Experience the commitment®

Samtykke understøttelse i SvarEksponeringService

Sundhedsdatastyrelsen
Udvidelse af SvarEksponeringService

Lautruphøj 10, DK-2750 Ballerup
02.09.2016 1.02

Indhold

1 Indledning

Dette dokument beskriver hvorledes den eksisterende SvarEksponeringService ændres således at denne kan indgå i samtykke filtrering af de laboratoriesvar, der returneres fra SvarEksponeringServicen.

Dokumentet forpligter ikke Leverandøren, men beskriver opgaven som estimatet er baseret på.

Dokumentet beskriver det brugsrelaterede anvendelsesmønster for den udvidede svareksponerings-service samt tekniske overvejelser og standards, der benyttes. Da SvarEksponeringServicen kun udstiller data, der benyttes i eksterne brugergrænseflader (skærmbilleder), indeholder dokumentet ikke beskrivelser af bruger grænseflader, men kun system-grænseflader.

1.1 Læsevejledning

Dokumentet er rettet mod:

1. Kundens deltagere der skal vurdering løsningen
2. Læsere der ønsker overblik over hvorledes servicen fungerer sammen med omgivende løsninger
3. Eksterne interessenter, som skal bidrage til den samlede løsning.

Alle læsere bør læse afsnit 3.1, der indeholder den overordnede beskrivelse af hvorledes servicen fungerer i samspil med omgivende systemer. Dette skal sikre at alle har samme opfattelse af, hvorledes opgaven løses på tværs af bidragsydere.

Kundens deltagere bør forholde sig til indholdet af kapitel 2, der beskriver afgrænsningen af opgaven. Indholdet i kapitel 2 er brugt som afsæt til at udarbejde løsningsbeskrivelsen.

1.2 Referencer og baggrundsmateriale

Betegnelse	Bemærkning
SJ2 – filtrering af laboratoriesvar v1.2.pptx	Lakesides beskrivelse af opgaven.
SvarEksponeringService ServiceKontrakt.pdf	CGI's beskrivelse af servicekontrakt
Detailplan	Tidsplan og estimater

2 Behovsopgørelse

Kunden har ikke udarbejdet en behovsopgørelse. De behov, der er angivet i beskrivelsen udtrykker de behov, CGI har udledt af dialogmøder og tilsvarende.

2.1 Baggrund

Der er i stigende grad fokus på sikkerhed og beskyttelse af data. Dette kommer eksempelvist til udtryk i forbindelse med udstilling af laboratoriesvar i sundhedsjournalen. Sundhedsjournalen undergår pt. en omlægning, der blandet andet skal sikre at brugere ikke har mulighed for at se informationer om borgere der har frabedt sig elektronisk indhentning jf. sundhedslovens §42a.

Sundhedsjournalen får sine data fra eksterne kilder. Derfor er der brug for at alle eksterne kilder understøtter muligheden for at filtrere data i henhold til samtykke regler.

Der er allerede udviklet en Samtykkekomponent, der understøtter registrering af samtykke. Samtykkekomponenten udstiller herudover services, som skal benyttes til filtrering af data, der eksponeres for brugere i fx sundhedsjournalen.

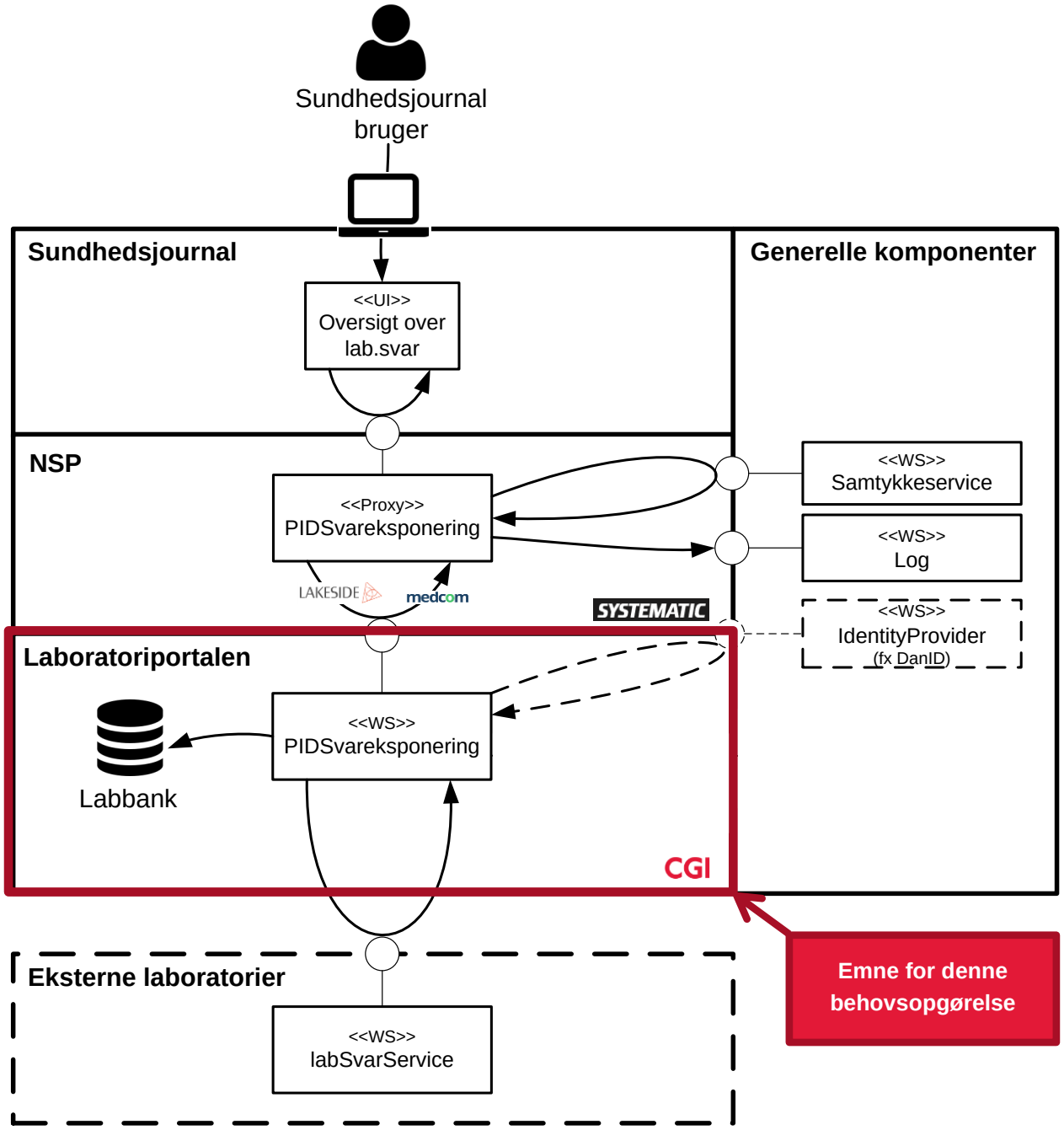
For at;

- sikre en ensartet brug af samtykkeservices og samtidigt
- optimere anvendelsen af den nationale serviceplatform og endeligt
- sikre at samtykke information ikke tilgås af mange forskellige løsninger

er det besluttet at alle datakilder ikke selv skal benytte samtykke services, men blot beriger service svar med information, der sætter den nationale service platform i stand til at udføre samtykke filtreringen.

Den nationale service platform har ligeledes ansvaret for at logge 'hvem, der har set hvad, hvornår' samt håndtering af værdispringsreglen.

Ansvarsfordelingen mellem sundhedsjournalen, den nationale service platform, log, samtykke komponenten og Laboratorieportalen (SvarEksponeringServicen) er illustreret i figuren nedenfor:



Figur 1 - overbliksfigur - komponenter og ansvar

2.2 Funktionelle behov

De funktionelle behov er rettet mod tilpasning af den eksisterende SvarEksponeringService. Behov vendes mod de 2 hovedelementer i servicen:

- Request – kald af servicen
- Response – svar fra servicen

Behovene er udelukkende rettet mod den del af den samlede løsning, der er markeret med rødt i Figur 1 - overbliksfigur - komponenter og ansvar.

2.2.1 BEHOV VENDT MOD SERVICE SVAR

I forbindelse med udstilling af laboratoriesvar på sundhedsjournalen er der brug for at den eksisterende SvarEksponeringService udvides sådan at servicen sætter den nationale service platform i stand til at filtrere i henhold til samtykke. Konkret skal svaret fra SvarEksponeringServicen overholde PIH (Privacy Information Header). For mere information vedr. PIH, henvises til dokumenterne beskrevet i afsnit Referencer og baggrundsmateriale

Behov #1	**Udvidelse af svar fra SvarEksponeringServicen**		
Kategori:	-	Type:	Funktionel
Beskrivelse:	Den eksisterende SvarEksponeringService udvides med en Privacy Information Header (PIH), der sætter den nationale service platform i stand til at afgøre (via kald til Samtykkekomponenten) hvorvidt et/flere svar skal fra-sorteres det endelige svar til sundhedsjournalen. PIH skal indeholde nøglen; cprnr, SHAK/SOR-kode[1] og svardato samt referencer til de konkrete mappede- og leverandørsvar, der er knyttet til nøglen. De enkelte mappede- og leverandørsvar skal udvides med en entydig ID attribut der skaber relationen mellem PIH og svaret.		

2.2.2 BEHOV VENDT MOD INDGÅENDE KALD AF SERVICEN

2.2.2.1 AUTENTIFICERING

Der skelnes mellem autentificering af brugere og virksomheder. I første version af PIHSvarEksponeringServicen autentificeres på brugerniveau og i 2. version autentificeres på virksomhedsniveau.

Behov #2	**Autentificering**		
Kategori:	-	Type:	Funktionel
Beskrivelse:	PIHSvarEksponeringServicen skal kunne verificere brugere, der er identificeret med brugernavn og password i Laboratorieportalens brugerdatabase. Brugere der ikke har et kendt brugernavn og password i Laboratorieportalens database skal afvises.		

[1] SHAK eller SOR kode skal være for den rekvirerende afdeling. Ikke laboratoriet.

2.2.2.2 FILTRERING

Indgående kald til PIHSvarEksponeringServicen skal understøtte den filtrering, der pt. benyttes i den eksisterende svarEksporneringsservice – dvs. cprnr, periode og evt. valg laboratoriespecialer.

Behov #3	**Filtrering/søgekriterier**		
Kategori:	-	Type:	Funktionel
Beskrivelse:	PIHSvarEksponeringServicen skal kunne modtage samme filter/søgekriterier som den eksisterende SvarEksponeringService: • Cprnr • Periode (fra og til dato) • laboratoriespecialer		

Parametre der skal anvendes ved service kald, er specificeret i dokumentet SvarEksponering Servicekontrakt. Se afsnit Referencer og baggrundsmateriale

2.3 Non-funktionelle behov

Da der udelukkende er tale om ændring/udvidelse af den eksisterende SvarEksponeringService, er der ikke ændrede behov til emner, der ikke eksplicit er nævnt i behovsopgørelsen – eksempelvist er der ikke ændringer til:

- **Løsningsarkitektur** – Kunden har ingen præferencer i forhold til Leverandørens valg af løsningsarkitektur, men for at minimere omkostninger forventes det at PIHSvarEksponeringServicen følger den løsningsarkitektur, der allerede benyttes i den eksisterede SvarEksponeringService. Den eksisterende SvarEksponeringService skal genbruges.
- **Platformsarkitektur** – PIHSvarEksponeringServicen skal afvikles på den allerede etablerede platform idet det forventes at PIHSvarEksponeringServicen ikke fordrer yderligere investering i hverken dimensionering eller bestykning af hardware/software i nogen af de miljøer, der allerede er etableret.
- **Teknologisk platform** – Kunden har ingen præferencer i forhold til Leverandørens valg af teknisk platform, men for at minimere omkostninger, forventes det at der benyttes samme tekniske platform, teknologistak mv., som allerede anvendes i den eksisterende SvarEksponeringService.
- **Logning og fejlhåndtering** – ingen yderlige behov idet det forventes at der benyttes samme logning og fejlhåndtering som den eksisterende SvarEksponeringService
- **Monitorering og Service Level Agreement (SLA) målinger** – ingen yderligere behov idet det forventes at der benyttes sammen monitorering SLA målinger som den eksisterende SvarEksponeringService.
- **Overholdelse af love** – ingen yderligere behov i forhold til den eksisterende SvarEksponeringService.

2.3.1 DOKUMENTATION

Som dokumentation af PIHSvarEksponeringServicen skal Leverandøren udarbejde et servicekatalog, der kan anvendes af 3. part til konstruktion og test af kald af PIHSvarEksponeringServicen.

Behov #4	**Dokumentation**		
Kategori:	-	Type:	Non-funktionel
Beskrivelse:	Leverandøren skal udarbejde et Servicekatalog som specificerer: • Hvorledes 3. part får adgang til servicen • Hvorledes 3. part tester servicen • Eksempler på requst og response objekter • Forklaring af sammenhænge mellem PIH <location> elementerne og de tilhørende ID attributter på rekvistions- og leverandørsvar.		

Servicekataloget er dokumenteret i SvarEksponeringService Servicekontrakt.pdf

3 Løsningsbeskrivelse

Løsningsbeskrivelsen adresserer alle funktionelle- og non-funktionelle behov, der er beskrevet i behovsopgørelsen.

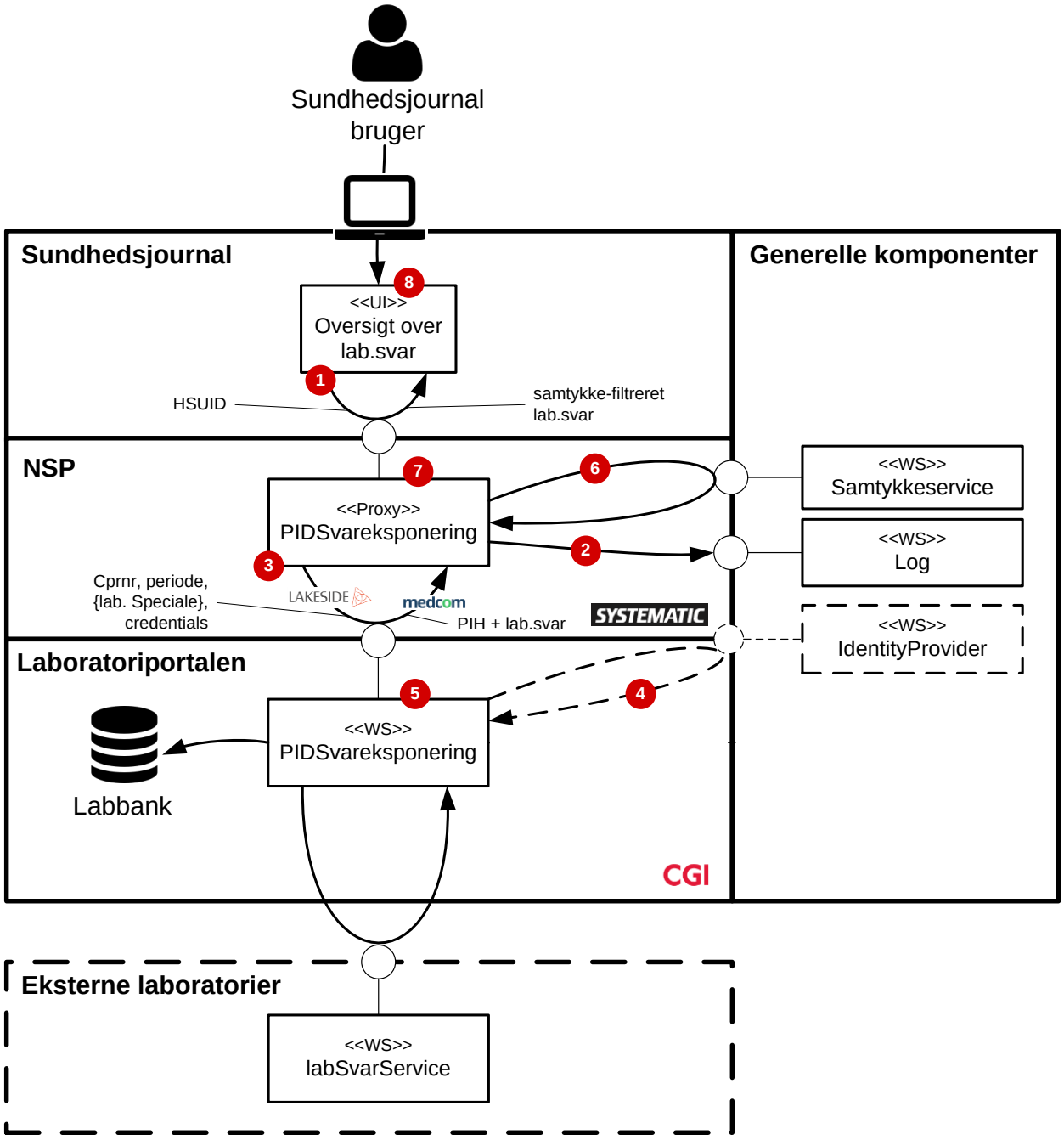
Kapitlet indledes med et overblik, der præciserer CGIs rolle i den samlede arkitektur. Overbliksafsnittet fastholder de enkelte leverandørers rolle/ansvar og indeholder samtidigt en summarisk beskrivelse af CGIs bidrag til den samlede løsning. Læsere der ikke har brug for detaljeret viden, vil ikke finde det nødvendigt at læse andet end dette afsnit.

Kapitlet indeholder derudover mere detaljerede beskrivelser af hvorledes løsningen adresserer de enkelte behov. Besvarelsen beskriver løsningen ud fra forskellige perspektiver:

- Et logisk perspektiv – hvor funktionelle behov adresseres
- Et teknisk perspektiv – hvor tekniske non-funktionelle behov adresseres. I dette afsnit beskrives også den dokumentation der leveres.

3.1 Overblik

Sundhedsjournalen kommunikerer ikke direkte med PIHSvarEksponeringServicen. Fra en bruger har bedt om at se oversigt over laboratoriesvar til oversigten er populeret, gennemløbes en række systemer, der har hver sit ansvar i forbindelse med dannelsen af oversigten over laboratoriesvar.



Figur 2 - flow gennem systemer ved besvarelse af forespørgsel på laboratoriesvar

Figuren ovenfor bruges som afsæt til at give det samlede billede af hvorledes informationer 'flyder' gennem de forskellige systemer.

3.1.1 STORY

Udgangspunktet er at brugeren ønsker at se en oversigt over laboratoriesvar for en given borger og en given periode (evt. yderligere afgrænset på laboratoriespecialer).

1 Når brugeren har valgt borger, periode + evt. laboratoriespeciale i sundhedsjournalens brugergrænseflade, kalder sundhedsjournalen web-servicen 'hentsvar' på den nationale serviceplatform (NSP). Ved kaldet til NSP, udfylder sundhedsjournalen data i den struktur, der er benævnt HSUID.

2 Når den nationale serviceplatform modtager kaldet logges at brugeren har udført kaldet.

3 Da NSP ikke selv indeholder laboratoriesvar, kalder NSP videre til PIHSvarEksponeringServicen. PIHSvarEksponeringServicen kaldes med input-parametrene, der har initieret kaldet. NSP trækker disse inputparametre ud af HSUID og kalder videre til PIHSvarEksponeringServicen.

4 Når PIHSvarEksponeringServicen modtager kaldet, valideres først at brugeren har lov til at se en oversigt over laboratoriesvar.

5 Såfremt brugeren/virksomheden har adgang til PIHSvarEksponeringServicen, kalder PIHsvareksponerinsservicen den eksisterende SvarEksponeringService, der finder alle kendte laboratoriesvar, der matcher inputparametrene. PIHSvarEksponeringServicen gennemløber hvert enkelt laboratoriesvar fra SvarEksponeringServicen og bygger indholdet i PIH. Som svar returnerer PIHSvarEksponeringServicen PIH (header) samt de tilhørende laboratoriesvar (body).

6 Når NSP modtager svaret fra PIHSvarEksponeringServicen, benytter NSP Samtykke komponenten til at afgøre hvorvidt der er laboratoriesvar, der ikke må returneres til brugeren (negativt samtykke). Dette gælder dog kun såfremt brugeren ikke har valgt at benytte værdispringsreglen – i givet fald returneres alle svar (ufiltreret).

7 NSP fjerner de laboratoriesvar, brugeren ikke har lov at se og summerer totale antal svar (fra PIHSvarEksponeringServicen) samt antal svar, der er filtreret fra i det endelige svar og sender dette tilbage til sundhedsjournalen.

8 Når sundhedsjournalen modtager svaret fra NSP, præsenteres dette endeligt for brugeren.

3.1.2 SYSTEM LEVERANDØR ROLLE/ANSVAR

System	Rolle/ansvar	Leverandør
Sundhedsjournalen	Brugerkommunikation Få input fra bruger (valg af borger, periode og laboratoriespeciale). Skal entydigt identificere brugeren og virksomheden. Præsentere laboratoriesvar for brugere med angivelse af om der findes skjulte svar.	Sundhedsdata-styrelsen
Den Nationale Service Platform (NSP)	Logning, filtrering i henhold til samtykke, håndtering af værdispring samt agere bindeled mellem anvender af laboratoriesvar og kilde for laboratoriesvar. Optræder som bindeled ved at udstille en 'proxy-service' der viderestiller til PIHSvarEksponeringServicen.	Systematic
Laboratorieportalen	Datakilde for alle laboratoriesvar. Udstilling af PIHSvarEksponeringService i henhold til denne løsningsbeskrivelse.	CGI
-	Definition af PIH samt generelle/tekniske problemstillinger vedr. håndtering af flow'et gennem kald gennem de forskellige systemer.	Lakeside

3.2 Det logiske perspektiv - funktionelle Behov [Behov #1 – 3]

Afsnittet forklarer hvorledes de funktionelle behov adresseres i løsningen.

Afsnittet er henvendt til læsere, der ønsker at forstå hvorledes PIHSvarEksponeringServicen er en overbygning på den eksisterende SvarEksponeringService samt forstå hvorledes PIH konstrueres.

3.2.1 PIHSVAREKSPONERINGSERVICEN

PIHSvarEksponeringServicen er en overbygning på den eksisterende SvarEksponeringService.

PIHSvarEksponeringServicen er en udvidelse i forhold til SvarEksponeringServicen idet denne:

- Vil indeholde en Privacy Information Header (PIH) jf. [Behov # 1]
- Validerer brugeradgang jf. [Behov #2]
- Vil bl.a. benytte nogle af samme filtre/søgekriterier som den eksisterende SvarEksponeringService jf. [Behov # 3]

3.2.1.1 BEHANDLING AF KALD TIL SERVICEN [BEHOV # 2, BEHOV # 3]

3.2.1.1.1 Autentificering [Behov # 2]

I første iteration, vil PIHSvarEksponeringServicen benytte helt samme autentifikationsmekanisme som benyttes i den eksisterende SvarEksponeringService. Dette betyder dels at brugeren skal være kendt i Laboratorieportalen og dels at brugeren skal være identificeret med brugernavn og password i kaldet til PIHSvarEksponeringServicen.
Første version af PIHSvarEksponeringServicen vil således blot kalde videre til den eksisterende SvarEksponeringService, der allerede foretager den ønskede autentificering af brugeren.

PIHSvarEksponeringServicen udfører ikke nogen form for autorisationsstyring. Brugeren/virksomheden forventes at have adgang til at se laboratoriesvar[2].

3.2.1.1.2 Filtrering af svar [Behov # 3]

PIHSvarEksponeringServicen er blot en overbygning på den eksisterende SvarEksponeringService. PIHSvarEksponeringServicen identificerer filtrene/søgekriterierne i det indkommende kald og bruger disse i opbygningen af kaldet til den eksisterende SvarEksponeringService. For beskrivelse af parametre til PIHSvarEksponeringServicen, se dokumentet SvarEksponeringService Servicekontrakt.pdf

3.2.1.1.3 Bemærkninger vedr. håndtering af fejl

PIHSvarEksponeringServicen returnerer følgende fejlkoder:

- AuthenticationError: Hvis brugeren/virksomheden ikke er autoriseret til at kalde servicen
- DataError: hvis der er syntaks-fejl i filtrene/søgekriterierne. Vil herudover indeholde en beskrivende tekst der forklarer fejlen (fx ugyldigt cprnr).
- SystemError: hvis der opstår programfejl i forbindelse med service kald.

[2] Der foretages en form for autorisation i forbindelse med samtykke filtreringen, der foretages af Systematic

NSP har ansvaret for at reagerer på disse fejl-koder. For mere information vedr. fejlhåndtering i SvarEksponeringService se dokumentet SvarEksponeringService Servicekontrakt.pdf

3.2.1.2 RETURNERING AF SVAR FRA SERVICEN [BEHOV # 1]

PIHSvarEksponeringServicen vil returnere en PIH som vist i

PIHSvarEksponeringServicen kalder den eksisterende SvarEksponeringService og behandler svaret fra denne til at opbygge PIH.

3.3 Det tekniske perspektiv

Afsnittet forklarer hvorledes de non-funktionelle behov adresseres i løsningen og er primært henvendt til læsere med teknisk baggrund.

3.3.1 DOKUMENTATIONEN [BEHOV # 4]

Løsningen giver ikke anledning til at den eksisterende dokumentation for Laboratorieportalen ændres – samme driftsvejledning, installationsvejledning, løsningsarkitekturbeskrivelse, datamodelbeskrivelse mv. er gældende.

3.3.1.1 SERVICEKATALOG

Servicekataloget følger de retningslinjer, der er specificeret behov # 4 og oplyse praktisk informationer vedr. eksterne leverandørers adgang til service (herunder også test af servicen), gennemgang af request- og response objekter, eksempler på request og response objekter samt indeholde en forklaring af hvorledes konsumenter af servicen navigerer mellem PIH-id angivelser for hhv. rekvisitioner og lab.svar og de faktiske rekvisitioner og labsvar i svar oversigten. Se afsnit Referencer og baggrundsmateriale

4 Proces og gennemførelse

CGI udfører kun afrapportering i det omfang kunden beder om dette og kunden har ansvaret for al projektstyring – herunder også styring på tværs af leverandører.

CGI har udarbejdet en detailplan, der viser hvornår servicekatalog, test-stub for PIHSvarEksponeringServicen og PIHsvarekponeringsservicen er klar til test hos Multimed. Detailplan findes i afsnit Referencer og baggrundsmateriale

På kundens opfordring deltager CGI i afklaringsmøder og lign. med kundens øvrige underleverandører.

Bilag A – Anvendt notation

4.1.1 BEHOV

Normalt inddeles behov i kategorier. Det er almindeligt at behov enten optræder som behov, som *skal* imødekommes af Leverandøren eller behov som *kan* imødekommes af Leverandøren. I det konkrete tilfælde giver dette ikke mening da der er tale om en timebaseret aftale.

Behov kategori	Beskrivelse
-	

Behov specificeres under benyttelse af nedenstående skema.

Behov #< >	<Behovets betegnelse>		
Kategori:	-	Type:	
Beskrivelse:			

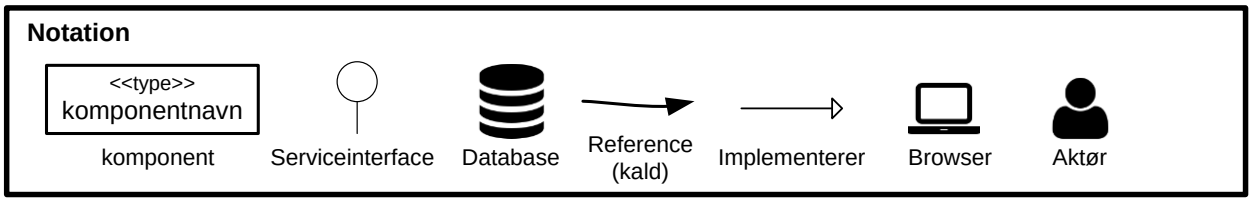
Type er en inddeling af behovet i følgende områder:

- Funktionelt (brugsorienterede behov).
- Ikke-funktionelt (teknisk orienterede behov).

Nederste række af tabellen indeholder en tekstuel beskrivelse af behovet.

4.1.2 FIGURER

Figurer der illustrerer systemlandskab benytter nedstående notationsform (tillempet UML):



En **komponent** er en selvstændig enhed der er bevidst afkoblet og uafhængig af de øvrige komponenter, der indgår i arkitekturen. Alle komponenter har en type. Denne er angivet over navnet på komponenten. Der opereres med:

- <<UI>> user interface – en komponent der understøtter kommunikation med en bruger
- <<WS>> web-service – en komponent der har ansvaret for at udføre en given operation (fx læse data, persistere data, kontrollere data etc.). Web-services kan installeres uafhængigt af omgivende komponenter og kan derfor skaleres selvstændigt. Web-services kender ikke til deres anvendere. Adgang til anvendelse af web-services reguleres gennem sikkerhedsmodeller.
- <<Proxy>> proxy – en proxy er typisk også en web-service. En proxy optræder i rollen andre web-services og simplificerer kald til underliggene web-services. En proxy orkestrerer kald til andre web-services og udfører dermed mange funktioner på én gang.
- <<Codelibraray>> kodebibliotek – kodestumper, der løser en given problemstilling og er beregnet for indlejring i fx web-services. Et kodebibliotek vil meget sjældent kunne anvendes isoleret og udarbejdes typisk for at løse komplekse problemstillinger. Hermed sikres en ensartet løsning af det givne problem og fejl kan isoleres til bestemte kodestumper.

Et **Serviceinterface** udtrykker den kommunikationsmodel, der benyttes ved kommunikation med en web-service. I praksis vil et Serviceinterface være tilgængeligt i en WSDL fil, der viser hvilke metoder, der kan kaldes samt signaturen for hver af disse metoder (input- og output parametre).

Database er en fil, en relationel database, no-sql database eller lign. til permanent opbevaring af data.

En **Reference** benyttes til at angive relationer mellem de forskellige komponenter i arkitekturen. Referencen er altid en-vejs og pilens retning angiver hvilken komponent, der refererer den anden.

En **Implementering** angiver at en given komponent benytter en anden komponent til at udføre dele af sit funktionsområde.

En **Browser** er en kanal, som brugeren benytter til at kommunikerer med UI – andre kanaler kunne være Smartphone, Tablet, Storskærm, PC eller lign.

En **Aktør** udtrykker en bestemt brugerrolle som benytter systemet med et bestemt formål.