

Rapport

Titel: **Konceptuell beskrivning av beroenden mellan BIF, NPÖ & HSA**

Version: **REV B**

Datum: **2009-03-20**

Kontaktpersoner: Sara Meunier, Ulf Palmgren, Lars Johansson,
Johan Zenk, Jan Edquist

Förord

Under första kvartalet 2009 utvecklas upphandlade tjänster för Nationell Patientöversikt (NPÖ) samt Bastjänster för Informationsförsörjning (BIF). NPÖ blir den första tillämpning som skall stödjas av BIF. För att möjliggöra detta krävs en analys av hur BIF och NPÖ skall samverka på konceptuell nivå ur såväl verksamhets- som tekniskt perspektiv. Styrande är Patientdatalagen med tillämpningsföreskrifter.

Ett uppdrag gavs till Arkitekturledningen i januari 2009 att beskriva hur åtkomst till information i NPÖ kan ske på ett lagenligt sätt med stöd av BIF. Juridiska, kliniska och tekniska förutsättningar skulle analyseras på konceptuell nivå så att resultatet kan utgöra grund för anslutningsanvisningar och checklistor. Resultatet av uppdraget levererades i februari 2009 i en rapport REV A. Därefter har inkomna synpunkter från NPÖ-projektet behandlas vilket resulterade i denna uppdaterade rapport, REV B.

Resultatet av uppdraget utgör inleverans till projektet ”BIF i praktiken”. Uppdragets fokus har varit konceptuell beskrivning av samband samt att beskriva de insatsområden som behövs för att få BIF och NPÖ att fungera i praktiken. Strävan har varit att få fram tydligt identifierade problembilder som underlag för nya/kompletterande beställningar för projekt/förvaltningsobjekt.

Uppdraget beskriver inte målbilden för systemsambanden på längre sikt. Uppdraget fokuserar på lösningar för BIF, NPÖ, HSA i närtid, vilket i vissa fall kan bli tillfälliga lösningar för att kunna komma igång. Avvikelse från den långsiktiga målbilden tas inte upp i detta dokument.

Vi som har utarbetat denna rapport är:

- Sara Meunier, Arkitekturledningen, SKL
- Ulf Palmgren, BIF-projektet & SLL
- Jan Edquist, NPÖ-projektet & ÖLL
- Johan Zenk, HSA-förvaltning & LiÖ
- Lars Johansson, HSA Förvaltning & SVR

Sammanfattning

Identifierade områden för fortsatt arbete

Hög prioritet, behöver vara på plats inför första anslutningen till NPÖ/BIF

Följande områden har identifierats som hög prioritet för att BIF och NPÖ skall fungera tillsammans i Örebro.

1. Behörighetsmodell behöver fastställas, se avsnitt 2.6, 3.1 och 4.3.5
2. Förändringar i HSA behöver införas, se avsnitt 3.1.2
3. Loggningsmodell behöver fastställas, se avsnitt 3.2
4. Beslut kring driftslösning BIF och praktiska prov behövs, se avsnitt 2.7 och
5. Gemensam testmiljö behöver tas i drift, se avsnitt 3.8

Medelhög prioritet, behöver vara på plats vid bredare utrullning av NPÖ/BIF

För att BIF och NPÖ skall bli hanterbart när utrullning sker till fler landsting behövs ytterligare åtgärder

6. Prestanda och tillgänglighet behöver analyseras, se avsnitt 3.3
7. Överenskommelser/avtal för anslutning till nationella tjänster behöver utformas, se avsnitt 2.3
8. Tjänstekatalog och adresseringsmodell behöver realiseras, se avsnitt 2.4 och 2.5
9. Kunskapsstöd/Supportfunktion behöver aktiveras hos förvaltningen, se avsnitt 2.8
10. Forum för ändringshantering behöver inrättas hos förvaltningen, se avsnitt 2.9
11. Organisationsförändringar - historik och spärr behöver utredas, se avsnitt 3.4
12. Kvalitetssäkrade/ E-undertecknade egenskaper behöver utredas, se avsnitt 3.5
13. Anslutningsanvisningar och checklistor behöver upprättas, se avsnitt 3.10

Detaljerad lösningsarkitektur

Innan den slutliga lösningsarkitekturen utformas måste verksamhetsperspektivet belysas för nedanstående arkitektur samt praktiska prover i form av referenstillämpning samt Proof of Concept genomföras.

En genomgång av projekten BIF och NPÖ samt leverantörernas lösningförslag återges nedan som några grunder kring deras arkitektur för att realisera BIF och NPÖ. Nedanstående punkter är ett urval av genomgången och som behöver verifieras i praktiska prover.

- För att NPÖ skall kunna hålla sina SLAer så är det troligt att NPÖ behöver ha BIF nära. Eftersom NPÖ är en central instans så behövs det också en egen instans av BIF eller koppling till en nationell instans. Detta är inte samma sak som central toppnod.
- Det är av arkitekturskäl nödvändigt med en rot- eller toppnod av BIF, för implementering/replikering av regelverk. För samtycke och spärr eller de andra tjänsterna har BIF utformats så att det enligt Logica inte skall behövas någon toppnod.
- Administration av samtycke och spärr skall enligt Logica kunna ske i vilken instans som helst, vilket sedan replikeras till samtliga instanser. På samma sätt går det även

att ta bort (inaktivera) spärr från valfri instans, dvs. inte bara från den instans där spärren upprättades.

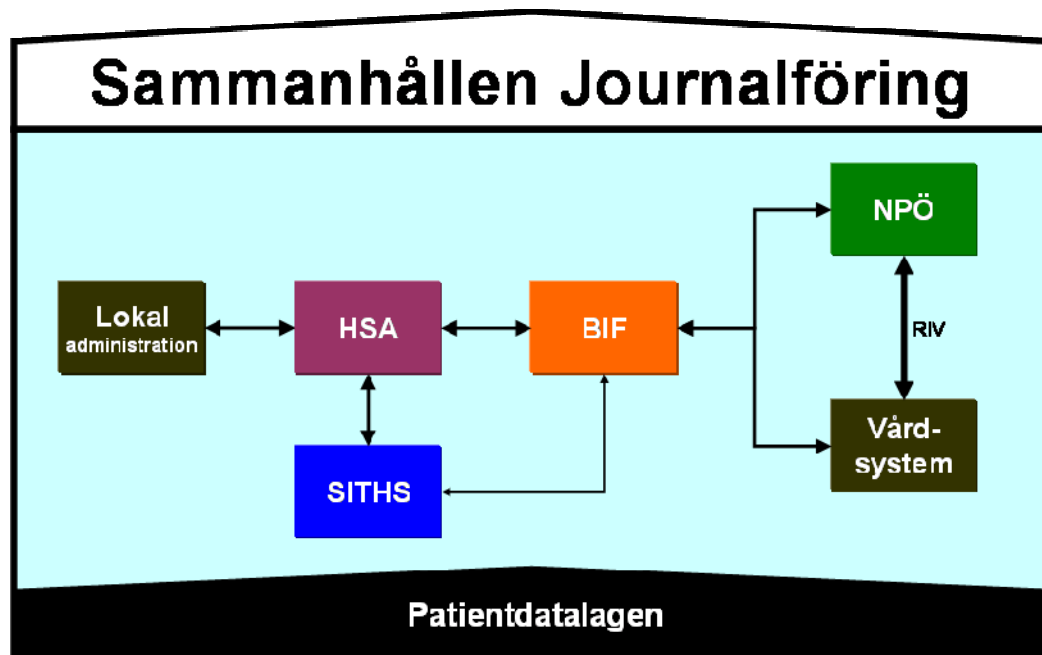
- Ingen begränsning av antalet instanser är satt i dagsläget. Det finns dock ingen motsättning i att börja med antagande om obegränsat antal instanser och sedan replikera upp på en viss nivå om det senare visar sig behövas. Behovet styrs bland annat av kraven i NPÖ, om inte NPÖ har fått tag på en befintlig spärr så kommer informationen att visas. Det är med andra ord viktigt att veta att spärren slår igenom i alla instanser inom rimlig tid. I praktiken förväntas inte antalet spärrar och förändring av spärrar bli särskilt stort.
- En redundant miljö för BIF kräver en lastbalanserare som fördelar lasten mellan instanserna.
- BIF-tjänsterna ansluts fysiskt till HSA lokalt eller centralt för att hämta uppgifter till SAML-biljetten. Anslutning mot central katalog är att föredra.
- Det kommer inte att ske någon åtkomstkontroll av vårddokumentation på respektive vårdsystem/anslutningstjänst utan detta initieras först av NPÖ centralt. Vårdsystemen levererar all information, dvs. spärrad och ospärrad vårddokumentation till NPÖ.

Innehållsförteckning

Förord.....	2
Sammanfattning	3
Identifierade områden för fortsatt arbete	3
Detaljerad lösningsarkitektur	3
1 Konceptuell beskrivning av samverkande tjänster.....	6
1.1 Patientdatalagen 2008:355	7
1.2 HSA, Elektronisk katalog för Vård och omsorg.	8
1.3 SITHS, Säker IT i Hälsa- och Sjukvård.....	8
1.4 BIF, Bastjänster för InformationsFörsörjning	8
1.5 NPÖ, Nationell PatientÖversikt.....	10
1.6 RIV , Regelverk för Interoperabilitet inom Vård och omsorg	10
1.7 Sjunet, Kommunikationsnätet för vård och omsorg.....	10
2 Samband.....	11
2.1 BIF i sitt sammanhang	11
2.2 NPÖ i sitt sammanhang.....	11
2.3 Anslutning till nationella tjänster	12
2.4 Lagring och åtkomst till IT-tjänster	14
2.5 Tjänsteadressering.....	15
2.6 Behörighetshantering	15
2.7 Driftsplattform, instanser av BIF och toppnod.....	17
2.8 Kundstöd/supportfunktion.	20
2.9 Ändringshantering.....	20
3 Insatsområden för ytterligare bearbetning.....	20
3.1 Behörighetshantering	20
3.2 Vad och var loggning skall utföras	24
3.3 Prestanda och tillgänglighet	26
3.4 Organisationsförändringar - historisk data och spärr problematik	27
3.5 Kvalitetssäkrade/ E-undertecknade egenskaper	28
3.6 RIV EN 13606 ska användas	28
3.7 NPÖ ska använda BIF.....	29
3.8 Testmiljö och testdata under utvecklingsfas och driftfas	29
3.9 Läkemedelsförteckningen	29
3.10 Anslutningsanvisningar och checklistor.....	29
4 Detaljerad lösningsarkitektur	32
4.1 HSA	32
4.2 SITHS	33
4.3 BIF	33
4.4 NPÖ	40
4.5 RIV	43
4.6 Sjunet	44

1 Konceptuell beskrivning av samverkande tjänster

Den nationella IT-strategin för vård och omsorg sätter fokus på gemensamma synsätt och lösningar för att förbättra tillgänglighet. För att uppnå visionen har ett antal nationella projekt initierats och som tillsammans kan realisera sammanhållen journalföring utifrån Patientdatalagens krav.



Bilden visar hur nationella tjänster i samverkan realiserar visionen Sammanhållen Journalföring i enlighet med patientdatalagen. Nedan beskrivs respektive tjänsts ansvarsområde:

Nationella tjänster	Beskrivning
HSA, Elektronisk katalog för vård och omsorg	Innehåller säkrade användar- och organisationsuppgifter, dvs. egenskaper. Dessa används av BIF:s regelverk för behörighetsstyrning och av SITHS vid utfärdande av elektroniska ID-handlingar.
SITHS, Säker IT i Hälso- och Sjukvård	Utfärdar kortlagrade elektroniska ID-handlingar baserat på uppgifterna i HSA. ID-handlingen används för att identifiera användaren. För att identifiera tjänster/system kan mjuka SITHS-certifikat utges som baseras på uppgifter om systemet som finns i HSA-katalogen
BIF, Bastjänster för InformationsFörsörjning	Syftet med BIF-tjänsterna är att på ett enhetligt sätt säkerställa den funktionella informationssäkerheten avseende IT-tjänsters hantering av vårdinformation inom hälso- och sjukvården, såväl inom som mellan organisationer: BIF kan hantera patientdatalagens krav gällande Stark Autentisering, Åtkomstkontroll (regler som nyttjar egenskaper placerade i HSA), Samtycke, Spärr, Utlämnande, Aktuell Patientrelation samt Logg och Logganalys. BIF omfattar nio IT-bastjänster där SVR

	vidareupplåter tjänsterna till nyttjare för fri användning i nyttjarens verksamhet.
NPÖ, Nationell PatientÖversikt	Realiserar sammanhållen journalföring där vårddokumentation från flera vårdgivare visas sammanställt.
RIV, Regelverk för Interoperabilitet inom Vård och omsorg	RIV regelverket skapades för att åstadkomma ett för vård och omsorg gemensamt regelverk för att säkerställa interoperabilitet mellan olika vård- och omsorgssystem dvs. bland annat underlätta ett strukturerat elektroniskt informationsutbyte.

Lokalt ansvar	Beskrivning
Lokal administration	Lokala system som försörjer HSA med användar- och organisationsuppgifter. Det är här verksamhetschef tilldelar rättigheter (egenskaper) till sina användare
Vårdsystem	Lokala vårdsystem som försörjer NPÖ med vårddokumentation

1.1 Patientdatalagen 2008:355

Referens	Beskrivning
Patientdatalag	Patientdatalag antagen 1/7 2008 (2007/08:126)
Socialstyrelsen anvisningar	SOSFS 2008:14 Informationshantering och journalföring i hälso- och sjukvården
Socialstyrelsen Handboken	Ett stöd för vårdgivare, verksamhetschefer, medicinskt ansvariga sjuksköterskor och hälso- och sjukvårdspersonal vid tillämpningen av Socialstyrelsens föreskrifter (2008:14) om informationshantering och journalföring i hälso- och sjukvården
PDLiP	Patientdatalagen i praktiken ett projekt av SKL

Den 1/7 2008 infördes en ny patientdatalag (Patientdatalagen 2008:355).

Informationshantering inom hälso- och sjukvården ska vara organiserad så att den tillgodoser **patientsäkerhet** och god kvalitet samt främjar **kostnadseffektivitet**. Personuppgifter ska utformas och i övrigt behandlas så att patienters och övriga registrerades **integritet respekteras**. Dokumenterade personuppgifter ska hanteras och förvaras så att obehöriga inte får tillgång till dem. Den som arbetar hos en vårdgivare får ta del av dokumenterade uppgifter om en patient endast om han eller hon **deltar i vården** av patienten eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården. (vårdrelation).

Konkreta nyheter i lagen:

- Vårdgivare ges direktåtkomst till andra vårdgivares vårddokumentation via sammanhållen journalföring.
- Patienten kan spärra del av information hos en vårdgivare. (t.ex. viss information som uppstått hos en vårdenhet)
- Patienten har rätt att ta del av loggar

- Patienten kan ges möjlighet att ta del av patientinformation och dokument över Internet. Detta kräver säker autentisering (e-legitimation)

Utöver detta finns anvisningar från Socialstyrelsen t.ex.:

- Vårdinformation över öppet nät (t.ex. SjuNet) kräver stark autentisering (e-legitimation)
- Vad som ska loggas
- Att loggar ska bevaras i 10 år

Under hösten 2008 bedrev SKL projektet ”Patientdatalagen i praktiken”. Projektets effektmål är att ska skapa förutsättningar för en nationell samsyn av tolkning och tillämpning av patientdatalagen, där regelverket uppfattas lika av de olika aktörerna och av patienterna. I rapporten från Patientdatalagen i Praktiken beskrivs vilka lagkrav som ställs och hur dessa tolkas.

Patientdatalagens krav gör att även befintliga system behöver anpassas likväl som lösningar som realiserar sammanhållen journalföring. Genom den nya lagen ges patienten möjlighet att spärra sina uppgifter. Datainspektionen har aviserat att man ska följa upp att kraven kring spärrar följs. Patienten skall enligt patientdatalagen kunna spärra information som tillhör en vårdenhet eller vårdprocess. Idag kan information vara tillgänglig inom ett helt sjukhus, vilket nu måste stramas upp. Av denna anledning så har systemleverantörer och landsting planerat att implementera spärrar i sina system.

1.2 HSA, Elektronisk katalog för Vård och omsorg.

HSA är en elektronisk katalog för aktuell enhets-, funktions- och personinformation. Uppläggning av uppgifter i HSA följer upprättad policy.

HSA kommer framöver att få en viktig roll för att registrera och söka IT-tjänster och dess gränssnittsbeskrivningar (RIV).

1.3 SITHS, Säker IT i Hälso- och Sjukvård

SITHS står för Säker IT i Hälso och Sjukvården och är en nationell säkerhetslösning. SITHS-modellen bygger på att anställda i vård och omsorg har ett personligt elektroniskt ID-kort med ett elektroniskt tjänstecertifikat.

Med hjälp av SITHS kan en vårdgivare identifiera sig och ge bevis för sin identitet, oberoende av organisatoriska och geografiska gränser.

Utgivning av SITHS certifikat förutsätter att uppgifterna finns publicerade i HSA-katalogen. Omvänt publicerar SITHS alla utgivna certifikat samt spärrlista i HSA-katalogen.

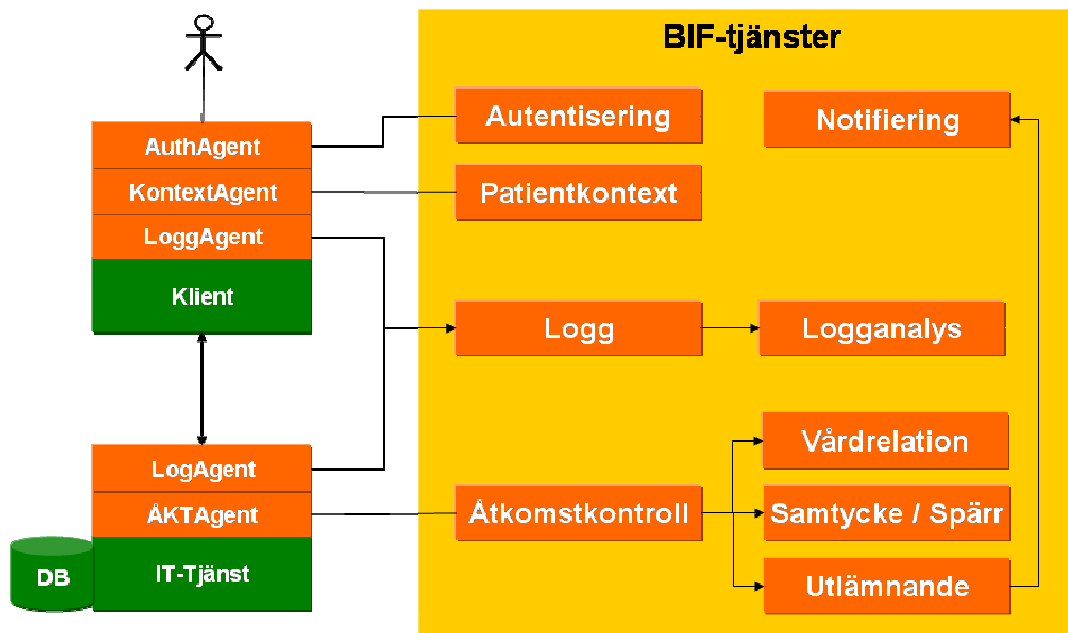
1.4 BIF, Bastjänster för InformationsFörsörjning

Bastjänster för informationsförsörjning, BIF, är en nationell säkerhetsinfrastruktur för vård och omsorg med syfte att säkra patienternas integritet och se till att endast rätt person får tillgång till rätt information i enlighet med patientdatalagen. Tjänsterna utgör en osynlig men nödvändig grund för vården och omsorgens IT-stöd såväl lokalt, regionalt som nationellt.

Avtalet omfattar nio IT-bastjänster där SVR vidareupplåter tjänsterna till nyttjare för fri användning i nyttjarens verksamhet.

Nyttjare är regioner, landsting, kommuner, privata och enskilda vårdgivare samt myndigheter och organisationer som använder och tillhandahåller lokala och nationella IT-tjänster.

Drift och driftsmiljön ansvarar respektive nyttjare själva för. BIF är utformat så att flera nyttjare kan dela på en gemensam driftsmiljö.



BIF består av följande 9 IT-bastjänster:

1. **Autentiseringstjänst** Kontrollerar att ett e-id är gällande och hämtar egenskaper för användaren från HSA. Tjänsten möjliggör SSO och sammanhållen utloggning för vårdgivarens samtliga system.
2. **Åtkomstkontroll** En avancerad tjänst som tillsammans med egenskaperna för användaren från HSA tillsammans med egenskaperna på den information användaren avser läsa, via regelverk kunna analysera om en person har giltiga skäl för tillgång.
3. **Samtyckestjänst** En tjänst som svarar på om patienten har gett sitt samtycke/spärr till sammanhållen journalföring mellan vårdgivare och inom vårdgivaren. Den ska också lagra information om registrerat samtycke, spärr och nödöppning.
4. **Loggtjänst** En tjänst dit alla ingående vårdssystem loggar sina säkerhetsrelaterade händelser på ett strukturerat sätt.
5. **Vårdrelationstjänst** En tjänst som svarar ja eller nej på om man har en vårdrelation med en patient. Registrering av vårdrelation sker från andra system (t.ex. inskrivning av patient) eller intygar användaren själv sin vårdrelation.
6. **Utlämnandetjänst** Datoriserad utlämning av journalhandling med menprövning.
7. **Patientkontext** Kontrollfunktion för att säkerställa att vårdpersonal har rätt patients information framme på datorskärmen om flera olika vårdssystem är igång.
8. **Logganalystjänst** Syftet med tjänsten är att söka ut, bearbeta och presentera logginformation. Detta görs bland annat för att upptäcka obehörig åtkomst till vårdinformation.

9. **Notifieringstjänst** Meddelar användare eller system när det finns nyheter eller uppdateringar att ta del av. Går att prenumerera på. Exempel är åtkomstkontrollen som notifierar regelförändringar eller utlämnande.

Delar av funktionaliteten för vissa IT-bastjänster finns i agenter, som är inkorporerade i en fasad. Agentens uppgift är att förenkla och effektivisera IT-bastjänstens funktion för tjänstekonsumenten. Detta för att förenkla vid integration av system med BIF.

1.5 NPÖ, Nationell PatientÖversikt

En patient har idag ofta kontakt med flera olika vård- och omsorgsgivare, som var och en registrerar och förvarar sin journalinformation lokalt. Eftersom det då blir svårt att få en helhetsbild av patienten uppstår ibland osäkerhet vid medicinska bedömningar och nya kontakter.

Nationell Patientöversikt gör det möjligt för behöriga användare att med patientens samtycke **hitta och titta** på viktig patientinformation som registrerats i vårdsystemen hos landsting, kommun och privata vårdgivare.

Informationsmängder såsom diagnoser, vårdokumentation, provresultat, läkemedelsordinationer och vårdplaner blir tillgängliga för alla anslutna huvudmän via ett webbgränssnitt samt via frågetjänstens API.

1.6 RIV , Regelverk för Interoperabilitet inom Vård och omsorg

RIV regelverket består av övergripande riktlinjer. För att uppnå semantisk interoperabilitet så finns det ett innehållsregelverk bestående av metदानvisningar för att beskriva och strukturera information dvs. ta fram informationsspecifikationer för varje informationsmängd (meddelande) och dokumentationsanvisningar för hur man dokumenterar resultatet (informationsspecifikationen). För att uppnå teknisk interoperabilitet finns ett tekniskt regelverk.

1.7 Sjunet, Kommunikationsnätet för vård och omsorg

Sjunet är hälso- och sjukvårdens kommunikationsnät för datakommunikation mellan vårdhuvudmän. Via Sjunet erhålls tillgång till gemensamma nationella tjänster över ett säkert och tillgängligt nät.

Tjänsterna SITHS, HSA, BIF och NPÖ kan idag endast nås via Sjunet.

2 Samband

I detta avsnitt beskrivs övergripande samband kring de samverkande IT-tjänsterna. Avsnittet inleds med beskrivning av BIF och NPÖ i sitt sammanhang och delas därefter in i olika områden som behöver hanteras för att få en fungerande helhet.

2.1 BIF i sitt sammanhang

BIF hanterar säkerhetsrelaterade delar i lösningar för sammanhållen journalföring men kan även integreras (helt eller delvis) med befintliga system. Med BIF kan bland annat patientens samtycken och spärrar hanteras samt logguppföljning. BIF i sig levereras som en produkt/programvara utan upprättade regler, modeller och drift.

Beroenden för BIF.

BIF Följande behöver tas fram och fastställas med bland annat PDLiP som grund.

- Behörighetsmodell
 - Resursmodell (för tjänst/system och vårddokumentation)
 - Aktörsmodell (Syfte, Specialuppdrag...)
 - Aktivitetsmodell (Läsa/Skriva/Signera...)
 - Regelverk (Verksamhetsregler)
 - Loggmodell
- Organisationsmodell (subset av HSA-organisationsträd för att identifiera Vårdgivare och Vårdenhet)
- Samtyckesmodell (inkl. Spärr)
- Vårdrelation
- Utlämnandemodell
- Avtal/Förteckning över vilka som ingått Sammanhållen Journalföring

RIV Används för att vårdanslutningar ska kommunicera med informationsstandard

HSA Innehåller attribut som används för rättighetsstyrning och loggning

SITHS Används för säker identifiering av aktör (kort för person och mjukt certifikat för IT-tjänst)

NPÖ Att använd resursmodell och loggmodell är gemensam

SjuNet Kommunikation mellan vårdgivare.

Patientdatalagen Regelverk för åtkomst

2.2 NPÖ i sitt sammanhang

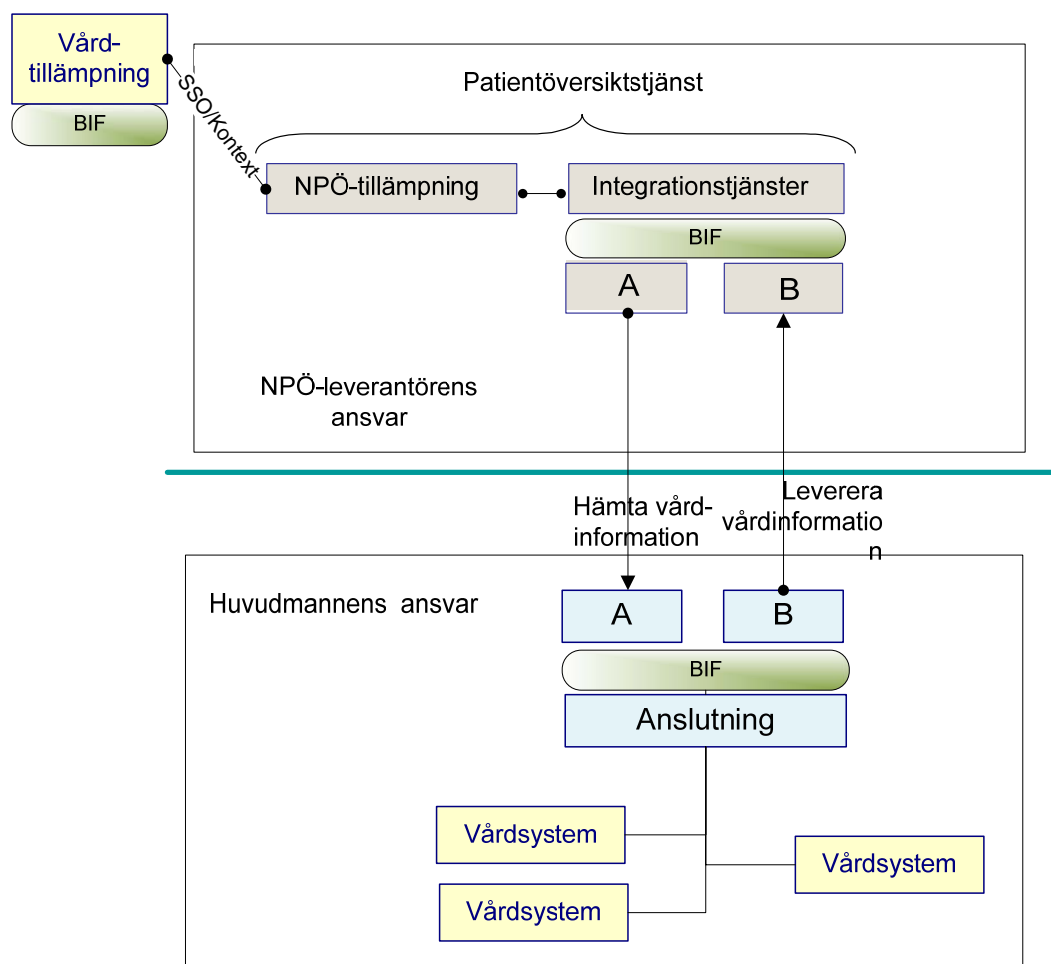
NPÖ kan användas som egen tillämpning eller integrerad som en del av ett annat vårdsystem. Dessutom kan frågegränssnittet i NPÖ ge möjlighet att presentera vårdinformation för en patient inne i en vårdtillämpning. Exempel på det sistnämnda är en vårdtillämpning där man skriver recept och samtidigt kan se uthämtade läkemedel för patienten med hjälp av NPÖ:s frågegränssnitt.

Beroenden för NPÖ, där några är indirekta beroenden via BIF: .

- RIV Används för att vårdanslutningar ska kommunicera med informationsstandard
- BIF Tät integration för rättigheter, åtkomst, samtycke, loggning mm
- HSA Innehåller attribut som används för rättighetsstyrning och loggning
- SITHS Används för säker identifiering av aktör (kort för person och mjukt certifikat för IT-tjänst)
- SjuNet Kommunikation mellan vårdgivare. Internet inte tillåtet för NPÖ

Patientdatalagen Regelverk för åtkomst

NPÖ ska baseras på BIF för att hantera autentisering och loggning. Samtycke och spärthantering enligt patientdatalagen ska också hanteras av BIF. Åtkomstkontrollen i BIF används med hjälp av regelverk från patientdatalagen och regelverk från verksamheten. För att hålla reda på om en vårdgivare har vårdrelation till vård- och omsorgstagaren (patienten) används vårdrelationstjänsten i BIF. När en användare använder flera tillämpningar samtidigt med NPÖ används kontexthanteringen i BIF så att alla aktiva tillämpningar använder sig av samma patient.



Figur visar var BIF är inkopplad i NPÖ

2.3 Anslutning till nationella tjänster

Vid användning av Nationella tjänster blir snabbt antalet parter mycket stort. Skall var och en teckna en överenskommelse med "alla" blir administrationen snart oöverstiglig.

I Patientdatalagen i Praktiken, del 1, har man pekat ett antal områden som ett avtal skall täcka, såsom att avtalen säkerställer att vårdgivarna uppfyller kraven enligt lagar, författningar och föreskrifter, eller att vårdgivare som ingår i sammanhållen journalföring måste säkerställa funktioner såsom anslutning till HSA och följa fastlagd policy för HSA. PDL i praktiken föreslår att varje Landsting/region inledningsvis tecknar avtal med de vårdgivare inom sitt område som vill ingå i sådant samarbete och att landstingen/regionen ges rätt att för övriga vårdgivares räkning träffa avtal med andra vårdgivare i syfte att utöka systemet innebärande sammanhållen journalföring.

För nationella tjänster som syftar till sammanhållen journalföring kan detta jämföras med att Sjukvårdsrådgivningen tecknar överenskommelser med parter som vill ingå i sådant samarbete och därmed ges rätt att utöka med fler avtalsparter som då successivt ansluts till sammanhållen journalföring. Dessutom kan respektive part ha överenskommelser med underliggande parter.

Rent praktiskt sker motsvarande hantering redan idag för flera förvaltningsobjekt, såsom HSA, SITHS och Sjunet. Där har detta lösts genom att en gemensam Policy tas fram och accepteras av alla parter. Sedan formulerar varje part som ansluter sig till tjänsterna ett dokument (policy statement, policytillämpning, självdeklaration etc.) som beskriver på vilket sätt respektive part uppfyller villkoren i Policyn. Dokumentet granskas av andra anslutna eller av en speciellt utvald granskningsgrupp innan anslutning. Godkända dokument publiceras så att andra anslutna kan se dokumentet och själv värdera om villkoren i policyn är uppfyllda.

Denna policy används sedan som referensram när revision sker av anslutna.

För befintliga tjänster finns olika nivåer av användare nämligen som konsument eller producenter/leverantörer av information. Motsvarande behov finns för BIF och NPÖ.

För NPÖ finns behov av anslutning, och därmed policy, för anslutning till patientöversiktstjänsten som konsument dvs. med möjlighet att ta del av andras information. Då finns det också behov att veta under vilka villkor informationen presenteras, kvalitetsmått, aktualitet, tekniska fakta, kontaktpersoner o.d.

Det finns också behov att, som producent/leverantör av information sätta upp regler för åtkomst samt beskriva tjänsten.

Vid upprättandet av sammanhållen journalföring är behovet liknande.

För BIF kommer lokala BIF-instanser att samverka med varandra och med nationell BIF-tjänst. För detta behövs en policy/regelverk samt ett godkännandeförfarande innan skarp anslutning.

2.3.1. Innehåll i policy

En Policy upprättas för BIF, NPÖ och sammanhållen journalföring.

En BIF-policy kan innehålla t.ex.

- Hur skall utrustningen skyddas
- Vilken organisation/support behövs lokalt
- Ansvarsförhållanden
- Referenser till tekniska dokument och specifikationer
- Regler för säkerhet och sekretess

Motsvarande policy för NPÖ kan innehålla ungefär samma punkter men dessutom

- Aktualitetskrav
- Informationsinnehåll
- Regler för vilka som får ta del av informationen

Sammanhållen journalföring har troligen ytterligare krav t.ex. krav på loggning och spårbarhet.

På samma sätt som för övriga förvaltningsobjekt kan ansvaret decentraliseras dvs. en vårdgivare (landsting, kommun, privat) lämnar in ett dokument för varje område och som beskriver sitt åtagande för samtliga tjänster och konsumenter.

2.3.2. Fortsatt arbete

Som en del av förberedelserna inför förvaltning av nationella tjänster behövs denna policy samt en paketering av anslutningsdokumentationen och förfarandet göras. Följande behöver tas fram:

- Policy för anslutning till BIF, NPÖ och sammanhållen journalföring behöver skrivas och godkännas
- Mall för ”dokument” behöver formuleras
- Granskningsgrupp behöver utses

2.4 Lagring och åtkomst till IT-tjänster

Information om IT-tjänster behöver publiceras så att såväl teknisk som administrativ information finns tillgänglig. Detta behövs exempelvis för en person med uppgift att utveckla eller underhålla en extern applikation. Personen behöver utläsa aktuell information om en tjänst som den externa applikationen ska konfigureras att använda. NPÖ och BIF är exempel på tjänster som behöver tillgängliggöra information så att andra kan nyttja dem. Exempel på information som behövs om tjänsterna är:

- WSDL-fil,
- DNS-namn,
- IP-adress,
- Teknisk och administrativ kontaktperson för tjänsten,
- Beskrivning av tjänsten,
- Gruppering enligt kodverk (journalssystem, labssystem, stödsystem, administrativt system m.m.)

Alternativet att som idag maila runt teknisk information om nationella tjänster såsom ”tjänstekontrakt” är på sikt ingen hållbar lösning.

Med hjälp av en tjänstekatalog kan en applikation eller tjänst söka och hämta information om andra tjänster. Det som benämns Tjänstekatalog är en nationellt driftad komponent-upsättning som "hör samman" med HSA och naturligt utvecklas och drifas av HSA-förvaltning. Konceptuellt finns detta beskrivet i VIT-bokens tekniska arkitektur, men Tjänstekatalogen är i dagsläget inte realiserad.

I grunden handlar det om livscykelhantering av nationella tjänsteinteraktioner: godkännande av ny interaktion, publicering av tekniska representationer (WSDL + scheman + ev. semantisk

beskrivning), revidering och versionshantering samt möjliggöra för implementatörer och konsumenter av interaktionerna att prenumerera på förändringar och att begära förändringar.

En tjänsteinteraktion är ett eller ett par tjänstekontrakt (maskinläsbara beskrivningar på WSDL-format med tillhörande och relaterade XML-Scheman).

2.4.1. Fortsatt arbete

Följande aktiviteter har identifierats för att få en fungerande tjänstekatalog för lagring och åtkomst till IT-tjänster:

- Nödvändiga uppgifter för IT-tjänster behöver definieras.
- Plats behöver göras i HSA för detta dvs. ev. nya attribut.
- Samverkan mellan HSA, tjänstekatalog och övriga komponenter i tjänsteplattformen behöver dokumenteras tillsammans med realiseringsstrategi för en första version.
- Rutiner för livscykelhantering av nationella tjänsteinteraktioner behöver arbetas fram.
- Beskrivning av anvisning RIV-HSA tjänst behöver uppdateras.
- Genom praktiska prov i ÖLL, eller i separat testmiljö, verifiera framtagen strategi.

2.5 Tjänsteadressering

För att få en fungerande samverkan behövs ett systematiskt angreppssätt för adressering av tjänster. Detta gäller bland annat adressen till NPÖ Integrationstjänst och översättning från system-id i index till en specifik adress/port där vårdsystemet/anslutningstjänsten befinner sig.

Koncept för tjänsteadressering har beskrivits i VIT-bokens tekniska arkitektur utgående från den övergripande målsättningen om stabila tjänsteadresser för kommunicerande parter. Där beskrivs också en schematisk en gemensam teknisk lösning. Att upprätthålla stabilitet innebär att kommunicerande parter kan förlita sig på ett HSAid (eller teknisk tjänsteadress) som är stabilt över tiden och tålig mot kontinuerlig konsolidering och förändring av vårdens IT-stöd så väl lokalt som centralt. Detta behov är speciellt stort när utvecklingstakten är hög. Även förflyttningen mellan faser i IT-stödets utvecklingsfaser (test, QA, produktion) är exempel på samma typ av förändringar. Adresseringsmodellen är framtagen i samverkan med en tänkt modell för certifikatshantering. Modellen har verifierats. Resultatet är en modell färdig att införas i HSA och med en teknisk strategi för att i runtime på ett systematiskt sätt säkra att tjänster når förväntade fördelar.

2.5.1. Fortsatt arbete

Följande aktiviteter har identifierats för att få en fungerande tjänsteadressering

- Framtagande av beskrivning för tjänsteadressering med avseende på behoven i BIF och NPÖ inklusive realiseringsstrategi.

2.6 Behörighetshantering

2.6.1. Förutsättningar

Behörighetshanteringen kan delas i två tidsmässigt åtskilda delar:

1. tilldelning (förändring och borttag) av behörigheter
2. tolkningen av behörigheten

En förutsättning för en korrekt tilldelning av behörighet är att man redan vid tilldelningstillfället är klar över hur den tilldelade behörigheten kommer att tolkas.

Enligt Patientdatalagen i Praktiken, del 1, är det verksamhetschefen som tilldelar behörighet. Behörighet avser såväl åtkomst inom den egna vårdenheten, andra vårdenheter inom den egna vårdgivaren samt direktåtkomst till annan vårdgivare som deltar i sammanhållen journalföring.

Enligt Patientdatalagen i praktiken, del 1, skall man vid behörighetstilldelning även skilja på aktiviteten läsa (vid sammanhållen journalföring är endast läsning tillåten) skriva, ändra och signera (gäller bara den egna vårdenheten).

Ytterligare krav kring behörigheter som arbetsgruppen för detta uppdrag har uppfattat är att:

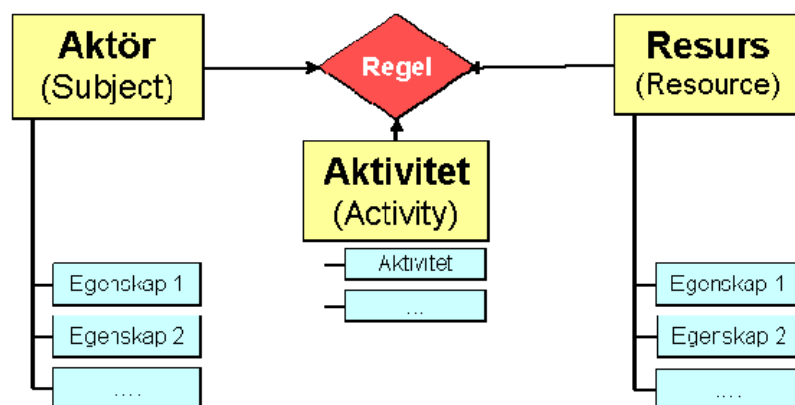
- Behörigheterna ska vara individuellt tilldelade.
- Behörighetstilldelning skall föregås av behovs- och riskanalys.
- Verksamhetschefen har ansvar för att behörigheterna är anpassade efter respektive medarbetares arbetsuppgifter/uppdrag.
- Varje behörighetstilldelning måste vara en medveten handling.
- Att vid tilldelningstillfället måste det för tilldelaren vara klart vad tilldelningen leder till.
- Att den som tilldelats behörighet skall ha tillgång till information som visar vilka rättigheter som har tilldelats och vilka verksamhetsuppdrag som därmed skall följas.

2.6.2. Egenskaper och roller

Det finns olika sätt att tilldela behörigheter såsom egenskapsbaserad (ABAC) och rollbaserad (RBAC), se rapport BIF ER. I BIF valdes ABAC som metod för åtkomstkontroll och språket, XACML, fanns med som funktionellt krav i upphandlingen.

Det finns ingen motsättning mellan ABAC och RBAC. Tvärtom så kan ABAC sägas innefatta RBAC genom att roller kan hanteras som aktörsegenskaper. Antalet egenskaper i ABAC är inte begränsat, men för enkelhet och initial behörighetsevaluering, föreslås en begränsning i antalet egenskaper.

En schematisk framställning av ABAC kan se ut enligt figuren nedan.



Exempel på egenskaper är:

- Uppdrag, tillhörighet och roll
- Resursens identifierare, tillhörighet och resursgrupper

- Önskade handling med/mot resursen

Behörighetsadministrationen ska vara så enkel som möjligt och drömmen är att den ska kunna ske på ett enda ställe. Uppdraget för enskilda medarbetare inom samma yrkeskategori skiljer sig oftast inte. Genom att skapa aktörsegenskaper som beskriver verksamhetsuppdrag, som i sin tur innehåller den specifika behörighetsinformationen och knyta dessa till valfritt antal personer finns potential till en hanterbar lösning i ett första steg som kan byggas ut vartefter, med mer avancerade egenskaper efter behov.

Exempel på egenskap i form av verksamhetsuppdrag kan vara ”Sammanställd journal - bas”, eller ”Redigering av texter”.

2.6.3. Åtkomstkontrollens tillgång till egenskaperna

Aktörens egenskaper hämtas från certifikat, HSA och andra säkra källor och behövs vara tillgängliga för åtkomstkontrollen vid regelevaluering. Dessa egenskaper kan antingen paketeras i SAML-biljetten, eller så hämtas informationen från lämplig källa av åtkomstkontrollen.

Om alla behörighetsegenskaper läggs i SAML-biljetten finns risk att denna blir för tjock och tung. Det alternativa tillvägagångssätt, att låta Åtkomstkontrollen hämta alla behörighetsegenskaper vid varje tillfälle (cachning är inte acceptabelt annat än för mycket korta perioder), riskerar också att bli väldigt tidskrävande.

En möjlighet att kommunicera behörighetsinformationen är att skapa en tjänst som on-line hämtar ut och packar om behörigheterna i en lätthanterlig form. Från denna tjänst kan sedan Åtkomstkontrollen snabbt hämta relevant behörighetsinformationen, till exempel den som berör just den aktuella applikationen. Lösningen hänger ihop med hur egenskaperna har utformats.

För att uppnå ännu snabba svarstider och hög tillgänglighet kan det vara lämpligt att installera en Åtkomstkontroll-tjänst per applikationsinstans. Till denna kan tjänsten pusha ut relevant behörighetsinformation som kan lagras lokalt hos respektive Åtkomstkontroll.

Det är viktigt fastställa en första nivå på behörighetshantering och att snarast komma igång med praktiska prover för att verifiera antaganden och design.

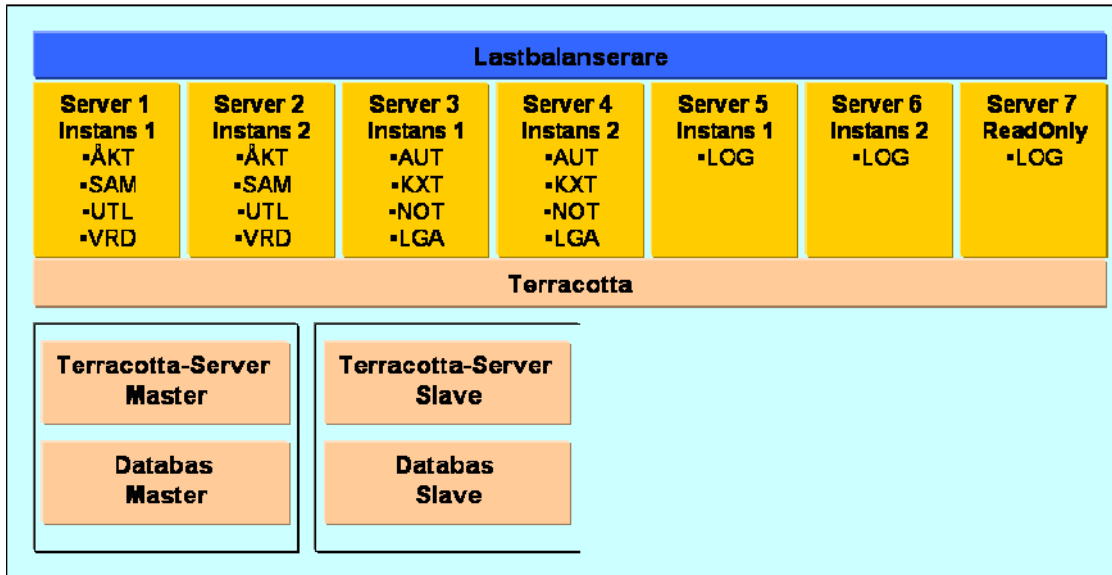
2.6.4. Fortsatt arbete

Följande aktiviteter har identifierats för att få en fungerande behörighetshantering:

- Upprätta en beskrivning av vilka behörighetsregler som behöver finnas för NPÖ.
- Tillsammans med experter inom området för ABAC och XACML (Axiomatics) och landstingsrepresentanter med tidigare erfarenhet av behörighetstilldelning utforma ett utkast med egenskaper och regler för NPÖ och sammanhållen journalföring. Detta inkluderar aktörsmodell, resursmodell, aktivitetsmodell och regler.
- Tillsammans med Patientdatalagen i Praktiken, gå igenom lagkrav och analysera lösningsalternativ på kort och lång sikt.
- Genom praktiska prov i ÖLL, eller i separat testmiljö, överväga och rekommendera lösning för åtkomstkontrollens tillgång till egenskaper.

2.7 Driftsplattform, instanser av BIF och toppnod

Varje nyttjare svarar själv för driftsplattform. BIF är byggt så att flera nyttjare kan dela på samma driftsplattform/instans.



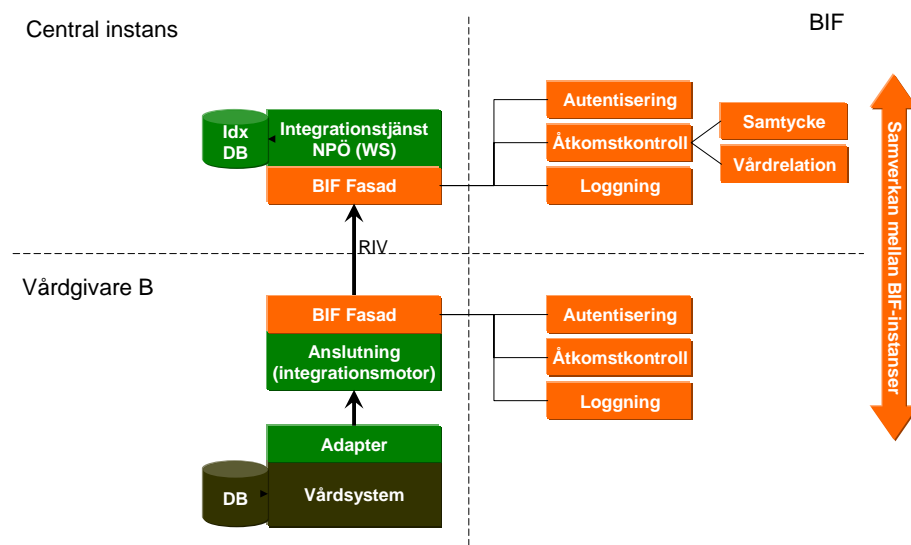
Bilden ovan är ett förslag gällande produktionsmiljö från Logica och utgör ett exempel på hur en redundant miljö kan sättas upp för att drifta BIF. Denna konfiguration kräver en lastbalanserare som fördelar lasten mellan instanserna.

Terracotta kommer att fylla två olika syften i BIF:

1. Terracotta användas för att, om IT-bastjänsterna är klustrade, alla instanser i klustret ska ha samma status.
2. Tillhandahålla objekt som delas mellan flera olika instanser.

Vissa objekt är viktiga att de är samma i olika instanser av tjänsterna men behöver trots detta inte vara långsiktigt persistenta (t.ex. SAML-biljett som är viktiga att de är lika för alla tjänster som efterfrågar dessa men som inte sparas i databas då de bara gäller en begränsad tid).

För att NPÖ skall kunna hålla sina SLAer så är det troligt att NPÖ kommer att behöva ha BIF nära. Det innebär en egen instans av BIF eller koppling till en nationell instans. Detta är inte samma sak som central toppnod.



2.7.1. Toppnoder

Det är av arkitekturskäl nödvändigt med en rot- eller toppnod av BIF, för implementering/replikering av regelverk. För samtycke och spärr eller de andra tjänsterna har BIF utformats så att det enligt Logica inte skall behövas någon toppnod. Administration av samtycke och spärr skall kunna ske i vilken instans som helst, vilket sedan replikeras till samtliga instanser. På samma sätt går det även att ta bort (inaktivera) spärr från valfri instans, dvs. inte bara från den instans där spärren upprättades.

BIF är uppbyggt så att patienten själv skall kunna ändra spärrar och dessa kommer att vara tillgängligt nationellt. När Vården på Webben har utvecklats mer skulle denna kunna peka mot den centrala instansen, dvs. endast en punkt och inte flera.

Det är bara implementering/replikering av regelverk som i dagsläget har designats med toppnod, ingen annan av BIF-tjänsterna har utformats med toppnod utan antas replikeras mellan varandra.

En struktur där det är många som skall delta i replikering kan bli problem. Det är dock svårt att simulera detta innan den exakta utrullningen av BIF är känd, såsom hur många instanser av samtycke som det kommer att finnas. Ingen begränsning är i dagsläget satt till antal instanser, men begränsning kan komma att behövas. .

Det finns dock ingen motsättning i att börja med obegränsat antal instanser och sedan replikera upp på en viss nivå om det senare visar sig behövas. Behovet styrs bland annat av kraven i NPÖ, om inte NPÖ har fått tag på en befintlig spärr så kommer informationen att visas. Det är med andra ord viktigt att veta att spärren slår igenom i alla instanser inom rimlig tid. I praktiken förväntas inte antalet spärrar och förändring av spärrar bli särskilt stort.

2.7.2. Driftsalternativ för nationella tillämpningar

1. Centralt driftad instans av BIF för nationella tjänster. Det behövs någon som är utsedd att drifva den instans av BIF som NPÖ behöver.
 - a. Ett alternativ är att driften upphandlas som tillägg till någon av de pågående nationella projekten (NPÖ, VpW 1.0 etc) och att någon av leverantörerna för tjänsterna även tar hand om drift av den centrala BIF instansen
 - b. Ett annat alternativ är att en separat upphandling av en gemensam driftleverantör för att hantera BIF för de nationella projekten
 - c. Denna instans av BIF skulle även kunna nyttjas som BIF-hotell för organisationer som inte vill drifva själv eller ännu inte hunnit sätta upp en egen instans. Resonemanget ovan måste då föras i lite större skala, dvs. upphandlad driftleverantör skall även kunna erbjuda kommuner, privata eller andra som önskar ha BIF som hotell
2. Varje driftsleverantör av en nationell applikation drifvar också nödvändiga BIF-tjänster för applikationen. Det finns dock i dagsläget inte inskrivet i avtalen för exempelvis NPÖ att drift av BIF skall ingå.

2.7.3. Fortsatt arbete

Följande aktiviteter har identifierats för att få en fungerande driftslösning för BIF

- Beslut kring driftsalternativ för nationella tillämpningar

- Införa lösning som på kort sikt klarar behovet av anslutning i ÖLL. Örebro kan själva tillhandahålla den centrala instansen för NPÖ i den första anslutningen, men innan fler landsting släpps på behöver lösningen ses över.
- Beskriva strategi för att klara resterande anslutningar tillsammans med handlingsplan
- Genom praktiska prov eller i separat testmiljö, analysera antal instanser och toppnod.

2.8 Kundstöd/supportfunktion.

Med många samverkande tjänster på olika nivåer blir felanalys och felrättning mycket komplicerad. Inom ramen för Sjunet-upphandlingen tecknades avtal om en Nationell kundtjänst med ett övergripande ansvar för att ta emot fel-/störningsinformation, analysera, sända vidare till relevant part, bevaka att ärendet åtgärdas samt sända information åter till anmälaren.

Involverade parter i nationella lösningar måste förbinda sig att ta emot, åtgärda och återrapportera ärenden från Nationella kundtjänsten.

Även integrationsstöd behöver finnas, så att de som vill ansluta sin produkt till nationella tjänster kan testa detta i sitt sammanhang.

2.8.1. Fortsatt arbete

Skapa regler och rutiner för samverkan mellan den gemensamma nationella kundtjänsten, med lokala supportavdelningar och helpdesk/servicedesk för respektive tjänst (SITHS, HSA, BIF, NPÖ). Detta arbetet drivs förslagsvis av förvaltningen på SVR.

2.9 Ändringshantering

Med många tjänster, leverantörer och instanser kommer det att finnas ett stort beroende av koordinering av ändringshantering. En förändring i en tjänst kan påverka/störa en eller fler nationella eller lokala tjänster. Förändringar måste tidigt aviseras och beslutas samt meddelas till berörda på ett tydligt sätt.

2.9.1. Fortsatt arbete

Ett forum för ändringshantering måste inrättas med mandat att förändra, påverka eller kanske stoppa förändringar i tjänster. Detta forum måste också koordinera genomförandet av förändringar.

3 Insatsområden för ytterligare bearbetning

I kapitlet om samband beskrivs olika områden som behöver fungera i en helhet.

Problematiken kring några av dessa områden har fördjupats i detta kapitel. Dessa områden har högsta prioritet för att realisering av BIF och NPÖ skall vara möjlig under 2009.

3.1 Behörighetshantering

För att den egenskapsbaserade rättighetskontrollen skall fungera behöver attributen för både Aktör och Resurs definieras. Därefter kan regler byggas med hjälp av dessa attribut.

3.1.1. Behörighetsmodell

En behörighetsmodell innehåller flera delar, resursmodell, aktörsmodell, aktivitetsmodell och regelverk.

Resursmodellen innehåller exempelvis var journalen är upprättad, vem som gjorde den, vilken vårdenhet tillhör den osv. Resursmodellen är i dagsläget inte beslutad på nationell nivå.

Resursmodellen har ett samband med loggning, dvs. om jag vill logga åtkomst så behöver loggen hantera både aktör och resurs, eftersom det är de tillsammans som skapar rättigheter och därmed även behövs för uppföljning.

Aktörsmodellen beskriver vilka egenskaper aktören måste uppvisa för att få åtkomst. Varje åtkomsttilldelning bör vara ett medvetet val.

Aktivitetsmodell beskriver vilka aktiviteter som kan utföras, till exempel läsa, skapa osv.

När både resursmodell och aktörsmodell med innehållet i SAML-biljetten är klart så återstår att skriva regler. Dessa regler ligger i BIF Åtkomstkontroll.

Ovanstående modeller och regelverk måste tas fram nationellt. Inom en organisation kan man komplettera med lokala regler.

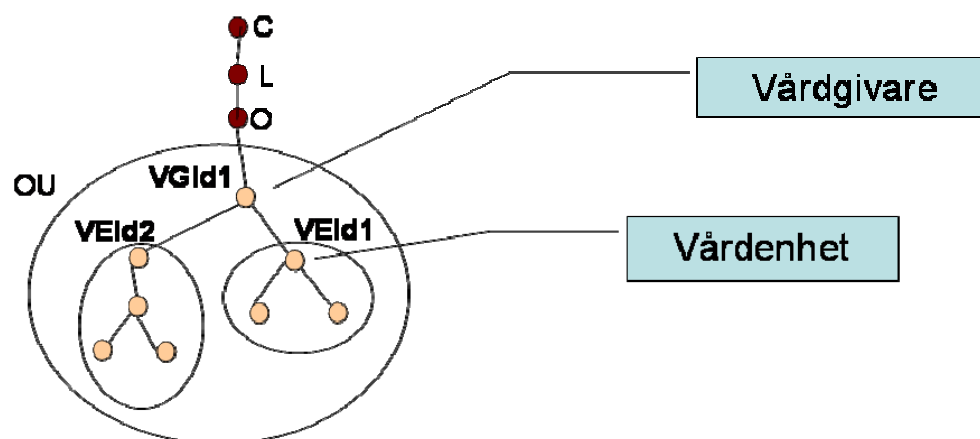
3.1.2. Förändringar i HSA

När behörighetsmodellen är satt kommer det kräva ändringar och tillägg i HSA. Detta innebär i praktiken att landstingen behöver fylla på med korrekt information i sina kataloger innan BIF och NPÖ kommer att fungera.

3.1.3. Tillgång till vårdgivare/vårdenhet i HSA

Beroende på hur behörighetsmodellen utformas kan tillgång till vårdgivare/vårdenhet i HSA bli kritiskt.

I patientdatalagen (PDL) och SoS föreskrifter finns krav på att vårdgivare och vårdenhet ska kunna beskrivas.



Utifrån organisationsstrukturen i HSA-katalogen behöver Vårdgivare och Vårdenhet kunna utläsas. Patientdatalagen i praktiken definierar Vårdenhet som den/de enheter som har en och samma verksamhetschef.

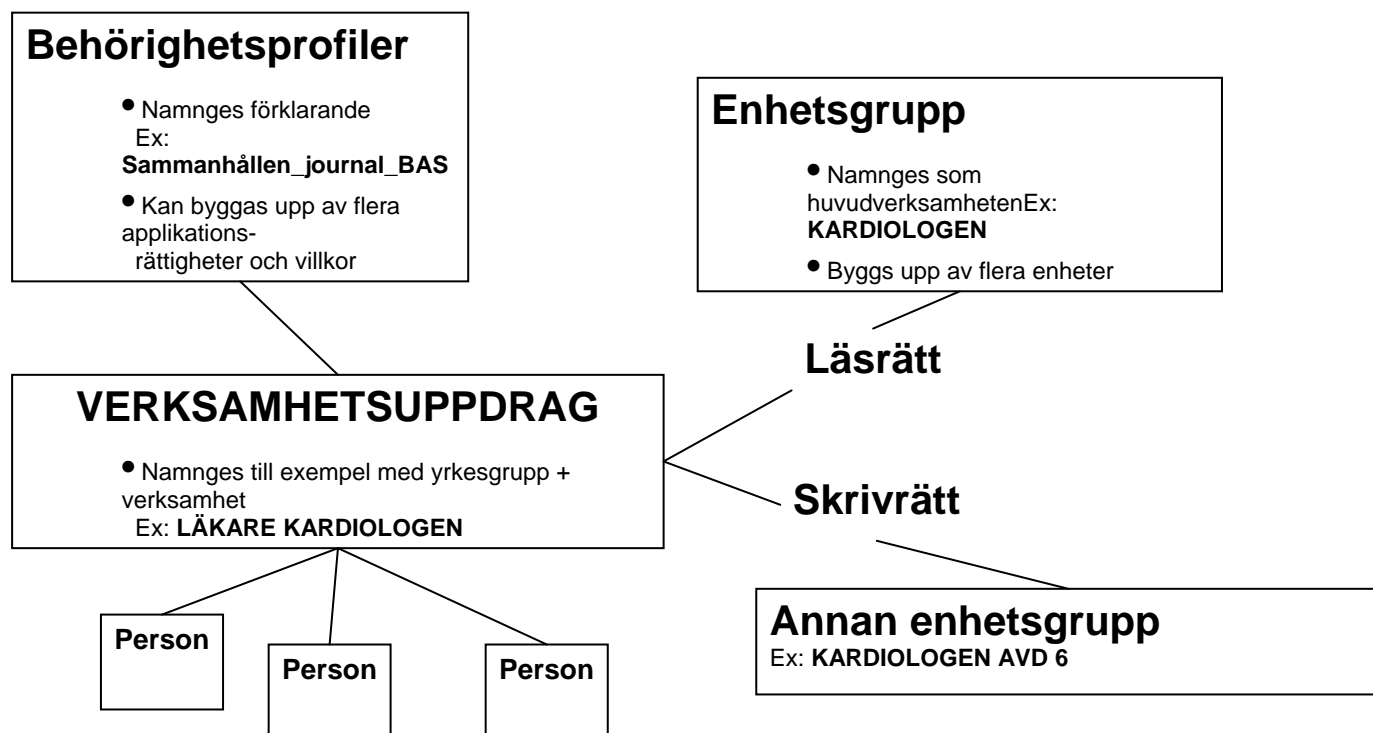
För att, i enlighet med PDL, kunna koppla spärrar och samtycke till Vårdgivare (sekretessområde) och Vårdenhet måste dessa kunna identifieras för att spärrkontroll och samtycke skall fungera. Det gäller både för Aktör (vilken vårdenhet verkar användaren vid just vid detta tillfälle) och Resurs (vem som äger vårddokumentationen).

HSA är en hierarkisk katalog och det är inte klart och tydligt att Vårdenhet kan knytas till en gren i en hierarki. Detta gör att det är svårt att i dagsläget läsa ut denna information ur katalogen.

3.1.4. Exempel på behörighetsmodell från LiÖ

Verksamhetsuppdrag

Ett Verksamhetsuppdrag (=VU) består av behörighetsprofiler (vilka funktioner man får utföra), läsrättigheter (var i organisationen (Vårdgivaren) man får se information) och skrivrättigheter (var i organisationen (Vårdenheten) man får ändra information), se figur



Det möjliga innehållet i behörighetsprofilerna styrs av de olika applikationerna som behörighet ska ges till. Om vi till exempel antar att man har kommit fram till att i NPÖ det bara är meningsfullt att skilja på möjligheten att se allt utom utlämnade läkemedel och se utlämnade läkemedel så talar NPÖ organisationen om att det finns två olika behörigheter; "Sammanhållen_journal_Bas" och "Sammanhållen_journal_Läkemedel". Den lokala administratören kan sedan, enligt sin verksamhetschefs instruktioner, lägga in bara den första eller båda beroende hur respektive VU ska utformas.

Läs(skriv)rättigheterna har bara en funktion när man vill begränsa vad man får se (förändra) till en (eller flera) vårdenheter. I NPÖ fallet behövs inga sådana begränsningar men säg att i samma VU också lagts in behörigheter för en lokal applikation för att hantera labremisser. Då är tillagt behörighetsprofiler som styr att användaren får till exempel läsa remisser och svar och skriva remisser. Sedan styr läsrättigheten vilka enheters remisser och svar användaren får se och skrivrättigheten styr på vilka enheter den får skapa remisser på.

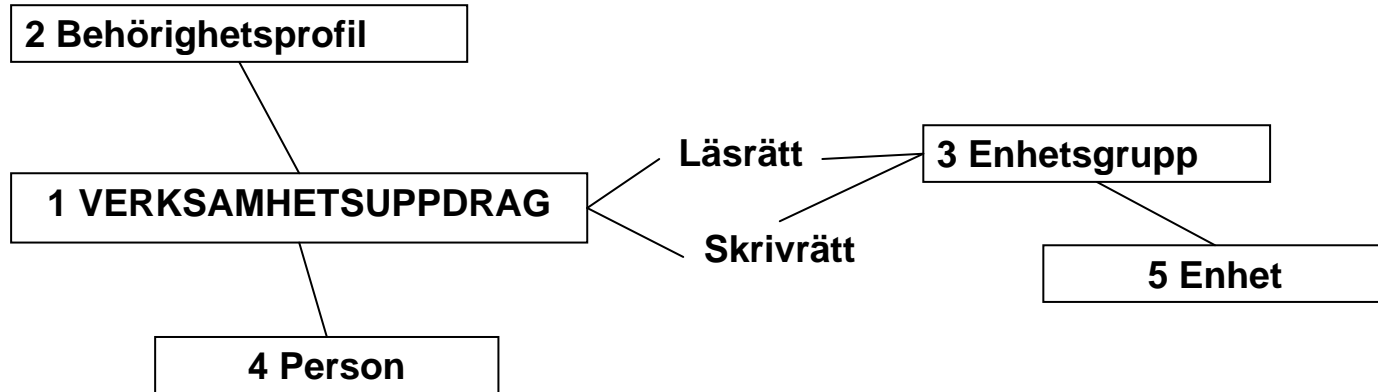
Alla delar av VU lagras i HSA. Skapandet hanteras som all annan information i HSA, det vill säga i de flesta fall skapas den lokalt och synkas ut i HSA men inget hindrar att den skapas direkt i HSA. Till exempel är det vettigt att behörighetsprofilerna som berör de nationella applikationerna skapas och lagras på ett ställe.

Regeltolkning

Användaren måste, när den autentiserar sig, ange vilket VU (om den har flera tillgängliga) den vill använda sig av. Ur katalogen extraheras de aktuella uppgifterna för Verksamhetsuppdraget och används vid regeltolkningen

Realisering av Verksamhetsuppdrag i katalogen

I katalogen skapas ett antal nya objektclasser för att realisera VU



1 Verksamhetsuppdrag

- Skapas på respektive administratörsnivå
- Administratören för ett VU, och bara denna, kan koppla en person var som helst i katalogen till "sitt" VU
- Pekare från VU till person
- Lagrar namn på behörighetsprofilen
- Har ett HSAid
- Namnges till exempel med yrkesgrupp + verksamhet
Ex: **LÅKARE KARDIOLOGEN**

2 Behörighetsprofil

- Definieras av respektive applikation
- Skapas av en central administratör
- Lagras i en gren av tjänsteträdet
- Har ett HSAid
- Namnges förklarande
Ex: **Sammanhållen_journal_BAS**
- Kan byggas upp av flera applikationsrättigheter och villkor

3 Enhetsgrupp

- Skapas på respektive administratörsnivå
- Administratören för en enhet, och bara denna, kan koppla en enhet till en enhetsgrupp
- Administratören för en enhetsgrupp, och bara denna, kan koppla en enhetsgrupp till ett VU
- Pekare från enhetsgruppen till VU
- Pekarna är av två sorter, läs och skriv
- Har ett HSAid
- Namnges förklarande
Ex: **NEUROKIR MOTT**

4 Person

- Pekare från personen till VU

5 Enhet

- Pekare från enheten till enhetsgruppen

3.1.5. Exempel på behörighetsmodell från Örebro läns landsting

Inom Örebro läns landsting har man två organisatoriska begrepp att styra behörighet med:

- Medicinsk enhet(vårdcentral eller klinik) där finns ett medicinsk ansvar (MedUnit)
- Vårdavdelning/Mottagning detta är platsen för undersökning/behandling (CareUnit)

All vårdinformation stämplas med både dessa begrepp.

Med denna modell ser man vårdavdelningar/mottagningar(hotellkedja) som en parallell struktur till kliniker/vårdcentraler. Denna modell fungerar också bra på tekniska avdelningar som IVA och Akutmottagning

I allmänhet har en läkare behörighet för patienter som finns inom den medicinska enhet(kliniken eller vårdcentral som har det medicinska ansvaret). Detta oberoende på vilken vårdavdelning eller mottagning patienten är på.

Motsatta förhållande rör vårdpersonalen som är behörig till alla patienter som vårdas på en vårdavdelning oberoende vilken medicinsk enhet patienten hör till.

Denna behörighetsmodell kräver att informationen är märkt både med medicinsk enhet (klinik eller vårdcentral) och vårdavdelning(eller mottagning). Tyvärr har de flesta vårdsystem enbart begreppet vårdenhet(vårdavdelning, mottagning). Detta kan ge behörighetsproblem med storavdelningar som vårdar patienter från flera medicinska ansvarsområden (kliner, vårdcentraler).

3.2 Vad och var loggning skall utföras

Vårdgivaren är skyldig att föra logg över elektronisk åtkomst inom vårdgivaren. Vårdgivaren skall dokumentera regelbunden och systematisk loggningskontroll i syftet att förebygga, konstatera och beivra otillåten eller obefogad åtkomst till uppgifter. Kravet på loggningskontroll avser åtkomst inom vårdgivarens inre sekretessområde och direktåtkomst vid sammanhållen journalföring.

Den vårdgivare som tilldelat behörighet för åtkomst ansvarar också för loggningskontrollen. Av loggarna skall framgå vilka åtgärder som vidtagits med patientuppgifterna, vilken vårdenhet som vidtagit åtgärderna och tidpunkten för åtgärden. Patientens och användarens identitet skall framgå.

Loggarna skall omfatta all åtkomst – dvs. även administrativ och teknisk personal omfattas och loggarna ska arkiveras i 10 år.

Vårdgivaren har också skyldighet att på patientens begäran lämna ut loggningsuppgifter. Dessa uppgifter skall vara så tydligt utformade så att patienten kan bedöma om åtkomsten till journaluppgifterna varit befogade eller inte. Det innebär att loggningsinformationen skall innehålla uppgift om vårdenhet och tidpunkt då någon tagit del av journaluppgifter. Beträffande offentliga vårdgivare skall – om patienten så begär - även namnen på de personer

som varit inloggade utlämnas efter sekretessprövning i enlighet med Tryckfrihetsförordningen och Sekretesslagen¹.

Det finns behov och önskemål angående loggning ute i projekten. Kort kan dessa delas upp i tre grupper.

- Vad som skall kunna följas upp
 - Verksamhetens uppföljning om obefogad åtkomst
 - Lex Maria, dvs. se exakt vad en aktör vid en viss tidpunkt tagit del av
 - Patientens möjlighet att se vilka som haft åtkomst
- Var loggning skall ske
 - I tillämpningen som visar upp informationen, dvs. vet exakt vad användaren har presenterats
 - I tjänsten som levererat informationen, här vet man vad som lämnat tjänsten, men inte vad användaren har fått se.
 - I åtkomstkontrollen (det är tillämpningen som hanterar vad som levereras, en optimering kan vara att inte upprepa identiska tidigare ställda åtkomstfrågor utan återanvända dessa i tillämpningen, dvs. åtkomstkontrollen kommer ej att veta allt som lämnar tillämpning eller tjänst).
- Vad som ska loggas
 - ska ”medicinsk” information ingå
 - referens till journalsystem där informationen skapats
 - recno eller annan unik identifierare till informationsposten
 - I NPÖ är förslaget att endast logga t.ex. att en översiktsvy valts, inte dess innehåll och var ingående uppgifter kommer ifrån.

Om HSA skall användas som underlag för loggposter/logganalys så behövs information om vem som utfört aktiviteten. För detta behövs information om vilka egenskaper som behövs för säker identifikation inte bara av individ utan också om uppdrag och tillhörighet. Kanske något ytterligare som vi inte känner till idag.

För loggning kan antingen hela informationsmassan skrivas i loggposten (identitet i klartext, tillhörighet i organisationen, uppdrag, personliga egenskaper m.m). Alternativet är att logga HSA-ID och tidpunkt och söka resten i ”Historiska HSA”.

Problemet är kopplat både till Vårdenhetsproblematiken och ev. till Historikproblematiken.

I BIF- tjänsterna kommer att finnas tjänster för loggtjänst och logganalys.

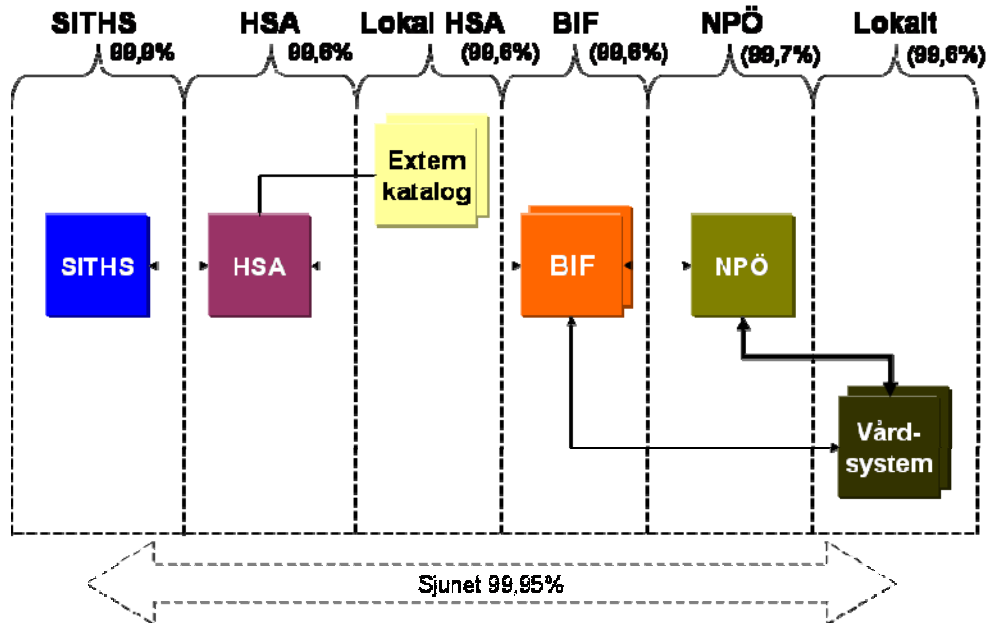
Exempel på var loggning behövs: *A är en tillämpning som hämtar 30 st epikriser från alla källor där patienten förekommer, sorterar resultatet och visar för användaren de 10 senaste posterna, där några kommer från B, någon från C osv. Det som loggats i B är med andra ord inte det som användaren har fått se i tillämpning A. Det är bara tillämpningen hos A som kan logga vad som faktiskt presenteras för användaren – dvs. det urval som tillämpningen gör ur det som returneras från tjänsten.*

¹ SOSFS 2008:14 2 kap, PDL 4 och 5 kap

Loggbehovet behöver definieras och vilka uppgifter som skall loggas klargöras.

3.3 Prestanda och tillgänglighet

För att få den tillgänglighet som slutanvändaren kräver, måste varje delsystem se till att de harmonierar med de system som är beroende av dem samt de som de har beroenden till. Beräkningar måste göras så att det totala systemet uppfyller användarnas tillgänglighetskrav,



Ovanstående bild är ej komplett men visar de i lösningen centrala tjänsterna. Tillgänglighetsvärdena angivna inom parantes är ej verkliga värden då dessa i dagsläget ej är kända.

Tjänsterna har beroenden till varandra och kräver därmed hög tillgänglighet. Om någon tjänst i kedjan fallerar utblir i flera fall tillgängligheten totalt.

Några av de viktigaste beroenden och dess konsekvens vid ett fel:

- SITHS
 - Utgivning av kort (tex reservkort kan ej utges)
 - Spärrkontroll fungerar ej (t.ex. inloggning i BIF fungerar ej)
- HSA
 - Hämta egenskaper som BIF behöver (användaren kommer ej in i systemet)
 - Utgivning av SITHS kort/certifikat (fungerar ej utan att egenskaperna kan hämtas från HSA.)
- BIF
 - Om vitala delar av BIF är nere alternativt att nödvändiga stödtjänster (t.ex. SITHS, HSA, Sjunet, DNS) är nere kommer användaren inte att komma in i system som är anslutna till BIF.
- NPÖ
 - Om NPÖ är nere kan ingen läsa vårddokumentation (en central instans)
- Vårdsystem

- Vid ett stopp kan NPÖ ej visa vårddokumentation (detaljerad vy) från vårdsystemet

3.3.1. Service Level Agreement (SLA)

Ett vanligt sätt att försöka uppnå önskad tillgänglighet att göra en Service Level Agreement (SLA) med sin leverantör. SLA är ett avtal som uppförs mellan kund och leverantör med avsikt att garantera en viss nivå av service och support.

Nedan visas exempel på beräkning av tillgänglighet. Tillgänglighetsvärdena är ej verkliga värden då dessa i dagsläget ej är kända. Av ingående tjänster visas att enligt avtalade SLA:er så kan det i sämsta fall handla om 15 timmar nertid per månad som enligt avtalet är tillåtet.

Tjänst/System	SLA tillgänglighet	Nertid timmar per månad	Nertid timmar per år
SITHS	99,90%	0,74	8,76
HSA	99,60%	2,98	35,04
Lokal extern katalog	99,60%	2,98	35,04
BIF	99,60%	2,98	35,04
NPÖ	99,70%	2,23	26,28
Vårdsystem	99,60%	2,98	35,04
Sjunet	99,95%	0,37	4,38
Totalt	97,97%	15,12	178,07

För att uppnå en önskad tillgänglighet totalt måste varje underliggande system inte bara kunna matcha det totala kravet på tillgänglighet, utan också överstiga den. Beräkning av en tillämpnings tillgänglighet multipliceras för varje underliggande systems maximala nertid.

Till denna nertid kan servicefönster tillkomma, och i sämsta fall har varje tjänst olika avtalade tillfällen där servicefönster tillåts, dvs. tjänsten tas ned för underhåll och uppdateringar.

En annan tillkommande faktor kan vara inställelsetid vid fel. Här får man avväga om det räcker med kontorstid och utökad tid utanför kontorstid innan felsökning och felavhjälpning påbörjas.

För att få en acceptabel tillgänglighet är det mycket viktigt att SLA värdena för respektive tjänst sätt på rätt nivå. En analys rekommenderas där verksamhetens krav på tillgänglighet matchas mot tjänsternas SLA:er.

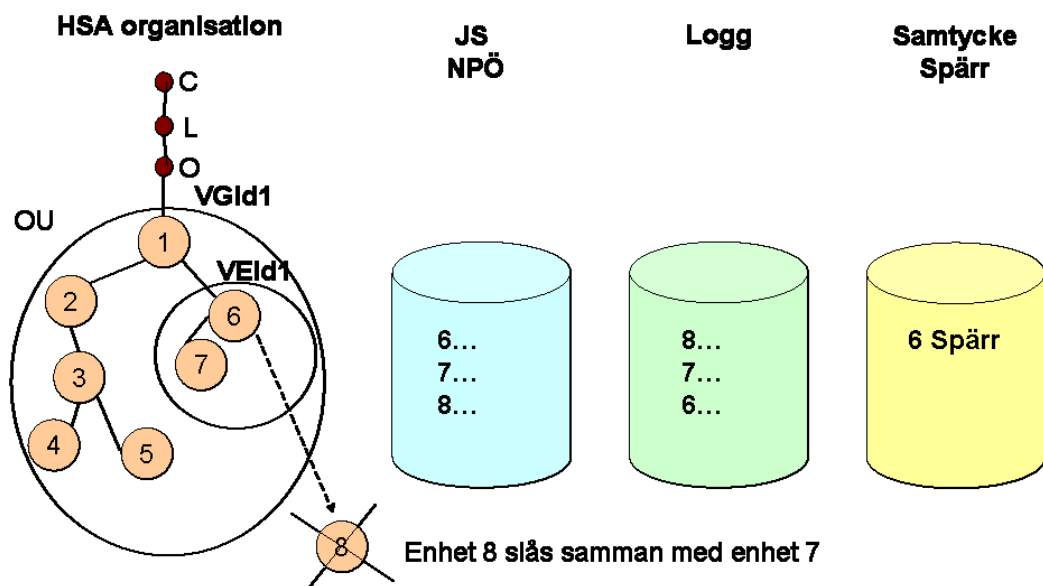
3.4 Organisationsförändringar - historisk data och spärr problematik

Vissa förändringar av personer, organisation och tjänster behöver sparas. Nedanför listas några.

- **Behörighetsstyrande (BIF).** Vem äger informationen idag?
- **Historiskt (HSA).** Vem upprättade dokumentet?

3.4.1. Behörighetsstyrande t.ex. spärrproblematik

För BIF är den behörighetsstyrande punkten mycket viktig. Det finns en komplexitet genom att information spärras och denna spärr får inte försvinna om en organisationsförändring sker. En enhet kan försvinna organisatoriskt, men ur verksamhetssyfte finns den kvar.



3.4.2. Historik

HSA är idag en aktuell katalog som enbart återspeglar nuläget. Det har förekommit propåer från olika projekt på behov av historik i HSA dvs. att få tillgång till information om organisation (och personer) bakåt i tiden.

Örebro har bland annat lyft upp att NPÖ antagligen behöver tillgång till historisk information genom HSA.

En utredning gjordes inom ramen för HSA under våren 2008 som resulterade i ett förslag till hur historik kan införas i HSA om behovet uppkommer och krav på detta ställs

En förbättrad beskrivning behövs om vilka uppgifter efterfrågas, med vilken frekvens, inom vilken tid, med vilken behörighet med mera. Detta för att förstå hur belastningen förväntas bli. Behöver man historisk information inom någon dag, eller är det mycket gammal information?

Viktigt är att i detta arbete värdera om andra tillvägagångssätt kan vara effektivare.

3.5 Kvalitetssäkrade/ E-undertecknade egenskaper

”Alla” poster som används vid behörighetstilldelning måste vara kvalitetssäkrade.

Grundtanken är att uppgiften skall skyddas mot förändring. Detta kan göras på flera sätt. En komplicerad och resurskrävande möjlighet är att ha e-undertecknade (signerade) egenskaper. I dag finns det svårigheter att realisera detta i och med att egenskaperna kommer från lokala kataloger/källor t.ex. PA-system och där signering idag ej sker. Utredning behöver ske kring vilka möjligheter som finns på kort respektive lång sikt att uppfylla detta.

Först behöver det belysas vad vi behöver för skydd och för vilka uppgifter. Sedan hur vi löser detta, där signering är en av flera möjligheter. Då måste det vara tydligt vad som skall signeras, varför, var i informationskedjan det är relevant och om det är möjligt att paketera flera uppgifter.

Värdet av signerade egenskaper bör ställas mot prestandaförluster som det kan medföra.

3.6 RIV EN 13606 ska användas

Initialt använder NPÖ Del 1 i EN 13606. Det finns även andra delar i standarden, såsom Arketyper. Arketyper kommer på sikt att kräva annat lagringsformat i vårdsystemen.

3.7 NPÖ ska använda BIF

Under provdriften använder NPÖ en intern åtkomstkontroll med roller baserat på HSA-attribut (PaTitleCode, PrescriptionCode). SITHS används för autentisering. BIF kommer att ersätta denna tillfälliga lösning under hösten 2009.

3.8 Testmiljö och testdata under utvecklingsfas och driftfas

De flesta tjänster som under produktion har behov av HSA har också behov av att testa denna anslutning under utvecklingsfasen. För HSA finns två testutrustningar för olika ändamål.

De flesta system kommer också att vidareutvecklas och har därmed också behov av tillgång till testmiljö även efter produktionssättning.

Även andra infrastrukturkomponenter behöver testas såsom SITHS med hjälp av testcertifikat eller åtkomst till en testmiljö med definierat innehåll och fejkade personer. I processen behöver hantering och fastställande av testdata tas om hand innan volym av anslutningar kommer igång. Det finns ett behov av att samordna testdata och testmiljöer.

För NPÖ finns testmiljö för vårdinformation av testkaraktär. Det saknas idag möjlighet att kontrollera verkligt data inför en driftstart i NPÖ.

För BIF finns det en testmiljö med i upphandlingen. Denna är inte i dagsläget sammankopplad med Sjunet. Helhetstester med HSA och SITHS går med andra ord inte att göra och det saknas idag en testmiljö för leverantörer och landsting.

För det fortfatta arbetet är det viktigt att det finns tillgång till en testmiljö med alla ingående komponenter (SITHS, HSA, BIF, NPÖ samt att den skall finnas på SJUNET).

3.9 Läkemedelsförteckningen

I dagsläget är inte Apotekets läkemedelstjänst BIF anpassad, vilket innebär att samtyckestjänsten i BIF inte kan användas. Samtycket för läkemedel är dessutom riktad för person och inte organisation. På sikt måste Apotekets läkemedelstjänst BIF anpassas och Apoteket bör kopplas mot BIF-tjänster. Innan dess kan befintlig lösning användas.

3.10 Anslutningsanvisningar och checklistor

Tidigare beskrevs att anslutning till nationella tjänster bör göras på ett samordnat sätt. Policys bör upprättas och dessa bör kompletteras med anslutningsanvisningar och checklistor. Nedan finns några reflektioner av vad som behöver klargöras och vad som kan ingå i anslutningsanvisningar och checklistor.

Jag ska ansluta mitt landsting/organisation

- Var får jag information att det finns?
- Vem vänder jag mig till?
 - Är det en kontaktyta på SVR och som förmedlar
 - eller är det en lista på olika som ska kontaktas?
 - HSA förvaltning
 - SITHS förvaltning
 - BIF Förvaltning
 - NPÖ Förvaltning

-
- Vilka formella dokument/avtal ska processas/skrivas på?
 - Lista....
- Vad är det jag själv behöver hantera på hemmaplan?
 - Olika checklistor beroende på egen installation eller hotell...
 - Ska jag ha flera miljöer (drift/test osv) eller räcker det med 1 miljö?
 - Är det någon utbildning som behövs?
- Är det några krav som ställs på mina klientdatorer?
 - Vilka är dessa i så fall?
- Hur får jag de delar/program jag behöver?
- Var vänder jag mig för att få support
 - Förenat med kostnad/serviceavtal? (BIF debiterar fast pris per ärende)
- Hur verifierar jag att allt är i funktion
 - Vilka testmöjligheter finns?
 - Vilka testmiljöer ska användas?
- Vad behöver konfigureras för att ingå i ”gemenskapen”
- Verifiering av kvalitet på grunddata t.ex egenskaper i HSA, roller i system, uppdatering av uppgifter, behörigheter o.d.
- När allt är klart,
 - Ska det godkännas/certifieras?

Nu vill jag ansluta system X

- Vem vänder jag mig till?
 - Kan jag hänvisa leverantören direkt till denne,
 - Eller måste jag förmedla
- Finns några testmiljöer
 - Hur kommer jag åt dessa
 - Testdata
 - Support
 -

När allt är igång

- Kommer det att finnas servicefönster i respektive tjänst?
 - Orsakar det avbrott för mina användare
 - Vem aviserar dessa? Hur kommer jag med i denna sändlista?
 - Vem samordnar servicefönster för de nationella tjänsterna?
- Behöver jag utföra uppdateringar?

- Vem får jag dessa av (Förvaltning)
- Är uppdateringarna/patcharna testade (integrationstestade)?
- Hur kan jag påverka nästa version?
 - Användargrupper
 - Förslagslåda
 - Vem hanterar detta?

3.10.1. Erfarenhet från Örebro

Í Örebro har redan ett första arbete påbörjats med att ansluta NPÖ. Följande erfarenheter kan hämtas från det arbetet.

NPÖ Checklista inför anslutning av vårdssystem

- Konsolidera vårdinformation
- Minimera antalet anslutningspunkter för NPÖ.
- Fåtal vårdinformationssystem
- Fåtal instanser av varje vårdssystem
- Ställningstagande urval
 - Avlidna?
 - Egna reservnummer exkluderas
 - Personer med skyddad adress kan bli avslöjade på var de varit och var de ska
 - Vad är en kontakt?
 - Periodurval och vilket datum ska väljas
 - Ska vissa vårdenheter uteslutas?
 - Rättsmedicin., Ungdomsmottagning
- Regelverk enligt Patientdatalagen
- Ensning av begrepp och termer
- HSA-katalogen
 - HSA-ID/HSA-information finns i vårdinformationssystemet?
 - Kommuner ska anslutas
 - Kvalité och attribut (Verksamhetskod, PrescriptionCode mm)
- Inför e-tjänstekort och BIF

NPÖ ställningstagande för hur ansluta vårdssystem vad ska göras?

- Pull eller Push?
- Index eller data?
- Integrationsmotor?
- Format? - internt XML-format till integrationspunkt? EN 13606 från vårdssystemet?

- Vilka informationsmängder kan vara med?

4 Detaljerad lösningsarkitektur

På vägen mot det långsiktiga målet kommer tjänsterna att realiseras i en form som gör att nytta kan uppnås i stegvis. Det är av största vikt att NPÖ och BIF kan realiseras under 2009 i några landsting, visa på skapad nytta och även ge erfarenheter och underlag för fortsatt implementering och utveckling. Det betyder att avsteg kan behöva göras från den långsiktiga målbilden, men att lösningsarkitekturen skall vara så framtidssäker som möjlig.

Detta avsnitt beskriver lösningsarkitekturen för respektive tjänst för realisering på kort sikt, dvs. under 2009-2010.

4.1 HSA

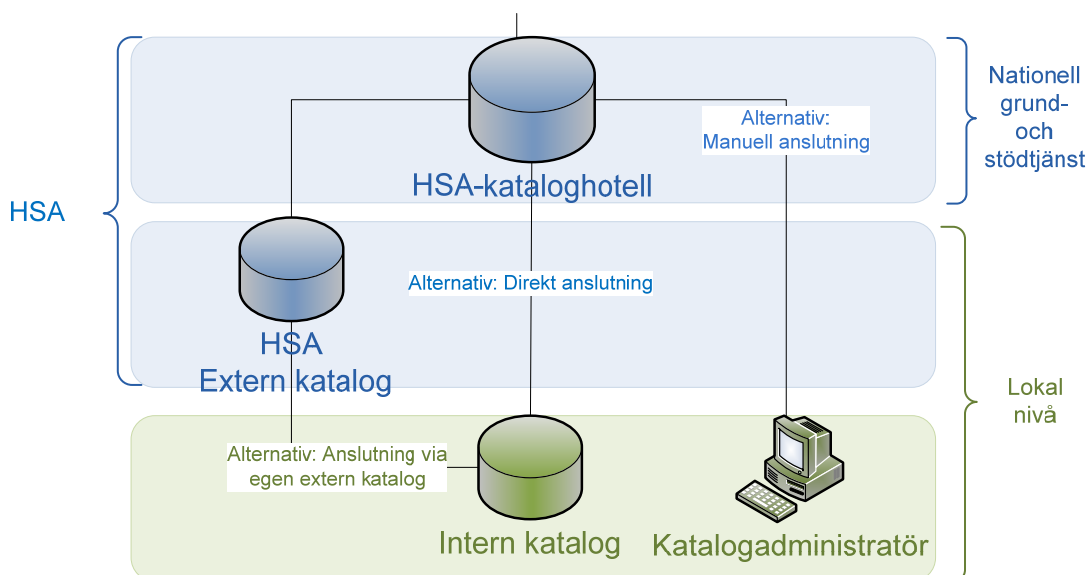
Referenser	Beskrivning
HSA dokumentation	HSA Policy HPT-mall RIV HSA struktur och innehåll Värdebilagor till RIV-dokumentet

HSA är en kritisk faktor för tillgänglighet till nationella tjänster.

Tillgängligheten till HSA regleras genom SLA med tjänsteleverantören. Tydliga SLA-krav är inte dokumenterade från respektive tjänst men kvalificerad gissning är gjord i pågående upphandling och dessa krav kan förändras genom omförhandling av avtal. Detta SLA gäller kataloghotell och centrala komponenter. För anslutna kataloger med egna HSA-instanser är det respektive katalogägare som definierar sin SLA.

Med det distribuerade ansvaret för katalogdrift är det personalen i "det egna" landstinget som blir drabbat om den egna katalogen fallerar.

Varje tjänst som utnyttjar HSA behöver göra en riskanalys, konsekvensbeskrivning och kontinuitetsplan för (bl.a) det fall att HSA inte är tillgänglig. Ett alternativ kan vara att nyttja den interna katalogen som fallback.



Anslutning till HSA kan ske mot antingen den lokalt placerade externa katalogen eller mot HSA. I vissa fall har lokal extern katalog ersatts av HSA-hotellet, där antingen en lokal valfri källa kan användas för att publicera till hotellet eller så kan ett webbgränssnitt nyttjas för att administrera direkt i hotellet, se bild ovan.

BIF-tjänsterna ansluts fysiskt till HSA lokalt eller centralt för att hämta uppgifter till SAML-biljetten. För nationella tjänster är anslutning mot central katalog är att föredra.

4.2 SITHS

Referenser	Beskrivning
SITHS dokument regelverk	<p>SITHS CA-policy Certifikatpolicy för utfärdande av hälso- och sjukvårdscertifikat (HCC)</p> <p>SITHS RA-policy RA-policy för utfärdande av hälso- och sjukvårdscertifikat (HCC)</p> <p>Telia CPS Telia Certification Practice Statement</p> <p>SITHS HCC specifikation Specifikation för Hälso- och sjukvårdscertifikat (HCC)</p>

SITHS-modellen bygger på att anställda i vård och omsorg har ett personligt elektroniskt ID-kort med ett elektroniskt tjänstecertifikat. Detta används för att säkert identifiera och autentisera personer.

SITHS används också för att på ett säkert sätt identifiera och autentisera IT-tjänster.

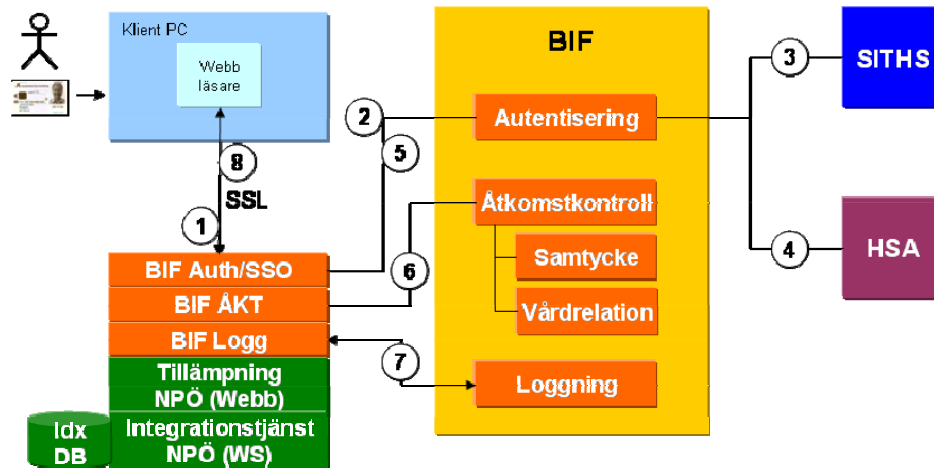
4.3 BIF

Referenser	Beskrivning
BIF Teknisk beskrivning	Tekniskt underlag som varit specifikation för upphandling av BIF
Avtalsbilaga A	Beskriver i stort de ingående komponenterna i Logicas leverans
BIF - Software Architecture Document	Arkitekturbeskrivning
BIF - Funktionsbeskrivning	Övergripande funktionsbeskrivning
BIF - Installations- och Konfigurationsanvisning	Beskriver krav och uppsättning av driftsmiljö för BIF.
BIF - Konstruktionsanvisning	Konstruktionsanvisningar för anslutande system/tillämpningar
BIF - Gränssnittbeskrivning	Gränssnittsbeskrivningar för anslutande system/tillämpningar
BIF – Användarhandbok	Beskriver administration av BIF

Axiomatics Policy Server Handbook	Beskriver administration av regler
BIF - Egenskaper för Åtkomstkontroll	Beskriver de egenskaper som används för att kontrollera åtkomsten till BIF IT-bastjänster

4.3.1. Autentisering, ett anslutningsexempel av en webbtillämpning

Nedan visas hur en anslutning av ett system till BIF och övriga stödsystem för autentisering/SSO kan implementeras. Flödet beskrivs starkt förenklat.

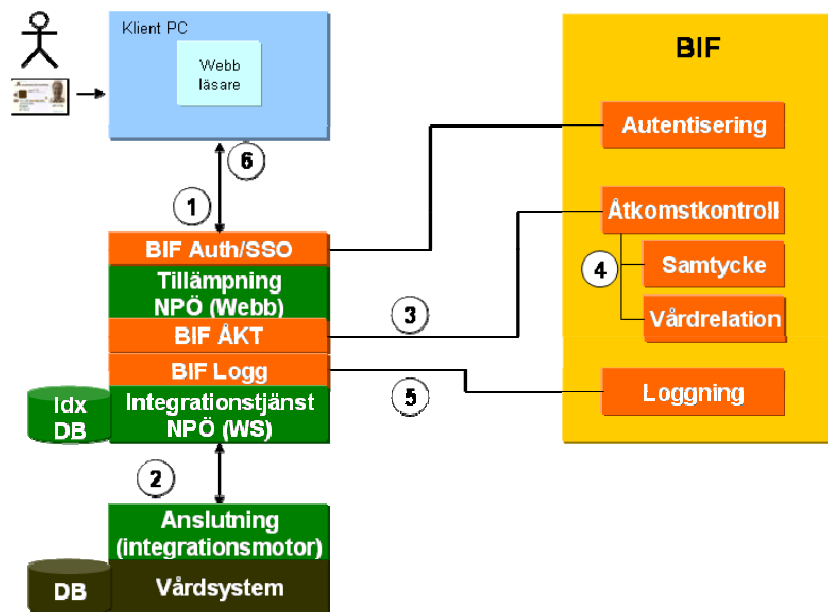


Grundförutsättning är att användaren har ett SITHS-kort med giltigt certifikat, att arbetsstationen har programvaran NetID installerad (ingår i SITHS).

- Användaren startar webbläsaren med adressen till NPÖ.
- I NPÖ implementeras en BIF agent som kontaktar BIF autentiseringstjänst
 - Om användaren inte redan är autentiserad får användaren autentisera sig och ange sin pinkod. Nu har autentiseringstjänsten användarens certifikat och en signering som visar att "rätt" användare "befinner sig bakom" kortet.
 - Om användaren redan är autentiserad (SSO) returneras befintlig biljett till steg 5.
- Certifikatet användaren nyttjat kontrolleras mot SITHS att det inte har spärrats.
- Autentiseringstjänsten hämtar sedan från HSA-katalogen de egenskaper som ska stoppas in i biljetten.
 - Om användaren har flera verksamhetsuppdrag och/eller syften kommer användaren att via dialog, som hanteras i autentiseringstjänsten, välja vilket av uppdraget/syftet som nu är aktuellt
- NPÖ:s BIF autentiseringsagent får nu användarens biljett.
- Nästa steg är att NPÖ kontrollerar om just denna användare får köra NPÖ. Via Åtkomstkontroll formulerar NPÖ en fråga till BIF åtkomstkontrolltjänst
 - NPÖ har i förväg definierat regelverk för åtkomst. NPÖ är i detta skede resursen i resursmodellen.
 - Skulle NPÖ vilja visa olika information beroende på vilken roll användaren har, exempelvis användare eller administratör, är det möjligt att NPÖ ställer denna fråga mot åtkomstkontrollen och utifrån användarens behörighetsegenskaper visas information.
- NPÖ loggar att användaren kommit in i NPÖ-tillämpningen.

8. Användaren får därefter tillgång till NPÖ via webbläsaren.

4.3.2. Anslutningsexempel läsa vårddokumentation i NPÖ



Notera att det i denna implementation inte sker någon åtkomstkontroll av vårddokumentationen på respektive vårdsystem/anslutningstjänst utan detta utförs först av NPÖ centralt. Vårdsystemen levererar all information, dvs. spärrad och ospärrad vårddokumentation.

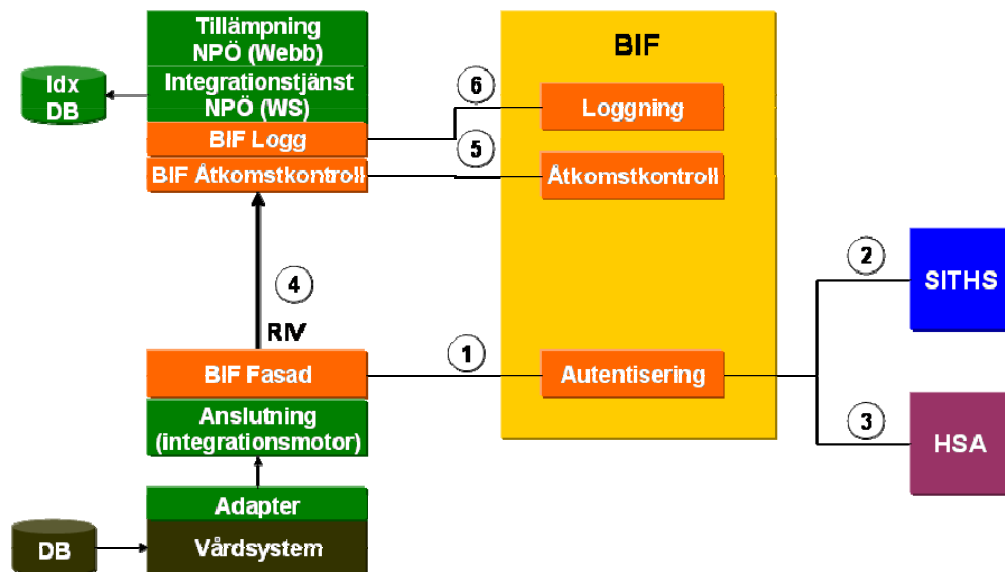
Grundförutsättning är att användaren är autentiserad och att NPÖ har uppdaterats av vårdsystemen gällande index och att vårdinformationen finns i vårdsystemen.

1. Användaren begär att få se vårddokumentation för en specifik patient.
 - a. Ange personnummer och kontrollera att patient finns
 - b. Registrera vårdrelation om det saknas (BIF)
 - c. Registrera samtycke om det saknas (BIF)
 - d. Registrera samtycke till läkemedelsförteckning, se insatsområde "läkemedelsförteckning" (om det saknas och användaren har förskrivarrätt (HSA-attribut))
 - e. Eventuella kontextanslutna tillämpningar byter kontext till ny patient (BIF)
 - f. Logga vald patient (BIF)
2. NPÖ hämtar information från vårdsystemet.
 - a. Notera att ingen åtkomstkontroll med spärr/samtycke/vårdrelation sker i detta skede.
 - b. Informationen hämtas från vårdsystemet (RIV, BIF)
3. NPÖ Åtkomstkontrollerar
 - a. NPÖ ställer en fråga till åtkomstkontrolltjänsten

- b. Åtkomstkontrolltjänsten evaluerar matchande regler samt hämtar spärrar, samtycken och vårdrelation från underliggande tjänster. Utifrån regelevalueringen returneras **Ja** eller **Nej** på frågan.
 - c. De informationsmängder som användaren begär att få se loggas av NPÖ till loggtjänsten.
4. NPÖ visar vårdinformationen
- a. Användaren presenteras i NPÖ begärda uppgifter där ett Ja erhållits från åtkomstkontrolltjänsten.
 - b. Användaren kan därefter välja mer detaljerad information.
 - c. Användarens aktiva val loggas (BIF)
 - d. Ny åtkomstkontroll sker genom kontroll med samtycke/spärrar/vårdrelation (BIF)
 - e. Detaljerad vårdinformation hämtas från vårdsystem (RIV,BIF)

4.3.3. Anslutningsexempel uppdatering av NPÖ.

Följande exempel visar hur ett vårdssystem uppdaterar index/DB i NPÖ och där BIF-specifika delar är i fokus.



Uppdatering av NPÖ index (eller data) från Vårdsystemet sker med regelbunden periodicitet. Då anslutningstjänsten har ny information som ska uppdatera NPÖ sker följande steg (starkt förenklat):

1. BIF-fasaden hämtar en biljett från autentiseringstjänsten och uppvisare ett mjukt certifikat (SITHS HCC Funktion).
2. SITHS kontrollerar att certifikatet inte är återkallat.
3. Autentiseringstjänsten hämtar sedan från HSA katalogen de egenskaper som ska stoppas in i SAML-biljetten.
4. BIF-fasaden paketerar meddelandet i RIV struktur samt hanterar signering och kryptering av meddelandeinnehållet om så önskas. Sedan anropas NPÖ Integrationstjänst.
5. Åtkomstkontroll för systemanvändare (tjänst)
 - a. SAML-biljetten kontrolleras
 - b. Åtkomstkontroll via regelverk.
 - c. Dekryptering och verifiering av Fasaden i BIF
6. Anropet loggas
7. Integrationstjänsten i NPÖ uppdaterar index.

4.3.4. BIF förvaltning med nationell kundtjänst

Nationell kundtjänst tillhandahålls av Sjunet SPOC, för levererade nät- och värdetjänster. Kundtjänsten tar emot och hanterar snabb felklassificering av felanmälningar och eskalerar till rätt instans dygnet runt, årets alla dagar. Den nationella kundtjänsten utgör "First Line Support" för nationella IT-tjänster.

Logicas "Service Desk" tar emot BIF-relaterade incidentanmälningar via kundportalen PrimePortal, som är en central punkt för informationsdelning, självbetjäning och tjänsterapportering.

Varje incident klassificeras efter hur allvarligt problemet bedöms vara i följande incidentprioriteter Critical, High, Medium Low.

"Service Desk" utgör en "single-point-of-contact" med incident-, problem-, fel- och förändringshantering. "Service Desk" ansvarar även för kontinuerlig återkoppling av ärendestatus till nyttjarens "First Line Support".

Regler, rutiner, processer med mera för samverkan och samarbete mellan olika helpdesk/servicedesk måste etableras så att ansvar och förhållanden regleras så tydligt som möjligt.

4.3.5. Administration och åtkomst till spärrar och samtycke

Samtycke och spärr ska kunna spridas till och vara åtkomliga för alla system/organisationer.

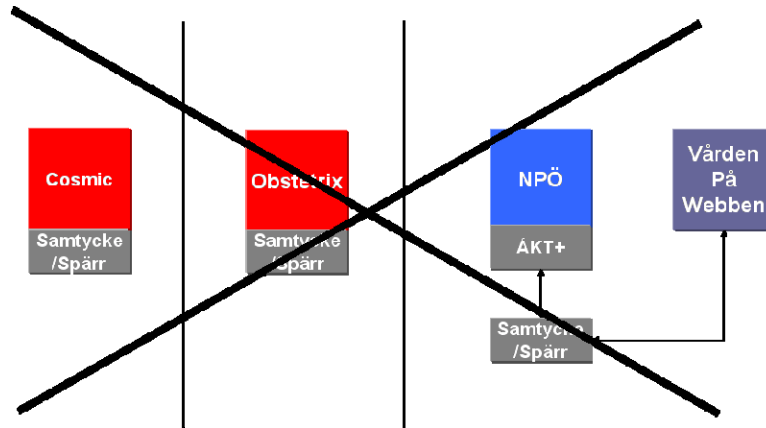
Hantering av spärrar sker idag på olika sätt, varje vårdsystem implementerar sin mekanism för att registrera spärrar inom sitt system. I praktiken betyder det att alla system hanterar spärrad information på sitt eget format (informationsmodell) inuti sitt system.

Men när en patient vill spärra informationen är det inte rimligt att de ska behöva hålla reda på var informationen finns. Frihetsgraderna för patientens spärrar är också mycket stora, t.ex. kan den spärra informationen på en vårdenhets, se exempel nedan.

Det betyder att alla system måste antingen använda samtyckestjänsten för att hitta information, eller kunna "prenumerera" på spärrar och samtycken och översätta dessa till sitt eget format.

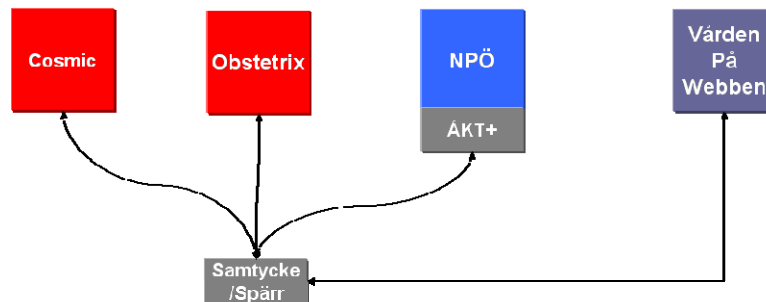
På vårdenheten Kvinnoklinik, finns 10 olika system, bland annat obstetriksystem, lab-system, operationsplaneringssystem etc. Patienten begär att information om en abort skall spärras. Administratören på vårdenheten måste då idag gå in i alla dessa system och administrera spärren.

Det är rimligt att anta att patienten själv kommer att administrera sina spärrar. Detta är inte möjligt om de hanteras lokalt i respektive system.

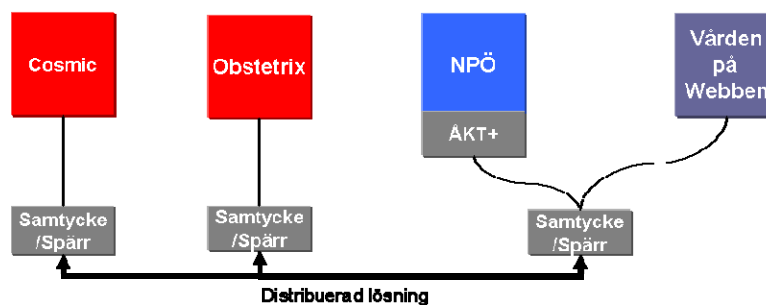


BIF erbjuder genom den upphandlade lösningen en gemensam spärrtjänst. Om alla system nyttjar denna så kommer den beskrivna problematiken att försvinna. Det innebär att man administrerar spärrar en gång och att både lokala system samt nationella, såsom NPÖ, nyttjar samma tjänst, se bild nedan.

Vid förfråga om spärrad information skall det lokala systemet kontrollera detta mot den nationella spärrtjänsten.



Att det skall vara en nationell tjänst betyder inte att det är en central instans, detta kan fortfarande hanteras som en distribuerad tjänst. BIF är uppbyggt så att samtycken distribueras till alla instanser.



Nödvändiga aktiviteter lokalt och nationellt:

- Befintliga system kommer att behöva realisera spärr enligt lagkrav
- När man lagrar en spärr skall detta ske i den gemensamma spärrtjänsten, d.v.s. BIF-spärrtjänst. Detta krav skall ställas mot leverantörerna.
- När man kontrollerar om spärrar finns skall gemensam spärrtjänst användas. Detta krav skall ställas mot leverantörerna.

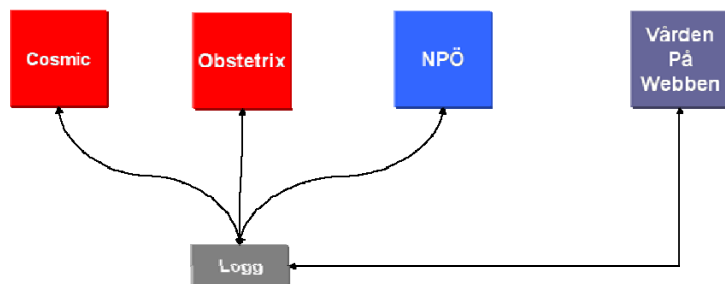
- Så länge landstingen inte har löst koppling mellan de lokala systemen och BIF-spärrtjänst kommer spärrar behöva administreras direkt i den centrala spärrtjänsten för att patientens spärr skall effektueras i sammanhållen journalföring. Observera att problemen på lokal nivå inte hanteras genom detta.

4.3.6. Administration och åtkomst till loggar

På samma sätt har patienten rätt att få information om den direktåtkomst och elektroniska åtkomst som har förekommit. Liknande behov kommer då att uppstå kring loggning.

En patient som vill ha information om den åtkomst som funnits måste få detta från varje system om loggar hanteras lokalt. Detta kommer att bli en administrativ börda.

För behovet att försörja t.ex. Vården på Webben bör gemensam loggtjänst nyttjas.



För uppföljning måste varje vårdgivare kunna se sin del i samtliga loggtjänster/instanser via BIF Logganalystjänst.

Nödvändiga aktiviteter lokalt och nationellt:

- Befintliga system kommer att behöva realisera loggning enligt lagkrav
- Logg för åtkomst till systemet skall lagras i den lokala instansen av loggtjänsten, dvs. BIF-loggtjänst. Detta krav skall ställas mot leverantörerna.
- Systemleverantörer kommer att efterfråga vilket gränssnitt för lagring av logg som Regelverket för loggning måste klargöras

4.4 NPÖ

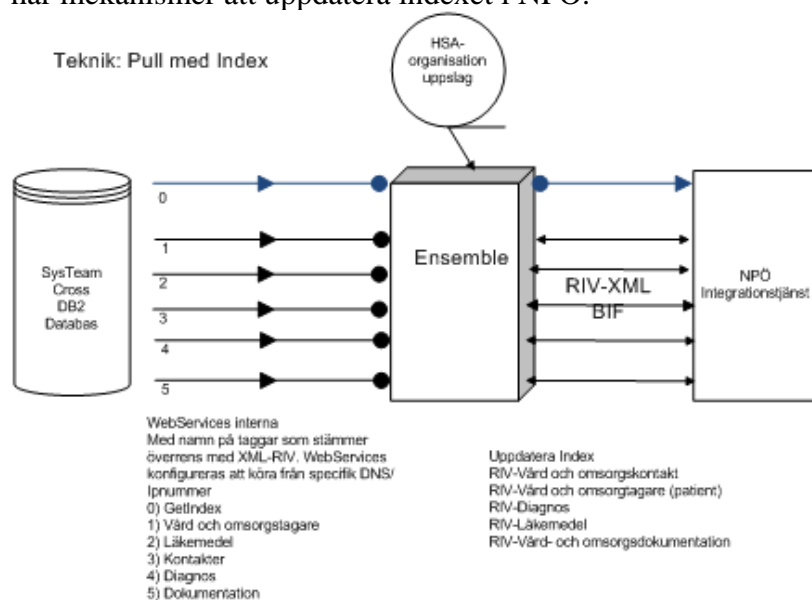
Referenser	Beskrivning
Gränssnittsbeskrivning NPÖ	Beskriver tjänster som används för att hämta information till NPÖ från vårdsystemen. (svarsgränssnitt) samt leverera information till tillämpning från NPÖ (frågegränssnitt)
Interaktionsmönster NPÖ	Beskriver interaktionsmönster och metodbeskrivningar (inkl parametrar) för kommunikation mellan NPÖ och vårdsystem.
Tillämpningsanvisning Nationell patientöversikt	Beskrivning av vilka informationsmängder som ingår och hur RIV:s informationsmodeller ska användas i NPÖ

4.4.1. NPÖ Index

I NPÖ finns idag ett tunt index som innehåller personnummer, url, instans av vårdssystem (som har ett tilldelat HSA-ID) och kod för vilken informationsmängd (16 typer finns idag) som finns i vårdsystemet. Eftersom en patient inte förekommer i alla vårdssystem i Sverige är detta en fullt möjlig lösning för enklare skärmbilder utan prestandaproblem. Först när användaren frågar efter informationen så hämtas vårdinformationen. När man håller ett tunt index har man mindre problem med att hantera konsistensproblem mellan vårdsystemet och NPÖ.

För att kunna klara patientöversiktsskärmbilden som innehåller många informationsmängder finns ett utökat index. Det utökade indexet är mer komplext att hålla konsistent.

Uppdatering av index sker antingen på initiativ från NPÖ (PULL) eller på initiativ från vårdsystemen (PUSH). Det är troligt att uppdatering av NPÖ:s index sker minst 1ggr/dygn. (För det utökade indexet krävs det oftare). Tjänsten ska ha ett SITHS-certifikat och kryptera informationsöverföringen via BIF. Även patienter med spärrar kommer med i indexet. Det är först när användaren vill se vårdinformationen som åtkomstkontrollen i BIF används för att filtrera informationen utifrån spärrar och behörighet. Med PUSH menar man att vårdsystemet har mekanismer att uppdatera indexet i NPÖ.



Figur. Exempel på vårdanslutning. Tekniken som valts är att NPÖ anropar vårdsystemet(PULL) för att uppdatera NPÖ med Index. När användaren begär information anropas vårdsystemet. I detta fall används ett internt XML-format. Konvertering till EN 13606 sker i integrationsmotorn där informationen även kompletteras med katalogdata från HSA-katalogen.

4.4.2. NPÖ vårdinformation som mellanlager

Vårdinformationen kan även mellanlagras i NPÖ. Orsaken till det kan t.ex. vara när vårdsystemet inte klarar prestandamässigt för mycket förfrågningar. Ett annat tillfälle kan vara t.ex. provsvar från ett labbsystem där NPÖ ses som en ren provmottagare. Även spärrad information lagras i detta fall i NPÖ och det är först när användaren efterfrågar informationen som åtkomstkontrollen filtrerar spärrad information. BIF koppling finns när vårdsystemen uppdaterar index eller data. För samma informationstyp kan man blanda anslutningar med index eller mellanlagerteknik.

Vid själva uppdateringen av index eller mellanlager sker enbart en enkel åtkomstkontroll som kontrollerar att den aktuella tjänsten får göra den efterfrågade åtgärden. I åtkomstkontrollen vid anslutningen används inte samtycke och vårdrelation.

4.4.3. NPÖ läsning av vårdinformation

När användaren begär information i NPÖ, kontrollerar NPÖ i indexinformationen var information om patienten finns (informationen kan finnas i vårdsystemet eller i ett mellanlager i NPÖ). I samband med att informationen hämtas filtreras information med hjälp av åtkomstkontrollen i BIF. Åtkomstkontrollen kontrollerar med Samtyckestjänsten och Vårdrelationstjänsten. På detta sätt förhindrar man att spärrad information visas.

NPÖ loggar användarens aktiva val via BIF till loggningstjänsten.

4.4.4. NPÖ, Driftsplattform för Patientöversiktstjänsten

TietoEnator driftar NPÖ som en tjänst över SjuNet.

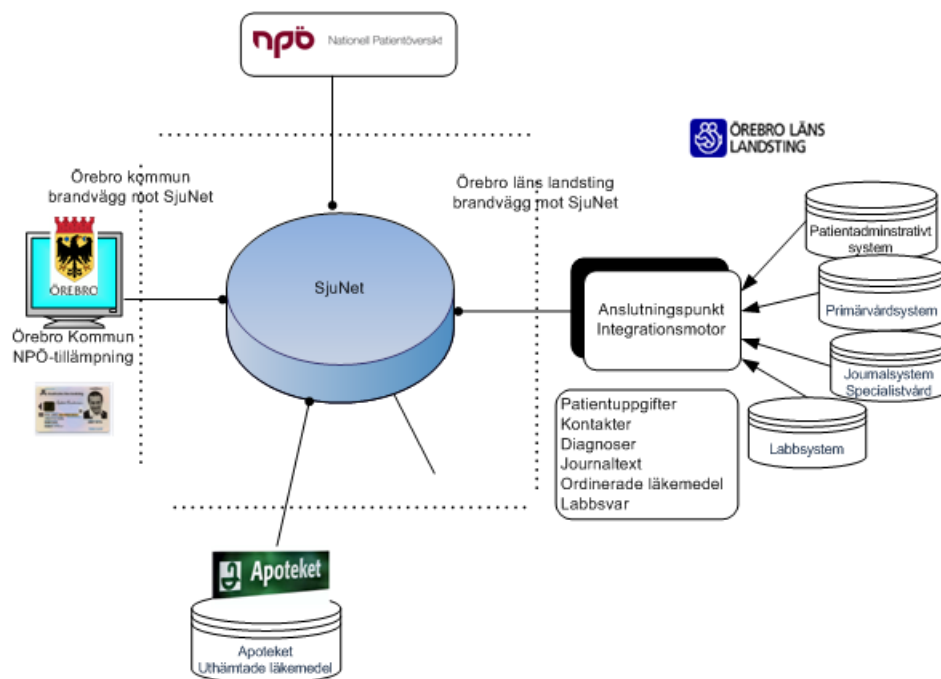
Inom patientöversiktstjänsten finns följande komponenter:

HUB	Innehåller indexinformationen
Edge Gateway	Gränssnitt för att hämta information från vårdsystemen eller fungerar som mellandatalager för vårdinformation som kräver mellanlager
Access GateWay	Frågegränssnitt mot NPÖ som används av NPÖs användargränssnitt eller fristående tillämpningar.
Tillämpning	Webbaserat stöd för Internet Explorer och Firefox

4.4.5. NPÖ, Driftplattform för Anslutningen mot vårdsystemen

Vårdgivaren ansvarar för anslutningarna till vårdsystemen. Anslutningstjänsten kan se olika ut beroende på hur konsoliderad vårdinformation är. Det viktiga är att mellan NPÖ och vårdanslutning ska RIV användas som informationsgränssnitt. RIV baseras på den europeiska standarden EN 13606.

Om man använder sig av en anslutningstjänst i form av en integrationsmotor kan vårdsystem ha interna gränssnitt som mappas om i en integrationsmotor till RIV-meddelanden (EN 13606).



Figur visar hur anslutningen ser ut i Örebro under provdriften. Här är det främst kommunen som konsumerar vårdinformation som landstinget producerar och sköter driften av anslutningen till vårdsystemet.

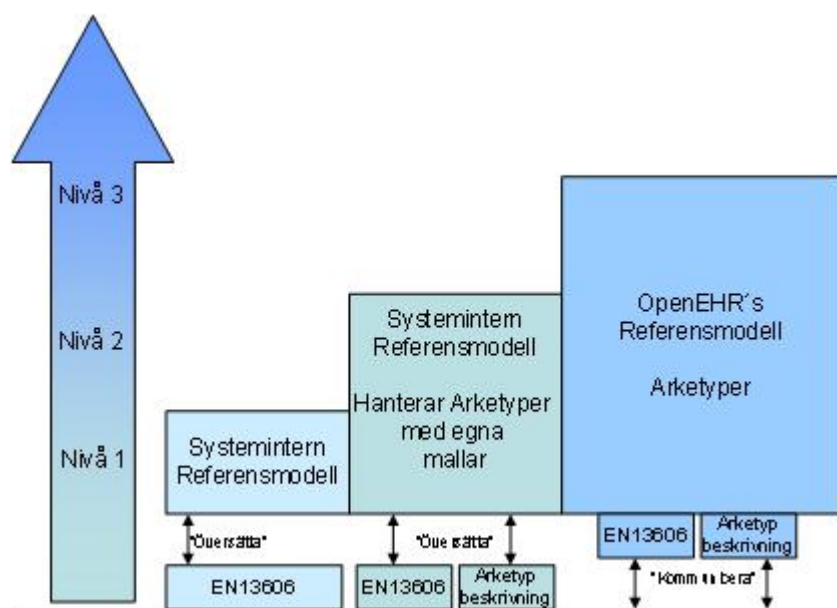
4.5 RIV

Referenser	Beskrivning
RIV-specifikationer för NPÖ	
RIV_V-TIM_v_1_0.pdf	
prRIV_EN_13606_profil_lev20080605.pdf	
RIV Tekniska Anvisningar	
Revidering av V-TIM till standard	

RIV regelverket skapades för att åstadkomma ett för vård och omsorg gemensamt regelverk för att säkerställa interoperabilitet mellan olika vård- och omsorgssystem dvs. bland annat underlätta ett strukturerat elektroniskt informationsutbyte. Utbytet kan ske mellan olika vård- och omsorgsgivare eller mellan vård- och omsorgsgivare och apotek, myndigheter och motsvarande organisationer. Interoperabiliteten brukar delas in i semantisk interoperabilitet, som berör informationens innehåll och struktur samt teknisk interoperabilitet, som avser säkerhet och kommunikation.

Beställarledningen vid SKL har beslutat om att inriktningen för arbetet med semantisk interoperabilitet i den svenska vården och omsorgen är att följa och tillämpa den europeiska standardansatsen EN 13606 (EHRcom) och dess rekommendationer.

Anpassningen kommer att ske stegvis, se bild nedan.



På Nivå 1 ligger fokus på kommunikation av information, vilket sker enligt EN13606-del 1's referensmodell utan att arketyper eller att openEHRs RM finns implementerad i berörda IT-stöd. Innehållet i meddelandet specificeras utifrån en arketypp/template. Detta sker t.ex. idag i första implementeringen av NPÖ.

Under transporten paketeras informationen som ett RIV-meddelande i enlighet med RIV tekniska anvisningar.

4.6 Sjunet

Referenser	Beskrivning
Sjunetavtal - Ramavtal	Bilaga A – Tjänstebeskrivning. Bilaga B – Priser: Ompaketerad och bifogas som Anslutningsavtalets Bilaga 3 Bilaga C – Anslutningsavtal: Bifogat trepartsavtal enl. nedan Bilaga D – Rutiner: Ersätts av Servicehandboken

Sjunet är ett VLAN (Virtuellt LAN), som för närvarande drivs av vår Nätoperatör, TDC. Samtliga landsting, ett antal kommuner, ett antal privata vårdgivare inkl Praktikertjänst och Capio, Skatteverket samt ett femtiotal leverantörer, inklusive Apoteket, är idag anslutna till Sjunet. Sammanlagt ca 130 anslutna.

Sjunet skall betraktas som ett, för ackrediterade nyttjare, öppet och kvalitetssäkrat nät med syfte att tillhandahålla hög tillgänglighet och god prestanda för alla aktörer inom Svensk Vård och Omsorg. Enbart aktörer inom vård och omsorg får ansluta sig och utbyta information över nätet. Granskningsrutiner möjliggör att informationssäkerhet enligt anslutningsavtal kan upprätthållas över tid. Sammantaget med att Internet inte är anslutet till Sjunet, gör att största hotet mot informationssäkerheten kommer från respektive nyttjares system och interna nätverk. Till skillnad från Internet, finns möjligheten att ställa krav på och kontrollera alla anslutna nyttjare med avseende på informationssäkerhet.