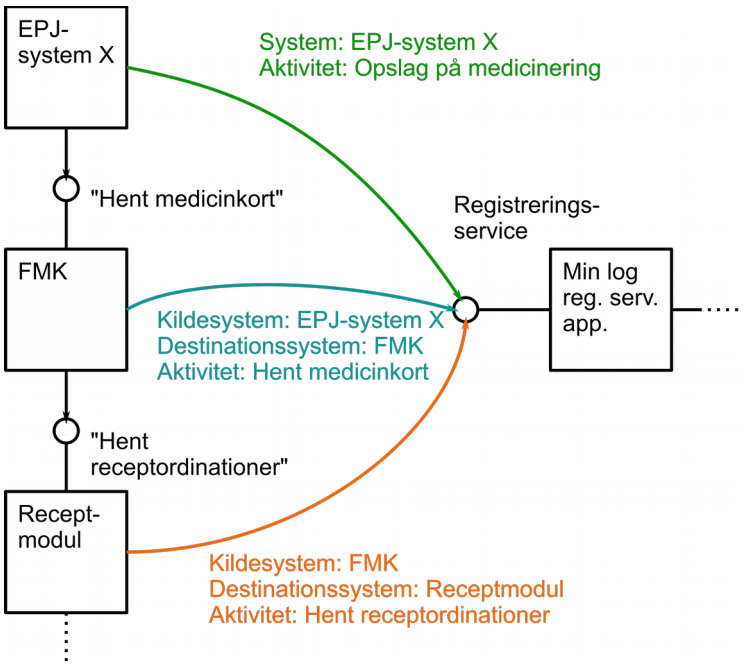


Figur 2: Eksempel hvor EPJ-system, FMK og receptmodulet alle logger, og FMK og receptmodulet understøtter at services kaldes med CorrelationID-id og for receptmodulets vedkommende også en liste af systemnavne.

5.2.2 Sammenkædning udledt ud fra log-data

MinLog 2 får en lidt mere kompliceret opgave med at sammenkæde kald hvis der ikke sendes et CorrelationId. I så fald sammenkædes ud fra:

- PersonIdentifier (borgerens CPR-nummer) incl. source-attribut
- DateTime eller From- og ToDateTime uden tidspunkt
- Navn på kildesystem og destinationssystem.
- Eventuelt OrganisationId incl. source attribut. Alternativt OrganisationName, hvis OrganisationId ikke er angivet. Begge dele kræver dog at det kan sikres at systemer logger med samme OrganisationId eller OrganisationName.



Figur 3: Eksempel hvor EPJ-system, FMK og receptmodulet alle logger, og FMK og ingen systemer understøtter at services kaldes med CorrelationID eller en liste af systemnavne ud over navnet på det kaldende system.

5.3 Gruppering af log-data

En væsentlig funktionalitet i Minlog 2, er at opslagsservicen kan aflevere log-data grupperet.

Log-data kan grupperes for en sammenhængende serie af opslag, der i denne sammenhæng skal forstås som en behandling, inlæggelse eller en enkelt kontakt til sundhedsvæsenet. Dvs. hvor det kan være et ønske om at gruppere log-data fra en række opslag f.eks. opstået ved en borgers besøg hos lægen, ambulant behandling, receptudlevering mm.

Grupperingen kan enten udledes af Minlog 2, baseret på antagelser omkring hvordan data er tilgået, eller ud fra det medsendte CorrelationId. Forud for grupperingen bør log-data fra forskellige systemer så vidt muligt være sammenkædet som beskrevet under 5.2 Sammenkædning af log-data.

Alternativt kan grupperingen ske ud fra simplere parametre som dato, organisation eller sundhedsfaglig.

5.3.1 Gruppering for opslagssammenhæng, ud fra CorrelationId

Såfremt systemet, der kalder registreringsservicen kan medsende et CorrelationId, vil dette blive anvendt til gruppering. For EPJ-systemers vedkommende kan CorrelationId f.eks. svare til forløbs-id eller lignende.

Følgende felter anvendes til gruppering i samme gruppe:

- PersonIdentifier (borgerens CPR-nummer) incl. source attribut
- SystemName

- OrganisationId incl. source attribut. Alternativt OrganisationName, hvis OrganisationId ikke er angivet.
- CorrelationId

Det er afsendersystemets ansvar at CorrelationId er unikt for det pågældende system og organisation (dvs. for samme SystemName og OrganisationId/OrganisationName) og dækker en ”konsultation”, ”kontakt”, ”behandling” m.v. (dette defineres i Vejledninger og retningslinjer). PersonIdentifer bør strengt taget ikke være nødvendigt, men anvendes i gruppering for at sikre mod fejl.

5.3.2 Gruppering for opslagssammenhæng, udledt ud fra logdata

Såfremt systemet der kalder registreringsservicen *ikke* kan medsende et CorrelationId (hvilket er situationen i dag) skal information til gruppering udledes af øvrige data. Grupperingen vil være baseret på at opslag foretaget samme dag af en person med tilknytning til samme organisation vil skulle grupperes, dvs. at følgende felter anvendes til gruppering i samme gruppe:

- PersonIdentifier (borgerens CPR-nummer) incl. source attribut
- DateTime eller From- og ToDateTime uden tidspunkt
- OrganisationId incl. source-attribut.

Er opslaget foretaget via et EPJ-system kan det forekomme at samme organisation registreres med forskellige SKS- eller SOR-koder. F.eks. opslag foretaget af ”Akutmodtagelse” og ”Medicinsk afsnit” på samme sygehus. Niveauet der bør anvendes til registrering defineres i Vejledninger og retningslinjer.

Idet feltet OrganisationId ikke er obligatorisk og ikke vil forekomme f.eks. ved opslag foretaget af borger, forældremyndighedsindehaver, værge mm. vil der alternativt blive grupperet på:

- PersonIdentifier (borgerens CPR-nummer) incl source attribut
- DateTime eller From- og ToDateTime for logningen uden tidspunkt
- UserPersonIdentifier incl. source attribut

5.3.3 Gruppering på dato, organisation eller sundhedsfaglig

Gruppering på dato, organisation eller sundhedsfaglig er noget simplere for et opslagssammenhæng. Der kan grupperes på:

- Datoen handlingen er udført (element DateTime). Såfremt der anvendes et dato-interval (elementer FromDateTime – ToDateTime) vil dette kunne strække sig over to datoer (i teorien flere), i så fald vil log-data blive returneret for begge (alle) datoer.
- Organisationen (element OrganisationId incl. source-attribut eller OrganisationName). Er organisationen angivet med f.eks. SKS-koder kan det ske at organisationen er angivet i forskellige niveauer, disse vil i så fald blive returneret separat for alle anvendte koder.
- Den sundhedsfaglige aktør der har udført handlingen (element UserPersonIdentifier).

- Den autoriserede sundhedsperson handlingen er udført på vegne af (element OnBehalfOf-PersonIdentifier).

5.4 Filtreringsflag ved sammenkædning og gruppering

Filtrering angivet i ”Filter”-elementet har aktuelt to mulige værdier, ”Ikke borger” og ”Ikke Ikke forældremyndighedsindehaver”. Se evt. 4.2.2 Filter flag – for data ikke relevant i borgeropslag og 4.2.3 Filter flag – for data ikke i forældremyndighedsindehaver-opslag.

I forbindelse med sammenkædning og gruppering vil de to flag skulle opføre sig på samme måde:

5.4.1 Filter "Ikke forældremyndighedsindehaver"

Forældremyndighedsindehaver må ikke se deres børns præventionsmidler, selv om barnet er under 15 år. Log-data markeret med filteret ”Ikke forældremyndighedsindehaver” vil derfor i denne situation ikke blive returneret.

Ved opslag uden gruppering er opgaven simpel, log-data markeret med ”Ikke forældremyndigheds-indehaver” skal filtreres fra i svaret på opslagsservicen i svaret til borgeren hvor denne optræder som forældremyndighedsindehaver, og på opslagstidspunktet. Ved opslag på borgerens egne data sker der ingen filtrering ud fra dette flag.

Ved gruppering kan det forekomme at visse log-data i gruppen er markeret med ”Ikke forældre-myndighedsindehaver” og andre ikke. Eneste konsekvente mulighed er at filtrere de enkelte log-data fra. Alternativt kunne ”Ikke forældremyndighedsindehaver”-markeringen have en ”smittende” virkning på resten af gruppen. Dette vil dog ikke kunne gennemføres konsekvent, idet grupper ikke er konstante størrelser, men log-data i en gruppe kan løbende komme til eller blive slettet.

Det er klientens ansvar at sikre at ”Ikke forældremyndighedsindehaver”-flaget ved logning til MinLog 2 sættes korrekt.

Indholdet i LogDataGroup som beskrevet i 6.3.2 Grupperet svar skal svare til indholdet i de underliggende LogDataEntry-elementer efter at filtreringen er foretaget, således at de generelle principper for gruppering er overholdt efter at data er filtreret fra.

5.4.2 Filter "Ikke borger"

For Log-data markeret med ”Ikke borger” vil kun enkelte log-data markeret med ”Ikke borger” blive filtreret fra. Dvs. på samme måde som ”Ikke forældremyndighedsindehaver”. Her er kompleksiteten dog mindre, idet der typisk ikke vil være behov for at skjule en sammenhæng.

6 Opslagsservice

Opslagsservicen skal understøtte at den direkte bruges af et klient-system til at vise logninger. Der udstilles en samlet opslagsservice, der afhængigt af hvilke parametre den kaldes med kan returnere:

- Borgerrettet log-data, dvs. til ”MinLog”, således at borgeren kan se hvilke opslag der er foretaget på borgerens sundhedsdata, evt. også såfremt borgeren optræder som forældremyndighedsindehaver, fuldmagtshaver eller værge.

- Log-data til medhjælpsloggen, til at autoriserede sundhedspersoner kan se hvad deres evt. medhjælpere slår op på deres vegne.
- (Option) Data til ”register-indsigt”, dvs. til at samtlige aktører kan få indblik i hvad der er logget omkring aktørens opslag.

6.1.1 Gruppering

I tilfælde af at en borger foretager et opslag, er der behov for at foretage en gruppering for at skjule kompleksiteten (dvs. som beskrevet i afsnittene 5.2 Sammenkædning af log-data og 5.3 Gruppering af log-data). Borgeren vil typisk være interesseret i hvilken organisation og evt. person, der har foretaget opslaget, sjældent i hvilke enkelte servicekald, der er foretaget. Der er ikke taget stilling til hvorvidt gruppering skal foretaget løbende (f.eks. via et baggrundsjob) eller ved opslag, dette afgøres forud for implementeringsfasen.

I tilfælde af at en læge foretager et opslag på medhjælpsloggen, eller en aktør foretager et opslag på hvad der er foretaget på vegne af denne, så vil der kunne findes mange registreringer. I dette tilfælde vil der kunne være registreret store datamængder, og en gruppering vil derfor være relevant for at skabe overblik.

Typen af gruppering angives i opslaget, eller kan fravælges. Fravalg af gruppering anvendes først og fremmest idet der kan være visse systemer der kan vælge at implementere grupperingen selv, evt. til eksport-formål, og endeligt at såfremt det vælges at implementere gruppering på opslagstidspunktet kan der være en performancegevinst såfremt flere løsninger generelt fravælger gruppering.

6.1.2 Filtrering på målgruppe, ud fra "Filter"-flag angivet i registreringsservicen

I kaldet til registerservicen kan der være angivet en eller flere målgrupper via et eller flere Filter-elementer. Afhængt af hvorledes servicen kaldes (hvilket person-id der anvendes) vil data blive returneret svarende til hvad de er angivet i Filter-elementerne. Dvs. at et tilsvarende filter-element skal *ikke* angives i opslagsservicen, idet dette er implicit givet ud fra hvilket person-id der anvendes.

6.1.3 Opslag med dato-interval

Servicen skal understøtte at klienter eller brugere vælger at slå op i et datointerval, og ønsker data sorteret med både nyeste og ældste først.

6.1.4 Paginering og RegCode

Servicen skal desuden understøtte at data kan returneres pagineret, afhængigt af hvad der angives i opslaget. Såfremt data retureres pagineret skal der sikres at pagineringen understøtter at logninger returneres sorteret med nyeste eller ældste først.

I MinLog version 1 er der anvendt en ”RegCode” til paginering. RegCode indeholder i MinLog version 1 et uuid, der dannes af MinLog, og anvendes til at identificere en logning.

I MinLog 2 vil der fortsat blive anvendt en RegCode til paginering. Desuden vil RegCode blive anvendt i forbindelse med detalje-opslag, se under 6.2.4 Eksempel 4: Opslag på detaljer. Hvorvidt der i MinLog version 2 anvendes uuid'er eller andre koder (f.eks. tidsstempel + løbenummer)

besluttes først endeligt i implementeringsfasen. Snitfladen beskrevet i dette dokument kræver ikke at det nødvendigvis er uuid'er der anvendes.

Såfremt der ikke ønskes paginering kan dette angives i forespørgslen. Eksempelvis kan der være ønsket at data returneres uden gruppering, til klienter der selv vil foretage en gruppering, eksportere data eller lignende.

6.1.5 Filtrering på kritikalitet og type af opslag

Opslag på f.eks. privatmarkerede data som er foretaget med samtykke eller værdispring kan være særligt interessante for borgeren eller en autoriseret sundhedsperson at følge op på. Der kan angives to typer af filtre der enten virker ved at lade logninger med de angivne værdier passere eller stoppe dem.

Eksempelvis gør følgende filter at kun privatmarkerede data som der er slået op på med værdispring eller "uden angivelse" vil blive returneret (se evt. tabellen i afsnit 4.2.4).

```
<FilterPass>
      <Criticality>Privatmarkeret</Criticality>
      <Addition>Værdispring</Addition>
      <Addition/>
</FilterPass>
```

Modsat gør følgende filter at logninger på ikke-privatmarkerede data der er slået op på med angivelse af samtykke, værdispring eller "uden angivelse" ikke returneres i svaret.

```
<FilterStop>
      <Criticality/>
      <Addition>Samtykke</Addition>
      <Addition>Værdispring</Addition>
      <Addition/>
</FilterStop>
```

I begge tilfælde svarer filteret til et opslag som (uden at det teknisk nødvendigvis skal implementeres sådan):

… Criticality IN (*liste af angivne Criticality-værdier*)
AND Addition IN (*liste af angivne* Addition-*værdier*)

6.1.6 Logning af opslag

Opslagsservice skal validere om borgeren eller sundhedspersonen må fortage opslaget og samtidig logge at det er udført/forsøgt opslag til MinLog.

For borgere gælder at både andres og egne opslag logges, for at kunne identificere misbrug.

For sundhedsfaglige gælder at opslag på egne ikke data logges, dvs. at opslag i medhjælpsloggen eller opslag på hvad der er logget omkring aktøren selv (register-indsigt) ikke logges.

6.1.7 Sikkerhedsmodel

Opslagsservicen udstiller en DGWS snitflade for sundhedsfagliges tilgang og en IDWS snitflade for borgernes opslag.

Tilgangen til DGWS snitfladen kræver at MOCES-baseret SOSI-STS-signeret idkort. IDWS snitfladen kan tilgås med at POCES-baseret IDWS identity token udstedt af NemLogin-STS'en.

For såvel idkort som identity token validerer servicen signatur, autentifikationsniveau, trust (til hhv. SOSI føderationen og NemLogin føderationen) og gyldighed.

6.2 Forespørgsel

Opslagsservicen kaldes med et antal parametre, der angiver hvilke data der forespørges på, og på hvilken måde data ønskes returneret.

- Der kan slås op på borgerens CPR-nummer i PersonIdentifier.
- Der kan slås op på hvad der er foretaget på vegne af en sundhedsperson i elementet OnBehalfOfPersonIdentifier.
- Der kan slås op på hvad der er logget omkring aktøren i UserPersonIdentifier.
- Eller der kan slås op på en liste af RegCode-elementer, for derved at lave en ”drill down” hvis der ønskes at se på indholdet af LogDataEntry for en eller flere gruppe. Ved opslag med en eller flere RegCode-elementer vil der være visse af de øvrige parametre der ikke giver mening.

Forud for implementeringsfasen, når en endelig snitfladebeskrivelse udarbejdes, skal det afgøres og beskrives hvorvidt de forskellige opslagsmuligheder kan kombineres i samme opslag.

6.2.1 Eksempel 1: Borger-opslag i "MinLog" med CPR-nummer.

Eksemplet viser en borgers opslag i ”MinLog” med borgens CPR-nummer eller evt. erstatnings-CPR-nummer i elementet PersonIdentifier.

```
<ListLogStatementsRequest>
      <PersonIdentifier source="CPR">1111111118</PersonIdentifier>
      <Grouping>Correlation</Grouping>
      <Details>None</Details>
      <Chronologic>true</Chronologic>
      <FromDateTime>2015-11-13T13:14:17Z</FromDateTime>
      <ToDateTime>2099-12-31-23:59:59Z</ToDateTime>
      <PageSize>20</PageSize>
      <AfterRegCode>b1fb4fd5-a4f0-48f6-b84d-248ea17e5512</AfterRegCode>
<ListLogStatementsRequest>
```

Opslaget vil se ud som ovenstående, uanset om det er borgerens opslag på egne data, eller om det er en forældremyndighedsindehavers opslag på et barns CPR-nummer, hvor barnets CPR-nummer vil være angivet i PersonIdentifier og forældremyndighedsindehavers CPR-nummer i certifikatet.

6.2.2 Eksempel 2: Opslag i medhjælpsloggen

Eksemplet viser opslag i medhjælpsloggen ud fra CPR-nummer (m.v.) angivet i elementet ”OnBehalfOfPersonIdentifier”.

```
<ListLogStatementsRequest>
      <OnBehalfOfPersonIdentifier source="CPR">1111111118</OnBehalfOfPersonIdentifier>
      <Grouping>Date</Grouping>
      <Details>All</Details>
      <Chronologic>true</Chronologic>
      <FromDateTime>2015-11-13T13:14:17Z</FromDateTime>
      <ToDateTime>2099-12-31-23:59:59Z</ToDateTime>
      <PageSize>20</PageSize>
```

```
     <AfterRegCode>b1fb4fd5-a4f0-48f6-b84d-248ea17e5512</AfterRegCode>
<ListLogStatementsRequest>
```

6.2.3 Eksempel 3: Opslag for "register-indsigt"

Det sidste eksempel viser et opslag foretaget af en borger eller en sundhedsperson for ”register-indsigt” (option). Aktørens CPR-nummer angives i UserPersonIdentifier.

```
<ListLogStatementsRequest>
     <UserPersonIdentifier source="CPR">1111111118</UserPersonIdentifier>
     <Grouping>None</Grouping>
     <Chronologic>true</Chronologic>
     <FromDateTime>2015-12-31T00:00:00Z</FromDateTime>
<ListLogStatementsRequest>
```

6.2.4 Eksempel 4: Opslag på detaljer

Eksemplet viser på opslag på detaljer, med en liste af RegCode-værdier returneret i et af de tidligere opslag. Desuden angives PersonIdentifier, OnBehalfOfPersonIdentifier eller UserPersonIdentifier). Dette anvendes dels til at udlede typen af opslag (MinLog, medhjælpslog, eller ”register-indsigt”), dels som ekstra sikring af at der ikke returneres data for forskellige borgere i opslaget, og endeligt kan servicen evt. anvende værdien til internt at optimere opslaget.

```
<ListLogStatementsRequest>
     <OnBehalfOfPersonIdentifier source="CPR">1111111118</OnBehalfOfPersonIdentifier>
     <RegCode>5a5f1247-baf7-4d57-9c40-91eb5999bc84</RegCode>
     <RegCode>3a4a117c-f2e2-4226-ab6e-4ba84fffeb30</RegCode>
     <RegCode>31b8de05-b3f1-4aef-b132-8f24cbf6b3d0</RegCode>
     <Grouping>None</Grouping>
     <Chronologic>true</Chronologic>
<ListLogStatementsRequest>
```

6.2.5 Indhold i kald-dokumentet

Følgende elementer anvendes i opslaget:

Navn	**Beskrivelse**	**Definition**	**Kardinalitet**
LogDataList-Request	Rod-element for forespørgslen.		1
PersonIdentifier	CPR-nummer eller evt. erstatnings-CPR-nummer på borgeren der er slået op på. Anvendes til ”MinLog”-opslag.	Streng af længde 50	1, valg mellem en af *Person-Identifier-elementerne eller liste af RegCode
PersonIdentifier source attribut	Kilde til ID for borgerens CPR-nummer m.v.	Streng, defineret som en union af en enumeration af CPR, E-CPR, ... og en Streng med max længde 200	1 (attributten er obligatorisk på elementet PersonIdentifier, når elementet forekommer)

OnBehalfOf-PersonIdentifier	CPR-nummer eller evt. erstatnings-CPR-nummer på brugeren handlingen er udført på vegne af. Anvendes til opslag i medhjælpsloggen.	Streng af længde 501, valg mellem en af *Person-Identifier-elementerne eller liste af RegCode	0-1, valg mellem en af *Person-Identifier-elementerne eller liste af RegCode
OnBehalfOf-PersonIdentifier source attribut	Kilde til ID for OnBehalfOfPersonIdentifier	Streng, defineret som en union af en enumeration af CPR, E-CPR, ... og en Streng med max længde 200	1 (attributten er obligatorisk på elementet OnBehalfOf-PersonIdentifier, når elementet forekommer)
UserPerson-Identifier	CPR-nummer eller evt. erstatnings-CPR-nummer på brugeren handlingen er af. Anvendes til opslag til ”register-indsigt”.	Streng af længde 50	0-1, valg mellem en af *Person-Identifier-elementerne eller liste af RegCode
UserPerson-Identifier source attribut	Kilde til ID for UserPersonIdentifier	Streng, defineret som en union af en enumeration af CPR, E-CPR, ... og en Streng med max længde 200	1 (attributten er obligatorisk på elementet UserPerson-Identifier, når elementet forekommer)
RegCode	Liste af RegCode-værdier for grupper der ønskes detaljer for.	Streng med max længde på 36 tegn (svarende til at feltet evt. kan indeholde en uuid)	1-*, valg mellem PersonIdentifier, OnBehalfOf-PersonIdentifier eller liste af RegCode
Grouping	Angivelse af hvorledes svaret returneres: - Ikke grupperet eller grupperet efter: - Opslagssammenhæng (CorrelationId) - Dato - Organisation - Brugeren der har udført handlingen - Sundhedspersonen handlingen er udført på	Streng, defineret som en union af en enumeration af ”None”, ”Correlation”, ”Date”, ”Organisation”,	1

	vegne af Gruppering er beskrevet i afsnit 5.1 Gruppering af log-data.	”UserPerson”, ”OnBehalfOf-Person” og en Streng med max længde 50	
Details	Angivelse af hvorvidt et grupperet svare skal indeholde detaljer. Elementet skal angives hvis der anvendes gruppering, anvendes der ikke gruppering bør elementet ikke angives.	Streng, defineret som en union af en enumeration af ”None”, ”All” og en Streng med max længde 50	0-1
FilterPass	Filtrering på kritikalitet og type af opslag der ønskes returneret, se afsnit 6.1.5.		0-1 Valg mellem FilterPass, FilterStop eller intet filter
FilterPass/ Criticality	Et antal angivelser af kritikalitet til filtreringen (privatmarkeret eller ingen angivelse)	Streng, defineret som en union af en enumeration af niveau for kritikalitet, og en Streng med max længde 50 tegn	0-*
FilterPass/ Addition	Et antal angivelser af tilføjelser til filtreringen (samtykke, værdispring eller ingen angivelse)	Streng, defineret som en union af en enumeration, og en Streng med max længde 50 tegn	0-*
FilterStop	Filtrering på kritikalitet og type af opslag der ikke ønskes returneret, se afsnit 6.1.5.		0-1 Valg mellem FilterPass, FilterStop eller intet filter
FilterStop/ Criticality	Et antal angivelser af kritikalitet til filtreringen (privatmarkeret eller ingen angivelse)	Streng, defineret som en union af en enumeration af niveau for kritikalitet, og en Streng med max længde 50	0-*

		tegn	
FilterStop/ Addition	Et antal angivelser af tilføjelser til filtreringen (samtykke, værdispring eller ingen angivelse)	Streng, defineret som en union af en enumeration, og en Streng med max længde 50 tegn	0-*
Chronologic	Med true angives at data returneres i kronologisk rækkefølge, med false i omvendt kronologisk rækkefølge.	Boolean	1
FromDateTime	Der returneres data fra og med dette tidspunkt, angivet med sekunders præcision.	DateTime med pattern der sikrer anvendelse af zulu-tid	0-1
ToDateTime	Der returneres data til og med dette tidspunkt.	DateTime med pattern der sikrer anvendelse af zulu-tid	0-1
PageSize	Det maksimale antal datasæt der ønskes returneret. Er grouped = true gælder antallet antal grupper, Er grouped = false gælder antallet antal LogDataEntry i svaret. Er der ikke angivet en PageSize vil der blive anvendt en deafult-værdi. Denne fastlægges i implementeringsfasen.	Integer, med en restriction > 0	0-1
AfterRegCode	Element der anvendes ved paginering, ved opslag efter det første. Værdien angiver den sidste RegCode (afhængigt af Chronologic for den første eller sidste returneres, hvorefter næste side ønskes)	Streng med max længde på 36 tegn (svarende til at feltet evt. kan indeholde en uuid)	0-1

6.3 Svar

Svaret vil enten være grupperet eller en liste af LogDataEntry, der ikke er grupperede.

6.3.1 Anonymisering af sundhedsperson i svar

Ved udstilling af data fra MinLog 2 i borgeropslaget kan der i borgeropslaget ske en anonymisering af informationer omkring sundhedspersonen. Formålet er at sikre en passende balance mellem borgerens ret til information og beskyttelse af sundhedspersoners identitet.

De præcise regler for hvordan anonymisering af informationer omkring sundhedspersonen evt. vil foregå er aktuelt ikke afklaret. Elementerne er alle optionelle i svaret i opslagsservicen, og bør derfor kunne understøtte at elementer som f.eks. id og navn ikke returneres.

6.3.2 Grupperet svar

Det grupperede svar indeholder data grupperet som beskrevet i afsnit 5.3 Gruppering af log-data.

Hver gruppe er indeholdt i et LogDataGroup, med værdier udledt af gruppens indhold. Såfremt der i forespørgselen er angivet at svaret skal indeholde detaljer (Details-elementet indeholder ”All”) returneres også hvert LogDataEntry i gruppen.

Grupper er ikke statiske. Der kan løbende blive tilføjet data, også data der har et DateTime (alternativt From- og ToDateTime) der er ældre end data der allerede er registreret. Desuden vil der efter to år skulle slettes data, svarende til hvad der allerede sker i den eksisterende MinLog-løsning. RegCode for gruppen kan derfor være enten en selvstændig RegCode eller en RegCode for et element i gruppen, f.eks. for den yngste registrering. Dette fastlægges og beskrives i forbindelse med løsningsdesign forud for implementation af funktionaliteten.

```
<ListLogStatementsResponse>
     <LogDataGroup>
          <RegCode>93fd6c7e-8296-4ba1-8bfb-23744bcd1678</RegCode>
          <NumberOfLogDataEntries>42</NumberOfLogDataEntries>
          <Source>
               <SystemName>COSMIC</SystemName>
               <CorrelationId>07f59cdb-28f5-4bab-ac18-fd618235d386</CorrelationId>
          </Source>
          <Destination>
               <SystemName>FMK</SystemName>
               <Criticality>Værdispring</Criticality>
               <FromDateTime>2015-11-13T13:14:15Z</FromDateTime>
               <ToDateTime>2015-11-13T13:14:17Z</ToDateTime>
               <OrganisationId source="SOR">240971000016006</OrganisationId>
               <OrganisationName>Sygehus Sønderjylland</OrganisationName>
               <PersonIdentifier source="CPR">1111111118</PersonIdentifier>
               <PersonName>Anita Andersen</PersonName>
               <CorrelationId>07f59cdb-28f5-4bab-ac18-fd618235d386</CorrelationId>
               <UserPersonIdentifier source="CPR">0101014444</UserPersonIdentifier>
               <UserPersonName>Bente Bendtsen</UserPersonName>
               <OnBehalfOfPersonIdentifier source="CPR">1212128888</OnBehalfOfPr...
               <OnBehalfOfPersonName>Christan Christensen</OnBehalfOfPersonName>
          </Destination>

          <LogDataEntry>
               <RegCode>5a5f1247-baf7-4d57-9c40-91eb5999bc84</RegCode>
               <Source>
                    <SystemName>COSMIC</SystemName>
                    <CorrelationId>07f59cdb-28f5-4bab-ac18-fd618235d386</CorrelationId>
               </Source>
               <Destination>
```

```
                    <SystemName>FMK</SystemName>
                    <Activity>Hent medicinkort</Activity>
                    <Criticality>Værdispring</Criticality>
                    <DateTime>2015-11-13T13:14:15Z</DateTime>
                    <OrganisationId source="SOR">240971000016006</OrganisationId>
                    <OrganisationName>Sygehus Sønderjylland</OrganisationName>
                    <PersonIdentifier source="CPR">1111111118</PersonIdentifier>
                    <PersonName>Anita Andersen</PersonName>
                    <SequenceNumber>1</SequenceNumber>
                    <CorrelationId>07f59cdb-28f5-4bab-ac18-fd618235d386</CorrelationId>
                    <UserPersonIdentifier source="CPR">0101014444</UserPersonIdentifier>
                    <UserPersonName>Bente Bendtsen</UserPersonName>
                    <OnBehalfOfPersonIdentifier source="CPR">1212128888</OnBehalfOfPr...
                    <OnBehalfOfPersonName>Christan Christensen</OnBehalfOfPersonName>
                    <Filter>Ikke borger</Filter>
               <Destination>
          <LogDataEntry>

          <LogDataEntry>
               <RegCode>3a4a117c-f2e2-4226-ab6e-4ba84fffeb30</RegCode>
               <Source>
                    <SystemName>COSMIC</SystemName>
                    <CorrelationId>07f59cdb-28f5-4bab-ac18-fd618235d386</Correl...
               </Source>
               <Destination>
                    <SystemName>FMK</SystemName>
                    <Activity>Hent lægemiddelordination</Activity>
                    <Criticality>Værdispring</Criticality>
                    <DateTime>2015-11-13T13:14:17Z</DateTime>
                    <OrganisationId source="SOR">240971000016006</OrganisationId>
                    <OrganisationName>Sygehus Sønderjylland</OrganisationName>
                    <PersonIdentifier source="CPR">1111111118</PersonIdentifier>
                    <SequenceNumber>2</SequenceNumber>
                    <CorrelationId>07f59cdb-28f5-4bab-ac18-fd618235d386</Correl...
                    <UserPersonIdentifier source="CPR">0101014444</UserPersonIdentifier>
                    <UserPersonName>Bente Bendtsen</UserPersonName>
                    <OnBehalfOfPersonIdentifier source="CPR">1212128888</OnBehalfOfPe...
                    <OnBehalfOfPersonName>Christan Christensen</OnBehalfOfPersonName>
               </Destination>
          <LogDataEntry>
          ...
     </LogDataGroup>
     ...
     <MoreAvailiable>93fd6c7e-8296-4ba1-8bfb-23744bcd1678</MoreAvailiable>
<ListLogStatementsResponse>
```

I tabellen herunder er beskrevet de elementer der kan returneres i svaret. Elementer med samme navn kan forekomme mere end én gang, og skal så læses i kontekst af elementet på niveauet derover.

For elementer direkte under LogDataGroup gælder generelt (dvs. med enkelte undtagelser som angivet i tabellen herunder) at såfremt alle tilsvarende værdier i de LogDataEntry-elementer der befinder sig i den pågældende LogDataGroup indeholder samme værdi, returneres værdien elementet under LogDataGroup. Dette gælder uanset hvad der er angivet i ”Grouping”.

I tabellen herunder er de elementer denne generelle regel gælder for markeret med ∩, og beskrivelsen af feltet indholds kan evt. findes længere nede i tabellen.

Eksempel:

En LogDataGroup har tre elementer LogDataEntry-elementer under sig.

OnBehalfOfPersonIdentifier indeholder hhv. CPR-nummer 300272-1242 og to gange 310469-3301, værdien OnBehalfOfPersonIdentifier vil derfor ikke findes under LogDataGroup.

OrganisationId og OrganisationName indeholder alle tre gange hhv. ydernummer 66974 og strengen ”Lægerne Vestergade”, disse to felter vil derfor findes med dette indhold direkte under LogData-Group.

Navn	**Beskrivelse**	**Definition**	**Kardinalitet**
ListLogStatements Response	Rod-element for svaret.		1
LogDataGroup	Rod-elementet for en gruppe.		0..*, dog ikke flere end evt. angivet i PageSize eller evt. default-værdi.
NumberOf-LogDataEntries	Antal logninger i gruppen, dvs. svarende til antal LogDataEntry-elementer der kan returneres.	Integer, med en restriction > 0	1
LogDataGroup/ RegCode	Id for gruppen, og anvendes ved paginering og detalje-opslag. Id svarer til et element i gruppen, som beskrevet herover.	Streng med max længde på 36 tegn (svarende til at feltet evt. kan indeholde en uuid)	1
LogDataGroup/ Source	∩ Opslagene kan være foretaget af samme kildesystem, men kan også komme fra en kæde af registreringskald fra forskellige systemer.		0-1
LogDataGroup/ Source/Source[/...]	∩		0-1
LogDataGroup/ Source/ SystemName	∩ Såfremt der er grupperet en kæde af opslag fra forskellige systemer vil systemnavnene være forskellige, og derfor ikke returneret i gruppen.	∩	0-1

LogDataGroup/ Source/ CorrelationId	∩ Såfremt CorrelationId er angivet i kaldet til registreringsservicen vil værdien være anvendt til gruppering og derfor forekomme for gruppen.	∩	0-1
LogDataGroup/ Destination	∩	∩	1
LogDataGroup/ Destination/ SystemName	∩	∩	0-1
LogDataGroup/ Destination/ Activity		∩	0-1
LogDataGroup/ Destination/ Reason	∩	∩	0-1
LogDataGroup/ Destination/ Criticality	∩	∩	0-1
LogDataGroup/ Destination/ FromDateTime	Ældste DateTime eller FromDateTime i gruppen	DateTime med pattern der sikrer anvendelse af zulu-tid	1
LogDataGroup/ Destination/ ToDateTime	Yngste DateTime eller ToDateTime i gruppen	DateTime med pattern der sikrer anvendelse af zulu-tid	1
LogDataGroup/ Destination/ OrganisationId	∩	∩	0-1
LogDataGroup/ OrganisationId/ Destination/ attribut source	∩	∩	1

LogDataGroup/ Destination/ OrganisationName	∩	∩	0-1
LogDataGroup/ Destination/ PersonIdentifier	∩	∩	0-1
LogDataGroup/ Destination/ PersonIdentifier source attribut	∩	∩	1
LogDataGroup/ Destination/ PersonName	∩	∩	0-1
LogDataGroup/ Destination/ CorrelationId	∩	∩	0-1
LogDataGroup/ Destination/ UserPerson-Identifier	∩	∩	0-1
LogDataGroup/ Destination/ UserPerson-Identifier source attribut	∩	∩	1
LogDataGroup/ Destination/ UserPersonName	∩	∩	0-1
LogDataGroup Destination/ UserRole	∩	∩	0-1
LogDataGroup/ Destination/ OnBehalfOf-PersonIdentifier	∩	∩	0-1

LogDataGroup/ Destination/ OnBehalfOf- PersonIdentifier source attribut	∩	∩	1
LogDataGroup/ Destination/ OnBehalfOf- PersonName	∩	∩	0-1
LogDataGroup/ Destination/ Filter	∩	∩	0-1
LogDataGroup/ LogDataEntry	Såfremt der i forespørgselen er angivet at svaret skal indeholde detaljer (Details-elementet indeholder ”All”) returneres også hvert LogDataEntry i gruppen.		0-*
LogDataGroup/ LogDataEntry/ RegCode	Id for LogDataEntry, og anvendes ved paginering.	Streng med max længde på 36 tegn (svarende til at feltet evt. kan indeholde en uuid)	1
LogDataGroup/ LogDataEntry/ Source	Element der indeholder information omkring det kaldende system, kildesystemet. Kildesystemet kan være udeladt i de tilfælde en bruger har slået direkte op på systemet.		0-1
LogDataGroup/ LogDataEntry/ Source/Source[/...]	Source-elementet kan igen indeholde et source-element. Dette anvendes såfremt kildesystemet igen er kaldt af et andet system, som vist i 4.2.8 Eksempel 3: Logning af opslag hvor tre systemer er involveret		0-1

LogDataGroup/ LogDataEntry/ Source/ SystemName	Navn, evt. forkortet, for det anvendte kilde-system	Streng med max længde på 25 tegn	1
LogDataGroup/ LogDataEntry/ Source/ CorrelationId	Et teknisk id, medsendt fra kildesystemet. Værdien anvendes til at identificere den sammenhæng som handlingen er gennemført i, eksempelvis et id for behandlingen eller indlæggelsen (EPJ) eller kontakten (LPS). Se afsnit 5.3 Gruppering af log-data. Værdien skal være unik for det anvendte system.	Streng med max længde på 46 tegn.	0-1
LogDataGroup/ LogDataEntry/ Destination	Element der indeholder information omkring og fra det kaldte system, destinations-systemet, dvs. det system der foretager logningen.		1
LogDataGroup/ LogDataEntry/ Destination/ SystemName	Navn, evt. forkortet, for det anvendte system, f.eks. ”FMK”.	Streng med max længde på 25 tegn	1
LogDataGroup/ LogDataEntry/ Destination/ Activity	Tekst der beskriver af den handling, som brugeren har udført eller forsøgt udført på kildesystemet. Eksempelvis ”hent medicinkort” på FMK. Datasættet fastlægges endeligt i forbindelse med udarbejdelse af vejledninger og retningslinjer.	Streng, max længde på 75 tegn	1

LogDataGroup/ LogDataEntry/ Destination/ Reason	Optionel tekst der beskriver årsagen til den handling, som brugeren har udført eller forsøgt udført på kildesystemet. Teksten anvendes kun i særlige tilfælde, hvor borgeren ikke har direkte kontakt til brugeren, eksempelvis ved support, fejlsøgning og tilskudsansøgninger. Teksten udfyldes af systemet, som en eller få forud-definerede tekster, og må ikke være en fritekst udfyldt af brugeren.	Streng, max længde på 50 tegn	0-1
LogDataGroup/ LogDataEntry/ Destination/ Criticality	Niveau for kritikalitet, f.eks: ”Normal”, ”Værdispring”, ”Privatmarkerede data”, … Er værdien ikke angivet svarer dette til ”Normal”. Datasættet fastlægges endeligt i forbindelse med udarbejdelse af vejledninger og retningslinjer.	Streng, defineret som en union af en enumeration af niveau for kritikalitet, og en Streng med max længde 50 tegn	0-1
LogDataGroup/ LogDataEntry/ Destination/ DateTime	DateTime-elementet indeholder en tids-angivelse for opslag på eller forsøg på handling på borgerens data. Dato og tid skal angives i zulu tid / UTC. I praksis gøres dette ved at tilføje Z efter tidsangivelsen, som vist i eksemplet, samt at korrigere for de 1-2 timers forskel (henholdsvis vinter- og sommertid) der er mellem dansk tid og UTC. Tiden angives med en præcision i sekunder.	DateTime med pattern der sikrer anvendelse af zulu-tid	0-1 Enten skal DateTime eller (FromDateTime og ToDateTime) forekomme. Dette skal modelleres i XML-skemaet.
LogDataGroup/ LogDataEntry/ Destination/ FromDateTime	Som alternativ til DateTime herover kan der være foretaget en gruppering af f.eks. FMK inden data er afleveret til MinLog 2. I så fald kan FromDateTime og ToDate-Time angive det interval hvor hændelserne er sket. FMK kan gruppere samme type service-kald foretaget inden for et tidsrum på samme borger og af samme aktør m.v.	DateTime med pattern der sikrer anvendelse af zulu-tid	0-1 Enten skal DateTime eller (FromDateTime og ToDateTime) forekomme. Dette skal modelleres i XML-skemaet.

LogDataGroup/ LogDataEntry/ Destination/ ToDateTime	Se FromDateTime herover.	DateTime med pattern der sikrer anvendelse af zulu-tid	0-1 Enten skal DateTime eller (FromDateTime og ToDateTime) forekomme. Dette skal modelleres i XML-skemaet.
LogDataGroup/ LogDataEntry/ Destination/ OrganisationId	ID for brugerens organisation.	Streng på max 200 tegn	0-1
LogDataGroup/ LogDataEntry/ Destination/ OrganisationId attribut source	Kilde til ID for brugerens organisation, defineret som en attribut på OrganisationId-elementet.	Streng, defineret som en union af en enumeration af SOR, SKS, Yder, CVR-P, CVR, Kommunekode og en Streng med max længde 200	1 (attributten er obligatorisk på elementet OrganisationId, når elementet forekommer)
LogDataGroup/ LogDataEntry/ Destination/ OrganisationName	Navn på brugens organisation	Streng med max længde 200	0-1
LogDataGroup/ LogDataEntry/ Destination/ PersonIdentifier	CPR-nummer eller evt. erstatnings-CPR-nummer på borgeren.	Streng af længde 50	1
LogDataGroup/ LogDataEntry/ Destination/ PersonIdentifier attribut source	Kilde til ID for borgerens CPR-nummer eller erstatnings-CPR-nummer. F.eks. ”CPR” for almindelige CPR-numre i CPR-regstret.	Streng, defineret som en union af en enumeration af CPR, E-CPR, ... og en Streng med max længde 200	1 (attributten er obligatorisk på elementet PersonIdentifier, når elementet forekommer)

LogDataGroup/ LogDataEntry/ Destination/ PersonName	Borgerens navn. Navnet kan være udeladt f.eks. hvis der er registreret et CPR-nummer men ikke et navn og CPR-nummer ikke kan slås op i CPR-registret.	Streng med max længde 147 tegn	0-1
LogDataGroup/ LogDataEntry/ Destination/ CorrelationID	Et teknisk id, medsendt fra kildesystemet. Værdien anvendes til at identificere den sammenhæng som handlingen er gennemført i, eksempelvis et id for behandlingen eller indlæggelsen (EPJ) eller kontakten (LPS). Se afsnit 5.3 Gruppering af log-data. Værdien skal være unik for det anvendte system.	Streng med max længde på 46 tegn.	0-1
LogDataGroup/ LogDataEntry/ Destination/ SequenceNumber	(Nyt felt) Et teknisk sekvens-nummer, angivet af afsender, der anvendes i forbindelse med fejlhåndtering. F.eks. et fortløbende nummer eller et uuid. Værdien skal være unikt i kaldet.	Streng med max længde på 36 tegn (svarende til at feltet evt. kan indeholde en uuid)	1
LogDataGroup/ LogDataEntry/ Destination/ UserPerson-Identifier	CPR-nummer eller evt. erstatnings-CPR-nummer på brugeren der har udført handlingen. Bemærk at dette format også tillader at der returneres anonymiserede id'er (eventuelt og i en senere fase), såfremt der skal sikres beskyttelse af sundhedspersonens identitet, 2.3.4 Beskyttelse af sundhedspersoners identitet. Dette vil i så fald fremgå af source-attributten.	Streng af længde 50	0-1
LogDataGroup/ LogDataEntry/ Destination/ UserPerson-Identifier attribut source	Kilde til UserPersonIndentifier. F.eks. "CPR" for almindelige CPR-numre i CPR-regstret.	Streng, defineret som en union af en enumeration af CPR, E-CPR, ... og en Streng med max længde 200	1 (attributten er obligatorisk på elementet UserPerson-Identifier, når elementet forekommer)

LogDataGroup/ LogDataEntry/ Destination/ UserPersonName	Navn på brugeren der har udført handlingen.	Streng med max længde 147 tegn	0-1
LogDataGroup/ LogDataEntry/ Destination/ UserRole	Brugerens rolle.	Streng af længde 200 (svarende til FMK's RequestedRole)	0-1
LogDataGroup/ LogDataEntry/ Destination/ OnBehalfOf-PersonIdentifier	CPR-nummer eller evt. erstatnings-CPR-nummer på brugeren handlingen er udført på vegne af. Bemærk at dette format også tillader at der returneres anonymiserede id'er (eventuelt og i en senere fase), såfremt der skal sikres beskyttelse af sundhedspersonens identitet, 2.3.4 Beskyttelse af sundhedspersoners identitet. Dette vil i så fald fremgå af source-attributten.	Streng med max længde 50	0-1
LogDataGroup/ LogDataEntry/ Destination/ OnBehalfOf-PersonIdentifier attribut source	Kilde til OnBehalfOfPersonIdentifier. F.eks. "CPR" for almindelige CPR-numre i CPR-regstret.	Streng, defineret som en union af en enumeration af CPR, E-CPR, ... og en Streng med max længde 200	1 (attributten er obligatorisk på elementet OnBehalfOf-PersonIdentifier, når elementet forekommer)
LogDataGroup/ LogDataEntry/ Destination/ OnBehalfOf-PersonNavn	Navn på brugeren handlingen er udført på vegne af.	Streng med max længde 147 tegn	0-1

LogDataGroup/ LogDataEntry/ Destination/ Filter	Et eller flere felter der anvendes til angivelse af hvilken målgruppe logningen skal filtreres fra for. Udelades feltet er der underforstået at logningen er relevant for alle.	Streng, aktuelt defineret som en union af en enumeration aktuelt indeholdende ” Ikke borger” , ”Ikke forældre-myndigheds-indehaver” og en Streng med max længde 50 tegn.	0-*
MoreAvailiable	Findes elementet i svaret angiver dette at der findes yderligere data. Værdien angiver den sidste RegCode for den sidste LogDataGroup, og værdien anvendes i AfterRegCode ved opslag på 2. og efterfølgende sider.	Streng med max længde på 36 tegn (svarende til at feltet evt. kan indeholde en uuid)	0-1

6.3.3 Ugrupperet svar

Foretages der ikke gruppering i svaret returneres en række LogDataEntry-elementer, sorteret som angivet i forespørgslen.

Svar-dokumentet vil ligne dokumentet for et grupperet svar, bortset fra at LogDataEntry-elementerne vil findes direkte under ListLogStatementsResponse-elementet:

```
<ListLogStatementsResponse>
     <LogDataEntry>
          ...
     <LogDataEntry>
     ...
     <MoreAvailiable>93fd6c7e-8296-4ba1-8bfb-23744bcd1678</MoreAvailiable>
<ListLogStatementsResponse>
```

Indholdet vil herudover svare til hvad der returneres for et grupperet svar.

6.4 Berigelse med stamdata

Ved opslag suppleres der med stamdata for person og organisation ud fra id’er, såfremt dette er muligt. I registreringsservicen er der ingen validering ud over en eventuel validering af formater, så det er ikke givet at en berigelse med stamdata er mulig.

Der beriges med organisationsdata og persondata, beskrevet i de to følgende afsnit.

Berigelse med stamdata sker ud fra et view på stamdatamodulets databaser. Principperne for anvendelse af stamdata fra stamdatamodulet afviges dermed, idet der ikke anvendes enkeltopslags-services eller kopiregisterservices. Dette er dog accepteret i MinLog 2-sammenhæng.

6.4.1 Berigelse med organisationsdata

I registreringsservicen er der muligt at angive OrganisationId og OrganisationName. Begge værdier er optionelle, men skal være angivet hvis aktøren har en organisation tilknyttet, dvs. er alt andet end en handling foretaget af en borger. De nærmere krav til anvendersystemernes brug af registrerings-servicen præciseres i et vejledningsdokument.

Er OrganisationId angivet anvendes dette til at forsøge at slå organisationsdata op i stamdata, ud fra hvad der er angivet i source-attributten:

SKS	Værdien forventes at indeholde sygehusafdelingskode (SHAK). Denne kan slås op i SOR-registret, eventuelt i SKS. Af historiske årsager anvendes SKS som source-værdi for SHAK-koder.
Yder	Værdien forventes at indeholde ydernummer, der slås op i yderregistret.
EAN-Lokationsnummer	Værdien forventes at indeholde et EAN-lokationsummer. Dette anvendes af apotekerne, og disse værdier kan slås op i SOR. Generelt kan EAN-lokationsnumre dog ikke forventes at findes i SOR.
Kommunekode	Værdien forventes at indeholde kommunekode, der er et forholdsvist statisk kodesæt.
CVR og CVR-P	Værdierne for CVR-nummer og CVR-P (P-nummer) tillades men beriges ikke, dvs. ignoreres i forbindelse med berigelse af data.
Andet	P.t. ikke definerede værdier ignoreres i forbindelse med berigelse af data.

Ud fra OrganisationId forsøges der at slå organisationsdata op i det register der svarer til hvad der er angivet i source-attributten. Dvs. yderregisteret hvis source er ”yder” osv. Ved opslaget skal der tages højde for at registreringsservicen kan kaldes med log-data bagud i tid. Dvs. at DateTime i logningen kan være være alt fra nogle få millisekunder til adskillige dage bagud i tid. Der skal derfor sikres at der kan slås op i historiske organisationsdata, således at navnet på nedlagte organisationer også kan findes.

Er OrganisationId ikke angivet, eller kan der ud fra OrganisationId ikke findes organisationsdata ved opslag i stamdata, anvendes i stedet OrganisationName såfremt dette er angivet i registrerings-servicen.

Endeligt er det muligt at der ikke er angivet organisationsdata, dvs. at hverken OrganisationId eller OrganisationName er angivet.

6.4.2 Berigelse med persondata

I registreringsservicen er der muligt at angive PersonIdentifier. Er PersonIdentifier angivet anvendes dette til at forsøge at slå organisationsdata op i stamdata, ud fra hvad der er angivet i source-attributten:

CPR	Værdien forventes at indeholde et CPR-nummer, der kan slås op i CPR-registret.
Autorisation	Værdien forventes at indeholde et autorisationskode, der kan slås op i autorisationsregistret.
eCPR	Værdien forventes at indeholde et erstatnings-CPR-nummer, aktuelt kan disse ikke slås op i et centralt register. Værdien ignoreres i forbindelse med berigelse af data.
Initialer	Anvendes til bagud-kompatibilitet til gamle receptserver-snitflader, og anvendes muligvis ikke til registreringer længere. Værdien forventes at indeholde initialer på brugeren og ignoreres i forbindelse med berigelse af data.
Andet	P.t. ikke definerede værdier ignoreres i forbindelse med berigelse af data.

Er det ikke muligt at berige med persondata returneres i stedet hvad der er angivet i det tilsvarende navne-element i registreringsservicen, og er der hverken angivet PersonIdentifier eller navn udelades navne-elementet i opslagsservicen.

7 Sletning af data

Data skal slettes efter to år. Dette gælder uanset kilden til data, og regler for opbevaring af data i klidesystemer. Forhold omkring sletning af data er uændret i MinLog 2, men i forbindelse med gruppering og paginering skal der overvejes hvad sletning af en del af data kan betyde.

Det er væsentligt at der sikres at sletning af data sker rettidigt og ikke låser databasen unødvendigt både for skrivninger men specielt for opslag.

8 Optioner og udvidelsesmuligheder

Herunder er beskrevet et antal umiddelbare udvidelsesmuligheder. Afsnit 2.3 Afgrænsninger indeholder desuden enkelte fremtidige udvidelsesmuligheder der ikke forventes at være omfattet af af MinLog 2 i første omgang.

8.1 Medhjælp

Der kan overvejes at udvide med funktionalitet til medhjælpen som aktør (se 3.3.2 (Option) Medhjælp) og udstille en tredje opslagsmulighed som beskrevet under 6.2.3 Eksempel 3: Opslag for

”register-indsigt”. Servicen kan anvendes af samtlige aktører for at slå op på hvad MinLog indeholder af informationer omkring aktørens handlinger.

Funktionaliteten er hovedsageligt beskrevet i ovenstående afsnit, og der er enkelte tilføjelser (markeret med grå tekst) få øvrige steder i teksten.

8.2 Fuldmagtshaver

Som option kan MinLog evt. udvides med funktionalitet til at fuldmagtshaver kan slå op på en borger der har givet vedkommende fuldmagt. Hertil anvendes fuldmagtsservicen udstillet af Digitaliseringsstyrelsen. Fuldmagtshaver optræder på samme måde borger og anvender borger-opslag, og er derfor ikke beskrevet yderligere i dette dokument.

8.3 Integration til E-boks

Som option kan registrering i MinLog 2 udvides med integration til E-boks. Der skal i så fald bl.a. specificeres:

- Efter hvilke kriterier der afgøres at der skal sendes data til E-boks. F.eks. ved samtykke og værdispring.
- Hvor ofte data sendes til E-boks, f.eks. ved månedens udgang.
- Hvordan data præsenteres.
- Alternativt om aftageren selv skal have mulighed for at konfigurere dette, f.eks. via sundhed.dk og FMK-online.

9 Bagud-kompatibilitet

I dag anvendes MinLog 1 af FMK, DDV, TAS og CRT, der alle afleverer logdata via den eksisterende registreringsservice. FMK-online anvender MinLog 1 opslagsservice til hhv. borgeropslag og opslag i medhjælpsloggen, og endeligt anvender Sundhed.dk MinLog 1 opslagsservice til borgeropslag alene.

Det er derfor nødvendigt at der samtidigt udstilles MinLog 1 og MinLog 2 opslags- og registreringsservices på de samme data. Der skal derfor sikres bagudkompatibilitet.

MinLog 1 registrering XML-element		**MinLog 2 registrering XML-element**	
Navn	**Kardinalitet og type**	**Navn**	**Kardinalitet og type**
Activity	[1] String	Destination/ Activity	[1] String, max 75 tegn
EventDateTime	[1] anySimpleType	Destination/ DateTime	[0-1] DateTime
HealthcareProfessional Organization/	[0-1] for ydre element [1] String	Destination/ OrganisationId	[0-1] Streng på max 200 tegn

OrganizationID			
HealthcareProfessional Organization/ OrganizationType	[0-1] for ydre element Enumeration af SHAK, SOR, YDERNUMMER, PNUMBER, CVRNUMBER, COMMUNAL-NUMBER	Destination/ OrganisationId attribut source	[1] Enumeration af SOR, SKS, Yder, CVR-P, CVR, Kommunekode SHAK oversættes til SKS
HealthcareProfessional OrganizationName	[0-1] String	Destination/ OrganisationName	[0-1] Streng på max 200 tegn
PersonCivil-RegistrationIdentifier	[1] String	Destination/ PersonIdentifier	[1] Streng på max 50 tegn Obligatorisk i registreringsservice men kan udelades i opslagsservice og skal udelades hvis CPR er f.eks. 0000000000.
-		Destination/ PersonIdentifier attribut source	[1] Enumeration Udfyldes med CPR evt. eCPR
CorrelationID	[1] String	Destination/ CorrelationID	[0-1] Streng af længde 46
SourceSystemIdentifier	[1] String	Source/ SystemName	[1] Streng på max 25 tegn
UserIdentifier	[1] String	Destination/ UserPerson-Identifier	[1-*] Streng på max 50 tegn. Obligatorisk i registreringsservice men kan udelades i opslagsservice og skal udelades hvis CPR er f.eks. 0000000000.
-		Destination/ UserPerson-Identifier attribut source	[1] Enumeration Udfyldes med CPR evt. E-CPR
UserIdentifier-OnBehalfOf	[0-1] String	Destination/ OnBehalfOf-PersonIdentifier	[0-1] Streng på max 50 tegn.

-		LogDataEntry/ Destination/ OnBehalfOf- PersonIdentifier attribut source	[1] Enumeration Udfyldes med CPR evt. eCPR eller Autorisation

10 Test

MinLog 2 forventes generelt at følge husreglerne for komponenter på NSP'en. Dette gælder også tests.

Endelig dokumentation skal beskrive anvendelse af de brugte værktøjer samt angive specifikke versioner deraf. Desuden skal dokumentation beskrive, hvordan de forskellige typer af tests skal udføres

10.1 Unittest

Der skal foretages automatiserede unittests af udviklet kode. Dette skal ifølge NSP husreglerne ske med JUnit3, JUnit4 (anbefalet) eller TestNG. Afvikling af unittests er en del af NSP bygge- og releaseprocessen, og skal enten indgå direkte i bygget, eller kunne udføres separat efter anvisning i medfølgende dokumentation.

Code-coverage af unit-tests skal måles ved anvendelse af enten Clover eller Cobertura. Code coverage forventes at være på 80%

10.2 Integrationstest

Der skal udføres integrationstests, på MinLog2 funktionalitet deployet på applikationsserveren. Integrationstesten skal bl.a. indeholde en test af registreringsservicen, transportlaget og opslagsservices.

Der skal udformes krav til udbygning af testmiljøerne, således at de nye egenskaber i MinLog2 kan testes i de fælles testmiljøer. Et kendt problem er manglende mulighed for at rekvirere testpersoner med faste familierelationer så forældremyndighedsindehaver/værge test kan udføres. Denne delopgave bør dække af den opgradering af test-miljøerne, der er aftalt i ØA-16.

10.3 Performance- og stabilitetstest

10.3.1 Forudsætninger for performance- og stabilitetstest

Performance test af komponenter bør foretages med JMeter.

Der skal sikres at performancetests tester registrering og opslagsservices. Herunder at de forskellige typer af opslag testes på realistiske datamængder, og med opslag der viser at paginering kan foretages med overholdelse af svartidskrav.

10.3.2 Baseline (og ramp-up-test)

Systemet der testes på skal være veldefineret. Der forventes at kravene til performance og stabilitet testes på testmiljøerne.

Der kan overvejes om det vil give mening at finde et veldefineret baseline for dette system, for at kunne relatere til evt. andre testsystemer der anvendes. Med en ramp-up-test identificeres baseline for systemets performance på det pågældende system.

Der stilles ikke krav om udførsel af ramp-up test.

10.3.3 Svartidstest

Formål

Formålet med svartidstesten er er at måle systemets svartider, som oplevet af brugere eller services, der anvender servicen der testes på.

Services under test

Registreringsservicen anvendes ikke direkte af brugere, det er dog alligevel væsentligt at registreringsservicen alene ikke er en begrænsende faktor. Dette testes hovedsageligt i load testen. Der skal dog foretages en svartidstest, der viser at svartiderne for registreringsservicen overholder de i afsnit 11.3 Svartider angivne værdier.

Det er væsentligt at opslagsservices testes. Opslagsservices bør som udgangspunkt testes i alle de varianter opslag kan foretages. Enkelte varianter kan dog udelades, hvis forskellen til en anden testet variant er testet andet sted til at være uden betydning, eksempelvis sortering kronologisk og omvendt kronologisk rækkefølge.

- Borger-opslag på ”MinLog”
  - Med gruppering
  - Uden gruppering
  - Med alle detaljer
  - Uden detaljer
  - Sorteret kronologisk
  - Sorteret omvendt kronologisk
  - Med angivelse af dato-interval
  - Uden dato-interval

- Sundhedspersoners på medhjælpsloggen
  - (Som Borger-opslag)

- Eventuelt opslag for ”register-indsigt”
  - (Som borger-opslag)

Svartiderne skal i alle tilfælde overholde de i afsnit 11.3 Svartider angivne værdier.

10.3.4 Load test

Formål

Formålet med load testen er at måle systemets performance.

Services under test

Registreringsservicen testes med de i afsnit 11.1 Datamængder og 11.2 Kald-mængder beskrevne belastninger for gennemsnitligt i dagtimerne pr. time og i travl time.

Opslagsservices testes. Det er væsentligt af de forskellige typer af opslag testes, på samme måde som angivet under Svartidstest herover. Der testes med de i afsnit 11.2 Kald-mængder beskrevne belastninger for kald gennemsnitligt i dagtimerne pr. time og kald i travl time.

10.3.5 Skalebarhedstest

Formål

Formålet med en skalebarhedstest er at afklare hvordan systemet agerer i takt med at belastningen øges.

Services under test

Det er væsentligt at registreringsservicen med udgangspunkt i de i afsnit 11.1 Datamængder og 11.2 Kald-mængder beskrevne belastninger, og at belastningen øges herfra. Det forventes at trafikken på registreringsservicen kan øges som konsekvens af at flere systemer vil logge til MinLog2.

For oplagsservicen forventes ikke væsentligt ændret belastning, det er dog væsentligt at få afklaret hvorledes denne service skalerer. Dette testes igen med udgangspunkt i de i afsnit 11.2 Kald-mængder beskrevne værdier, men der er ikke krav om at alle kombinationer beskrevet under Svartidstest testes, der kan f.eks. tages udgangspunkt i det dårligst performende opslag.

10.3.6 Stresstest

Formål

En stresstest foretages for at sikre, at systemet ikke bliver ustabilt under ekstremt højt load. Formålet med testen er i denne sammenhæng først og fremmest at at vise driftsmæssig stabilitet under unormale omstændigheder, f.eks. en en opstartsfase.

Som en del af stresstesten skal det fastslås, at systemet ”falder til ro” på et normalt leje, når perioden med ekstremt højt load igen er overstået.

Paginering bør som minimum testes her.

Services under test

Der skal foretages stresstest af registreringsservicen.

Stresstest vurderes være mindre relevant for opslagsservices, hvorfor der ikke er krav om at der foretages stresstest for denne.

10.3.7 Udholdenhedstest

Formål

En udholdenhedstest foretages for at sikre, at systemet ikke degraderer over tid.

Testen udføres ved at belaste systemet over i længere periode, mens systemets ressourceforbrug overvåges

Under testen er det normalt, at systemet har en initialt stigende ressourceforbrug, men ressourceforbruget bør efter en kort indkøringsperiode stabiliseres.

Services under test

Der skal foretages udholdenhedstest af registreringsservicen.

Udholdenhedstest vurderes være mindre relevant for opslagsservices, hvorfor der ikke er krav om at der foretages udholdenhedstest for denne.

11 Øvrige non-funktionelle krav

11.1 Datamængder

MinLog databasen indeholder 1.352.000.000 registreringer (januar 2017), den har et dagligt ind/ud flow på *i gennemsnit* ca. 2.4 millioner records. Registreringerne kommer fra FMK, Tilskudsansøgning-servicen (TAS) og CTR. Da andre dataleverandører på sigt vil levere MinLog registreringer vil antallet af registreringer stige.

Tal fra produktion viser at logdata fra FMK udgør langt den største del. For FMK antages det at 80% af registreringerne sker nogenlunde jævnt fordelt over 7 timer pr. døgn.

Dette giver følgende datamængder for MinLog 1 og med de *nuværende systemers logninger.*

Periode	Antal registreringer
Datamængde, normalværdi	1.352.000.000
Afledt tal for registreringer på en normal arbejdsdag (logdata for 2 år med 250 arbejdsdage/år)	2.400.000

I MinLog 2 udvides der med yderligere datafelter. Dette vil medføre at den samlede datamængde målt i GB vil vokse, men ikke målt i antal registreringer. Aktuelt er databasens størrelse omkring 200 GB. Med en passende normalisering af f.eks. source-attributter, enumerations m.v. bør datamængden med de nuvænde data fra FMK, TAS og CTR ikke vokse med mere end maksimalt 10%. Logningerne vil svare til 4.2.7 Eksempel 2: Logning af opslag fra andet system, dvs. ud over source-attributter, enumerations m.v. hovedsageligt yderligere et source-systemnavn. Efterhånden som ny funktionalitet i MinLog tages i brug vil denne datamængde dog forventes at vokse yderligere.

11.2 Kald-mængder

Registreringsservices kan indeholde lige fra en enkelt registrering pr. kald. og til ”mange” registreringer samlet i kald. Der er ikke defineret nogen øvre grænse, ud over hvad der er praktisk muligt i forhold til dokumentstørrelser og overførselstider.

Aktuelt (januar 2017) er registreringsservicen taget i brug af CTR, der ikke anvender en tilstrækkelig gruppering og i øvrigt har fejl i implementeringen, der betyder at der logges for meget data. Dette belaster registreringsservicen unødvendigt, og er rapporteret til CTR som fejl / uhensigtsmæssigheder der skal rettes. Tidligere hvor FMK var den væsentligste anvender har servicen ikke været voldsomt belastet. Bedste bud er at belastningen fra CTR ikke bør være mere end det dobbelte af den belastning der stammer fra FMK (CTR trafikken sker pga. receptudstedelser via FMK, og der er et begrænset antal recepter der udleveres på mere end 3 gange).

Opslagsservicen er i dag ikke voldsomt belastet, og det forventes heller ikke nogen større trafik på denne under normale omstændigheder. Dog skal servicen kunne tåle en større belastning end hvad der normalt forekommer i dag, for at kunne håndtere en pludselig interesse, eksempelvis som følge af misbrugssager i medierne.

Følgende er *nuværende kald- og datamængder* fra FMK, der udgør langt den væsentligste del. FMK opsamler logdata i et tidsvindue på 15 minutter. Antallet af service-kald der skal anvendes i MinLog2 er ikke fastlagt, men kan fastlægges i en implementationsfase og evt. senere optimeres.

Periode	Kaldmængder
Antal registreringskald fra FMK i et normalt døgn.	20.000
Antal registreringskald fra CTR i et normalt døgn.	400.000 – 500.000 Se bemærkning om CTR herover

Opslagsservices kaldes fra sundhed.dk og FMK-online:

Periode	Kaldmængder
Opslagsservice i alt, pr. dag	6000 service-kald
Opslagsservice i alt, gennemsnitligt i dagtimerne pr. time	600 service-kald
Opslagsservice, i travl time (2 gange ovenstående)	1200 service-kald

Lægers opslag på medhjælpsloggen udgør kun en mindre del af opslagene. Der sker mellem 100 og 200 opslag pr. uge, målt som opslag foretaget af unikke læger, dvs. hvor paginering ikke tælles som separate opslag.

11.3 Svartider

Servicemålene herunder er for henholdsvis MinLog 2 registreringsservices (svartider opdatering) og MinLog opslagsservices (Svartider forespørgsler).

Service	Servicemål
Svartider opdatering	95 % af tilfældene ≤ 6,5 sek
	98 % af tilfældene ≤ 15,5 sek

Svartider forespørgsler	95 % af tilfældene ≤ 2,5 sek
	98 % af tilfældene ≤ 5,5 sek

11.4 Auditlogning

Audit logning foregår også gennem log4j, til kategorien ”audit”. Auditlogning skal logge

- Tidspunkt (zulu tid)
- Bruger-id
- Type af anvendelse
- Borgeren
- CVR for kaldende system
- Sessions-id fra DGWS

Typen af anvendelse er metodekaldet (LogDataAdd). Dette er nødvendigt da der også auditlogges fra andre services.

11.5 SLA-logning

Service Level Agreement (SLA) logning understøttes ved hjælp af (SLA) logningsfunktionaliteten i NSPUtil. SLA-logningen logger kald til servicen og består bl.a. af:

- Tidspunkt for kald
- Navn på den invokerede metode
- Tidsmæssig længde på kaldet
- Id på den besked, der behandles.

11.6 Debug-logning

Fejl- og debuglogning implementeres vha. log4j i en separat debug-log. I denne log logges exceptions og stacktraces for evt. fejl der kastes samt, hvis konfigurationen sættes til ’debug’-niveau, et trace af flowid ved entry/exit af servicemetoderne.

Debuglogningen er implementeret for at muliggøre, i tilfælde af fejlsøgning, at man kan følge et flowid (og derved en besked) i mellem servicekald.

11.7 Krav til leverancer

NSP Operatøren har forskellige krav som skal være opfyldt ved en leverance til platformen:

- De nyeste husregler som bør følges: https://www.nspop.dk/display/web/Husregler
- Dokumentation: https://www.nspop.dk/display/web/NSP+projektets+dokumentationskrav
- Øvrig NSP dokumentation: https://www.nspop.dk/display/web/Dokumentation

Dette dokument bør også leveres med leverancen og derudover bør der også skrives en change.log eller tilsvarende hvor ændringer som ikke er fastholdt andre steder fastholdes.

12 Ændringslog

Dette afsnit indeholder ændringer og tilføjelser til beskrivelsen, som er kommet til efter at udviklingsopgaven er påbegyndt. Ændringer i dette afsnit er ikke nødvendigvis endnu aftalt med alle parter, med mindre dette fremgår af teksten.

12.1 Ændringer til version 1.6, 2016-03-24

12.1.1 Ændring: SessionID ændres til CorrelationID

Termen session-id er anvendt i mange andre sammenhænge, bl.a. i forbindelse med HTTP-sessioner og i MedCom-headeren. For at undgå misforståelser er den danske term ændret til ” opslags-sammenhæng”, og SessionID til CorrelationID.

12.1.2 Præcisering: Valideringsregler for …PersonIdentifier-felter

I tidligere versioner var der meget overordnet beskrevet at der skulle sikres at person-id’er indeholder meningsfyldte data. I afsnit 4.4 Valideringsregler er dette blevet præciseret.

Disse definitioner skal kunne udvides, således at nye og på nuværende tidspunk ukendte person-id’er kan anvendes. Dette gøres svarende til FMK’s konstruktion for OrganisationIdentifier, hvor der defineres en union af kendte definerede værdier og en simpel streng.

FMK’s definition for OrganisationIdentifier.xsd der kan findes på http://wiki.fmk.netic.dk/doku.php?id=fmk:1.4.6:wsdl_og_xml_skemaer

12.1.3 Præcisering: Opslag i stamdata

Afsnit 6.4 Berigelse med stamdata er tilføjet, med en beskrivelse af hvordan stamdata beriges på opslagstidspunktet. Det tidligere afsnit 5.1 om berigelse af organisationsnavn er flyttet til 6.4.1 Berigelse med organisationsdata. Der er tilføjet et tilsvarende afsnit 6.4.2 Berigelse med persondata.

12.1.4 Udvidelse: Felter til navn på borger, bruger og på vegne af

Registreringsservicen er udvidet med optionelle felter til navn på borger, bruger samt navn på brugeren handlingen er udført på vegne af. Dvs. felterne PersonName, UserPersonName og OnBehalfOfPersonName. Disse tre felter er optionelle, og kan udelades når der anvendes CPR-nummer, autorisationskode mm. Regler for hvornår anvendersystemerne skal anvende disse tre felter når registreringsservicen kaldes fastlægges og beskrives i vejledningsdokumentet. Felterne PersonName, UserPersonName og OnBehalfOfPersonName er udvidelser i forhold til MinLog (1) registreringsservicen.

I opslagsservicen er der på samme måde beskrevet felter til navn. I MinLog (1) findes der felter svarende til PersonName (borger), UserPersonName (bruger) og OnBehalfOfPersonName (bruger på vegne af). MinLog (1), og der udføres en berigelse omtrent svarende til hvad der er beskrevet i 6.4.2 Berigelse med persondata for at udfylde disse værdier med data. Disse felter mangler i tidligere versioner af løsningsbeskrivelsen.

MinLog (1) returnerer ”id ikke kendt” i navnefelterne hvis det ikke er muligt at slå op ud fra CPR-numer m.v. Kan der i MinLog 2 ikke slås op ud fra CPR-nummer, autorisationskode m.v. returneres navnet der er angivet i registreringsservicen, ellers udelades elementet.

12.2 Ændringer til version 1.7, 2017-05-09

12.2.1 Udvidelse: Reason-felt tilføjet

I registrerings- og opslagsservices er der tilføjet et optionelt reason-felt. Feltet anvendes ved opslag der umiddelbart ikke er oplagt for bruger hvorfor opslaget er sket. Eksempelvis i support-sammenhæng, ved behandling af tilskudsansøgniner m.v.

Reason-feltet er beskrevet i 4.2.9 Indhold i kald-dokumentet og 6.3.2 Grupperet svar.