SAD - Spärr

Dokumenthistorik

Datum	Version	Namn	Förändring
27 Jan 2021	1.0	Unknown User (lexhagenm)	Första version

Innehåll

1. Dokumentinformation

1.1. Syfte

Syftet med detta dokument är att beskriva systemarkitektur och teknisk realisering för Ineras spärrlösning. Spärrlösningen beskrivs utifrån hur den samverkar med andra system.

1.2. Målgrupp

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

2. Översiktlig beskrivning

2.1. Inledning

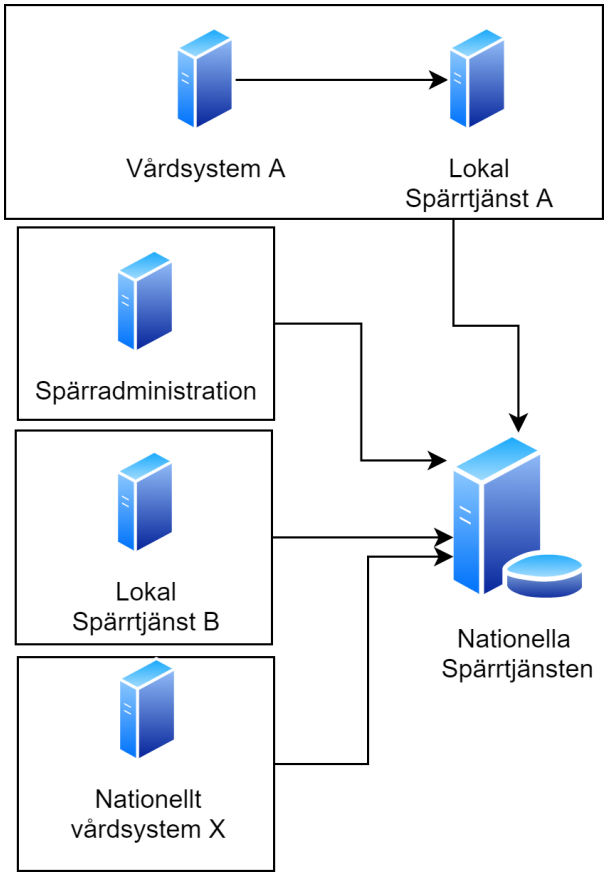
Stödtjänsten Spärr syftar till att stödja registrering och hantering av patientens önskan att spärra sina uppgifter i vårdens system enligt Patientdatalagen och Socialstyrelsens foreskrifter (HSLF-FS 2016:40 med handbok).
Tjänsten medger att spärren registreras och sedan tillgängliggörs för alla de vårdsystem som behöver utföra kontroll mot spärr. Spärren applicerar på informationshanteringen både inom det inre sekretessomradet (inom vårdgivarens verksamhet) och vid sammanhallen journalforing.
Såväl lokala/regionala vårdsystem såväl som nationella e-hälsotjänster kan nyttja Spärrtjänst.
Utformningen av Spärrtjänst tas sin grund i uppdraget Patientdatalagen i Praktiken (PDLiP), som syftat till att skapa förutsättningar för en nationell samsyn av tolkning och tillämpning av Patientdatalagen.

2.2. Sammanfattning

Arkitekturen för Spärrtjänst medger att vårdgivare, kommuner och regioner kan hantera sina "egna" spärrar i en spärradministrationstjänst där en kopia på spärren replikeras till den nationell tjänsten så att de blir tillgängliga för nationella tjänster som t.ex Nationell Patientöversikt.
Spärrar hanteras därför på två nivåer:

- ***Spärradministration*** en tjänst för spärradministration där spärren hanteras (registreras, hävs etc).
- ***Nationell spärrtjänst*** samlar *kopior* med grundläggande data om *alla* spärrar genom replikering från vårdgivarnas spärrtjänster.

Registrerad spärrinformation utbyts genom RIV tjänstekontrakt. Bilden nedan illustrerar hur vårdsystem kan integrera sig med spärrtjänsten samt hur spärrtjänsterna samverkar med varandra.



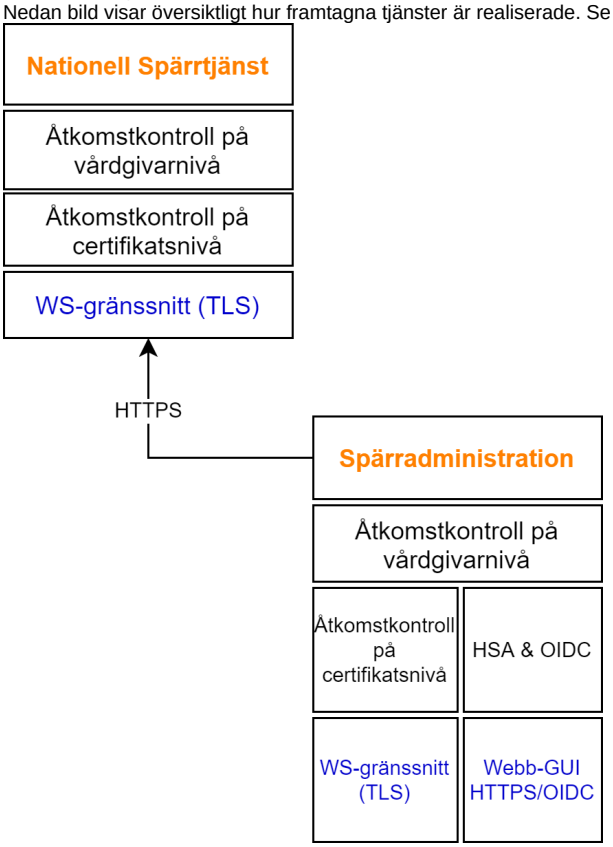
Figur: Stödtjänster för hantering av spärr av patientuppgifter enligt PDL.

Vårdgivarens spärrtjänst
Vårdgivarens spärrtjänst håller originalen för de spärrar som vårdgivaren registrerar för patientens räkning.
Spärrar administreras antingen direkt via ett webbaserat användargränssnitt eller via integration mot webbtjänstegränssnittet.
Vårdgivarens spärrtjänst hanterar ett utökat format för spärrar som inkluderar information om vem som registrerat spärren och när spärren registrerades.
Vårdgivarens spärrtjänst kan implementeras på olika sätt förutsatt att den uppfyller de standardiserade tjänstekontrakt som krävs för att samverkan ska fungera med andra system.
Lokal spärrtjänst levereras från och med denna version inte som nedladdningsbar produkt. Lokala Säkerhetstjänster 2.17 är den sista version som kan laddas ner men Inera rekommenderar att vårdgivaren använder Ineras tjänst för Spärradministration.
Ineras tjänst för Spärradministration driftas av Inera för anslutna vårdgivare. Flera vårdgivare/huvudmän kan därmed dela på en gemensam installation.

Nationell spärrtjänst
Den nationella spärrtjänsten är en centraliserad tjänst som har till uppgift att tillhandahålla ett samlat spärrunderlag för de e-hälsotjänster som opererar på det nationella planet som t ex Nationell Patientöversikt där patientinformation samlas från många olika vårdgivare över regiongränser. Dessa tjänster behöver göra kontroll mot patientens samlade spärrar oavsett var dessa har registrerats.
Det sker ingen direkt administration av spärrar i den nationella spärrtjänsten då enbart kopior av spärrarna tas emot från den lokala spärradministrationstjänsten. Den nationella spärrtjänsten lagrar endast den grundläggande kärna av spärrinformation som behövs för att kunna utföra spärrkontroll i vårdsystemen.

Vårdsystem
En spärr "nyttjas" genom webbtjänsteintegration från ett vårdsystem som utför spärrkontroll och kontrollerar om angiven vårdinformationen är spärrad eller inte. Vårdsystemet kan välja att hämta ett spärrunderlag för intern kontroll eller att fråga tjänsten om spärr föreligger för viss informationsåtkomst.

Realiserade tjänster
Nedan bild visar översiktligt hur framtagna tjänster är realiserade. Se vidare under Teknisk lösning för mer information.



Figur: Översiktlig intern realisering spärrtjänst.

2.3. Tillgänglighet på tjänstekontrakt

Spärrtjänsten realiserar version 4 av de tjänstekontrakt som specificeras i dess tjänstekontraktsbeskrivningar inom RIV-TA domänerna (se [T4]). Nedan anges vilka kontrakt som är tillgängliga inom Vårdgivarens (lokalt) respektive Nationell spärrtjänst.

2.3.1. Version 2

Inte tillgänglig i denna version.

2.3.2. Version 3

Inte tillgänglig i denna version.

2.3.3. Version 4

Tjänst	Nationellt	Lokalt
CheckBlocks	X	X *
GetBlocks	X	X *
RegisterBlock	X	
UnregisterBlock	X	
RegisterTemporaryRevoke	X	
UnregisterTemporaryRevoke	X	
GetExtendedBlocksForPatient		X
GetPatientIds	X	X *
RegisterExtendedBlock		X
RevokeExtendedBlock		X
DeleteExtendedBlock		X
RegisterTemporaryExtendedRevoke		X
CancelTemporaryExtendedRevoke		X

** Ej installerade i NTjP*

3. Målbild och principer

3.1. Verksamhetsmässiga mål

- Vårdgivare ska kunna nyttja stödtjänst för Spärr för att på ett rationellt och sammanhållet sätt hantera kravet på patientens spärr i sina vårdinformationssystem.
- En registrerad spärr ska kunna tillgängliggöras för alla vårdsystem som behöver ta hänsyn till spärren. Dubbelregistrering av patientens spärr ska undvikas.
- Spärrar ska kunna administreras antingen direkt via ett webbaserat användargränssnitt eller via integration mot webbtjänstegränssnitt.
- Det ska finnas historik att tillgå för att se vad som lagts in för patienten bakåt i tiden.
- Inloggade användare ska vara starkt autentiserade med hjälp av SITHS-kort.
- Alla användarrelaterade aktiviteter avseende spärrar (sätta, häva, ta bort, tillfälligt häva, lista spärrar etc) skall loggas.
- Det ska vara möjligt att ta ut rapporter över loggen och/eller exportera loggdata ur perspektiven:
    - spärrhantering för en enskild patient, respektive
    - en enskild medarbetares spärrhantering
- Patient skall kunna anges med identitet av typ Personnummer (PNR), Samordningsnummer (SNR), eller Nationellt Reservidentitet (NRID).
- Det skall vara möjligt att kopiera spärrar mellan vårdgivarens egna vårdenheter vid t ex omorganisation.
- Det skall vara möjligt att kopiera spärrar mellan en patients olika identiteter ifall patienten har flera som i fallet där en reservidentitet kopplas till ett personnummer.

3.2. Arkitekturella mål

3.2.1. Övergripande mål

- Följsamhet mot Nationella IT-strategin.
- Följsamhet mot RIV TA.
- Samverkan med externa system ska så långt som möjligt utformas i enlighet med gällande versioner av tekniska anvisningar så som T-bokens referensarkitektur, tekniska målbilder för nationella tjänster och RIV tekniska anvisningar.
- Återanvändning av nationellt framtagen och driftsatt infrastruktur maximeras.

3.2.2. Specifika mål

- RIVTA2.1 Säkerhetsmodell ska gälla för tjänstegränssnitten.
- Vårdsystem ska kunna välja att hämta ett spärrunderlag för intern kontroll eller att fråga tjänsten om spärr föreligger för viss informationsåtkomst.

3.2.3. Planerade avsteg

- Inga planer finns att leverera Spärradministrationstjänsten för lokal installation.

3.3. Prioriterade områden

3.4. Avgränsningar

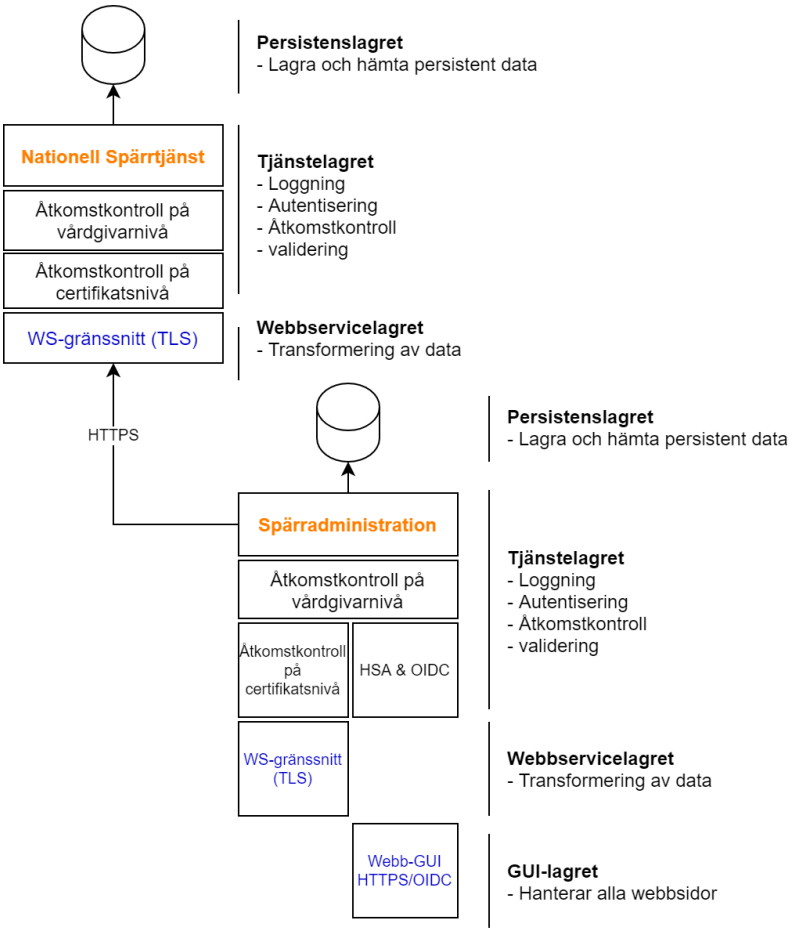
I projektet har inte ingått att realisera tjänstekontrakt för patientingång. Syftet med patientingången är att patienten själv på sikt ska erbjudas möjlighet att via mina vårdkontakter se de spärrar som lagts in för dennes räkning.

Denna version av Spärrtjänsten planeras inte att göras tillgänglig för lokal installation då det av Inera rekommenderade sättet att administrera spärrar numer är att använda molntjänsten.

4. Teknisk lösning

4.1. Översikt

Nedan bild visar övergripande hur tjänsterna nationell och lokal spärrtjänst är realiserade:



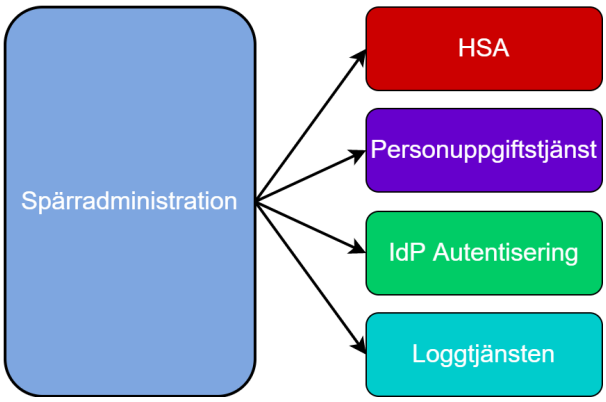
Figur: Intern vy av realiserad tjänst .

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

- Persistenslagret: Hanterar persistens mot databasen.
- Tjänstelagret: Hanterar autentisering, åtkomstkontroll, validering, loggning samt transaktionshantering.
- Webbtjänstelagret: Transformerar XML-data till tjänsteobjekt och vice versa.
- GUI-lagret: Hanterar autentisering och webbsidor för slutanvändare.

4.1.1. Beroenden

Bilden nedan visar översiktligt beroenden till andra system och tjänster som Spärradministration har. Se [T1-6]



Figur: Beroenden i Spärradministration

4.2. Arkitekturellt signifikanta delar av lösningen

4.2.1. Autentisering via OIDC och SITHS certifikat

Användargränssnittet för vårdgivarens spärrtjänst använder OIDC och SITHS certifikat som autentiseringsteknik. I användarens biljett lagras certifikatsuppgifter och egenskaper från HSA-katalogen som användaren fått vid autentiseringen. Dessa uppgifter följer användaren under dennes HTTP-session.
Då slutanvändare skall autentisera sig mot användargränssnittet samt då ett vårdsystem skall anropa webbtjänstegränssnittet måste dessa klienter presentera sitt certifikat. Certifikaten som används är SITHS, för vårdsystem ett mjukt funktionscertifikat och för användare ett SITHS-kort.

4.2.2. Auktorisation

För åtkomst från vårdsystem via tjänstekontrakt styrs åtkomst genom att man i tjänsten konfigurerar vilka certifikat som ges åtkomst till systemet och på vilka vårdgivare dessa tillåts operera. Auktorisation kan även hanteras i Tjänsteplattform om tjänster konsumeras via sådan.
En spärr registreras antingen på vårdenhetsnivå (inre) eller vårdgivarenivå (yttre). I både fallen så lagras alltid ett vårdgivar-id, t.ex. "ABC". Gällande åtkomst i så gäller detta på vårdgivarnivå enligt följande:

- En spärradministratör med uppdrag på vårdgivar-id "*ABC*" får endast möjlig åtkomst (titta/editera/radera, etc...) till spärrar vars vårdgivar-id är "*ABC*"
- Ett anslutet journalsystem (konfigurerat med access till vårdgivar-id "XYZ") får endast möjlig åtkomst (titta/editera/radera, etc...) till spärrar vars vårdgivar-id är "*XYZ*". Dock kommer *samtliga* spärrar i systemet att få genomslag vid en spärrkontroll.
- Ett anslutet journalsystem (konfigurerat med access till vårdgivar-id "XYZ") får endast registrera spärrar/tillfälliga hävningar på vårdgivare vars vårdgivar-id är "*XYZ*".

4.2.3. HSA Webbtjänst (HSA-RIV)

Spärradministrationstjänstens gränssnitt kräver att användare finns upplagda i den HSA-katalog som tjänsten kopplas till. Användarens HSA-id från dennes SITHS-kort måste vara åtkomligt i HSA-katalogen och finnas upplagd med rätt egenskaper och medarbetaruppdrag för att användaren skall ges åtkomst till användargränssnittet.

4.2.4. Webbtjänster

Integrerande vårdsystem kan anropa spärrtjänsterna med webbtjänsteteknik. Denna teknik följer RIV 2.0-standarden, se referens S6.

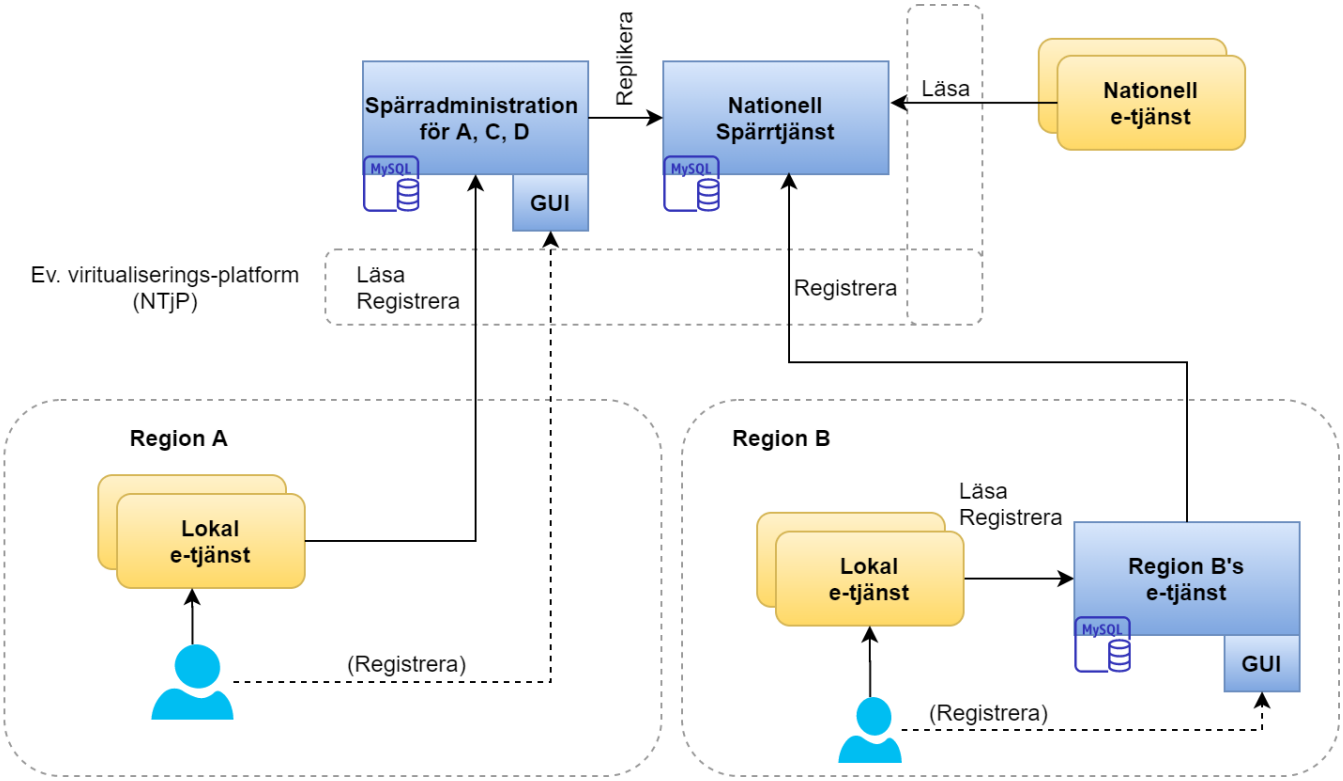
4.2.5. Replikering till nationell tjänst

En implementation av en lokal Spärrtjänst ska ansluta mot det nationella tjänstekontraktet, så att bilden av patientens spärrar blir komplett i nationella tjänsten.
Vårdgivarens spärrtjänst (lokal eller i delad molntjänst) replikerar enkelriktat mot den nationella tjänsten för att samla spärrdata nationellt. Den nationella spärrtjänstens enda uppgift är att lagra kopior av alla de lokala instansernas data. Så fort en förändring av spärrdata sker i vårdgivarens tjänst så skickas detta upp till den nationella.

4.2.6. Unikt nationellt spärr-id

Spärr-id måste vara nationellt unikt då det samlade spärrunderlaget behöver hanteras i nationell tjänst. För att garantera detta behöver ett format väljas som garanterar att id:et blir unikt vid sammanställning i den nationella spärrtjänsten. För detta rekommenderas att välja GUID-format.

5. Logisk arkitektur

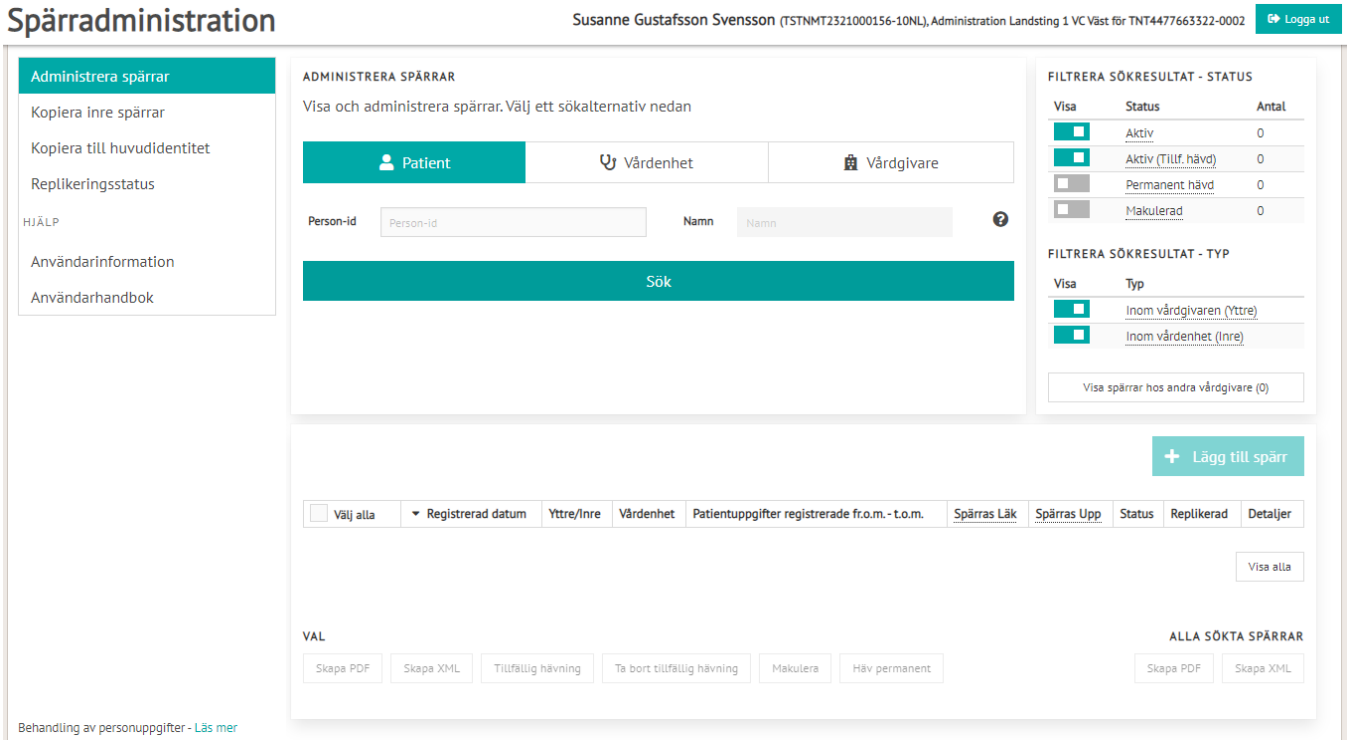


Figur: Logisk systemöversikt och gränsytor i samverkan.

6. Användargränssnitt

6.1. Användargränssnitt för hälso- och sjukvårdspersonal

Användargränssnittet är framtaget med ramverket Angular och är kompatibelt med alla de större webbläsarna på marknaden idag.



Figur: Registrering av spärr.

6.2. Kravbild för tillgänglighetskrav

Följande webbläsare har testats:

- Chrome
- Internet Explorer 11
- Microsoft Edge som baseras på Chromium

SITHS-programvara som testats är Net iD 6.8.x på Windows 10.

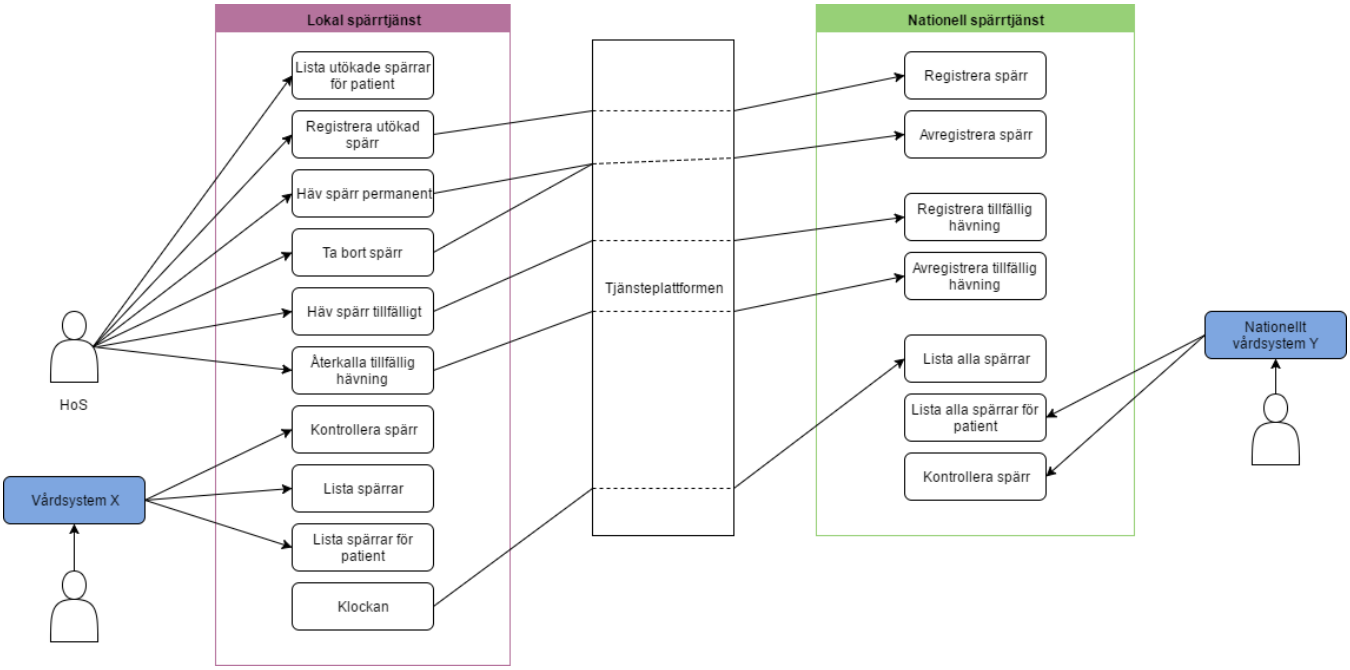
Framtida versioner av Net iD, webbläsare och operativsystem måste kvalitetssäkras löpande.

7. Användningsfall

Alla spärrtjänstens användningsfall är realiserade som webbtjänster. Dessa är också tillgängliga i användargränssnittet med undantag för "Kontrollera spärrar" (CheckBlocks) som är en ren integrationsfunktion.

7.1. Användningsfall - Översikt

1. Lista spärrar
2. Lista spärrar för patient
3. Registrera spärr
4. Avregistrera spärr
5. Registrera tillfällig hävning
6. Avregistrera tillfällig hävning
7. Kontrollera spärrar
8. Lista utökade spärrar för patient
9. Registrera utökad spärr
10. Häv spärr permanent
11. Häv spärr tillfälligt
12. Återkalla tillfällig hävning
13. Ta bort spärr



Figur: Schematisk (förenklad) användningsfallsöversikt.

7.2. Aktörsinformation

7.2.1. Vårdsystem

I det fall tjänstegränssnitten nyttjas i den lokala spärrtjänsten så kan vårdsystem hantera spärrar. Sett ur spärrtjänstens perspektiv så är aktören inte slutanvändaren av vårdsystemet, utan vårdsystemet självt. Vårdsystemet agerar å användarens vägnar. Vårdsystemet har ett unikt HSA-id.

7.2.2. HoS

I det fall användargränssnittet nyttjas i den lokala spärrtjänsten så är aktören en Hälso- och Sjukvårdsperson (HoS) som hanterar spärrar. I första hand en spärradministratör. Vårdsystemet har ett unikt HSA-id samt övriga uppgifter såsom vårdgivartillhörighet.

7.2.3. Klockan

Den lokala spärrtjänstens klocka startar ett tätt återkommande jobb för att synkronisera/hämta nationellt spärrdata från den nationella spärrtjänsten. Detta sker i bakgrunden utan någon mänsklig interaktion.

7.3. Logisk realisering

Begreppet "utökad" förekommer i denna SAD för att förtydliga att objektet avser en lokal, utökad dataform. Det nationella formatet för spärrar är mindre och innehåller endast den datamängd som verkligen krävs för att utföra spärrkontroll.

7.3.1. Flöde AF - Lista spärrar

Returnerar en lista med grundläggande spärrar för alla patienter som har minst en aktiv spärr samt därtill hörande aktiva tillfälliga hävningar. Syftet är dels att kunna åstadkomma import av spärrar i de vårdsystem som saknar möjlighet till on-line slagning, dels att anropande vårdsystem enkelt ska kunna undanta patienter utan spärr från spärrkontroll (dvs. förenkla i normalfallet).

7.3.2. Flöde AF - Lista spärrar för patient

Operationen har samma funktion som Lista spärrar för alla, men är begränsat till en specifik patient. Syftet är att användas on-line av vårdsystem som ska kontrollera spärrar för aktuell patient i samband med att vårdinformation ska visas.

7.3.3. Flöde AF – Registrera spärr

Registrerar en kopia på ett grundläggande spärrobjekt.

7.3.4. Flöde AF – Avregistrera spärr

Operationen tar bort en tidigare registrerad kopia på ett grundläggande spärrobjekt. Används i alla former där en spärr inte längre skall gälla.

7.3.5. Flöde AF – Registrera tillfällig hävning

Operationen registrerar en tillfällig hävning av en spärr. Till skillnad från permanent hävning, som gäller hela spärren, är en tillfällig hävning begränsad till att gälla en viss HoS-person eller en viss vårdenhet. Av det skälet kan flera tillfälliga hävningar existera samtidigt för samma spärr.

7.3.6. Flöde AF – Avregistrera tillfällig hävning

Operationen tar bort en tidigare registrerad tillfällig hävning. Används då den tillfälliga hävningen inte längre är tillämplig vid kontroll av åtkomst till vårdinformation.

7.3.7. Flöde AF – Kontrollera spärrar

Utför spärrkontroll genom att jämföra metadata om vårdinformation med patientens spärrar. Som svar erhålles vilken vårdinformation som är spärrad utifrån frågeunderlaget. Vårdsystemet kan därmed undanta denna från att visas för användaren.

7.3.8. Flöde AF – Lista utökade spärrar för patient

Returnerar alla utökade spärrobjekt och utökade tillfälliga hävningar för en viss patient. Notera att denna operation, till skillnad från Lista spärrar för patient, syftar till att administrera spärrar, inte kontrollera tillgång till vårdinformation. Urvalet är därför inte begränsat till enbart aktuella spärrar utan även ogiltiga.

7.3.9. Flöde AF – Registrera utökad spärr

Lagrar ett nytt utökat spärrobjekt.

7.3.10. Flöde AF – Häv spärr permanent

Häver en sedan tidigare registrerad spärr och gör spärren permanent ogiltig.

7.3.11. Flöde AF – Häv spärr tillfälligt

Operationen registrerar en tillfällig hävning av en spärr. Till skillnad från permanent hävning, som gäller hela spärren, är en tillfällig hävning begränsad till att gälla en viss HoS-person eller en viss vårdenhet. Av det skälet kan flera tillfälliga hävningar existera samtidigt för samma spärr.

7.3.12. Flöde AF – Återkalla tillfällig hävning

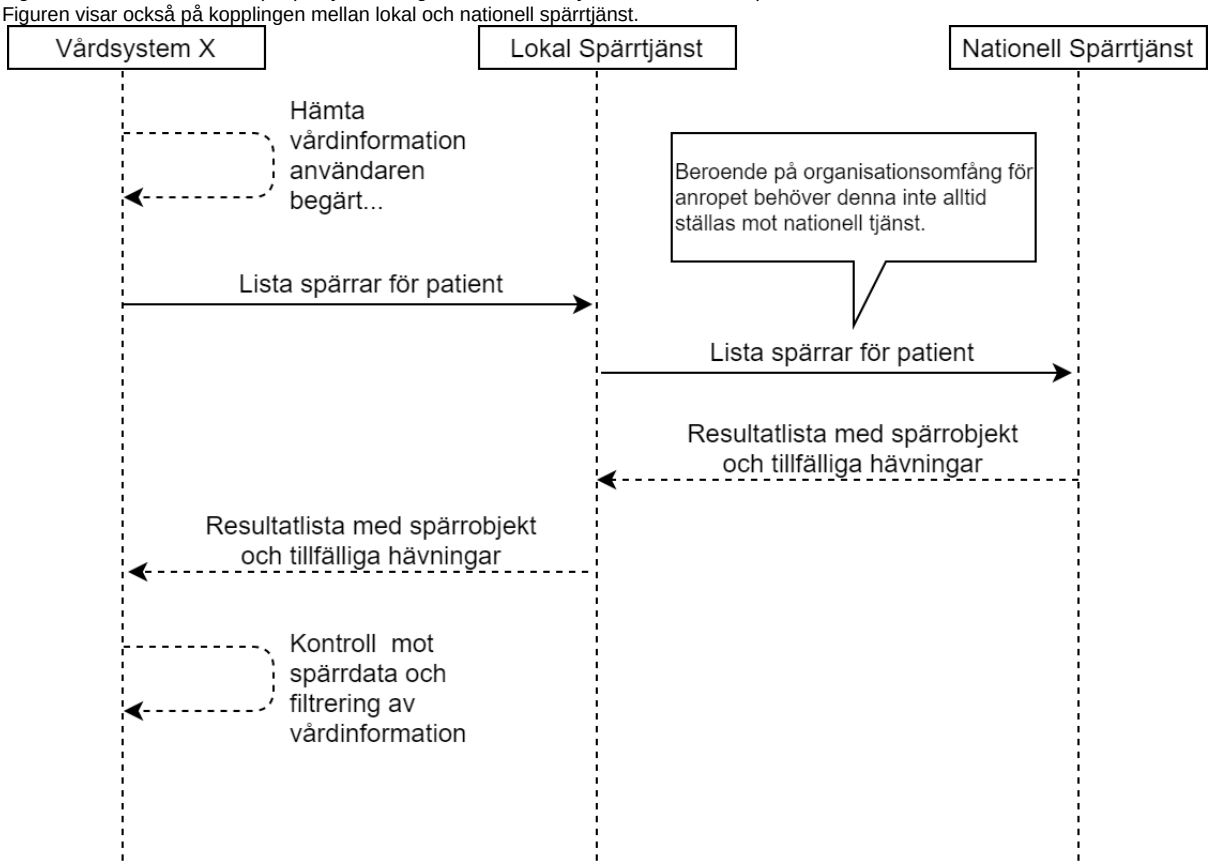
Operationen återkallar/makulerar en sedan tidigare registrerad tillfällig hävning av spärr. Spärren blir således aktiv igen för den/de aktör(er) som den tillfälliga hävningen avsåg.

7.3.13. Flöde AF – Ta bort spärr

Tar bort (makulerar) en sedan tidigare registrerad spärr. Spärren raderas inte fysiskt utan markeras som makulerad. Spärrar tas endast bort till följd av felregistrering. Detta skall inte förväxlas med permanent hävning.

7.3.14. Flöde AF – Vårdsystem

Figuren nedan visar ett exempel på systemintegration där "Vårdsystem X" inhämtar spärrar och kontrollerar huruvida vårdinformation är spärrad eller inte. Figuren visar också på kopplingen mellan lokal och nationell spärrtjänst.



Figur: Sekvensdiagram – Lista spärrar och utföra spärrkontroll.

8. Uppfyllande av icke-funktionella krav

8.1. Icke-funktionella krav från verksamheten

8.1.1. Svarstider

I implementerad spärrtjänst håller funktioner avsedda för slutanvändare, såsom Registrera spärr, Lista spärrar för patient generellt sätt svarstider under en sekund.
Synkroniseringsmetoder såsom "Lista alla spärrar" håller svarstider på mellan en och 30 sekunder beroende på antalet spärrar.

8.1.2. Tillgänglighet

Kontroll av spärrar är en kritisk funktion i vårdsystem vilket gör att tillgänglighet på spärrdata är av stor vikt.
Principer för hög tillgänglighet:
Vårdgivarens spärrtjänst skall inte bli otillgänglig då den nationella spärrtjänsten ej kan nås. Det ska alltså fortfarande gå att hämta och registrera spärrar på vårdgivarens nivå. Replikering som inte kan utföras köas upp tills den nationella noden åter är tillgänglig.
Detsamma rekommenderas för anslutna vårdsystem, som ej bör bli otillgängliga då spärrtjänst inte kan nås. För att öka tillgängligheten på dessa vårdsystem så kan dessa, om möjligt, lagra de senast hämtade spärruppgifterna från spärrtjänst. Eftersom verksamhetens process för att registrera en spärr som begärts av en patient kan ta timmar, snarare än minuter, så kan normalt också vårdsystemen fungera utan senaste spärrstatus vid tillfällen då spärrtjänsten är otillgänglig.
Specifika krav överenskommes i avtal om drift av tjänst. Eftersom lokal spärrtjänst är en produkt så bestämmer brukaren delvis själv vilken infrastruktur som skall stödja hög tillgänglighet såsom redundans, backup, m.m.

8.1.3. Volymskrav

Hänsyn har tagits till den mängd användare och spärrar som förväntas existera på nationell nivå. Arkitekturen har utformats så att spärrtjänsten hanterar storleksordningen "tusentals" spärrar och förväntar sig inte "miljontals".

8.2. Icke-funktionella krav från Systemägaren/Förvaltaren

8.2.1. Test

Specifika krav överenskommes i avtal om drift av tjänst.

8.2.2. Konfigurationsstyrning

Specifika krav överenskommes i avtal om drift av tjänst.

8.2.3. SLA-övervakning

Specifika krav överenskommes i avtal om drift av tjänst.

9. Informationsmodell

9.1. Allmänt

Använda definitioner bygger på [S8] RIV-specifikation PDLiP (Patientdatalagen i Praktiken) med vissa tillägg.
Övergripande modell

Figur 8: Till varje spärr kan kopplas 0 eller fler tillfälliga hävningar.

För mer information om datatyperna, se tjänstekontrakt som informationsspecifikation för spärrtjänsten [T4].

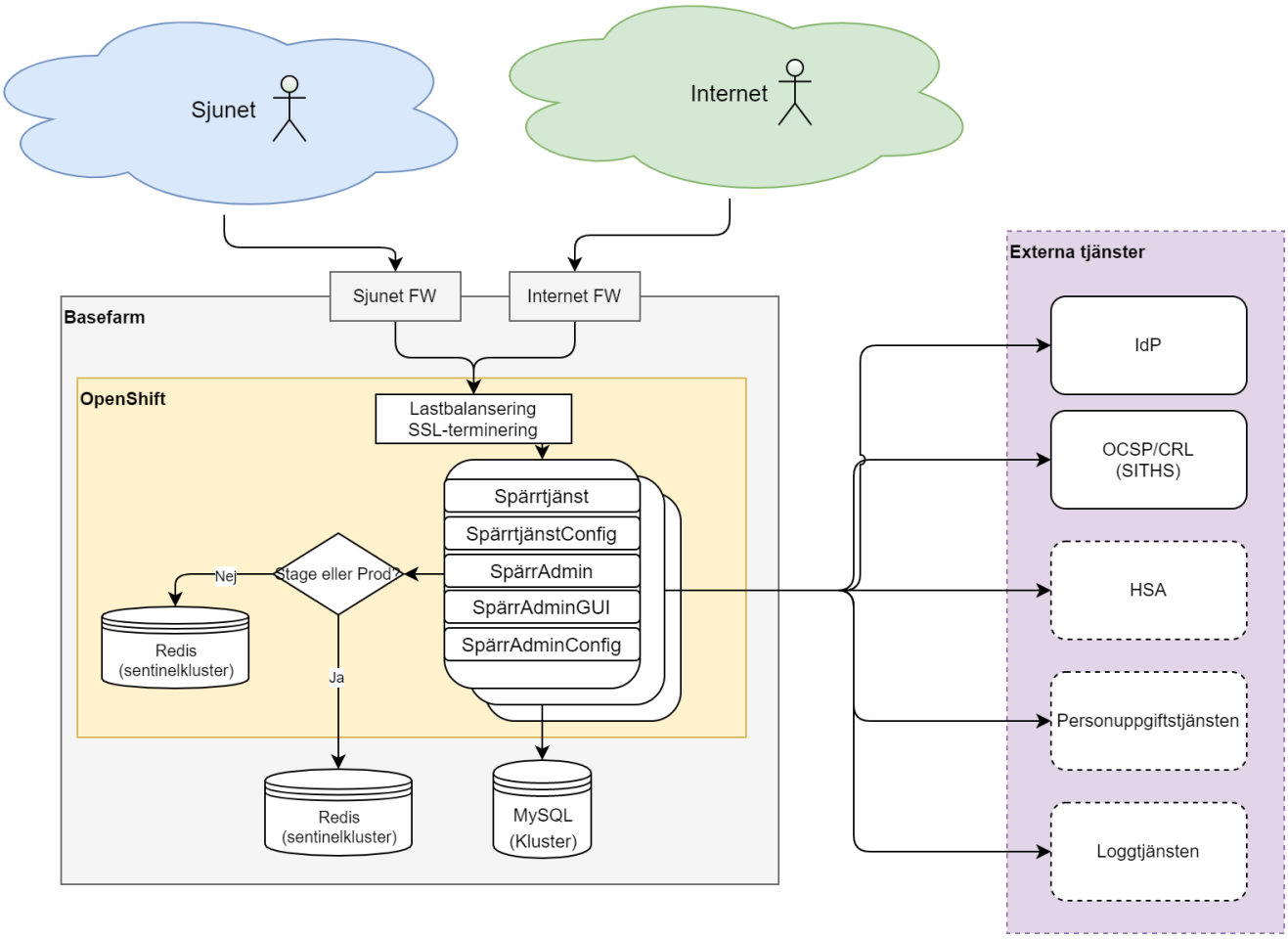
10. Driftaspekter

Till skillnad från tidigare version av spärrtjänsten som ingick i installationen av Säkerhetstjänster så paketeras inte denna version för traditionell installation i Linux eller Windows.

Inera driftar numera sina applikationer i containerbaserade miljöer som OpenShift. Leveransen av de olika delarna av Ineras spärrlösning byggs nu därför endast till jar-filer som sedan byggs in i image-filer för deploy i specifik OpenShift-miljö.

11. Lösningsöversikt

Nedanstående figur visar det infrastruktursförslag som ges vid drift av lokal och/eller nationell spärrtjänst. I detta fall visar bilden en lokal spärrtjänst på Sjunet som anslutits till nationell spärrtjänst.



Figur: Lösningsöversikt - Fysisk vy.

11.1. Fysisk miljö

Den fysiska miljön för spärrtjänsten beror på huvudmannens val av systemkonfiguration. Se föregående översiktsbild.

11.2. Programvaror

Spärrtjänsten kräver följande programvara:

- Java OpenJDK 11 – 64 bit
- MySQL Server 8.0 (eller högre) – 64 bit
- Redis

11.3. Detaljerad information

Ej specificerat

11.4. Produktionssättning och överlämning till förvaltning

Ej specificerat

12. Följsamhet mot T-bokens styrande principer

12.1.1. 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.	Uppfyllt. Lokal spärrtjänst fungerar utan extern koppling till nationell spärrtjänst. Det är även möjligt att hålla cachad information i vårdsystemet så att detta kan fungera helt utan externt beroende vid kontroll mot spärr.
Verksamhetskritiska nationella stödtjänster (t.ex. tillgång till behörighetsstyrande information) erbjuder möjlighet till lokala instanser som med tillräcklig aktualitet hålls uppdaterade med nationell master.	Uppfyllt. Arkitekturen med vårdgivarens spärrtjänst och nationell spärrtjänst stödjer detta. Även applicerbart för HSA-katalogen som används av den lokala spärrtjänsten.
Krav mellan integrerande parter regleras genom integrationsavtal. Integrationsavtal är det avtal där informationsägaren godkänner att en ett visst system får agera 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.	Uppfyllt. Integrationsavtal krävs för att ansluta mot nationell spärrtjänst. Brukaren av lokal spärrtjänst avgör själv genom åtkomstkontrollstyrning vilka integrationer som sker i dennes installation.
Arkitekturen måste möjliggöra tillräcklig tillgänglighet vid flera samverkande system.	Understöds genom att • samverkan med nationella delar inte behöver sänka tillgänglighet på lokala. • Nationella e-tjänster kan slå mot samlat spärrunderlag i nationell spärrtjänst oavsett om lokala installationer är tillgängliga eller ej.
En sammantagen tolkning av tillämpliga lagar och förordningars konsekvenser för teknisk realisering av informationsfångst, utbyte och lagring.	Tolkning av lagrum kring spärrhantering har skett i PLDiP(Cehis) samt i separat samverkansprojekt. Tekniskt utbyte mellan samverkande system sker enligt RIV TA (T-boken)
Förutsättningar för spårbarhet etableras i form av loggningsregler för komponenter som deltar i säkert informationsutbyte.	Spärrtjänsten loggar all informationsåtkomst på ett enhetligt format. Nationella spärrinstansen nyttjar den nationella instansen av Loggtjänst.
Interoperabla, internationellt beprövade och för leverantörer tillgängliga standarder tillämpas för kommunikation mellan parter som har upprättat tillit.	Uppfyllt. Spärrtjänsten följer RIV-TA 2.0 och i övrigt kända standarder för säkerhet och autentisering, bland annat SAML 2.0.

12.1.2. 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 eller andra organisatoriska avgränsningar i nationella tjänstekontrakt.	Uppfyllt. Spärrtjänstens kontrakt är nationellt gångbara och innehåller inga lokala /organisationsspecifika begränsningar.
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.	Se tjänstebeskrivning Spärr.
Integration ska ske över en integrationsinfrastruktur (t.ex. virtualiseringsplattform) som möjliggör uppföljning av tjänsteproducenters fullföljande av SLA.	Tjänstekontrakten är möjliga att nyttja via en virtualiseringsplattform (tjänsteplattform).
System och e-tjänster som upphandlas kan utökas med fler organisationer som kunder utan krav på infrastrukturella ingrepp (jämför s.k. SaaS)	Uppfyllt. Spärrtjänsten kan hantera flera samtidiga organisationer/huvudmän i samma delade instans.

12.1.3. 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.	Uppfyllt. RIV TA 2 för samverkan. Logisk adressering baserad på ägaren till spärrdatat.	
En arkitektur som skapar lös koppling mellan konsumenter och producenter, avseende adressering och standarder för kommunikation.	Uppfyllt. RIV TA 2 för samverkan.	
En nationell integrationspunkt ska kunna erbjudas för varje nationellt standardiserat tjänstekontrakt, som en fasad mot bakomliggande brokiga systemlandskap.	Tjänstekontrakten för replikering till nationell tjänst sker mot en nationell integrationspunkt och kan erbjudas via Tjänsteplattform.	
Nationella tjänstekontrakt förvaltas i en nationellt koordinerad förvaltning.	Enligt RIV TA.	
För en process inom vård och omsorg kan flera tjänstekontrakt ingå. Därför är det viktigt att alla tjänstekontrakt baseras på en gemensam referensmodell för informationsstruktur.	Baseras på RIV-modell PDLiP.	
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: • *Nationellt bryggar informationen (semantisk översättning) eller* • *Nationellt införlivar externt förvaltat tjänstekontrakt som standard.* *Observera att semantisk bryggning av information till vårdens referensmodell förutsätter en nationell förvaltning av bryggningstjänster.* *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.	Uppfyllt. Tillämpas vid implementation / anslutning av vårdsystem till spärrtjänster	
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).	Uppfyllt. Spärrtjänsten följer RIV-TA 2.0.	

12.1.4. IT5: Lokalt driven e-tjänsteförsörjning		
Förutsättningar att uppfylla	*Uppfyllnad*	
När utveckling av källkod är en del av en tjänsteleverans skall följande beaktas: • *Alla leveranser tillgängliggörs under öppen källkodslicens. Valet av licensformer samordnas nationellt genom rekommendationer.* • *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").* • *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.* • *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.* • *Gemensam referensmodell för e-tjänsters interna uppbyggnad stimulerar och förenklar återanvändning och överföring av förvaltningsansvar mellan organisationer.*	Ej uppfyllt. Realiseringen av spärrtjänsten lämnas ej ut som öppen källkod.	
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.	<Ej tillämpbar>	
Utveckling sker mot globalt dominerande 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.	Uppfyllt. Spärrtjänsten är en fristående produkt som endast kräver databasen MySQL som tillägg - vilken kan nyttjas utan kostnad.	

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>	

12.1.5. IT6: Samverkan i federation

Förutsättningar	*Uppfyllnad*	
Att gemensamma gränssnitt i alla federativa utbyten finns framtagna och beskrivna, vilket möjliggör kostnadseffektiva och leverantörsneutrala lösningar.	Uppfyllt. Alla integrationspunkter består av nationella tjänstekontrakt. Federation via SAML2, RIV TA 2.1.	
Det behövs organ och processer för att godkänna utgivare av elektroniska identitetsintyg och certifikat som är giltiga i federationen.	Enligt SITHS policy för certifikat för personal och system. För utgivning av identitetsintyg enligt SAML kommer det att behöva skapas en process för att godkänna flera utgivare i federationen.	
Aktörer i olika nät, inklusive öppna nät ska vara välkomna i elektronisk samverkan genom att samverkande komponenter är säkra.	Uppfyllt. Realiseringen av spärrtjänsten nyttjar säker kommunikation i form av TLS med dubbelriktad autentisering.	
Att Ingående parter i federationen är överens om ett antal gemensamma ståndpunkter: • *att stark autentisering likställs med 2-faktors autentisering* • *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* • *att tillämpa en gemensam certifikat- och utfärdarpolicy, likvärdig med SITHS, som ett minimikrav för egen eller annans PKI* • *att sträva mot en autentiseringslösning, framför flera olika, för att realisera stark autentisering i den egna organisationen och i federation* • *att enbart acceptera SAMLv2, eller senare version, vid identitetsfederering samt tydliggöra att det i förekommande fall är det enda sättet att logga in och säkerställa det inte finns någon bakväg in* • *att tillämpa ett gemensamt ramverk för att ingå i en federation* • *att tillämpa en gemensam katalogpolicy, med utgångspunkt från HSA policy, som ett minimikrav för egna kataloger* • *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* • *att sträva efter att möjliggöra kontroll av trafik till och från den egna infrastrukturen i en eller få kontrollpunkter* • *att utgå från att kommunikation över Internet och Sjunet har ett likvärdigt skyddsbehov*	Lösningen stödjer en sådan kommande federation genom användning av Autentisering: • Nationell extern idP/Autentiseringstjänst med SAML2 som bas(eller kompatibel lokal dito för lokal tjänst) • SITHS-kort / certifikat och tillhörande utfärdarpolicys HSA: HSA som katalogtjänst; från HSA hämtas alla användaregenskaper såsom rättigheter. Nät: Oavsett vilket nät som används säkras tjänsterna enligt ovan, d v s i grunden utgår lösningen ifrån att samma skyddsbehov finns i båda fallen. För exponering mot Internet följs även Sjunets säkerhetsregler, vilket tillför ytterligare skyddsmekanismer (ytterligare separat DMZ). Tjänster som exponeras via Tjänsteplattformen använder den nätverksexponering mot Internet som Tjänsteplattformen tillhandahåller. Exponering av tjänster på Internet hanteras separat och dokumenteras i för det avsedd SAD.	

13. Referenser

13.1. Styrande dokument

Ref	Dokument ID	Dokument/Beskrivning
S1	IT-strategi	http://rivta.se/documents/ARK_0022/
S2	T-boken	http://rivta.se/documents/ARK_0019/
S3	RIV	Dokument kan laddas ner från http://www.rivta.se/
S4	HSLF-FS 2016:40	Föreskrift och handbok hos Socialstyrelsen
S5	VIT-boken	Dokumentet kan laddas ner från: https://www.inera.se/digitalisering/arkitektur/
S6	RIV Tekniska Anvisningar	http://www.rivta.se/
S7	Nationella tjänsteplattformen	http://skltp.se/
S8	RIV PDLiP	RIV-specifikation för PDL i praktiken http://rivta.se/documents/ARK_0031/
S9	SAMBI	
S10	Lokala Säkerhetstjänster 2.17	Lokala Säkerhetstjänster
S11	Användarhandbok	Användarhandbok Spärradministration

13.2. Stödjande dokument

Ref	Dokument ID	Dokument/Beskrivning
R1	SAD-mall	Arkitekturledningens mall för SAD http://rivta.se/documents/ARK_0013/
R2	RIVTA BP2.1	RIV Tekniska Anvisningar Basic Profile 2.1 http://rivta.se/documents/ARK_0002/
R3	Binära bilagor	RIV Tekniska Anvisningar Binära bilagor http://rivta.se/documents/ARK_0038/

13.3. Integrationstjänster

I tabellen kan referenser förekomma som inte direkt är nyttjade i tjänsten. Enbart rader refererade i denna SAD nyttjas.

Ref	Dokument ID	Dokument/Beskrivning
T1	HSA	Uppslag av uppgifter från HSA sker via RIV-kontrakt. **Nyttjade tjänstekontrakt** **HSA-RIV** **infrastructure:directory:organization** GetHealthCareUnitList:2 **infrastructure:directory:employee** GetEmployeeIncludingProtectedPerson:2
T3	TK-Logg	Tjänstedomän: riv:informationsecurity:auditing:log http://rivta.se/domains/informationsecurity_auditing_log.html
T4	TK-Spärr	Tjänstedomän: riv:informationsecurity:authorization:blocking http://rivta.se/domains/informationsecurity_authorization_blocking.html

13.4. Plattformsfunktioner

I tabellen kan referenser förekomma som inte direkt är nyttjade i tjänsten. Enbart rader refererade i denna SAD nyttjas.

Ref	Dokument ID	Dokument/Beskrivning
P1	Säkerhetstjänster	https://www.inera.se/sakerhetstjanster Allmän anslutningsdokumentation och förutsättningar för nyttjande.
P2	HSA	https://www.inera.se/hsa HSA används i lösningen för att tillhanda kvalitetssäkrade uppgifter om personer och funktioner/system. Grundläggande rättighetshetstilldelning utgår från HSA. Befintlig koppling till HSA-tjänsten nyttjas i den webbapplikation som finns för administration av stödtjänsterna. Stödtjänsten själv nyttjar inte HSA-tjänsten.
P3	SITHS	https://www.inera.se/siths SITHS-kort används för säker inloggning, ger stöd för stark autentisering av användare.
P4	Tjänsteplattform	http://skltp.se/ Tjänsteplattform, lokalt såväl som nationellt, är en möjlig förmedlare av tjänsterna. Tillför möjlighet till internetanslutning samt förenkling av integrationspunkterna och vägval för att hitta viss producerande tjänst.