inera

# *Tjänster för Samtycke och Patientrelation enligt PDL*

SAD

# Innehållsförteckning

# Figurer

# 1. Dokumentinformation

## 1.1. Syfte

Syftet med detta dokument är att beskriva arkitekturen för på Samtycke- respektive Patientrelationstjänst.
Den övergripande arktitekturen, och tillhörande nationella tjänstekontrakt, applicerar på alla implementationer av stödtjänster för samtycke och patientrelation som ska kunna samverka i en federation..
Vidare beskrivs lösningsarkitekturen för de implementationer som tas fram under ledning av Inera AB på uppdrag av Cehis.

## 1.2. Målgrupp

De huvudsakliga målgrupperna för detta dokument är beställare, arkitekturledningen, systemarkitekter och utvecklingsteam.

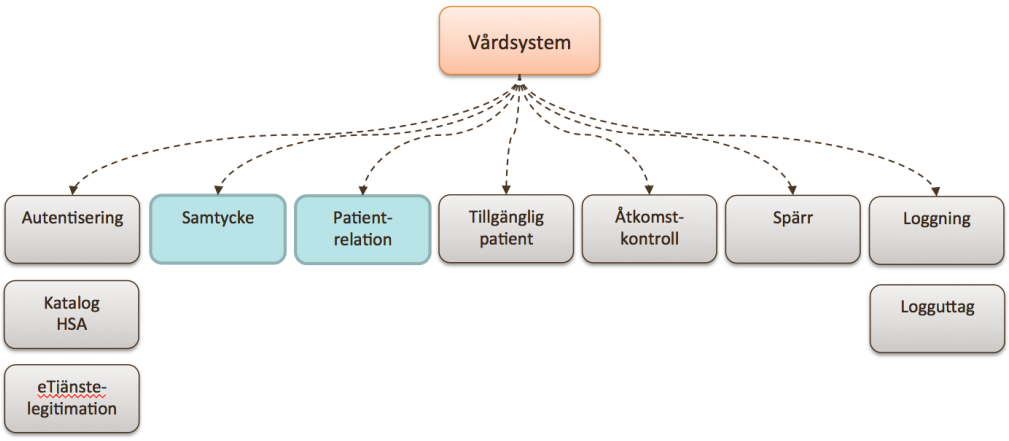
## 1.3. Revisionsinformation

| Revisionshistorik | | | |
|---|---|---|---|
| Version | Datum | Författare | Kommentar |
| 0.1 | | Per Mützell | Första version<br>Använt RIV-mall för SAD för att utgöra underlag för slutlig SAD. |
| 0.2 | | Per Mützell | Justerad arkitektur och princip för nationella läskontrakt; kräver ingen nationell nod för samtycke och patientrelation.<br>Påverkan på befintlig ÅKT-tjänst av ovan ändring. |
| 0.3 | | Per Mützell | Fler användningsfall och arkitekturella mönster |
| 0.31 | 2012-03-13 | Per Mützell | Redaktionellt |
| PA1 | 2012-03-27 | Per Mützell | Reviderad efter första granskning. Ska kompletteras med bland annat intern realisering av driftsaspekter. |
| PA2 | 2012-05-07 | | |

# 2. Översiktlig beskrivning

## 2.1. Sammanfattning

Säkerhetstjänsterna Samtycke och Patientrelation syftar till att stödja processen att hantera relationen patient till vårdpersonal samt samtycke till direktåtkomst inom sammanhållen journalföring enligt Patientdatalagen. Modellen för detta baserar sig på PDLiP-arbetet (Patientdatalagen i Praktiken) som CeHis initierat och som resulterat i RIV-specifikation PDLiP [S8].
Tjänster med motsvarande funktionalitet är idag i drift som stöd till Nationell Patientöversikt för att där hantera PDLs krav på samtycke och patientrelation.




**Figur 1: Säkerhetstjänster översikt.**

Den vidareutvecklingen av tjänsterna som här kravställs syftar till dels till att anpassa tjänsterna till den nationella referensarkitekturen (T-boken) och dels att skapa en arkitektur där tjänsterna kan konsumeras på ett enklare och mer flexibelt sätt både på det lokala och nationella planet.

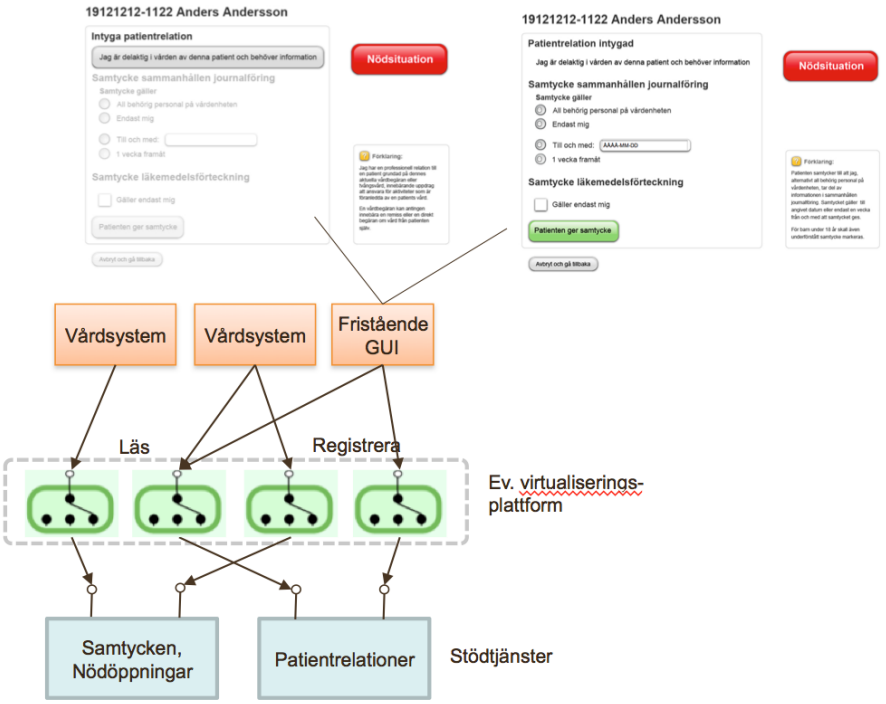
Mer specifikt innebär vidareutvecklingen att

- tjänstegränssnitt (tjänstekontrakt) enligt RIV TA 2.1 [R2] tas fram [T1,T2]
- tjänsterna anpassas till säkerhetsmodellen för RIV TA, vilket bidrar till enklare anslutning och ökad teknisk interoperabilitet
- tjänster på lokalt och nationellt plan kan samverka genom tydliga kontrakt
- vårdsystem som ansluts binds till tjänstekontrakt – inte en specifik lösning. Det gör att huvudmän som använder samma vårdsystemsleverantör inte är bundna till samma val av stödtjänst

- tjänsteplattformar kan nyttjas för att konsolidera tjänsteutbudet och förenkla anslutningar

Se vidare "Arkitekturella mål" för specifika krav på utvecklingen.

Nedan figur visar principiellt hur stödtjänsterna kan konsumeras från vårdsystem eller andra fristående e-tjänster.




**Figur 1: Nyttjande av stödtjänster för hantering av samtycke och patientrelation.**

Genom nyttjande av stödtjänster kan samma registrerade samtycke för åtkomst till andra vårdgivares uppgifter återanvändas i flera vårdsystem och e-tjänster, såväl lokala som nationella. Detta för att vårdpersonalen ska slippa multipla registreringar av samma sak. Allt efter regelverket tillåter kan samtycken och patientrelationerna anges att gälla för viss utsträckning i tid och för den personal det omfattar, t ex samtycke för alla medarbetare på vårdenheten under en vecka.

Vårdsystem får möjlighet att läsa/kontrollera samtyckesuppgifterna i stödtjänsterna, och användare kan göra registreringar, antingen genom dennes ordinarie vårdsystem (typiskt journalsystemet) eller via ett fristående gränssnitt, t ex i en portal eller i samband med att nationell e-tjänst nyttjas.

# 3. Målbild och principer

## 3.1. Verksamhetsmässig målbild

Följande verksamhetskopplade mål och krav finns för tjänsterna:

- Processer som hanterar sammanhållen journalföring där vårdinformationen finns i en eller flera system/e-tjänster, lokalt eller nationellt, ska kunna använda en konsoliderad hantering av patientrelation och samtycke för direktåtkomst enligt PDL.
- Tjänsten ska även stödja begreppet nödöppning att använda när inte samtycke är möjligt att få från patienten och det råder fara för patientens liv och hälsa.
- Hälso- och sjukvårdpersonalen ska få stöd att på ett enkelt sätt registrera patientens samtycke och patientrelation, dess varaktighet och för vem/vilka registreringen gäller.
- Samtycken och patientrelationer ska kunna få genomslag i anslutna e-tjänster, såväl lokala som nationella, t ex både i det egna vårdsystemet och i nationell patientöversikt, så att dubbelregistreringar undvikes.
- Det ska finnas historik att tillgå för att se vad som lagts in för patienten bakåt i tiden.
- Inloggad personal ska vara starkt autentiserade, med SITHS eID eller motsvarande godkänd lösning.
  Notera att detta krav gäller inloggning i de applikationer som interagerar med de bakomliggande tjänsterna.
- All hantering ska loggas och loggen ska kunna tillgängliggöras vid den uppföljning av personalens aktiviteter (via loggar) som verksamheten är lagstadgade att utföra. De verktyg som används för övrig liknande uppföljning för åtkomst till nationella e-tjänster ska kunna användas. Se vidare under 11.11 Spårbarhet.

## 3.2. Arkitekturella mål

### 3.2.1. Generella mål

- Följsamhet mot Nationella IT-strategin.
- Lösningen utformas i enlighet med gällande versioner av tekniska anvisningar så som T-bokens referensarkitektur [S2], tekniska målbilder för nationella tjänster och RIV tekniska anvisningar.
- Återanvändning av nationellt framtagna säkerhetslösningar och nationell katalogtjänst

### 3.2.2. Specifika mål

- Tjänstegränssnitt (tjänstekontrakt) för all extern funktionalitet utan krav på specifik lokalt installerad programvara (Software Development Kit, SDK).
- RIVTA2.1 Basic Profile Säkerhetsmodell för tjänstegränssnitten [R2]. Transportsäkerhet ersätter meddelandesäkerhet.
- Kan nyttja tjänst genom att tjänsten litar på anropande system utan att systemet måste ha en säkerhetsbiljett för slutanvändaren (trust mellan system).
- Möjligt att nyttja tjänsterna var och en för sig efter behov (fristående tjänster).
- Tjänsterna kan publiceras på tjänsteplattform (virtualiseringsplattform), nationellt och/eller lokalt.
- Stöd för en distribuerad arkitektur, där det är möjligt för en region/landsting/kommun att upprätthålla egna instanser av tjänsterna alternativt gemensamma molnbaserade tjänster, och samtidigt kunna samverka nationellt med samtycke och patientrelation i nationella e-tjänster (Ersätter befintlig replikeringsmekanism).

### 3.2.3. Planerade avsteg

Inga planerade avsteg.

## 3.3. Prioriterade områden

I denna utveckling är prioriterat att anpassa tjänsterna till den nationella referensarkitekturen.

Tjänsten Samtycke hanterar idag samtycke till direktåtkomst till sammanhållen journalföring enligt PDL. Utvecklingen ska möjliggöra att andra samtycketjänster (t ex för LF-samtycke hos Apotekens Service AB) parallellt kan existera och fungera tillsammans i arkitekturen. Det möjliggörs genom att använda referensarkitekturen och skapa fristående SOA-tjänster som kan samverka hos konsumerande system.

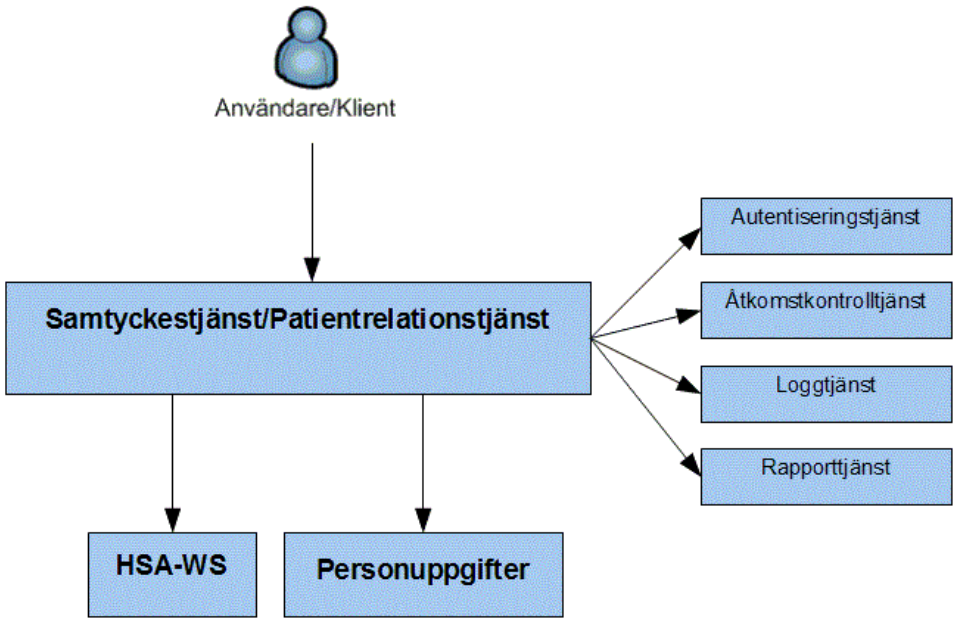
Andra typer av samtycken ska också kunna implementeras i konceptet, vilket tas höjd för, men i övrigt ligger utanför den vidareutveckling som beskrivs i detta dokument.[1]

1 Vid förfrågningar angående vidareutveckling av Inera Säkerhetstjänster, vänd er till Säkerhetstjänsters förvaltning, se http://inera.se/Infrastrukturtjanster/Sakerhetstjanster/

# 4. Teknisk lösning

## 4.1. Översikt

Bilden nedan visar översiktligt beroenden till andra system och tjänster som Samtyckestjänsten och Patienrelationstjänsten har.




**Figur 2: Systemberoenden till andra system och tjänster.**

Autentiseringstjänsten används för att autentisera användare av systemet.

Åtkomstkontrolltjänsten används för att kontrollera åtkomst för användare av systemet.

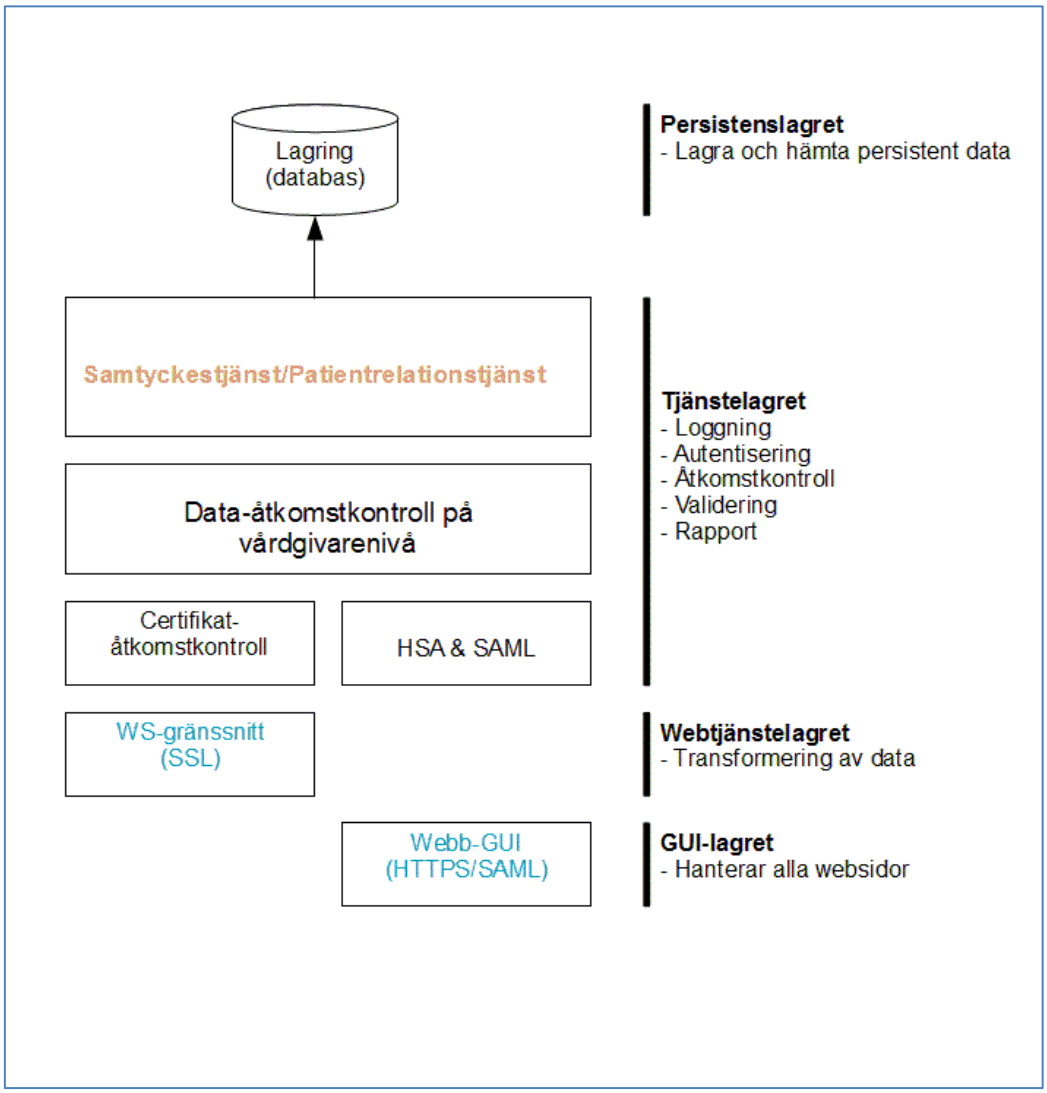
Loggtjänsten används för att logga aktiviteter och möjliggöra uppföljning av händelser.

Rapporttjänsten används för att generera rapporter för loggуppföljning. Formatet på rapporter som genereras kan vara XML eller PDF.

HSA-WS är en katalog tjänst som håller användarinformation där användare som vill få åtkomst till tjänsterna måste finnas uplagda.

Personuppgifter är ett tjänstekontrakt som nyttjas för att hämta personuppgifter för patienter. Personuppgifter nyttjar bla SPAR som är Statens personadressregister och som är ett offentligt register som omfattar alla personer som finns folkbokförda i Sverige, både svenska och utländska medborgare.

Bilden nedan visar övergripande hur samtyckestjänsten och patientrelationstjänsten är realiserade.




**Figur 3: Intern vy av realiserade tjänster.**

De båda tjänsterna har implementerats med en gemensam Java-plattform. I plattformen ingår grundläggande teknik såsom autentisering, loggning, åtkomstkontroll, webbtjänstestack o databashantering. På plattformen läggs sedan verksamhetsmodulen och dessa paketeras till två olika system. Följande skiktning gäller för de båda systemen:

- Persistenslagret: Hanterar persistens mot databasen.
- Tjänstelagret
  - Certifikat-autentisering på web service anrop sker via Autentiseringen.
  - Kontroll av behörighet sker via Åtkomstkontrollen. Behörighetskontroll sker på vårdgivarenivå.
  - Loggning sker via gränsnitt för Loggning och utförs vid alla typer av registreringar, makulering, återkallan och uttag av rapporter. HSA katalogen nyttjas för att hämta information om aktör.
  - Validering utförs på inkommande data. Tjäsntekontraktet Personuppgifter nyttjas vid registrering för att validera angivet personnummer och hämta personnummer uppgifter.
  - Uttag av rapport för logguppföljning. Loggdata returneras efter åtkomstkontroll på vårdgivarenivå.
- Webbtjänstelagret: Transformerar XML-data till tjänsteobjekt och vice versa.
- GUI-lagret: Hanterar SAML-autentisering och webbsidor för slutanvändare genom att nyttja Autentisering.

Det är möjligt att konfigurera tjänsterna på olika sätt när ett system ska installeras. Vid installation kan man välja att ha ett system som är helt fristående eller om man vill nyttja en eller flera av säkerhetstjänstens tjänster.

När en lokal installation av Samtyckestjänsten eller Patientrelationstjänst installeras kan man välja att nyttja säkerhetstjänsten. Om man väljer det alternativet installeras proxys mot Autentisering, Åtkomstkontroll, Loggning och Rapport och lokala anropen skickas vidare till säkerhetstjänsten. Regler för åtkomstkontroll måste då konfigureras i Axiomatics. Loggning sker mot loggkategori ’bifverksamhetslogg’ och befintliga logganalyser i Logganalystjänsten används för att generera rapport för logguppföljning.

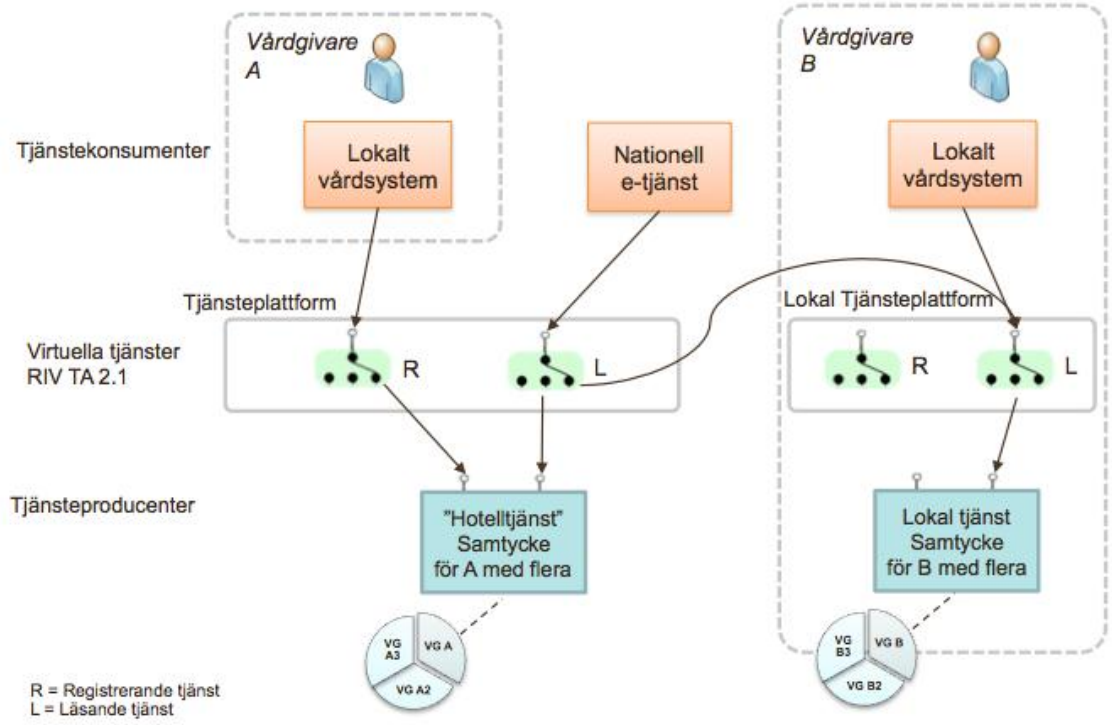
Det är även möljigt att bara konfigurera någon av dessa att gå mot säkerhetstjänsterna. Loggtjänst och Rapporttjänst måste däremot konfigureras lika.

När en lokal installation av Samtyckestjänst eller patientrelationstjänst installeras och man inte vill ha beroenden till säkerhetstjänsten installeras lokala implementationer av Autentisering, Åtkomstkontroll, Loggning och Rapporttjänsten.

Säkerhetstjänsten har en lokal installation av Samtyckestjänsten och Patientrelationstjänsten installerad. Det är fullt möjligt att nyttja dessa av andra system som av någon anledning ej vill installera och använda egen lokal Samtyckes och/eller Patientrelationstjänst.

Arkitekturen för tjänsterna och dess externa gränsytor byggs för att passa in i CeHis nationella referensarkitektur för interoperabla lösningar för hälso- och sjukvården. Referensarkitekturen är inriktad på en tjänsteorienterad arkitektur där funktionalitet utförs av en SOA-tjänst som antingen är nationell eller lokal och som i regel rör information som ägs av en vårdgivare.

RIV Tekniska Anvisningar 2.1 används som standard för hur SOA-gränssnitten (”tjänstekontrakten”) realiseras.




**Figur 4: Principer för samverkande tjänster för hantering av samtycke och patientrelation (i figur exemplifieras med samtycke)**

**Notera** att en viss instans av stödtjänst för samtycke respektive patientrelation typiskt hanterar flera vårdgivares information. För att visa på principerna ges exempel utifrån två fiktiva vårdgivare A och B.

Bilden ovan visar en systemöversikt där vårdsystem och användare interagerar med stödtjänster för samtycke. Motsvarande applicerar på stödtjänst för patientrelation. Tjänsterna kan delas upp i huvudtyperna Registrera-tjänster och Läsa-tjänster.

Det är valfritt var användargränssnittet för att registrera samtycket realiseras, i ett separat gränssnitt mot samtyckestjänsten (som i fallet NPÖ) eller i respektive vårdsystem/e-tjänst. Oavsett var sparas samtycket i samtyckestjänsten för aktuell vårdgivare.

Samtyckes- och patientrelationsstjänst *kan* installeras och nyttjas fristående eller i kombination med andra tjänster.
Tjänstekontrakten kan realiseras oberoende av *var* delsystemen realiseras. Man kan således

välja att nyttja en mellan huvudmän delad molntjänst ("hotelltjänst") för funktionen Samtycke- och Patientrelationstjänst, alternativt en "egen" lokal installation.

Nationella e-tjänster, t ex NPÖ, får genom tjänstekontrakten ett gränssnitt till de samtycken och patientrelationer som behövs för dess hantering av direktåtkomst inom den sammanhållna journalföringen.

Viktigt att notera är att lösningen inte inkluderar en replikering av den samlade bilden av alla samtycken i riket till en central nod. Tjänster som behöver samlad bild, t ex Patientens samlade samtycken, blir nationella aggrerande tjänster i integrationslagret som samlar ihop resultat från de samtyckestjänster som ingår.

Befintliga tjänster inom Inera Säkerhetstjänster återanvänds och anpassas till den nya arkitekturen.
Sammanfattningsvis görs följande arkitekturmässiga anpassningar för tjänsterna:

- Tjänsterna för Samtycke och Patientrelation friläggs så att de blir möjliga att instansiera som fristående tjänster
- Tjänsternas gränssnitt anpassas till RIV TA Basic Profile 2.1.
- Tjänsterna tillgängliggörs genom publicering via nationell Tjänsteplattform
- Applikationsdelar som anropar tjänster för Samtycke och Patientrelation styrs om till de nya tjänstekontrakten.

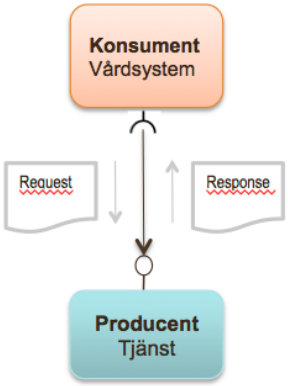
## 4.2. Signifikanta delar av lösningen

### 4.2.1. Tjänsteinteraktioner - princip för tekniska gränssnitt

Alla integrationsmönster som ingår i denna arkitekturbeskrivning baseras på nyttjande av löst kopplade tjänstegränssnitt mot tjänsterna (tjänstekontrakt), utan beroende till specifika agenter eller programmeringsbibliotek (SDK:er).

Det är självklart möjligt att använda och alternativt tillverka ett programmeringsbibliotek för en specifik plattform, men integrationspunkterna (kontrakten) mellan systemen är de bakomliggande tjänstekontrakten.

Nedan figur visar principen för de tjänsteinteraktioner som ingår i tjänstekontrakten. Kontraktet reglerar hela samspelet mellan konsument och producent.




**Figur 5: Tjänsteinteraktion, Typfall "fråga - svar"**

Integrerande vårdsystem anropar tjänsterna med webbtjänsteteknik enligt profilen RIV TA 2.1 [R2]. Det innebär i korthet att

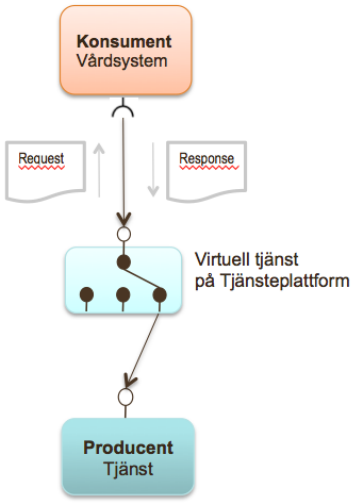
- att tjänstekonsumenten har ett servercertifikat och kan hantera TLS/SSL med klientautentisering för säker kommunikation med tjänsteproducenten.
- att tjänstekonsumenten kan skicka och ta emot XML över HTTPS

### 4.2.2. Tjänsteplattform

Tjänstekontrakten är så utformade att anropet kan ställas mot en virtuell tjänst på en tjänsteplattform som sedan kan routas till korrekt tjänsteproducent.
Se vidare [S7] för mer information om tjänsteplattform och dess förvaltning.

Detta är en vital del av lösningen för de nationella tjänstekontrakten; t ex kontraktet för

läsning av aktuella samtycken för en viss patient och vårdgivare förutsätter att anropet kan routas till den samtyckestjänst som håller informationen för den vårdgivaren.




**Figur 6: Tjänsteinteraktion, Typfall "fråga - svar". Anrop via tjänsteplattform.**

### 4.2.3. Autentisering och auktorisation av slutanvändare i webbklienter

I lösningen ingår fristående användargränssnitt i form av webbklienter:

- Webbklient för vårdpersonal att registrera patientrelation, samtycke och nödsituation
- Webbklient för administration av tjänsterna

Den förra kan användas i samverkan med en webbapplikation för att utföra registreringarna (exempel på det är NPÖs lösning). Alternativt implementeras användarfunktionerna, t ex registrera samtycket, inom applikationen självt. Är det en patientingång, t ex MVK, hanteras funktioner och autentisering inom ramen för denna ingång.

För autentisering av personal som användare enligt ovan används:

- Stark autentisering via eTjänstelegitimation. Lösningen är konfigurerad för SITHS eTjänstekort, men är i övrigt inte bunden till just SITHS som utgivare av kort/certifikat.
- Nationell katalogtjänst för uthämtande av egenskaper kopplade till användaren.
- Stöd för val av aktivt medarbetaruppdrag enligt HSA[2].

[2] Befintlig integration med HSA-WS tjänst nyttjas i webbapplikation, se [T3] samt arktekturellt beslut i [B1]

- SAML2.0 för utställande av intyg med identitets- och auktorisationsunderlag.

Används hotelltjänsten för samtyckeshanteringen, nyttjas även den nationella noden för autentisering. Installeras en egen lokal instans av webbklient/tjänst, kan alternativt en fristående autentiseringsfunktion användas.

### 4.2.4. Ramverk för realisering av ingående tjänsteproducenter

Tjänsteproducenterna är internt uppbyggda med hjälp av följande tekniska ramverk:

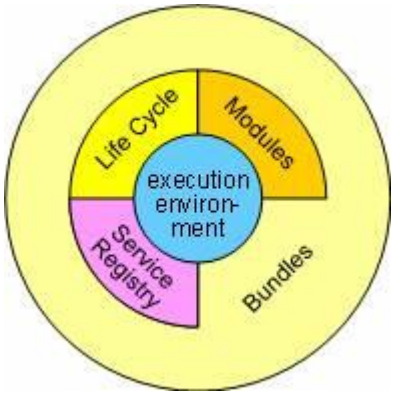
**Java**

Java används för att realisera tjänsterna och möjliggöra exekvering på olika miljöer.

**OSGi ramverk**

Den Java-plattform som tjänsteproducenterna bygger på är i botten en OSGi-lösning som medger löst kopplade komponenter, så kallade bundlar, som kan uppgraderas individuellt. Det är också möjligt att på ett smidigt sätt växla mellan olika implementationer av samma gränssnitt. Detta skapar en mycket flexibel och pluggbar plattform. OSGi är en komponentmodell med stöd för att hantera olika versioner/implementationer av samma komponent samtidigt samt att dynamiskt kunna byta ut komponenter under drift.

Ramverket tillhandahåller en standardiserad miljö för applikationer (bundlar) och består av fyra lager.




L0: Execution Environment – Exekverande miljö

L1: Modules – Moduler/Komponenter

L2: Life Cycle – Livscykel hantering

L3: Service Registry - Tjänsteregister


L0: Execution environment – Specificerar Java miljön.

Java 2 konfigurationer och profiler som J2SE, CDC, CLDC, MIDP o.s.v. är alla möjliga att använda som exekveringsmiljöer.


L1: Modules – Definierar policies för klass laddning.

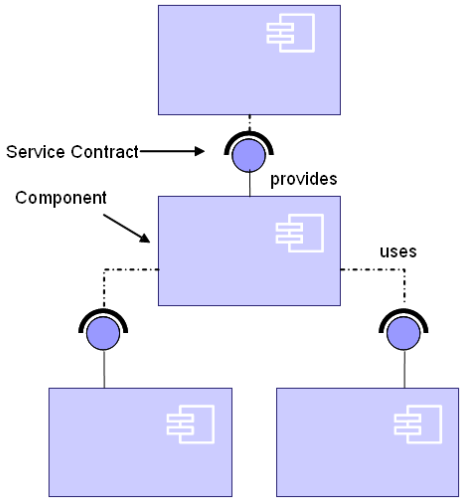
OSGi ramverket är en kraftfull och strikt modell för class loading som bygger på Javas mekanismer för att ladda klasser men är utbyggt för att bättre hantera moduler/komponenter. I Java finns det normalt bara en classpath som innehåller alla klasser och resurser men med OSGi Modules får varje modul en egen privat classpath och allt som ska exponeras utanför en modul måste specificeras explicit.


L2: Life Cycle – Hanterar dynamisk installation, start, stopp, uppdatering och avinstallation av bundlar. Life Cycle använder sig av Modules för att utföra klassladdning men tillhandahåller ett API för hantering av moduler under drift.


L3: Service Registry – Tillhandahåller en dynamisk samarbetsmodell för bundlar. Bundlar kan samarbeta via traditionell klassdelning vilket inte är så kompatibelt med dynamisk installtion och avinstallation av kod, därför tillhandahåller Service Registry en modell för att kunna dela objekt mellan olika bundlar. Ett antal händelser är specificerade för att hantera att tjänster kommer och går, tjänster i detta fall är vanliga Java objekt. Många tjänster motsvarar server funktionalitet t.ex. en HTTP server medan andra kan vara vilket verksamhetsobjekt som helst.

En applikation i OSGi plattformen kallas för en bundle och kan beskrivas som ett vanlig Java ARchive (JAR) med ett utökat Manifest. Manifestet i en bundle specificerar vad den exporterar och vilka beroenden den har för att kunna exekvera i OSGi miljön.

En OSGi bundel innehåller vanliga Java klasser (POJO) som inte behöver vara beroende av OGSi API:t eller känna till att de exekveras som en OSGi bundle.



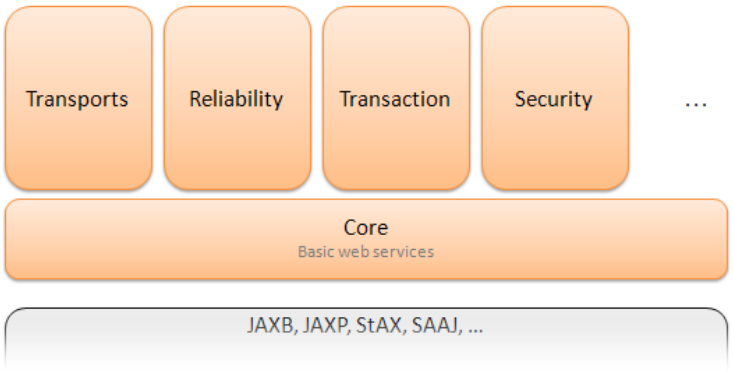

**Figur 8 Schematisk överblick över en OSGi bundle**

Varje komponent/bundle specificerar vad den tillhandahåller och vad den använder.

Om Servicekontraktet överensstämmer kopplar OSGi miljön ihop den komponent som tillhandahåller tjänsten med den som nyttjar tjänsten.

### Metro

Metro är den webbtjänstestack som används inom tjänsteproducenterna. Den inkluderar bl.a. JAX-WS, WSIT, JAXB och implementation för många av de WS-* standarder som nyttjas av tjänsteproducenterna.
Tjänsteproducenterna realisering följer RIV TA 2.1.

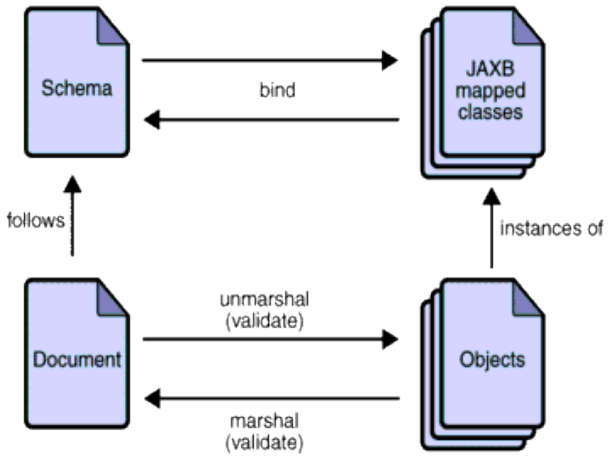



**Figur 9 Metro webbtjänstestack**

**JAX-WS** är grundstommen för utveckling av SOAP baserade webbtjänster inom Java och är en standardteknologi i Java.

JAX-WS version 2.1.7 nyttjas av samtycke och patientrelationstjänsterna**JAXB** binder XML schemat till Java klasser vilket gör det enkelt att hantera XML data. JAXB är en standardteknologi i Java

JAXB version 2.1.11 nyttjas av samtycke och patientrelationstjänsterna.



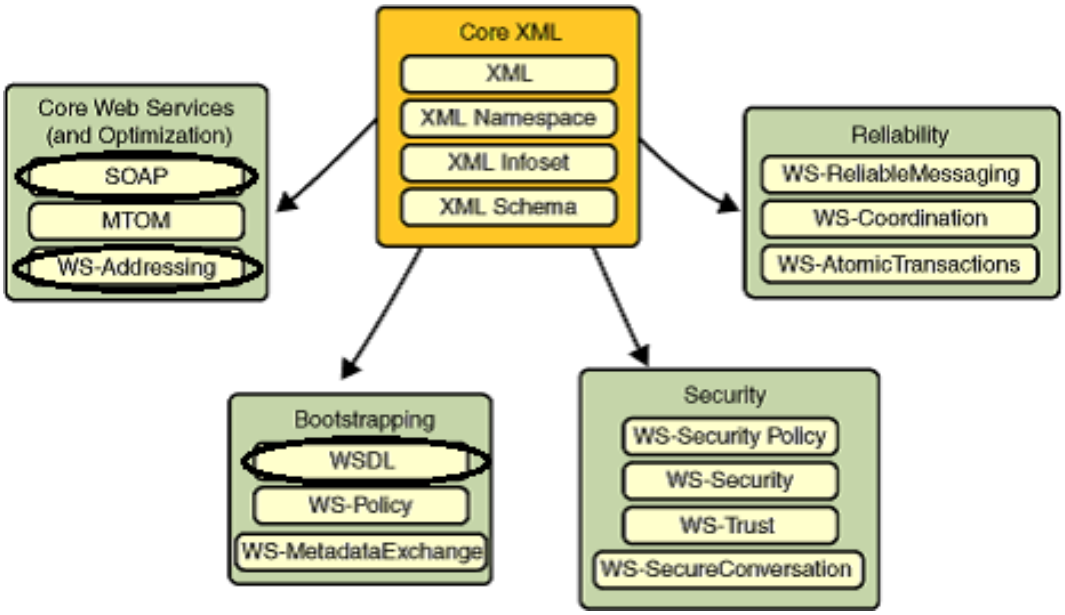

**Figur 10 JAXB - Bindning av schema till Java klasser**

**WSIT (**Web Services Interoperability Technologies**)** är en implementation som utökar JAX-WS med mekanismer för att kommunicera med andra webbtjänstestackar på ett interoperabelt sätt, i synnerhet för Windows Communication Foundation (WCF).

WSIT innehåller stöd för meddelande optimering, säker meddelande transport, säkerhet osv. Det finns även stöd för bootstrapping och konfiguration.

WSIT ramverket är en implementation som utökar JAX-WS och JAXB. Bilden nedan visar vilka underliggande tjänster som är implementerade för varje område. De inringade tjänsterna är de som nyttjas av Samtyckesstänsten och patientrelationstjänsten.

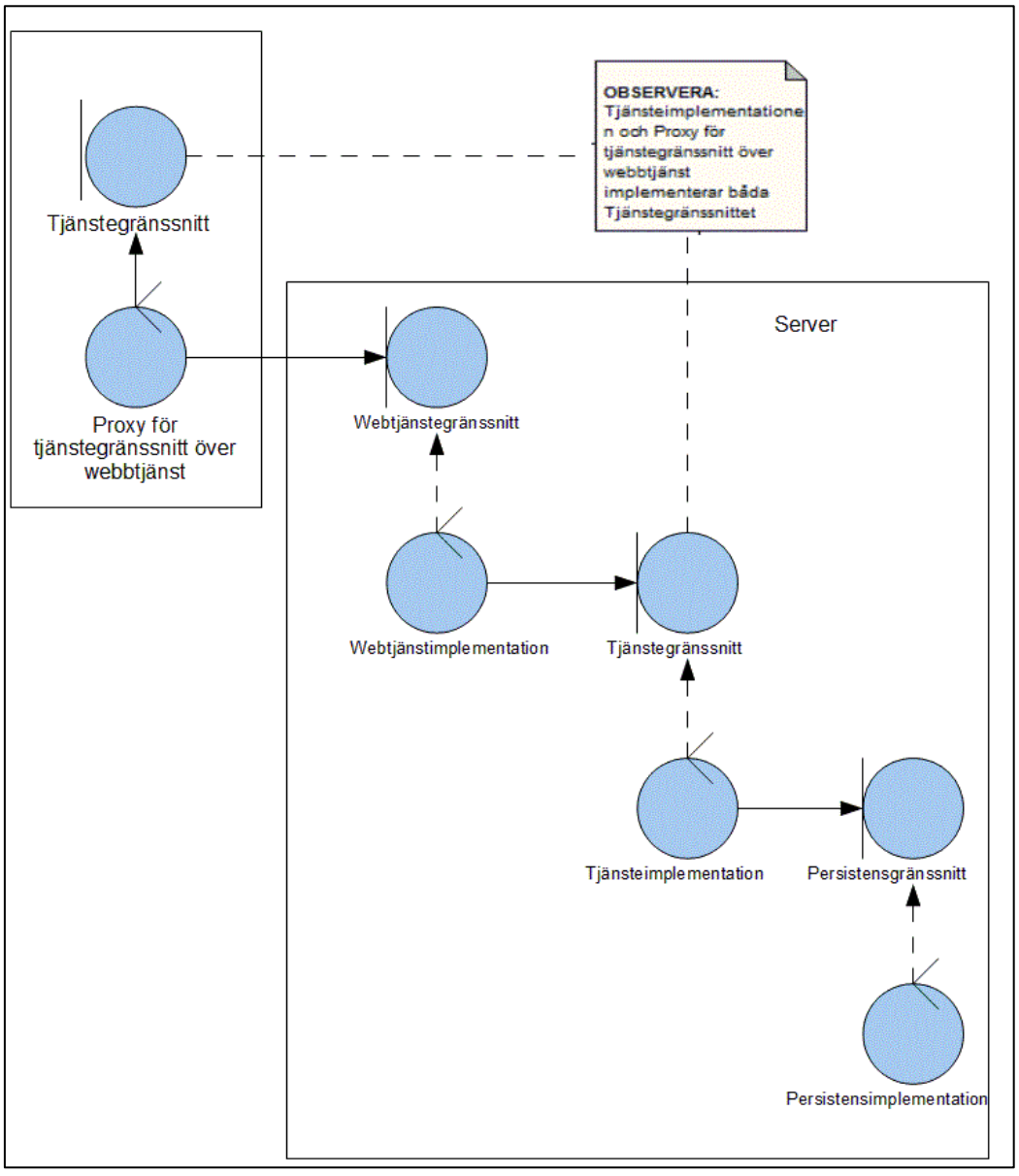
WSIT version 1.5 nyttjas av samtycke och patientrelationstjänsterna.




**Figur 11 WSIT Web Service Features (inringade tjänsterna nyttjas av Samtyckestjänsten och Patientrelationstjänsten)**

### Tjänstepaketering

Tjänsteproducenterna följer internt samma mönster för paketstruktur för att möjliggöra olika deployment scenarier, för att t ex möjliggöra skalbarhet för att öka prestanda.




**Figur 12 Tjänstepaketering**

Pakteringen ger även möjligheten att nyttja deltjänster såsom loggning och loggutdrag från andra logg implementationer.

### 4.2.5. Ramverk för realisering av ingående användargränssnitt/webbklienter

Ingående användargränssnitt nyttjar Google Web Toolkit (GWT) teknik som är kompatibelt med alla de större webbläsarna på marknaden idag.

# 5. Användargränssnitt

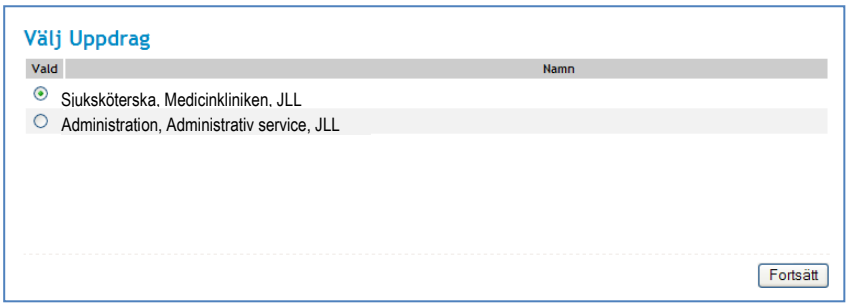
## 5.1. Användargränssnitt slutanvändare

Flera av säkerhetsfunktionerna sker "bakom scenen" utan att användarens ser något gränssnitt. Några användargränssnitt (webbklienter) finns dock med i lösningen.

### 5.1.1. Användargränssnitt inloggning


**Figur 13: Dialog för att ange PIN till SITHS-kortet.**

PIN-dialogen genereras av programvara på arbetsstationen (Net iD) i samband med att en webbklient kräver klientautentisering med TLS/SSL (kortinloggning).



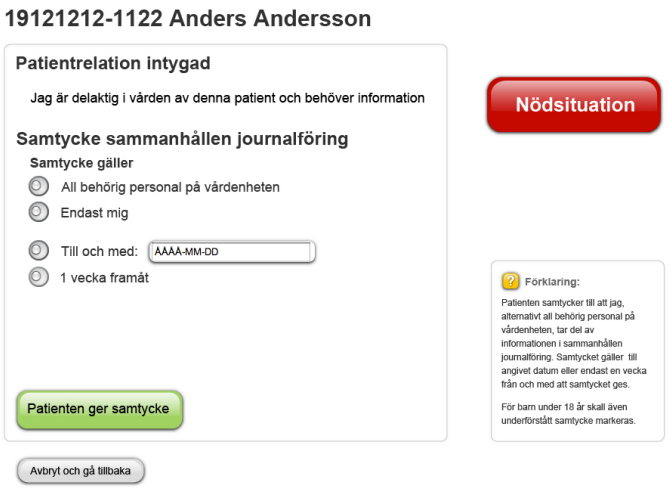

**Figur 14: Dialog för val av uppdrag (om flera finns)**

Dialogen för uppdragsval för användare kan implementeras på olika sätt. Ovan visas exempel från nationella säkerhetstjänsten.
Om användare har flera kopplade uppdrag (även kallat medarbetaruppdrag) i Nationell katalogtjänst (HSA), ska ett av uppdragen aktiveras genom ett val. Egenskaper kopplade till valt uppdrag som nyttjas i lösningen för auktorisation i webbklienter, se kap 4.2.3.

### 5.1.2. Användargränssnitt samtycke & patientrelation - vårdpersonal

Applikationen kan implementera eget användargränssnitt för att registrera samtycke och patientrelation, visa status för samtycke etc.

Som alternativ erbjuds ett externt användargränssnitt (en webbsida) som kan samverka med applikationen.




**Figur 15: Extern dialog (webbsida) för registrering av samtycke, patientrelation och nödsituation.**

Användardialogen för samtycke kan utformas att täcka flera typer av samtycken, där alla nödvändiga samtycken kan registreras sammanhållet. Detta för att underlätta för användaren och undvika många olika dialogrutor. De bakomliggande samtyckesregistreringarna görs dock i respektive bakomliggande tjänst, t ex samtycke till Läkemedelsförteckning respektive samtycke till direktåtkomst till den sammanhållna journalinformationen.

För mer information hur applikation kan interagera med det fristående webbgränssnittet ovan se [B2].

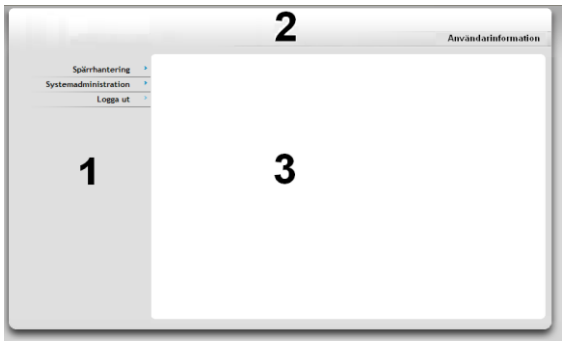
### 5.1.3. Användargränssnitt för administration

För den administration som behövs för samtycken och patientrelationer, finns ett särskilt användargränssnitt mot tjänsten. Se vidare användarhandbok [TBD] .

## 5.2. Utformning av användargränssnitt

Utformning av nya användargränssnitt (t ex samtyckesdialog) samordnas med look-and-feel i övriga användargränssnitt mot Inera Säkerhetstjänster, där befintliga dialoger för registrera samtycke och spärradministration utgör mall.

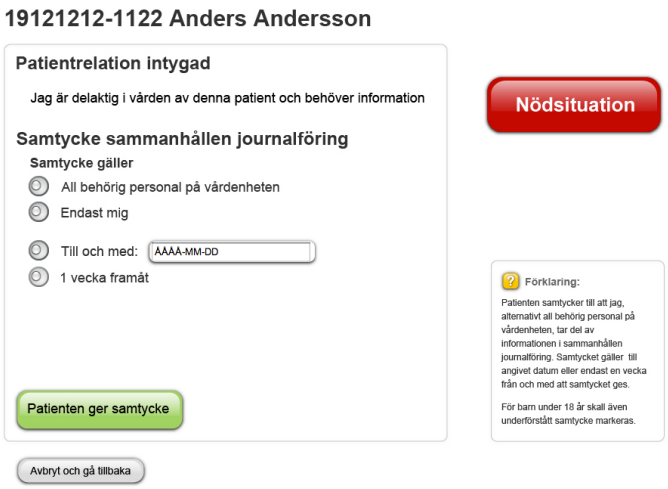
Användargränssnitt för administratörer innehåller tre huvudområden enligt figuren nedan. 1 är menyn för funktionsval, 2 är toppmenyn med allmän information och 3 är vyn som visar information beroende på funktionsval.




**Figur 16: Utformning av användargränssnitt.**

Användargränssnittet för slutanvändare (extern webbsidan) är utformat efter principerna

- Enkelhet och avskalat men informativt
- Så få knapptryckningar som möjligt




**Figur 17: Extern webbsida.**

## 5.3. Systemkrav för ingående användargränssnitt (webbklienter)

Genom användande av Google Web Toolkit (GWT) teknik görs användargränssnitt kompatibla med dagens vanliga webbläsare.

Som minimum kommer följande webbläsare att verifieras i tester:

- Internet Explorer 7, 8, 9

Programvara för hantering av eTjänstekort/eID: Net iD 5.3.0 eller senare

Operativsystem: Windows XP SP3 eller Windows 7.

Framtida versioner av programvara för eTjänstekort/eID, webbläsare och operativsystem måste kvalitetssäkras löpande.

# 6. Användningsfallsöversikt

## 6.1. Användningsfall - Översikt

[TBD]

Figur 18: Schematisk användningsfallsöversikt

## 6.2. Signifikanta användningsfall

Följande är en, icke uttömmande, förteckning över användningsfall som driver arkitekturen.

- Vårdpersonal registrerar
  - patientrelation
  - samtycke
  - nödöppning
- Administratör, på uppdrag av vårdverksamheten
  - makulerar samtycke resp. nödöppning resp patientrelation, vid en felregistrering
  - återkallar samtycke, på patientens begäran (med vårdpersonal som ombud)
- Vårdsystem
  - Läser ut underlag från stödtjänsterna för intern kontroll mot patientrelation och samtycke.
  - Utför kontroll mot patientrelation respektive samtycke, genom anrop till stödtjänsterna
  - Registrerar patientrelation och samtycke i stödtjänst.
- Vårdpersonal - åtkomst till vårdinformation i flera steg i olika delsystem
  1. Användaren utgår från information denne har kring patienten inom sin egen vårdgivare i eget system.
  2. Användare väljer informationsvy, ev. i annat delsystem. som omfattar uppgifter även från andra vårdgivare (direktåtkomst).
  3. Kontroll sker av samtycke/nödöppning och patientrelation.
  4. Om saknas, visas dialog för registrering, och ny kontroll att kraven är uppfyllda utförs.
  5. Användaren kommer vidare till önskad informationsvy.

## 6.3. Aktörsinformation

Nedan sammanställs de aktörer som behöver agera i användningsfallen.

### 6.3.1. Aktörstyp 1: Vårdpersonal

### 6.3.2. Aktörstyp 2: Administratör (hos verksamheten)

### 6.3.3. Aktörstyp 3: System

# 7. Tjänstekontrakt

*Nedan lista är en översikt av de tjänster som ingår för att stödja hanteringen av samtycke/nödöppningar och patientrelationer i vårdsystemen.*

*Tjänstekontraktet Personuppgifter nyttjas av stödtjänsterna för att hämta personuppgifter för patienter.*

*För en mer utförlig information se beskrivningar i [T1], [T2] och [T4].*

Registrera-tjänster, *med utökad information*

- Registrera, med utökad information
  - samtycke
  - nödöppning
  - patientrelation
- Återkalla, med utökad information
  - samtycke
  - nödöppning
  - patientrelation
- Makulera (ta bort), med utökad information [vid felregistrering]
  - samtycke
  - nödöppning
  - patientrelation

Lista-tjänster, *med grundinformation* [för att utföra intern kontroll av åtkomst]

- Lista för angiven patient och specificerad vårdgivare
  - samtycke
  - nödöppning
  - patientrelation
- Lista för alla patienter för specificerad vårdgivare
  - samtycke
  - nödöppning
  - patientrelation
- Lista för angiven personal

- patientrelationer

Kontrollera-tjänster, *kräver endast grundinformation*

- Kontrollera baserat på fråga med aktörsinformation och patient
  - samtycke
  - nödöppning
  - patientrelation

Lista-tjänster, *med utökad information* [för att visa och administrera]

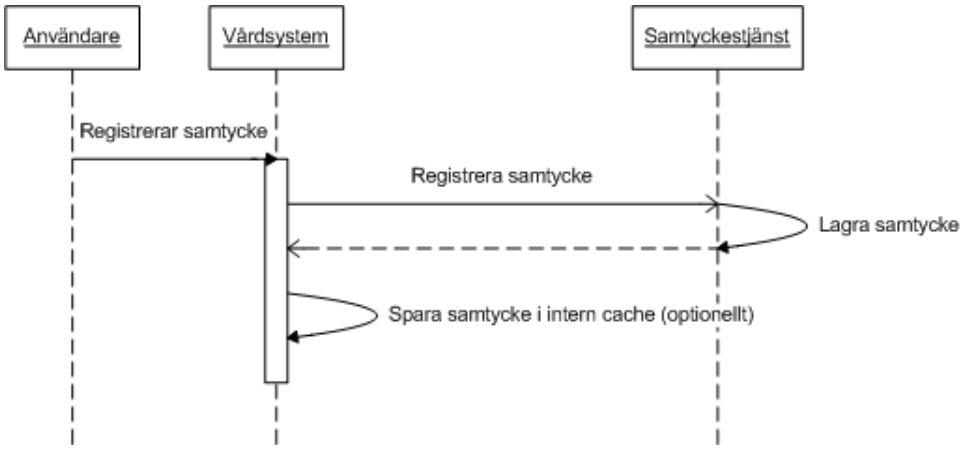
- Lista för angiven patient (för specificerade vårdgivare)
  - samtycke
  - nödöppning
  - patientrelation

Hämta personuppgifter [T4].

- Hämtar information för en viss patient.

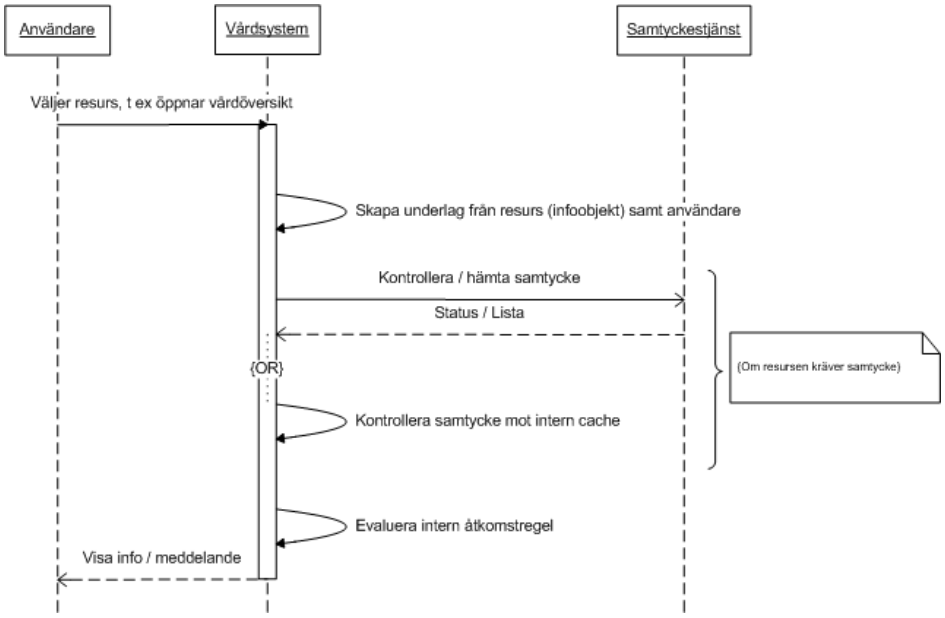
# 8. Sekvenser

Nedan följer exempel på typiska sekvenser, i nedan fall används samtycke för att åskådliggöra principerna.

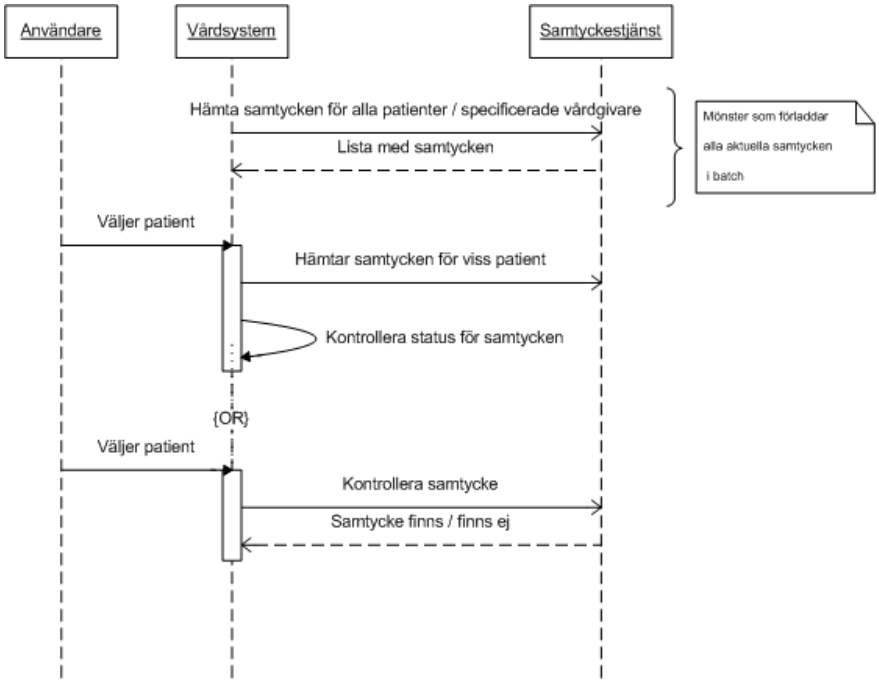



**Figur 19: Flöde - Samtyckesregistrering**

Notera att användargränssnittet för registreringen kan implementeras på olika sätt. I ovan fall byggs det in i vårdsystemet.




**Figur 20: Flöde - Åtkomstkontroll - intern**




**Figur 21: Flöde - Kontrollera samtycke - integrationsmönster**

Ovan figur visar olika tänkbara mönster för integration. Dessa kan användas var och en för sig eller i kombination. T ex är det tänkbart att använda förladdning i batch som en backup-metod till att kontrollera samtycket direkt mot tjänsten. Om tjänsten är otillgänglig kan det förladdade datat användas.

# 9. Uppfyllande av icke-funktionella krav

## 9.1. Icke-funktionella krav från verksamheten

### 9.1.1. Svarstider

Ej preciserade [TBD]

### 9.1.2. Tillgänglighet

Ej preciserade [TBD]

## 9.2. Icke-funktionella krav från Systemägaren/Förvaltaren

### 9.2.1. Test

Ej preciserade [TBD]

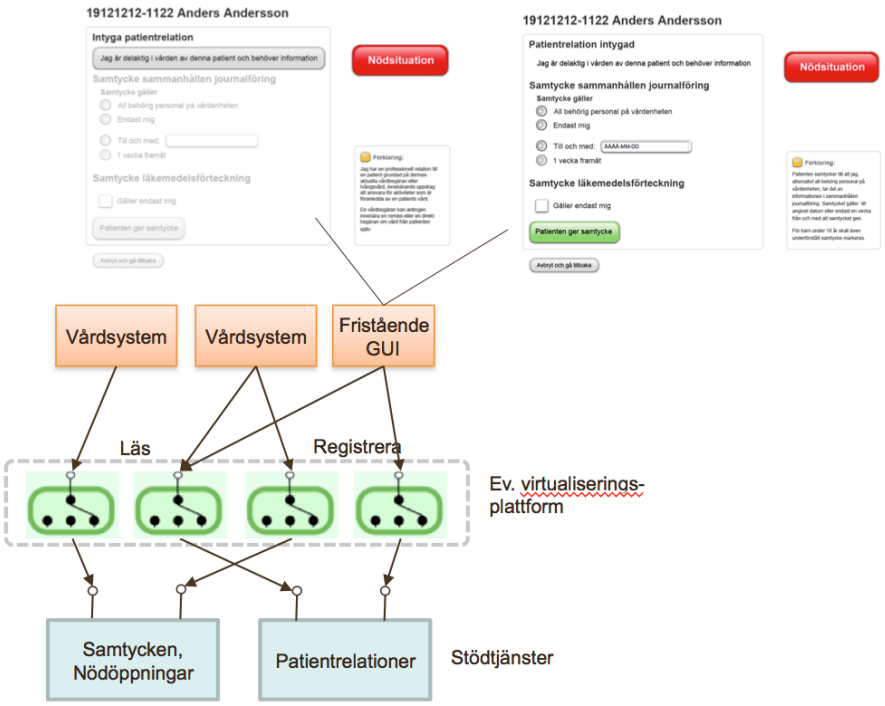
### 9.2.2. Konfigurationsstyrning

Ej preciserade [TBD]

### 9.2.3. SLA-övervakning

Ej preciserade [TBD]

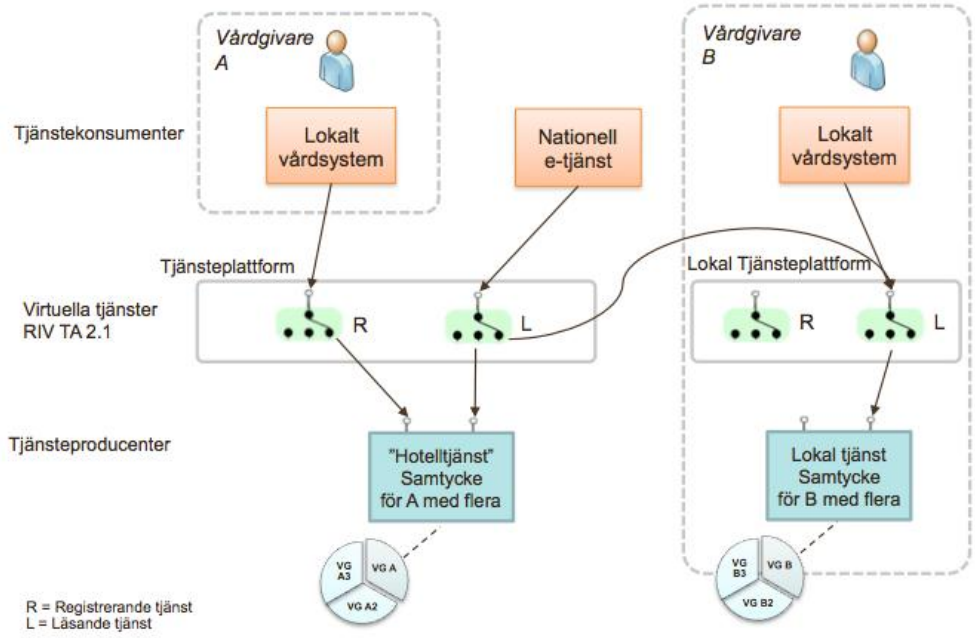
# 10. Logisk arkitektur




**Figur 22: Logisk vy: Konsumenter och producenttjänster - samtycke och patientrelation.**

I ovan sammanfattande bild representerar "Läs"-tjänster alla läsande tjänster (inklusive kontroll) och "Registrera"-tjänster alla tjänster som skriver till tjänsterna.

Arkitekturen följer T-bokens tekniska arkitektur [S2]. Konsumerande system kan vara lokala/regionala/nationella vårdsystem. Stödtjänsterna (producenttjänsterna) nås via virtualiseringsplattformar eller motsvarande.




**Figur 23: Principer för integration och samverkan, lokalt/regionalt och nationellt. Här exempel med Samtycke.**

Notera att en viss instans av stödtjänst för samtycke respektive patientrelation typiskt hanterar flera vårdgivares information. För att visa på principerna ges exempel utifrån två fiktiva vårdgivare A och B.

Ovan bild tar upp tre typiska mönster som arkitekturen hanterar:

- Nationell e-tjänst. Har behov av hantering av samtycke och patientrelation.
  Nyttjar centrala stödtjänster (hotelltjänster).
- Lokalt vårdsystem. Har behov av hantering av samtycke och patientrelation lokalt.
  Nyttjar centrala stödtjänster (hotelltjänster).
  Personalen använder även nationella tillämpningar (e-tjänster).
- Lokalt vårdsystem. Har behov av hantering av samtycke och patientrelation lokalt.
  Nyttjar egna lokala stödtjänster och ska kunna vara "självförsörjande".
  Personalen använder även nationella tillämpningar (e-tjänster).

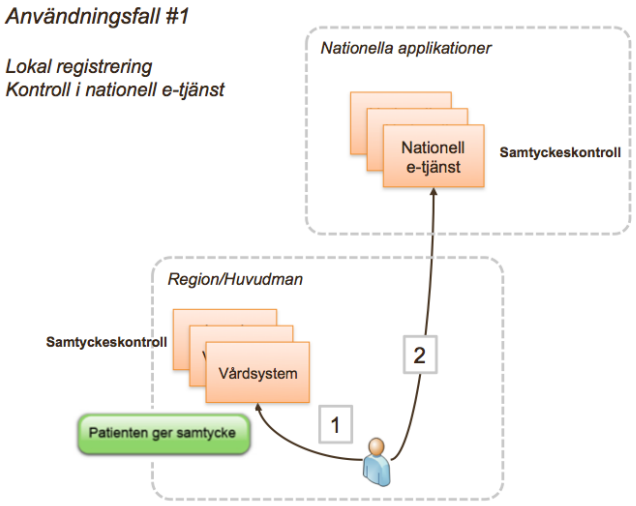
Alla tjänster är RIVTA21-anpassade och är möjliga att routas via en virtualiseringsplattform (Tjänsteplattform). För full funktionalitet förutsätts att vägval (routing) kan göras i ett integrationsskikt. På detta sätt kan nationell läsning och skrivning implementeras, utan att dessa anrop behöver påverkas om någon huvudman väljer en lokal implementation av tjänsten. Tjänsterna är designade att fungera lika väl på ett lokalt plan. Med fördel används en lokal tjänsteplattform, vilket dock inte är nödvändigt om syftet är endast att nå data i den egna installationen.

En anslutning av en lokal tjänst till den federativa nationella arkitekturen innebär att tillhandahålla den lokala tjänsten som tjänsteproducent för samtycke respektive patientrelation och registrera den i den nationella tjänsteplattformen.

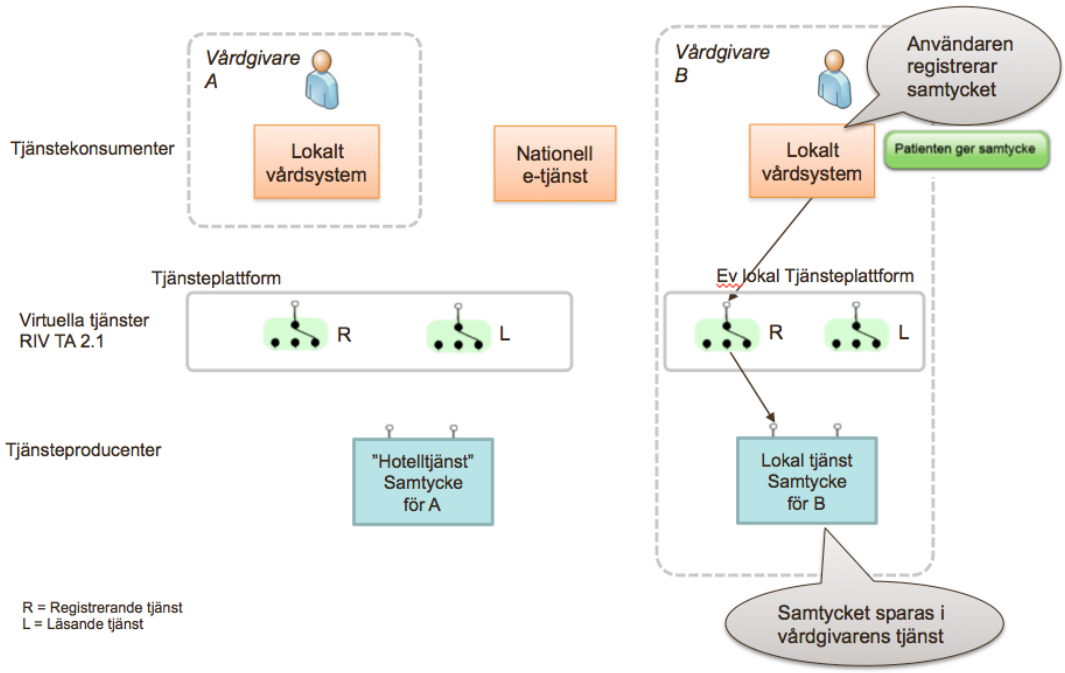
## 10.1. Mappning mot signifikanta användningsfall

I nedan fall används samtyckeregistreringar för att exemplifiera principerna. Samma principer är applicerbara på patientrelationstjänst.

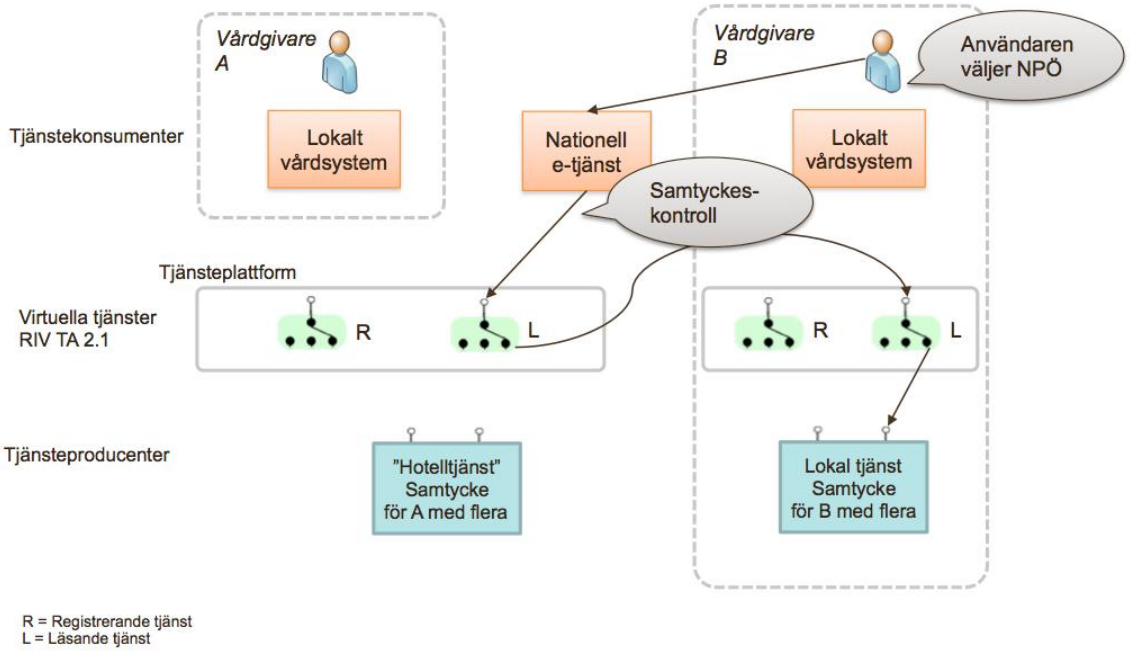
### 10.1.1. Lokala registreringar - åtkomst till nationell e-tjänst




**Figur 24: Fall 1**



**Figur 25: Fall 1 - tjänsteanrop. Steg 1**



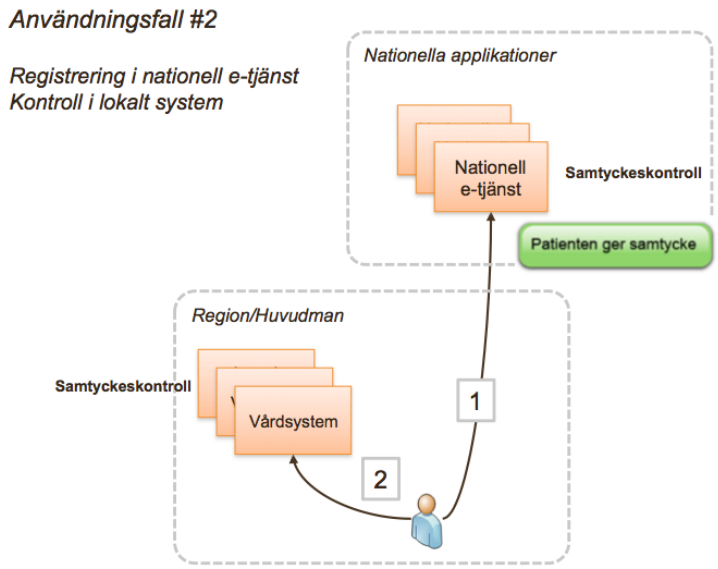

**Figur 26: Fall 1 - tjänsteanrop. Steg 2**

Ovan styrs anropen till rätt tjänsteproducent genom den logiska adresseringen som bygger på vilken huvudman/vårdgivare som användaren är inloggad på via dennes medarbetaruppdrag.

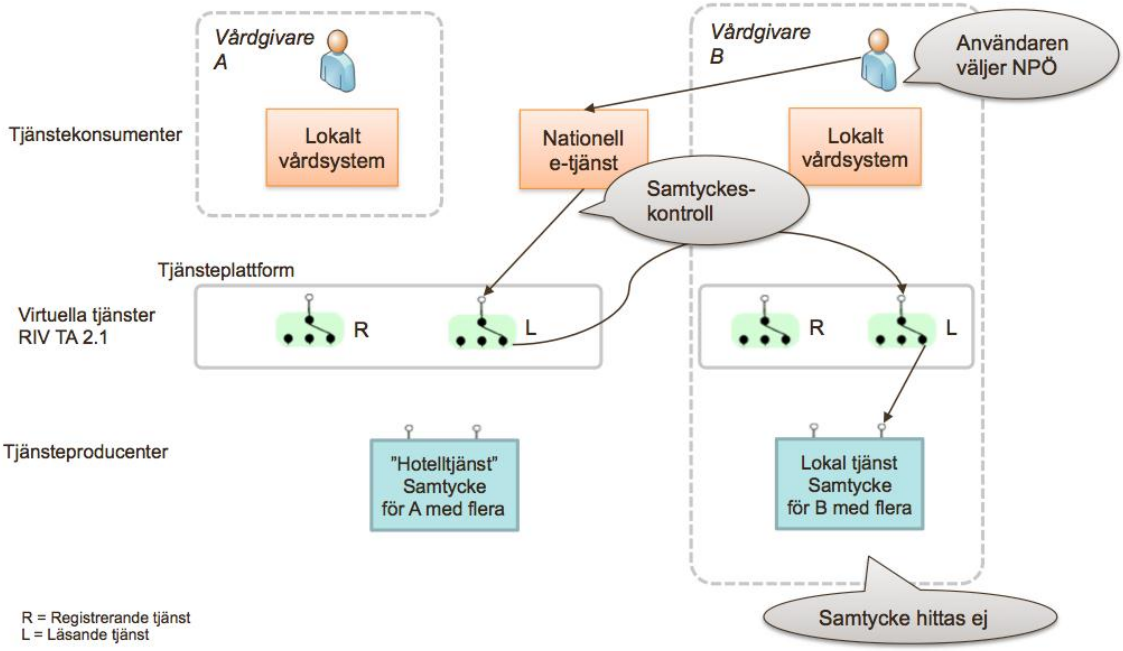
Det finns en viktig tillgänglighetsaspekt att tänka på här. Den nationella e-tjänsten blir beroende av en lokal tjänst hos den huvudman vars användare nyttjar den nationella e-tjänsten. Om den lokala tjänsten är nere, får det dock bara påverkan på användare som har uppdrag hos huvudmannen/vårdgivaren. Samtycken som lagras i vårdgivarens tjänst berör endast personal hos vårdgivare, eller mer korrekt: har uppdrag hos vårdgivaren, och det är endast för dem som anropet routas till den lokala tjänsten.

Detta är en viktig princip  i arkitekturen. Tillgängligheten för den nationella etjänsten bör inte påverkas generellt (för alla) av en huvudmans beslut att hantera en lokal installation för t ex sin samtyckeshantering.

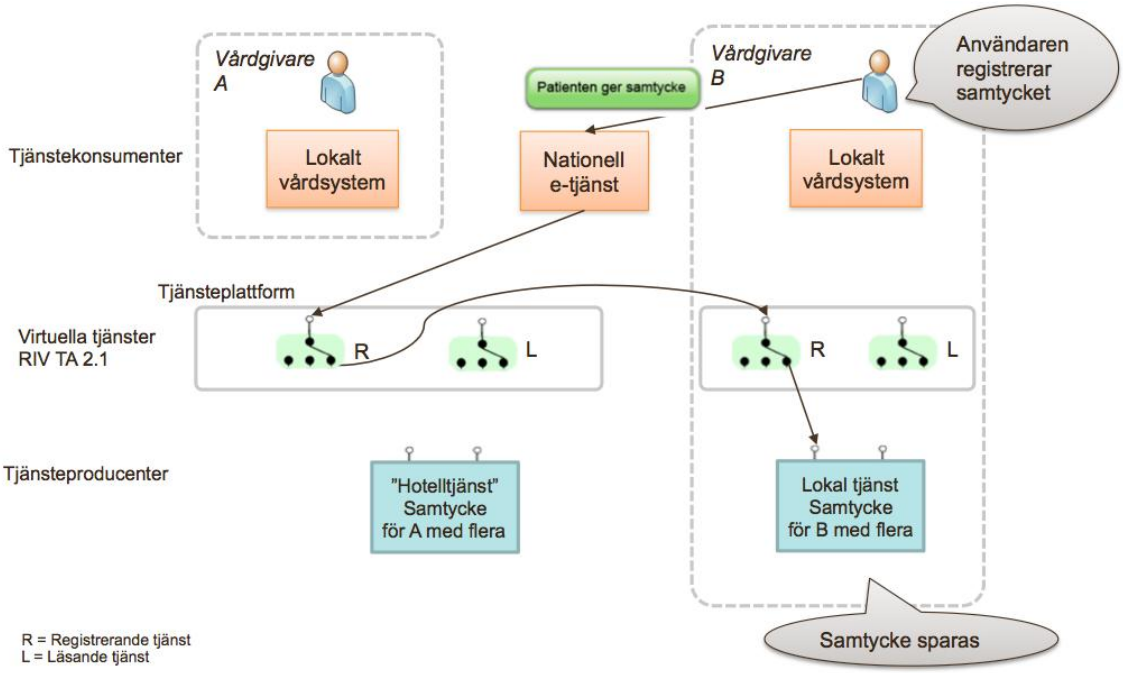
### 10.1.2. Åtkomst till nationell e-tjänst, nationell registrering




**Figur 27: Fall 2**

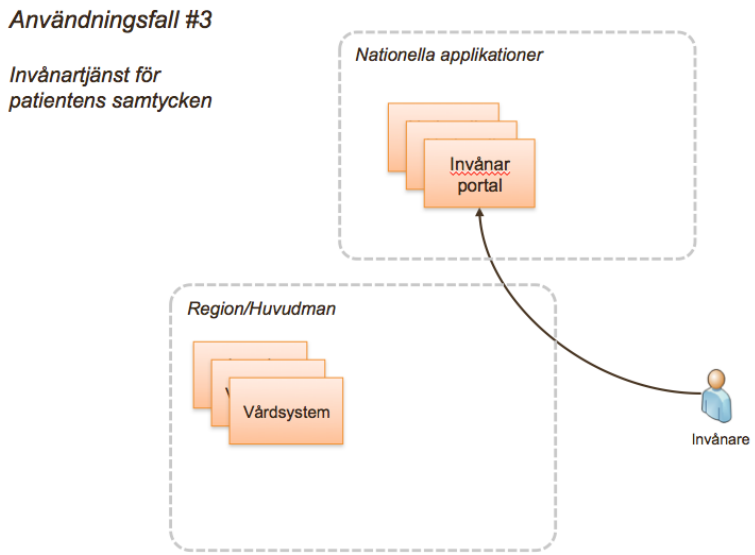



**Figur 28: Fall 2 - tjänsteanrop. Steg 1**

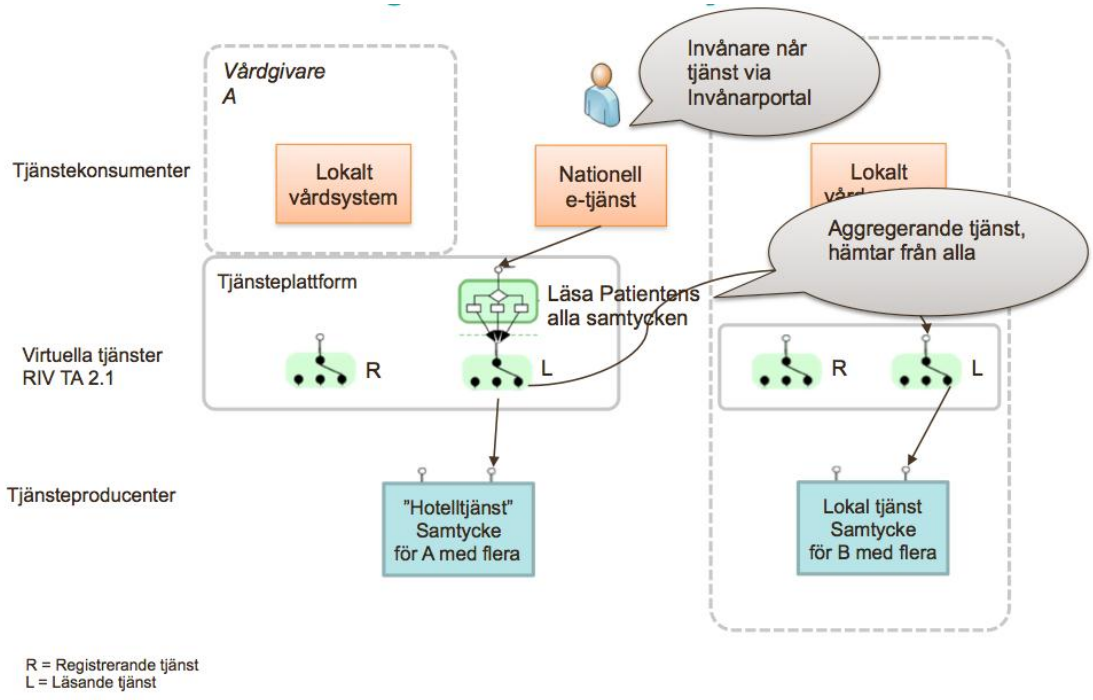



**Figur 29: Fall 2 - tjänsteanrop. Steg 2**

### 10.1.3. Nationell Läsning ”Patientens samtycken”




**Figur 30: Fall 3**

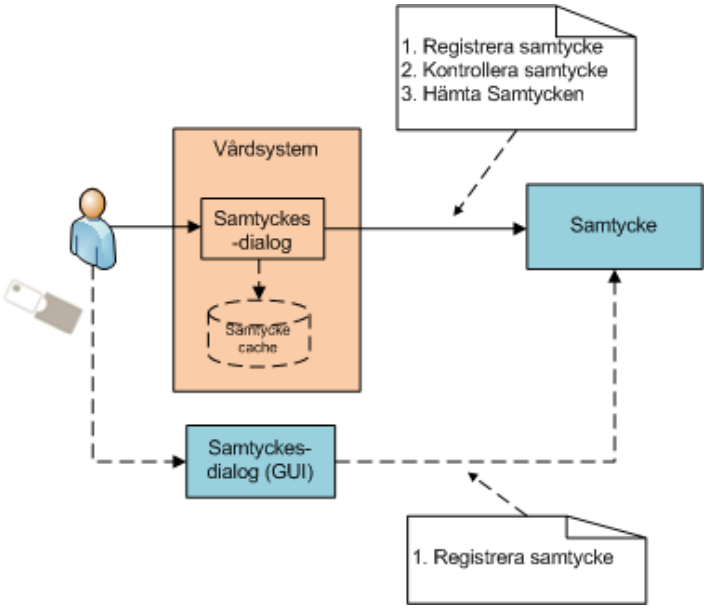



**Figur 31: Fall 3 - tjänsteanrop.**

## 10.2. Beskrivning av arkitekturellt signifikanta delar av lösningen

Nedan används samtyckestjänst som exempel för att beskriva typiska integrationsscenarier.

### 10.2.1. Integrationsscenarier




**Figur 32: Integrationsmönster för samtyckeshantering**

I Samtyckestjänsten kan samtycken registreras för senare återanvändning i process och IT-stöd. För att kontrollera existens av samtycke kan olika integrationsmönster användas:

1. Kontrollera om samtycke finns för viss patient visavi den användare som är inloggad. Tjänsten svarar "ja/nej".
2. Hämta samtycken avseende viss patient och vårdgivare och utför intern kontroll.
3. Hämta samtycken avseende specificerade vårdgivare (bulkhämta) och utför intern kontroll.

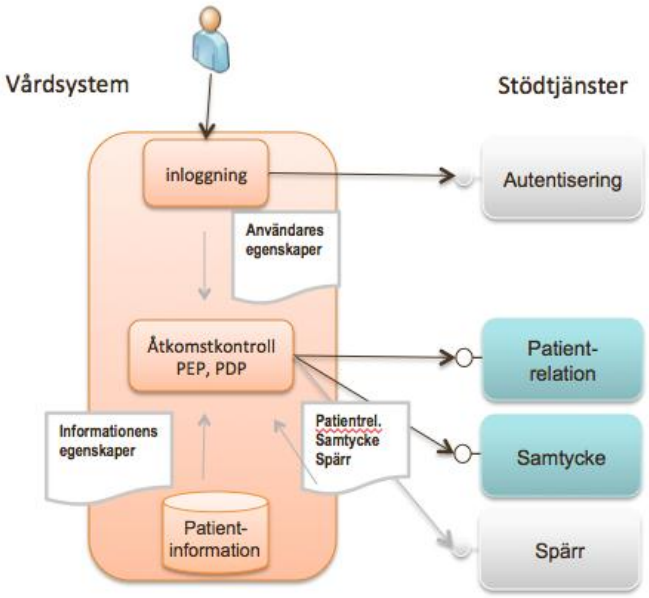
En samtyckescache kan upprätthållas som kan användas ifall extern tjänst blir otillgänglig.

Användargränssnitt för samtyckesdialog kan antingen implementeras inom vårdsystemet, alternativt så nyttjas ett fristående GUI för samtyckesregistrering.

I alternativ 3 (bulkhämta) kan om så önskas även avregistreringar returneras (t ex återkallat samtycke). Det kan användas ifall vårdsystemet endast hämtar förändrade data så att avregistrerade kan tas bort.

### 10.2.2. Åtkomstkontroll

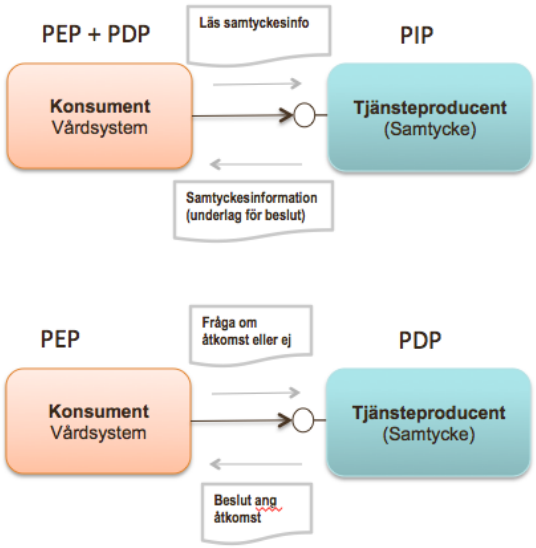
Med stöd av tjänsterna kan ett vårdsystem implementera en kontroll om åtkomst ska ges till viss patientinformation. Beslutet kan baseras på om patientrelation, samtycke och spärr (kompletterande tjänst) finns, samt vilka egenskaper användaren och patientinformationen har.




**Figur 33: Interaktionsmönster för åtkomstkontroll där flera underlag vägs samman i beslutet. Vårdsystemet är här både PEP och PDP.**

Antingen implementerar vårdsystemet alla beslutsregler som behövs; vårdsystemet agerar då PDP (Policy Decision Point) och stödtjänsterna PIP (Policy Information Point) genom att tillhandahålla underlagen till besluten: samtycken, patientrelationer och användares rättigheter/egenskaper, hämtas från de gemensamma stödtjänsterna.

Alternativt kan vårdsystemet delegera delbeslut till stödtjänsterna; stödtjänsten agerar då PDP och vårdsystemet PEP (Policy Enforcement Point) för det delbeslut stödtjänsten kan bidraga med.




**Figur 34: Principiella interaktionsmönster mot stödtjänst, där var ansvaret för PDP kan flyttas beroende på vilket tjänstekontrakt som nyttjas.**

### 10.2.3. Påverkan på nationell Åtkomstkontrolltjänst

Den nya arkitekturen med distribuerade samtyckestjänster innebär att kontroll mot samtycke för viss patient generellt sätt behöver göras mot en tjänst.
Det samlade underlaget, samtycken, patientrelationer etc, kan fås genom att sammanställa resultat från dessa tjänsteanrop.
Notera att det också innebär att den tidigare arkitekuren med en central nod som håller alla samtyckes- och patientrelationsunderlag för Åtkomstkontrolltjänsten inte upprätthålls som en generell service. Det är dock fortfarande möjligt att ställa samma typ av fråga direkt mot tjänstekontrakten och uppnå i princip samma effekt.

Följande anpassningar görs i de nationella tjänsterna

1. Samtyckesdialogen i Säkerhetstjänster styrs om på baksidan till RIV-tjänsterna (nationell skriv och läs). I övrigt anropas och returnerar dialogen som förut.
2. ÅKT-regel (”PDL-regeln”) i Säkerhetstjänster som idag gör kontroll mot samtycke och patientrelation ändras; kontrollerna tas bort.
3. NPÖ gör idag separat kontroll av samtycke och patientrelation via ÅKT-tjänsten (specialregler). Dessa anrop styrs om till RIV-tjänsterna via Tjänsteplattformen. Anrop sker före Samtyckesdialogen för att se behov samt efteråt för att säkerställa korrekthet

# 11. Säkerhet

## 11.1. Infrastruktursäkerhet

Infrastrukturen för samtyckes- och patientrelationstjänsterna kräver att full tillgång till applikationsserver och databasserver begränsas. Om tillgång ges till någon av dessa kan användaren komma åt systemloggar samt spärrdata och förvanska dessa. Att begränsa åtkomsten löses normalt sett med en brandvägg samt att servrarna skyddas med användarnamn och ett starkt lösenord.

## 11.2. Riskanalys

Ej genomförd.

## 11.3. Riskminimering i den tekniska lösningen

Riskerna med den tekniska lösningen motverkas genom

- att använda beprövade integrationsmönster och standardiserade tekniker
- att erbjuda alternativa integrationsmönster för att möta olika förutsättningar hos systemleverantörerna
- att integrationspunkterna är löst kopplade tjänstekontrakt, vilket minskar risk för förvaltningsproblematik
- att arkitekturen medför skalbarhet genom att fler noder kan kopplas in efter behov
- att användagränssnitten baseras på GWT som bl.a förhindrar cross-site-scripting och POSTning av felaktiga formulärer m.m.

## 11.4. Intrångsskydd

<tillhör implementering>
Intrångsskydd finns för de nationella driftnoderna för säkerhetstjänsterna [P1].

Intrångsskyddet för de lokala installationerna beror på respektive huvudmans egen infrastruktur.

## 11.5. Insynsskydd (kryptering)

SSL/TLS används i all kommunikation med stödtjänsterna, säkerhetstjänsterna samt HSA.

## 11.6. Transportoförvanskning.

SSL/TLS används i all kommunikation med stödtjänsterna, säkerhetstjänsterna samt HSA.

## 11.7. Presentationskorrekt

Validering sker vid all registrering av data enligt de principer som gäller för respektive data vilket säkerställer att data är korrekt.

Tillgång till användargränssnitt kräver att användaren är inloggad med SITHS-kort.

Appliceras t ex på framtagande av anpassat användargränssnitt för samtyckesregistrering.

## 11.8. Dataintegritet (Oförvanskat över tid), riktighet

Riktigheten i systemloggar och persistent data (databas) skyddas med hjälp av respektive huvudmans egen infrastruktur och är inte en del av systemet.

## 11.9. Autentisering (”stark” vid behov enligt infoklassning)

Kopplar till krav vid åtkomst av vårdinformation enligt PDL. Samtliga inloggade användare ska vara starkt autentiserade.
I vården innebär det ofta inloggning med SITHS-kort.

## 11.10. Lagkrav

Se sammanställning i [S8].

## 11.11. Spårbarhet (loggning)

De aktiviteter som loggas, är all typ av registrering, återkallan och makulering. Även uppföljning genom rapportuttag loggas.

Om aktiviteten utförs i vårdsystemet, ansvarar vårdsystemet för den loggning som behövs. Utförs aktiviteten i applikation (användargränssnitt) mot stödtjänsterna, ansvarar den applikationen för nödvändig loggning.

Loggningen ska motsvara lagkraven på spårbarhet enligt PDL och Socialstyrelsens riktlinjer. Se även DI:s checklista för logguppföljning i vården.

Lösningen ska möjliggöra att hantera uppföljning av åtgärderna på ett sammanhållet sätt i verksamheten. Rapportuttag är möjligt genom administrationsgränssnittet. Rapport kan genereras baserad på händelser för en patient eller händelser för en användare.

<TBD - kompletteras>

# 12. Informationsmodell

Se [S8] som är styrande.

# 13. Datamodell

Här ges ett urval av datatyper som används i tjänsterna. För mer information se [T1] och [T2].

**patientconsent:PDLAssertion**

Datatyp som representerar ett intyg som ger direktåtkomst till andra vårdgivares information enligt PDL. Datatypen beskriver grundformatet för ett intyg.

| Namn | Datatyp | Beskrivning | Kardinalitet |
|---|---|---|---|
| assertionId | common:Id | Unik, global identifierare för intyget. | 1 |
| assertionType | patientconsent:AssertionType | Typ av intyg som ger direktåtkomst till information från andra vådgivare enligt PDL. Kan vara patientens samtycke eller nödsituation. | 1 |
| scope | patientconsent:Scope | Omfånget/tillämpningsområde på samtycket. | 1 |
| patientId | common:PersonIdValue | Patientens id nummer, kan vara personnummer, samordningsnummer alternativt reservnummer. | 1 |
| careProviderId | common:HsaId | Vårdgivare id. Intyget kopplas till den vårdgivare som medarbetaren är kopplad till via dennes aktuella medarbetaruppdrag. | 1 |
| careUnitId | common:HsaId | Vårdenhets id. Intyget kopplas till den vårdenhet som medarbetaren är kopplad till via dennes aktuella medarbetaruppdrag. | 1 |
| employeeId | common:HsaId | Medarbetare id. Om samtycket är personligt anges medarbetarens id. Om samtycket gäller all behörig personal på vårdenheten skall inget värde anges. | 0..1 |
| startDate | xs:dateTime | Startdatum för vilken giltighetstid samtycket avser. | 1 |
| endDate | xs:dateTime | Optionellt slutdatum för vilken giltighetstid samtycket avser. Om ett slutdatum är angivet gäller samtycket t.o.m denna tidpunkt. Om inget slutdatum anges, gäller samtycket tills det blir återkallat eller makulerat. | 0..1 |

| | | | |
|---|---|---|---|
| ownerId | common:OwnerId | Optionell identifierare för det system som skapade samtycket. Används endast för tekniskt bruk för t.ex. uppföljning och spårning. | 0..1 |

**patientconsent:ExtendedPDLAssertion**

Datatyp som representerar ett intyg med ett utökat format. Innehåller information vem som har begärt respektive registrerat intyget, samt om och när intyget är återkallat och/eller makulerat. Denna datatyp utökar datatypen patientconsent:PDLAssertion.

| Namn | Datatyp | Beskrivning | Kardinalitet |
|---|---|---|---|
| representedBy | common:PersonId | Ej obligatorisk information om den företrädare som ger samtycke (företräder patienten). | 0..1 |
| registrationInfo | common:Action | Innehåller information om vem som begärt och registrerat samtycket samt tidpunkten för begäran och registreringen. | 1..1 |
| cancellationInfo | common:ReasonAction | Ej obligatorisk information om återkallelse, innehåller vem som begärt och registrerat återkallelsen, tidpunkten för begäran och registreringen samt anledningen till återkallan. | 0..1 |

**patientrelationship:PatientRelation**

Datatyp som representerar en patientrelation enligt PDL. Datatypen beskriver grundformatet för ett intyg.

| Namn | Datatyp | Beskrivning | Kardinalitet |
|---|---|---|---|
| patientRelationId | common:Id | Unik, global identifierare för patientrelationen. | 1 |
| ownerId | common:OwnerId | Optionell identifierare för den aktör/system som skapat patientrelationen. Används endast för tekniskt bruk för t.ex. uppföljning och | 0..1 |

| | | | |
|---|---|---|---|
| | | spårning. | |
| endDate | xs:dateTime | Tidpunkts då giltigheten går ut för patientrelationen. | 1 |
| patientId | common:PersonIdValue | Patientens id nummer, kan vara personnummer, samordningsnummer alternativt reservnummer. | 1 |
| actor | common:Actor | Den användare som har en patientrelation med patienten. | 1 |

**patientrelationship:ExtendedPatientRelation**

Datatyp som representerar en patientrelation med ett utökat format. Innehåller information vem som har begärt respektive registrerat patientrelationen,

samt om och när patientrelationen är återkallad och/eller makulerat.

Denna datatyp utökar datatypen patientrelationship:PatientRelation.

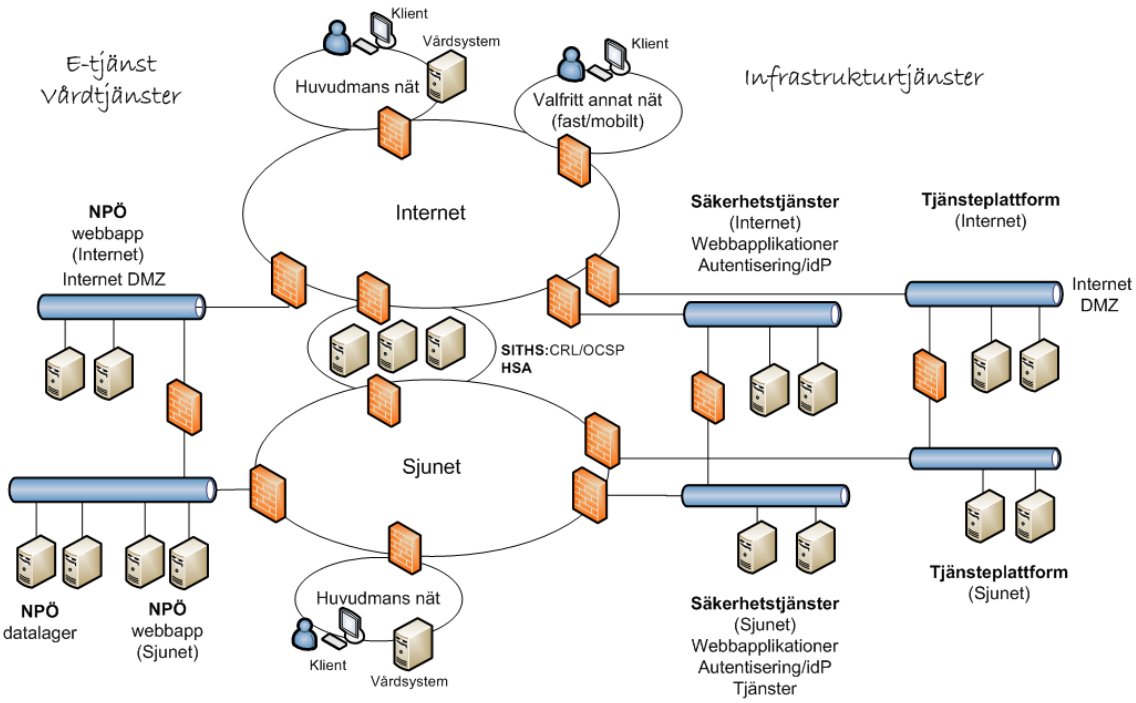
| Namn | Datatyp | Beskrivning | Kardinalitet |
|---|---|---|---|
| registrationInfo | common:Action | Innehåller vem som begärt och registrerat patientrelationen samt tid för begäran och registrering. | 1 |
| cancellationInfo | common:Action | Ej obligatorisk info om återkallelse, innehåller vem som begärt och registrerat återkallelsen samt tid för begäran och registrering. Samt anledning till återkallelse | 0..1 |
| deletionInfo | common:Action | Ej obligatorisk info om makulering, innehåller vem som begärt och registrerat makuleringen samt tid för begäran och registrering. Samt anledning till makulering | 0..1 |

# 14. Driftaspekter

(Skalbarhet, Versionshantering, Uppdatering utan avbrott)(Deployment vy)

<tillhör implementering, se dock översikt>

## 14.1. Översikt nätverksåtkomst




**Figur 35: Översikt nätverksåtkomst**

Det finns krav på att tjänsterna finns tillgängliga för anslutning både via Sjunet och Internet, eftersom alla huvudmän inte har Sjunet-anslutning. Detta kommer att hanteras enligt ovan principskiss.

De frontsidor som behövs för Internetexponering finns på en proxy i internet-dmz. Kommunikation går därmed aldrig direkt från internet till servrar som frontar mot Sjunet (Sjunets säkerhetskrav).

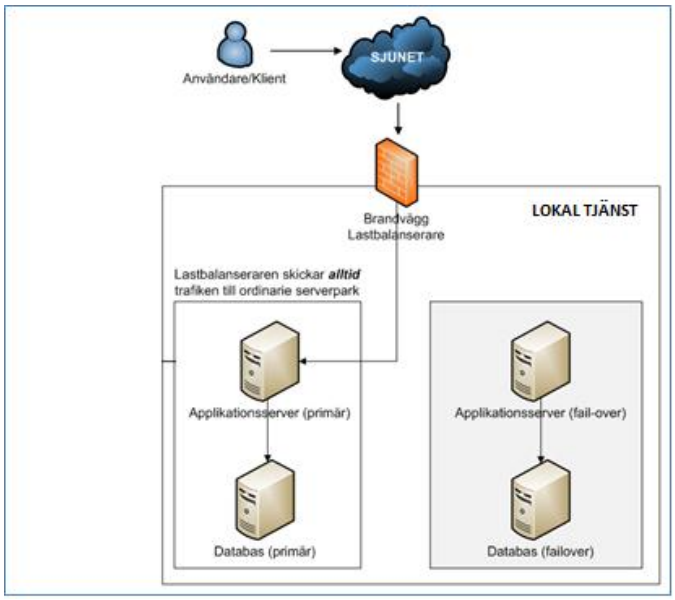
Tjänstekontrakt på Internet nyttjar nationella Tjänsteplattformens kommande miljö med tjänsteproxy för Internet.

Webbapplikationer på Internet nyttjar Säkerhetstjänsters proxy för Internet.

Kommunikation går säkrat via separata brandväggar mellan proxy-del och bakomliggande servrar. Kommunikation med stödtjänster som HSA-WS går över Sjunet och passerar aldrig internet-sidan.

## 14.2. Fysisk miljö

Den fysiska miljön för tjänsterna beror på huvudmannens val av systemkonfiguration. Se nedan samt föregående översiktsbild.




**Figur 36 Exempel fysik miljö**

## 14.3. Programvaror

Tjänsteproducenterna kräver följande programvaror:

- Java SE 6 – 64-bit
- MySQL Server version 5.5 eller högre – 64-bit

## 14.4. Detaljerad information

Ej specificerat.

## 14.5. Produktionssättning och överlämning till förvaltning

Ej specificerat.

# 15. Följsamhet mot T-bokens styrande principer

### 15.1.1. IT2: Informationssäkerhet

| Förutsättningar att uppfylla | Uppfyllnad |
|---|---|
| Verksamhetskritiskt IT-stöd designas för att möta verksamhetens krav på tillgänglighet vid frånfall av ett externt beroende. Ju fler beroenden till andra komponenters tillgänglighet, desto lägre egen tillgänglighet. | Säkerhetstjänsterna ska kunna konsumeras på vårdsystemets villkor. Det finns stöd för att förladda och mellanlagra underlag för beslut vårdsystemet behöver ta under en driftsituation, vilket kan användas om en säkerhetstjänst skulle tillfälligt vara otillgänglig.<br>Säkerhetstjänsterna är designade för dubblerade instanser för fail-over vid problem med hårdvara.<br>Det finns olika möjligheter att driftsätta säkerhetstjänsterna, antingen i lokal eller nationell regi för att maximera tillgängligheten efter behov.<br>Ett grundläggande krav är att användaren kan loggas in på ett säkert sätt med korrekta rättigheter från nationell katalogtjänst.<br>Om autentiseringstjänsten och/eller HSA är otillgänglig kan inte nya användare logga in i systemet; dock kan tillses att redan påloggade användare kan fortsätta att arbeta.<br>För SITHS-korten finns reservkortsrutiner som kan användas vid borttappade eller trasiga kort.<br>Loggning är designat så att applikationen inte stannar ifall Loggtjänst skulle vara temporärt otillgänglig. |
| Verksamhetskritiska nationella stödtjänster (t.ex. tillgång till behörighetsstyrande information) erbjuder möjlighet till lokala instanser som med tillräcklig aktualitet hålls uppdaterade med nationell master. | Ja, både lokal instans samt möjlighet att mellanlagra internt i applikation alternativt i anslutning till lokal tjänsteplattform.<br>Autentiseringstjänst kan vid behov sättas upp som lokal instans.<br>Tillgång till HSA-data lokalt torde stödjas genom möjligheterna till distribuerad kataloghantering. Detta kräver också att HSA-tjänsten implementeras lokalt. |
| Krav mellan integrerande parter regleras genom integrationsavtal. Integrationsavtal är det avtal där informationsägaren godkänner att en ett visst system får agera | Tillämpas för<br>- HSA-integrationen genom HSA Brukar Beskrivning (HBB) |

| | |
|---|---|
| mot information genom ett visst tjänstekontrakt. Exempelvis skall enligt integrationsprocessen för den nationella tjänsteplattformen ett avtalsnummer för ett integrationsavtal registreras i samband med att man "öppnar dörren" för en viss tjänstekonsument mot en viss kombination av informationsägare och tjänstekontrakt. | - Säkerhetstjänster genom integrationsavtal<br>- Tjänsteplattform genom integrationsavtal |
| Arkitekturen måste möjliggöra tillräcklig tillgänglighet vid flera samverkande system. | Uppfylls genom design för hög tillgänglighet enligt ovan. |
| En sammantagen tolkning av tillämpliga lagar och förordningars konsekvenser för teknisk realisering av informationsfångst, utbyte och lagring. | Se RIV-specifikation PDLiP [S8] |
| Förutsättningar för spårbarhet etableras i form av loggningsregler för komponenter som deltar i säkert informationsutbyte. | Uppfylls genom användande av nationell lösning för loggning för verksamhetens behov av uppföljning av aktiviteter. |
| Interoperabla, internationellt beprövade och för leverantörer tillgängliga standarder tillämpas för kommunikation mellan parter som har upprättat tillit. | Uppfylls för stödtjänsterna genom nyttjande av<br>- tekniska profilen RIV-TA BP 2.1<br><br>För webbklienter som ingår nyttjas för autentisering, SSO och auktorisation:<br>- SSL/TLS<br>- SAML 2.0 Webb SSO Profile<br>- SAML 2.0 Core, SAML Assertion |

### 15.1.2. IT3: Nationell funktionell skalbarhet

| Förutsättningar att uppfylla | Uppfyllnad |
|---|---|
| Nationella tjänstekontrakt definieras med nationell täckning som funktionell omfattning. Det är möjligt för ett centraliserat verksamhetssystem som användas av alla verksamheter i Sverige att realisera varje standardiserat tjänstekontrakt. Det får inte finnas underförstådda funktionella avgränsningar till regioner, kommuner, landsting eller andra organisatoriska avgränsningar i nationella tjänstekontrakt. | Uppfyllt |

| | |
|---|---|
| SLA ska definieras för varje tjänstekontrakt. Detta SLA ska ta hänsyn till framtida kapacitet för tjänstekontraktet med avseende på transaktionsvolym, variationer i användningsmönster och krav på tillgänglighet, i kombination med förmåga till kontinuerlig förändring. | Kommer att göras inom ramen för tjänsteförvaltningen.<br>Tillämpas idag för Säkerhetstjänster vid nyttjande i Nationell Patientöversikt. |
| Integration ska ske över en integrationsinfrastruktur (t.ex. virtualiseringsplattform) som möjliggör uppföljning av tjänsteproducenters fullföljande av SLA. | Uppfylles genom nyttjande av nationell tjänsteplattform.<br>Lokala tjänsteplattformar kan och bör också nyttjas. |
| System och e-tjänster som upphandlas kan utökas med fler organisationer som kunder utan krav på infrastrukturella ingrepp (jämför s.k. SaaS) | Uppfylles genom att<br>- Tjänsterna kan delas mellan vårdgivare efter behov genom s k logisk uppdelning.<br>- Stöd för godtycklig vårdgivare i HSA |

### 15.1.3. IT4: Lös koppling

| Förutsättningar att uppfylla | Uppfyllnad |
|---|---|
| Meddelandeutbyte baseras på att kommunikation etableras utgående från vem som äger informationen som ska konsumeras eller berikas, inte vilket system, plattform, datalager eller tekniskt gränssnitt som informationsägaren för stunden använder för att hantera informationen. Genom centralt administrerad förmedlingstjänst skapas lös koppling mellan informationskonsument och informationsägarens tekniska lösning. | Uppfylles genom användande av verksamhetsbaserad adressering (typiskt vårdgivare) enligt RIV TA. |
| En arkitektur som skapar lös koppling mellan konsumenter och producenter, avseende adressering och standarder för kommunikation. | Uppfylles, se Meddelandeutbyte och Interoperabla standards enligt ovan. |
| En nationell integrationspunkt ska kunna erbjudas för varje nationellt standardiserat tjänstekontrakt, som en fasad mot bakomliggande brokiga systemlandskap. | Tillämpas via nationell tjänsteplattform. |
| Nationella tjänstekontrakt förvaltas i en nationellt koordinerad förvaltning. | Ska tillämpas för de nationella tjänstekontrakten. |
| För en process inom vård och omsorg kan | Se RIV PDLiP [S8] för de informations- och |

| | |
|---|---|
| flera tjänstekontrakt ingå. Därför är det viktigt att alla tjänstekontrakt baseras på en gemensam referensmodell för informationsstruktur. | begreppsmodeller som utgör grund för lösningen. |
| Parter som samverkar i enlighet med arkitekturen integrerar med system hos parter som lyder under annan styrning (t.ex. myndigheter, kunder och leverantörer). Det kan leda till att vård- och omsorgsgivare antingen:<br>o Nationellt bryggar informationen (semantisk översättning) eller<br>o Nationellt införlivar externt förvaltat tjänstekontrakt som standard.<br>Observera att semantisk bryggning av information till vårdens referensmodell förutsätter en nationell förvaltning av bryggningstjänster.<br>För att införliva ett externt förvaltat tjänstekontrakt förutsätts en transparent, robust och uthållig tjänstekontraktsförvaltning hos den externa parten. | <Ej tillämpbar> |
| Befintliga system behöver anpassas till nationella tjänstekontrakt. Detta kan göras av leverantörer direkt i produkten, eller genom fristående integrationskomponenter (”anslutningar”). En anslutning bör ligga nära (logiskt vara en del av) det system som ansluts, oavsett om det är i rollen som konsument eller producent för anslutningen som genomförs. | Tillämpas vid implementation / anslutning av vårdsystem till säkerhetstjänster |
| Interoperabla standarder för meddelandeutbyte tillämpas, så att integration med till exempel en Web Service kan utföras utan att anropande system behöver tillföras en för tjänsteproducenten specialskriven integrationsmodul (s.k. agent). | Tillämpas, se Meddelandeutbyte och Interoperabla standards enligt ovan.<br>De interoperabla, web service-baserade gränssnitten, rekommenderas för integrationen för god förvaltningsbarhet. |

### 15.1.4. IT5: Lokalt driven e-tjänsteförsörjning

| Förutsättningar att uppfylla | Uppfyllnad |
|---|---|

| | |
|---|---|
| När utveckling av källkod är en del av en tjänsteleverans skall följande beaktas:<br>o Alla leveranser tillgängliggörs under öppen källkodslicens. Valet av licensformer samordnas nationellt genom rekommendationer.<br>o Utvecklingen bedrivs från start i en allmänt tillgänglig (över öppna nätverk) projektinfrastruktur där förvaltningsorganisation kan förändras över tiden inom ramen för en kontinuerligt tillgänglig projektinfrastruktur (analogi: ”Projektplatsen för e-tjänsteutveckling”).<br>o Det innebär full insyn och åtkomst för utvecklare till källkod, versionshantering, ärendehantering, stödforum och andra element i en projektinfrastruktur under projektets och förvaltningens hela livscykel.<br>o Upphandlade e-tjänster fungerar på de vanligaste plattformarna hos vårdgivarna och hos nationella driftspartners (Windows, Linux, Unix) t.ex. genom att vara byggda för att exekvera på en s.k. Java virtuell maskin.<br>o Gemensam referensmodell för e-tjänsters interna uppbyggnad stimulerar och förenklar återanvändning och överföring av förvaltningsansvar mellan organisationer.- | Tjänsterna enligt denna arkitektur och tillhörande tjänstekontrakt kan utvecklas fristående av valfri part.<br>Tjänstekontrakten publiceras och förvaltas av Inera enligt RIV tekniska anvisningar.<br><br>För de tjänstekomponenter som tas fram enligt denna SAD gäller att<br>o Tjänstekomponenterna utvecklas ovanpå open source komponenter<br>o Befintliga avtal om nyttjande ger nyttjanderätt till framtagna tjänstekomponenter, men inte tillgång till källkoden.<br>För villkor se avtal om nyttjande av och integration mot säkerhetstjänsterna.<br><br>o Plattformar<br>De tjänsterna som tas fram byggs på java-plattform för plattformsoberoende kod.<br>Installationspaketen levereras i första hand för Linux-plattformen.<br>Möjlighet finns att leverera virtuella instanser enligt OVF-standard (Open Virtual Format) på begäran för helt plattformsoberoende driftsättning.<br><br><TBD: komplettera> |
| Minsta möjliga – men tillräcklig – mängd standarder och stödjande gemensamma grundbultar för nationella e-tjänstekanaler säkerställer att även utvecklingsenheter i mindre organisationer kan bidra med e-tjänster för en integrerad användarupplevelse och att en gemensam back-office för anslutning av huvudmän till e-tjänster finns etablerad. I den mån etablerade standarder med bred tillämpning i kommersiella e-tjänster finns (t.ex. för single-sign-on), bör de användas i syfte att möjliggöra upphandling av hyllprodukter. | Se Interoperabla standards enligt ovan. |
| Utveckling sker mot globalt dominerande | Säkerhetstjänster bygger på open-source-produkter |

| | |
|---|---|
| portabilitetsstandarder i de fall mellanvara (applikationsservrar) tillämpas. Det är möjliggöraren för nyttjande av free-ware och lågkostnadsverktyg i organisationer som inte orkar bära tunga licenskostnader för komplexa utvecklingsverktyg och driftsplattformar. | för ingående mellanvara.<br><TBD: komplettera> |
| Nationell (eller regional – beroende på sammanhang vård/omsorg) förvaltning är etablerad (t.ex. s.k. Portal Governance), med effektiva processer för att införliva lokalt utvecklade e-tjänster i nationella e-tjänstekanaler. Systematisk och effektiv allokering av resurser för drift är en viktig grundförutsättning. | <Ej tillämpbar> |
| Genom lokal governance och tillämpning av det nationella regelverket får lokala projekt den stöttning som behövs för att från början bygga in förutsättningar för integration i samordnade (t.ex. nationella) e-tjänstekanaler. | <Ej tillämpbar> |

### 15.1.5. IT6: Samverkan i federation

| Förutsättningar | Uppfyllnad |
|---|---|
| Att gemensamma gränssnitt i alla federativa utbyten finns framtagna och beskrivna, vilket möjliggör kostnadseffektiva och leverantörsneutrala lösningar. | För tjänsteinteraktionerna med vårdsystem nyttjas tjänstekontrakt enligt RIV TA BP 2.1. |
| Det behövs organ och processer för att godkänna utgivare av elektroniska identitetsintyg och certifikat som är giltiga i federationen. | Ej fokus för denna leverans.<br><br>Närliggande federativa lösningar:<br>Det pågår arbete på Cehis/SKL för att etablera/ingå i federation med andra utgivare av identitetsintyg enligt SAML. |
| Aktörer i olika nät, inklusive öppna nät ska vara välkomna i elektronisk samverkan genom att samverkande komponenter är säkra. | Uppfylles, se kap 14.1 för säkert tillgängliggörande av tjänsterna på Internet.<br>Två-vägs SSL/TLS enligt RIV TA BP 2.1.<br><br>För webbapplikationer nyttjas SSL autentisering med stöd av certifikat samt SAML-intyg. |
| Att Ingående parter i federationen är överens om ett antal gemensamma ståndpunkter:<br>o att stark autentisering likställs med 2-faktors autentisering<br>o att vid samverkan acceptera följande metoder för stark autentisering; eID, PKI med lagring av nyckelpar på SmartCard eller motsvarande och metoder baserade på engångslösenord, antingen genererade i en fysisk enhet eller säkert distribuerad till fysisk enhet<br>o att tillämpa en gemensam certifikat- och utfärdarpolicy, likvärdig med SITHS, som ett minimikrav för egen eller annans PKI<br>o att sträva mot en autentiseringslösning, framför flera olika, för att realisera stark autentisering i den egna organisationen och i federation<br>o att enbart acceptera SAMLv2, eller senare version, vid identitetsfederering samt tydliggöra att det i förekommande fall är det enda sättet | Lösningen stödjer en sådan kommande federation genom användning av<br><br>Autentisering:<br>- Nationell extern idP/Autentiseringstjänst med SAML2 som bas<br>- SITHS-kort / certifikat och tillhörande utfärdarpolicys<br><br>HSA:<br>HSA som katalogtjänst; från HSA hämtas alla användaregenskaper såsom rättigheter.<br><br>Nät:<br>Tjänster som kommer att vara åtkomliga antingen via Internet eller Sjunet.<br>Oavsett vilket nät som används säkras tjänsterna enligt ovan, d v s i grunden utgår lösningen ifrån att samma skyddsbehov finns i båda fallen.<br>För exponering mot Internet följs även Sjunets säkerhetsregler, vilket tillför ytterligare skyddsmekanismer (ytterligare separat DMZ). |

| | |
|---|---|
| att logga in och säkerställa det inte finns någon bakväg in<br>o att tillämpa ett gemensamt ramverk för att ingå i en federation<br>o att tillämpa en gemensam katalogpolicy, med utgångspunkt från HSA policy, som ett minimikrav för egna kataloger<br>o att stäva mot att all gränsöverskridande kommunikation skall vara möjlig både över Sjunet och Internet. Det är den egna organisationen som beslutar vilken tillgänglighet som är tillräcklig för anslutningen<br>o att sträva efter att möjliggöra kontroll av trafik till och från den egna infrastrukturen i en eller få kontrollpunkter<br>o Att utgå från att kommunikation över Internet och Sjunet har ett likvärdigt skyddsbehov | Tjänster som exponeras via Tjänsteplattformen använder den nätverksexponering mot Internet som Tjänsteplattformen tillhandahåller. |

# 16. Referenser

## 16.1. Bilagor

| Ref | Dokument ID | Dokument |
|---|---|---|
| B1 | Arkitekturella beslut | |
| | | |

## 16.2. Styrande dokument

| Ref | Dokument ID | Dokument |
|---|---|---|
| S1 | IT-strategi | http://www.cehis.se/images/uploads/dokumentarkiv/Malbild_och_Fardplan_far_ehalsa_i_samverkan_101008.pdf |
| S2 | T-boken | http://www.cehis.se/images/uploads/dokumentarkiv/Referensarkitektur_vard_omsorg_VIT-bokens_tekniska_arkitektur_Rapport_110314_REV_B.pdf |
| S3 | RIV | Dokument kan laddas ner från http://www.cehis.se/arkitektur_regelverk/ |
| S4 | Målbild eHälsa | http://www.cehis.se/images/uploads/dokumentarkiv/Malbild_och_Fardplan_far_ehalsa_i_samverkan_101008.pdf |
| S5 | VIT-boken | Dokumentet kan laddas ner från: http://www.cehis.se/arkitektur_regelverk/ |
| S6 | RIV Tekniska Anvisningar | http://code.google.com/p/rivta/ |
| S7 | Nationella tjänsteplattformen | http://www.cehis.se/infrastruktur/tjansteplattform/ http://code.google.com/p/skltp/ |
| S8 | RIV PDLiP | RIV-specifikation för PDL i praktiken http://www.cehis.se/images/uploads/dokumentarkiv/PDLiP_RIV_10_specifikation_110926.pdf |

## 16.3. Stödjande dokument

| Ref | Dokument ID | Dokument |
|---|---|---|
| R1 | SAD-mall | Arkitekturledningens mall för SAD http://www.cehis.se/images/uploads/dokumentarkiv/RIV_21_Mall_Bilaga_41_SAD_Regelverk_110220.doc http://www.cehis.se/images/uploads/dokumentarkiv/RIV_21_Anvisning_Bilaga_41_SAD_Regelverk_110220.pdf |
| R2 | RIVTA BP2.1 | RIV Tekniska Anvisningar Basic Profile 2.1 |

## 16.4. Nyttjade integrationstjänster

| Ref | Dokument id | Dokument |
|---|---|---|
| Samtycke | T1 | Tjänstekontraktsbeskrivning Samtycke [**TBD**]<br>http://code.google.com/p/rivta/ |
| Patientrelation | T2 | Tjänstekontraktsbeskrivning Patientrelation [TBD]<br>http://code.google.com/p/rivta/ |
| HSA | T3 | *http://inera.se/Documents/Infrastrukturtjanster/Katalogtjanst_HSA/Stodjande/hsaws_anvandarhandledning.pdf*<br>Befintlig koppling till HSA-tjänsten nyttjas i den webbapplikation som finns för administration av stödtjänsterna. Stödtjänsten själv nyttjar inte HSA-tjänsten.<br>Notera att RIV TA Tjänstekontrakt för HSA är under utveckling och ska användas vid nya integrationer mot HSA, se även [B1]. |
| Personuppgifter | T4 | *http://code.google.com/p/rivta/source/browse/ServiceInteractions/riv/population/residentmaster/trunk/docs/Tjanstekontrakt%20Population%20Residentmaster%20-%20Beskrivning.doc*<br>Tjänstekontrakt som nyttjas för att hämta personuppgifter om patienter. |

## 16.5. Nyttjade plattformsfunktioner

| Ref | Dokument id | Beskrivning |
|---|---|---|
| Säkerhetstjänster | [P1] | http://inera.se/Infrastrukturtjanster/Sakerhetstjanster/Dokument-for-Sakerhetstjanster/<br>Allmän anslutningsdokumentation och förutsättningar för nyttjande. |
| Autentisering | [P1] | Autentiseringstjänsten används för interoperabel hantering av identitetsintyg (SAML2) med rättighetsstyrande attribut för användare. |
| Samtycke | [P1] | Samtyckestjänst används för enhetlig samtyckeshantering |
| Patientrelation | [P1] | Patientrelationstjänst används för enhetlig hantering av patientrelationer. |
| Åtkomstkontroll | [P1] | Åtkomstkontrolltjänst är en option som kan nyttjas för att hantera beslut om vad användare får göra och få tillgång till. |
| Logg | [P1] | Loggtjänst används för att säkerställa krav på spårbarhet och möjliggöra en enhetlig hantering av uppföljning av åtkomstloggarna. |
| HSA | [P2] | HSA används i lösningen för att tillhanda kvalitetssäkrade uppgifter om personer och funktioner/system. Grundläggande rättighetshetstilldelning utgår från HSA.<br>Befintlig koppling till HSA-tjänsten nyttjas i den webbapplikation |

| | | |
|---|---|---|
| | | som finns för administration av stödtjänsterna. Stödtjänsten själv nyttjar inte HSA-tjänsten. |
| SITHS | [P3] | SITHS-kort används för säker inloggning, ger stöd för stark autentisering av användare. |
| Tjänsteplattform | [P4] | Tjänsteplattform, lokalt såväl som nationellt, är en möjlig förmedlare av tjänsterna. Tillför möjlighet till internetåtkomst till tjänster, förenkling av integrationspunkterna och vägval för att hitta viss producerande tjänst.<br>http://www.cehis.se/infrastruktur/tjansteplattform/ |