



Litfärens

Guide till Säkerhetstjänster 2.0 – 2.x





Innehållsförteckning

1. Dokumentinformation	4
1.1 Inledning	4
1.2 Målgrupp	4
1.3 Revisionshistorik	4
2. Inledning	6
3. Översikt	7
4. Tjänstebeskrivning	10
4.1 Autentiseringstjänsten	10
4.1.1 Sammanfattning	10
4.1.2 Leverans	11
4.1.3 Förutsättningar för användning av tjänsten Autentisering	11
4.2 Spärrtjänsten	14
4.2.1 Sammanfattning	14
4.2.2 Leverans	15
4.2.3 Förutsättningar för att använda Spärrtjänsten	15
4.3 Samtyckes & Patientrelationstjänsten	16
4.3.1 Sammanfattning	16
4.3.2 Leverans	16
4.3.3 Förutsättningar för att använda Samtyckes & Patientrelationstjänsten	17
4.4 Loggtjänsten	18
4.4.1 Sammanfattning	18
4.4.2 Leverans	18
4.4.3 Förutsättningar för att använda Loggtjänsten	19
5. Adresser/URL	20
5.1 Exempelkod och nedladdningssite	20
5.2 Acceptanstest	20
5.2.1 Adresser tjänster för nationell Spärr, Samtycke, Patientrelation & Logg-acceptanstestmiljön (f.n enbart på Sjunet via direktanrop, ej via TP)	21
5.3 Produktionstest	23
5.4 Produktion	24



6. IP-adresser	25
7. Referenser	26
8. FAQ, exempel.....	28



1. Dokumentinformation

1.1 Inledning

Detta dokument ska hjälpa till att beskriva vad leveransen av Säkerhetstjänster 2.0 – 2.x består av inklusive en kort beskrivning av de olika funktionerna/tjänsterna som paketet Säkerhetstjänster består av.

1.2 Målgrupp

Målgruppen som detta dokument vänder sig till är dels de som vill få en överblick av Säkerhetstjänsterna, dels applikationer/system som avser att ansluta sig till någon av de tjänster som levereras av Säkerhetstjänster.

1.3 Revisionshistorik

Version	Datum	Författare	Kommentar
0.1	2013-01-29	Björn Skeppner	Första utgåva
0.2	2013-02-01	Björn Skeppner	Justeringar & tillägg
0.3	2013-02-04	Björn Skeppner	Justerad efter Tomas Fransson synpunkter
0.4	2013-02-05	Björn Skeppner	Justeringar efter synpunkter från Logica
1.0	2013-03-06	Björn Skeppner	Lagt till adresser till Spärr, Samtycke & Patientrelation
1.1	2013-03-15	Björn Skeppner	För bakåtkompatibilitet behålls 84XX för IdP'n, därför ny URL för autentiseringen
1.2	2013-04-02	Björn Skeppner	Lagt till adresser etc för prodtest
1.3	2013-04-10	Björn Skeppner	Fel portangivelse för url: https://prodtest.sakerhetstjanst.inera.se:8445/idp/saml Ska vara port: 8443
1.4	2013-10-02	Tomas Fransson	Acceptansmiljöns portar uppdaterade
1.5	2013-01-07	Tomas Fransson	Uppdateringar i samband med version 2.3 av lokal Säkerhetstjänst. Referenser till dokument



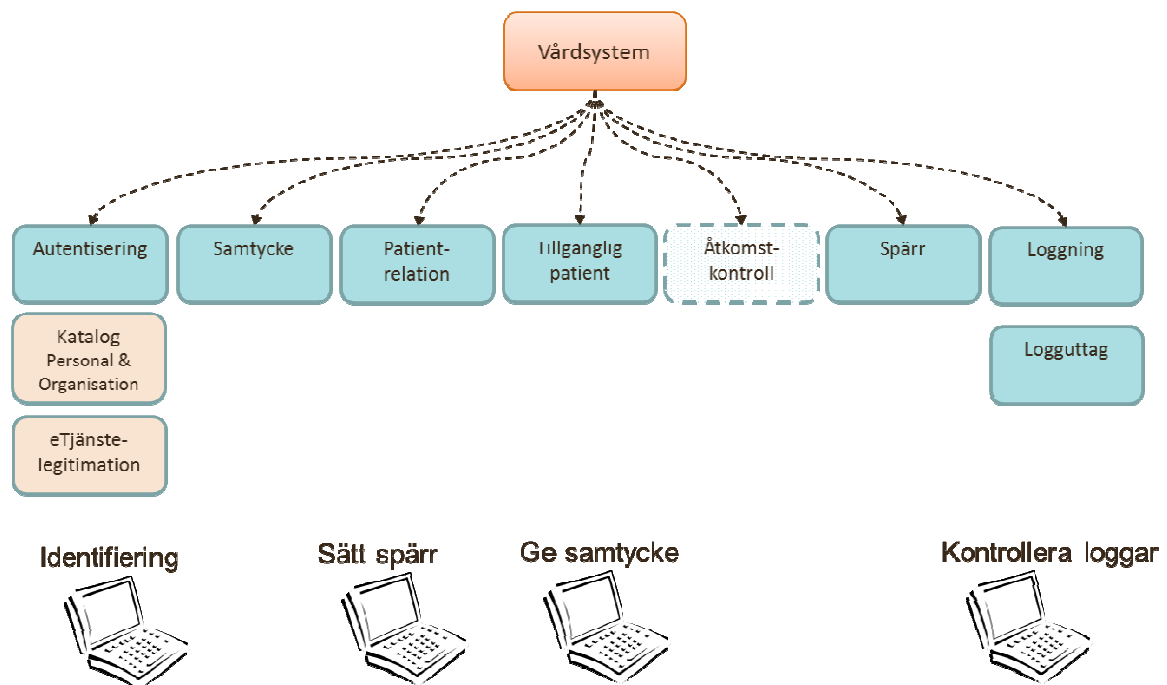
			på www.inera.se och Google code uppdaterade.
--	--	--	--



2. Inledning

Säkerhetstjänster 2.0 - 2.x är den senaste leveransen av den gamla BIF-tjänsten (Bastjänster för InformationsFörsörjning). Den största skillnaden mellan BIF och Säkerhetstjänster 2.x är att Säkerhetstjänsterna nu levereras som fristående tjänster och ej har direkt beroende till ingående tjänster –samt att de fristående kan installeras lokalt inom ett landsting eller hos en vårdgivare.

Ingående tjänster enligt figur nedan:



Följande tjänster ingår i den ”nationella leveransen”, dvs levereras såsom en tillgänglig IT-tjänst:

- Autentisering (Nationella IdP'n)
- Samtyckestjänst (”hotelltjänst” för samtyckeshantering)
- Patientrelation (”hotelltjänst” för hantering av patientrelation)
- Tillgänglig patient (TGP-tjänst, för samverkan med ex. NPÖ)
- Spärrtjänst (dels som ”hotelltjänst”, dels som ”nationell toppnod” för replikerade spärrar)
- Loggtjänst (nationell tjänst för att lagra åtkomstloggar och nationell tjänst för loggrapporter)



Åtkomstkontrollen finns kvar för ”bakåtkompatibilitet” åt NPÖ men ingår formellt ej längre i leveransen av Säkerhetstjänsten. Förslag till nytt Tjänstekontrakt finns framtaget och kan erhållas från Säkerhetstjänsternas förvaltning.

Samtliga tjänster –utom TGP- kan laddas ned från CGIs FTP-site¹ för lokal installation av landsting. Detta kräver dock ett ”Avtal för användning av Säkerhetstjänster” som tecknas med Inera.

Erforderlig dokumentation finns dels på **Projektplatsen**, projekt **Säkerhetstjänster V2** (leveransdokument, release notes, installationsdokument, SAD etc), dels på RIV TA-siten (tjänstekontrakt & tjänstekontraktbeskrivningar) på <http://www.rivta.se>

Exempel på referensapplikationer –hur man använder RIV TA- finns på RIV TA-siten. Se ref [R20] & [R21]

3. Översikt

Kort beskrivning av ingående tjänster

Tjänst	Funktion	Lokal/ Nationell	Operativsystem för lokal installation
Autentisering	Autentiseringstjänsten har till uppgift att kontrollera och fastställa en användares identitet vid inloggning i ett IT-system. När en användare loggar in eller loggar ut från ett system sker detta på ett koordinerat sätt. Det innebär att kontroll av identitet endast behöver göras en gång, oavsett hur många system användaren loggar in i. Hur fungerar Autentiseringstjänsten? När en användare loggar in eller ansluter till ett IT-system måste användarens identitet kontrolleras och fastställas. Detta är Autentiseringstjänstens uppgift. Tjänsten sammanställer användarens uppgifter och intygar att de är korrekta. Denna information lagras sedan i en så kallad biljett, som används som underlag för styrning av rättigheter i de system och tjänster som biljetten används av.	L + N	Windows, Linux
Spärr	Spärrtjänsten registrerar spärrar och kontrollerar om en patient har spärrat tillgång till patientinformation inom och mellan vårdgivare.	L + N	Windows, Linux

¹ Se kapitel: Adresser



	<p>Hur fungerar Spärrtjänsten?</p> <p>För att en patient ska kunna spärra information, måste berörd organisation ha informerat patienten om möjligheten till detta, samt vilka konsekvenser detta kan innebära. Patienten kan därefter begära hos vilken vårdenhet/vårdgivare som informationen ska spärras. Det finns möjligheter för vårdgivaren att låta patienten undanta läkemedel och/eller varningar från att bli spärrade. Om det finns en spärr för en patients uppgifter, så gäller den alltid före eventuella registrerade samtycken och patientrelationer.</p> <p>En spärr fungerar så att patientuppgifter inom en viss vårdenhet (inre spärr) eller inom en vårdgivare (yttre spärr) blir spärrad för hälso- och sjukvårdspersonal som arbetar "utanför" denna vårdenhet eller vårdgivare. Inre spärrar kan tillfälligt hävas, antingen med en patients uttryckliga medgivande eller vid en nödsituation. Den tillfälliga hävningen är tidsbegränsad, och kan återkallas innan tidsbegränsningen gått ut</p>		
Samtycke	<p>Samtyckestjänsten registrerar och lagrar information om patientens samtycke till åtkomst av sammanhållen vårddokumentation. Tjänsten kan svara ja eller nej på frågan om en patient har gett sitt samtycke till att information får lämnas ut mellan vårdgivare.</p> <p>Hur fungerar Samtyckestjänsten?</p> <p>För att vårdpersonalen ska få åtkomst till patientens information hos andra vårdgivare krävs patientens samtycke. Utan samtycke, ingen åtkomst. Detta samtycke lagras i ett samtyckesintyg som innehåller uppgifter inom vilken tidsperiod samtycket ska gälla, och för vilken vårdpersonal/vårdenhet som detta samtycke ska gälla.</p> <p>Ett samtycke anger alltid vem/vilka som får ta del av patientens information. Vill patienten göra undantag och exkludera en vårdenhet eller liknande, hanteras detta via säkerhetstjänsten Spärr</p>	L + N	Windows, Linux
Patientrelation	<p>Patientrelationstjänsten registrerar och lagrar information om relationer mellan hälso- och sjukvårdspersonal och patienter. Tjänsten kan svara ja eller nej på frågan om en "vårdpersonal-till-patient-relation" existerar. Registrering av patientrelationen utförs manuellt.</p> <p>Hur fungerar Patientrelationstjänsten?</p> <p>Syftet med Patientrelationstjänsten är att administrera och intyga att hälso- och sjukvårdspersonal har en relation med patienten. I tjänsten registreras och lagras den relation som finns och tjänsten svarar ja eller nej på frågan om en patientrelation existerar.</p> <p>En förutsättning för tjänsten ska kunna fungera är att verksamheten har fastställt regler för vad som definierar en patientrelation</p>	L + N	Windows, Linux



Loggtjänst	<p>Loggtjänsten lagrar information om åtkomstrelaterade händelser från olika system på ett strukturerat sätt. Loggtjänsten innehåller även en rapportfunktion som kan användas för uppföljning av åtkomstloggar.</p> <p>Hur fungerar Loggtjänsten?</p> <p>Syftet med Loggtjänsten är att lagra uppgifter om vem som har begärt och haft åtkomst till vilken information, samt inom vilket uppdrag åtkomsten skedde. Detta för att man i efterhand ska kunna se om åtkomsten varit berättigad eller inte. Loggtjänsten tar emot åtkomstloggar från vårdssystem som bland annat innehåller uppgifter om användare, vårdenhet, aktuell patient, vilka åtgärder som vidtagits med patientuppgifterna, samt när detta skedde</p>	L + N	Windows, Linux
------------	--	-------	----------------

TGP och Åtkomstkontrollen beskriv ej i detta dokument då de hanteras separat.



4. Tjänstebeskrivning

4.1 Autentiseringstjänsten

4.1.1 Sammanfattning

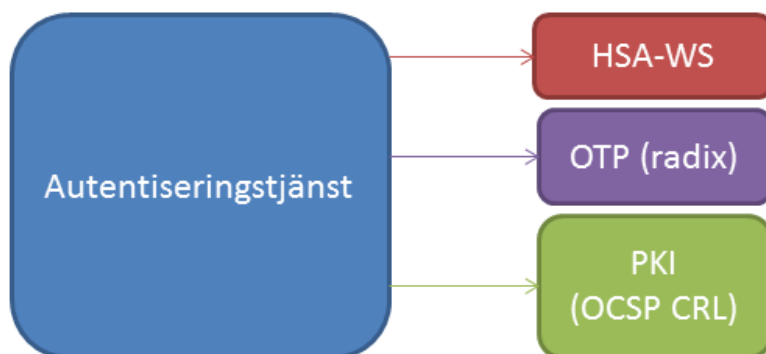
Autentiseringstjänsten syftar till att erbjuda vårdgivare och dess vårdssystem en säker autentisering av aktörer/vårdpersonal. Autentiseringstjänsten tillhandahåller s.k. single sign on inom webbapplikationer och för rika klienter, enligt väl definierade standarder, så som SAML Web SSO Profile.

Utöver detta rättar sig tjänsten efter den profil som begränsar, samt identifierar tekniker som måste realiseras, för att med säkerhet tillgodose funktionalitet i en federering mellan flertalet autentiseringstjänster (IdPer).

Tjänsten tillhandahåller också funktion för att på ett enhetligt sätt logga ut aktören från samtliga inloggade tjänsteleverantörer, s.k. koordinerad utloggning (single logout). Detta gäller endast om tjänsteleverantören har stöd för koordinerad utloggning, enligt SAMBI SAML Profilen.

Standardiseringsorganet OASIS har ett flertal standarder som identifierar problem, samt föreslår lösningar för dess problem. Dessa standarder, ex. SAML 2.0, används för att på ett standardiserat sätt implementera tjänsten. Vid en lyckad autentisering utfärdas ett s.k. SAML-intyg som beskriver aktören, samt dess egenskaper, som är tänkta att användas av ett ABAC (Attribute Based Access Control) behörighetssystem, dvs behörighet på egenskapsnivå, till skillnad från RBAC (Role Based Access Control) som har behörighet på roll nivå.

Aktörer som skall autentiseras måste vara upplagda i HSA katalogen. Om aktörer har två eller flera medarbetaruppdrag, måste aktören välja aktuellt uppdrag för autentiseringen. Om endast ett uppdrag finns väljs detta implicit. SAML profilen definierar vilken mängd egenskaper som tillhandahålls av tjänsten. Vid autentisering utan uppdragsval (dvs aktören saknar medarbetaruppdrag) innehåller utfärdat SAML-intyg endast sådana egenskaper som inte är uppdragsspecifika. För mer info se ref [R4] samt [R12] under [Referenser](#)





4.1.2 Leverans

Autentiseringstjänsten är dels tillgänglig såsom en IT-tjänst att användas av applikationer & system såsom en identifieringstjänst (IdP), dels såsom en nedladdningsbart installationspaket för Linux samt Windows Server för lokal installation.

Aktuell leverans är 2.0 – 2.x för produktionsmiljön, acceptanstestmiljö samt utvecklingsmiljö. För åtkomst, se [Adresser](#).

Med leveransen medföljer även exempelkod för en SP (tjänsteproducent). Denna exempelkod kan tjäna såsom en guide hur man implementerar en SAML-autentisering i en e-tjänst. Se [Adresser](#) för åtkomst till kodexemplet.

Styrande SAML-specifikation, vilken bl.a beskriver vilka attribut etc som levereras i biljetten är beskrivet i dokumentet: SAMBI SAML specifikation, referens [R12]

F.o.m version 2.0 av Säkerhetstjänster levereras ingen SDK såsom en formell del av leveransen. Befintlig SDK från 1.6-versionen kommer dock under en övergångsperiod finnas tillgänglig för att stödja NPÖ's behov. e-tjänster (SP'n) rekommenderas att använda någon av de tillgängliga SAML-ramverk som finns såsom öppen källkod. Ex Open SAML eller OIOSAML, se ref [R22] & [R23].

Från och med version 2.3 Lokala Säkerhetstjänster finns det även stöd för rika klienter. Autentiseringstjänsten kommer då för rika klienter följa protokollet WS Trust 1.3. I leveransen ingår exempelkod för hur man integrerar sina rika klienter mot autentiseringstjänsten.

4.1.3 Förutsättningar för användning av tjänsten Autentisering

Metadata

För att kunna samverka med övriga e-tjänster i en SAML-federation och erhålla trust mellan en e-tjänst (SP) och Autentiseringstjänsten (IdP) behöver man samverka kring metadatahanteringen. Dvs dela metadata mellan ingående e-tjänster i SAML-federationen. När SAMBI-federationen är etablerad och Säkerhetstjänsterna är anslutna till denna federation kommer metadatahanteringen ske genom en metadataserver, som driftas och förvaltas av .SE. Tillsvidare kommer dock metadatahanteringen att ske manuellt genom CGI's försorg. Ansluten e-tjänst måste således vara registrerat i Säkerhetstjänsternas metadata. Genom metadata kan man ex. specificera vilka attribut man önskar få från IdP'n och utbyta vilka nycklar som ska användas, adresser vid utloggning etc.

För åtkomst till metadata, se [Adresser](#)

Sjunet/internet

Observera att Autentiseringstjänsten dels finns tillgänglig på Sjunet, dels på internet. Om man som SP är tillgänglig på båda näten så behöver man konfigurera åtkomst för bägge nätverken.



Portöppningar

Följande portar behöver öppnas/vara öppna för **full** användning av Autentiseringstjänsten :

Produktionsmiljö

Port	Adress	Nät	Notering
8443, 8444	idp.sakerhetstjanst.inera.se	Internet	Autentiseringstjänsten
7443, 7444, 7445, 7446	sakerhetstjanst.inera.se	Internet	Administration Spärr, log etc
8443, 8444	idp.sakerhetstjanst.sjunet.org	Sjunet	Autentiseringstjänst
7443, 7444, 7445, 7446	sakerhetstjanst.sjunet.org	Sjunet	Administration Spärr, log etc

OBS! Portarna 7445 & 7446 används f.n ej men KAN komma att användas vid anslutning till SAMBI

Acceptanstestmiljö

Port	Adress	Nät	Notering
8443, 8444	idp.acctest.sakerhetstjanst.inera.se	Internet	Autentiseringstjänsten
7443, 7444, 7445, 7446	acctest.sakerhetstjanst.inera.se	Internet	Administration Spärr, log etc
8443, 8444	idp.acctest.sakerhetstjanst.sjunet.org	Sjunet	Autentiseringstjänst
7443, 7444, 7445, 7446	acctest.sakerhetstjanst.sjunet.org	Sjunet	Administration Spärr, log etc

OBS! Portarna 7445 & 7446 används f.n ej men KAN komma att användas vid anslutning till SAMBI

För detaljerad information om portöppningar, se dokument: SÄK 2 1 Information om portöppningar

SAML-bindningar

Säkerhetstjänster rekommenderar att en e-tjänst väljer HTTP Post istället för HTTP Artifact då detta val bl.a innebär mindre beroende till brandväggsöppningar.

SITHS



Autentisering sker genom inloggning med SITHS-kort. Eftersom det under en övergångsperiod kommer att finnas 2st versioner av SITHS, V3 resp CA V1 så behöver både arbetsstationen och e-tjänsten ha root-certifikat för bägge versionerna installerade.

HSA

Samtliga användare som vill nyttja Autentiseringstjänsten måste finnas registrerade i HSA-katalogen. Om man i denna katalog har >1 uppdrag måste man i samband med inloggning välja något av de uppdrag man har². Den organisation som önskar använda tjänsterna måste även den vara beskriven i HSA.

² Fr o m version 2.3 av Lokala Säkerhetstjänster så är autentisering och uppdragsval separerade. Se Release Notes [R1].



4.2 Spärrtjänsten

4.2.1 Sammanfattning

Arkitekturen för Spärrtjänst medger att vårdgivare, landsting/kommuner och regioner kan hantera sina "egna" spärrar och inte göra sig beroende av en enda nationell tjänst, både vad gäller tillgänglighet och vad gäller anpassning till sina lokala förutsättningar i form av befintliga vårdsystem, portaler och motsvarande.

Spärrar hanteras därför på två nivåer:

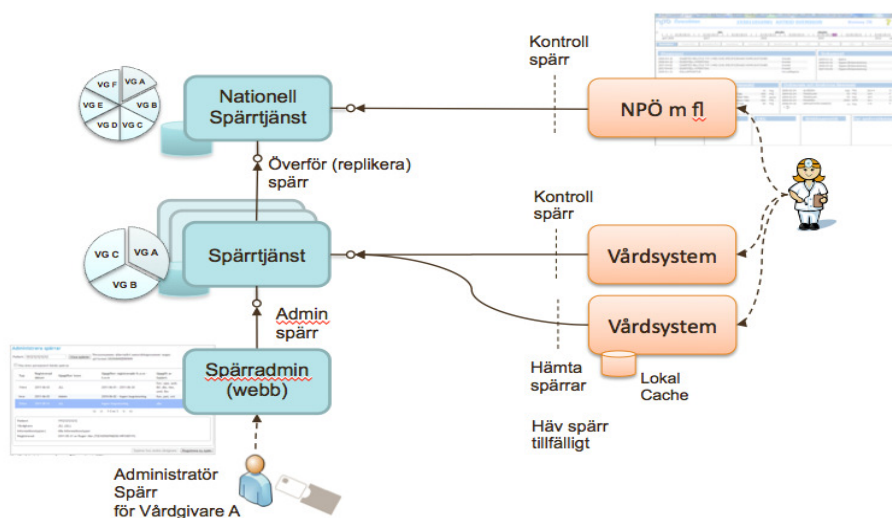
- **vårdgivarens Spärrtjänst** där spärren hanteras (registreras, hävs etc) för en eller flera vårdgivare. Spärrtjänsten kan vara en *lokal spärrtjänst* eller så nyttjas en *hotelltjänst* (molntjänst) för denna funktion.
- **nationell Spärrtjänst** samlar *kopior* med grundläggande data om *alla* spärrar genom replikering från vårdgivarnas spärrtjänster.

En vårdgivare kan således välja mellan att "hyra in sig" på det "nationella spärrhotellet" eller ladda ned och installera en lokal implementation av spärrtjänsten. Om vårdgivaren samverkar i sammanhållen journalföring, ex NPÖ behöver den lokala spärrtjänsten replikera sina spärrar till den nationella instansen av spärrtjänsten, detta för att ev spärrar på lokal nivå även ska spärra journalinformation i NPÖ.

OBS! Det åligger även det system som registrerar spärrar att logga denna händelse då tjänsten i sig ej gör detta.

För mer info, se SAD Spärrtjänst [R5] under [Referenser](#).

Spärrtjänsten interagerar med vårdsystemen genom Nationella tjänstekontrakt. Nationellt tjänstekontrakt används även för replikering av spärrar till den Nationella spärrtjänsten, se ref [R8] under [Referenser](#).





4.2.2 Leverans

Spärrtjänsten levereras enligt följande:

- Nationell spärrtjänst ("toppnod" där replikerade spärrar från lokala spärrtjänster lagras)
- Nationellt "spärrtjänsthotell" (tjänst för vårdgivare som ej önskar implementera lokal spärrtjänst)
- Lokal spärrtjänst (nedladdningsbar tjänst, Linux & Windows, för anslutning till lokala vårdsystem)
- Nationella Tjänstekontrakt (samtliga tjänstekontrakt för spärrtjänsten), se ref [R8]

För adresser till produktion, acceptanstest & utvecklingsmiljöer, se [Adresser](#).

4.2.3 Förutsättningar för att använda Spärrtjänsten

Spärrtjänsten har i princip 3st användningsfall:

- Nationella applikationer med sammanhållen journalföring (ex NPÖ)
- Lokala/regionala vårdsystem som har behov av spärrhantering på vårdgivarnivå. Detta kan ske genom att installera lokal spärrtjänst hos vårdgivaren, alt "hyra plats" på den nationella spärrtjänsten
- Administration av spärrar. Detta sker genom användande av GUI (websida). Vid lokal installation av spärrtjänst anropar man web-url till den lokala instansen. Vid användning av den nationella spärrtjänsten, anropas adressen till admin-gränssnittet till den nationella tjänsten. Se [Adresser](#)

Spärrtjänsten (oavsett lokal eller nationell tjänst) anropas via Nationella tjänstekontrakt, enligt RIV TA 2.1. Kommunikation sker via Tjänsteplattformen. För mer information kring tjänsterna, se ref [R8].

Kommunikation förutsätter SITHS funktionscertifikat. För information om aktuell SITHS-version, kontakta Säkerhetstjänsternas förvaltning. Anropande system måste ha ett HSA-id.

En lokal implementation av spärrtjänsten behöver vara ansluten till HSA-katalog via HSA-WS [R15] samt Personuppgiftstjänsten [R16]

Följande portar behöver öppnas:

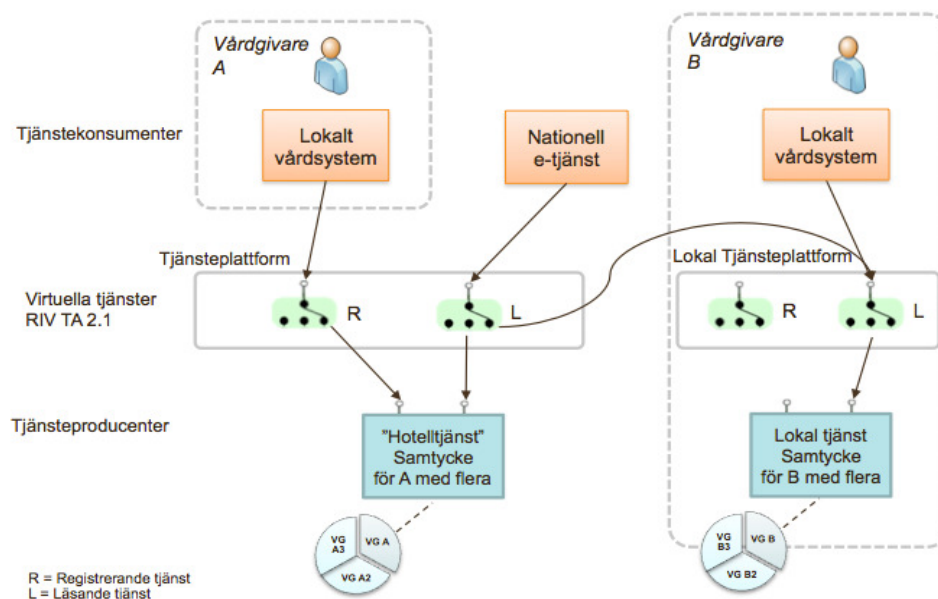
Produktion	Acceptanstest
7080	7080



4.3 Samtyckes & Patientrelationstjänsten

4.3.1 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 [R14]. Tjänster med motsvarande funktionalitet är idag i drift som stöd till Nationell Patientöversikt för att där hantera PDLs krav på samtycke och patientrelation.



4.3.2 Leverans

Samtyckes & patientrelationstjänsterna levereras dels som:

- En nationell "hotelltjänst" som man kan nyttja såsom vårdgivare med sitt vårdsystem om man ej önskar implementera en egen lokal instans
- Lokal Samtyckes & Patientrelationstjänst (nedladdningsbar tjänst, Linux & Windows, för anslutning till lokala vårdsystem)
- Nationella Tjänstekontrakt (se ref [R9] & [R10])

För adresser till produktion, acceptanstest & utvecklingsmiljöer, se [Adresser](#).



4.3.3 Förutsättningar för att använda Samtyckes & Patientrelationstjänsten

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. Alternativt kan man använda sig av Säkerhetstjänsternas tjänster.

Samtyckes/Patientrelationstjänsten anropas via Nationella tjänstekontrakt, enligt RIV TA 2.1. Kommunikation sker via Tjänsteplattformen. För mer information kring tjänsterna, se ref [R9 & R10].

OBS! Det åligger även det system som registrerar Samtycke/Patientrelation att logga denna händelse då tjänsten i sig ej gör detta.

Kommunikation förutsätter SITHS funktionscertifikat. För information om aktuell SITHS-version, kontakta Säkerhetstjänsternas förvaltning. Anropande system måste ha ett HSA-id.

En lokal implementation av Samtyckes/Patientrelationstjänsten behöver vara ansluten till HSA-katalog via HSA-WS [R15] samt Personuppgiftstjänsten [R16]

Följande portar behöver öppnas:

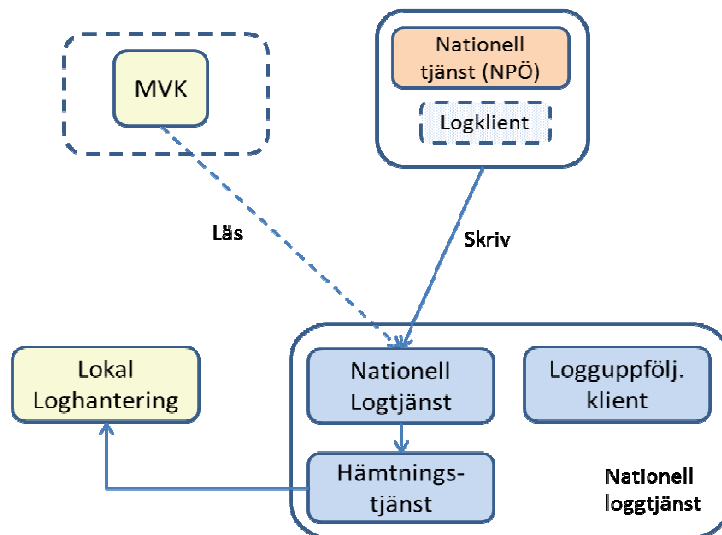
Produktion	Acceptanstest
7080	7080



4.4 Loggtjänsten

4.4.1 Sammanfattning

Säkerhetstjänsterna Central loggtjänsthantering syftar till att stödja processen att hantera kraven på uppföljning av verksamhetens åtkomst till patientinformation enligt Patientdatalagen och SOSFS 2008:14 §11 & §12. Modellen för detta baserar sig bl.a på PDLiP-arbetet samt utredningar av AL-S (AL-S Loggning i NPÖ) samt ett antal kravmöten med AL-S. Tjänster med motsvarande funktionalitet är idag i drift som stöd till Nationell Patientöversikt för att där hantera PDLs krav på loggning av åtkomst till vårdinformation.



4.4.2 Leverans

Loggtjänsten (se SAD, ref [R7]) levereras dels som:

- En nationell lagringstjänst för lagring av åtkomstinformation (åtkomstloggar) [R11]
- Läsande tjänster för åtkomst av åtkomstinformation [R11]
- Hämtningstjänst för ”bulkhämtning” av en vårdgivares åtkomstloggar för uppföljning i lokalt loggsystem [R17]
- GUI och loggrapporter för manuell uppföljning av åtkomstloggar [R7]

För adresser till produktion, acceptanstest & utvecklingsmiljöer, se [Adresser](#).



4.4.3 Förutsättningar för att använda Loggtjänsten

Den nationella loggtjänsten anropas dels via Nationella tjänstekontrakt, enligt RIV TA 2.1. Kommunikation sker idag direkt, dvs ej via Tjänsteplattformen, dels via ett speciellt tjänstekontrakt (ej RIV TA) såsom en Hämtningstjänst för överföring av åtkomstloggar till ett lokalt logguppföljningssystem. För mer information kring tjänsterna, se ref [R11 & R17].

Kommunikation förutsätter SITHS funktionscertifikat. För information om aktuell SITHS-version, kontakta Säkerhetstjänsternas förvaltning. Anropande system måste ha ett HSA-id.

Loggtjänsten finns från och med version 2.3 även som lokal tjänst.

Följande portar behöver öppnas:

Produktion	Acceptanstest
7080	7080



5. Adresser/URL

5.1 Exempelkod och nedladdnings-site

Tjänst	Adress	Kommentar
Nedladdnings-site	https://public.logica.com/~sakerhetstjanster/	Inloggningsuppgifter erhålles av CGI
Exempelkod SP	https://public.logica.com/~sakerhetstjanster_public/	user: public pwd: sak2013

5.2 Acceptanstest

Tjänst	Adress	Kommentar
Sjunet		
Autentisering	https://idp.acctest.sakerhetstjanst.sjunet.org:8443/idp/saml/sso/{binding}	
WEBadmin	https://acctest.sakerhetstjanst.sjunet.org:7443/spadmin	
Metadata IdP	https://idp.acctest.sakerhetstjanst.sjunet.org:8443/idp/saml	
Metadata SP	https://acctest.sakerhetstjanst.sjunet.org:7443/sp/saml	
Internet		
Autentisering	https://idp.acctest.sakerhetstjanst.inera.se:8443/idp/saml/sso/{binding}	
WEBadmin	https://acctest.sakerhetstjanst.inera.se:7443/spadmin	
Metadata IdP	https://idp.acctest.sakerhetstjanst.inera.se:8443/idp/saml	
Metadata SP	https://acctest.sakerhetstjanst.inera.se:7443/sp/saml	



5.2.1 Adresser tjänster för nationell Spärr, Samtycke, Patientrelation & Logg-acceptanstestmiljön (f.n enbart på Sjunet via direktanrop, ej via TP)

https://acctest.sakerhetstjanst.sjunet.org:7080/<tjänst_enligt_nedan>

Spärr Rivta 2.1
blockingNationalService/UnregisterTemporaryRevoke/2/rivtabp21
blockingNationalService/RegisterTemporaryRevoke/2/rivtabp21
blockingNationalService/UnregisterBlock/2/rivtabp21
blockingNationalService/RegisterBlock/2/rivtabp21
blockingNationalService/GetAllBlocksForPatient/2/rivtabp21
blockingNationalService/GetAllBlocks/2/rivtabp21
blockingNationalService/CheckBlocks/2/rivtabp21
blockingNationalService/PingForConfiguration/1/rivtab21

Samtycke Rivta 2.1
consentService/CancelExtendedConsent/1/rivtabp21
consentService/CheckConsent/1/rivtabp21
consentService/DeleteExtendedConsent/1/rivtabp21
consentService/GetConsentsForCareProvider/1/rivtabp21
consentService/GetConsentsForPatient/1/rivtabp21
consentService/GetExtendedConsentsForPatient/1/rivtabp21
consentService/PingForConfiguration/1/rivtab21
consentService/RegisterExtendedConsent/1/rivtabp21



Patientrelation Rivta 2.1

patientrelationService/GetPatientRelationsForCareProvider/1/rivtabp21

patientrelationService/GetPatientRelationsForPatient/1/rivtabp21

patientrelationService/DeleteExtendedPatientRelation/1/rivtabp21

patientrelationService/CancelExtendedPatientRelation/1/rivtabp21

patientrelationService/RegisterExtendedPatientRelation/1/rivtabp21

patientrelationService/GetExtendedPatientRelationsForPatient/1/rivtabp21

patientrelationService/CheckPatientRelation/1/rivtabp21

patientrelationService/PingForConfiguration/1/rivtab21

Logg Rivta 2.1

logService/StoreLog/1/rivtabp21

logService/PingForConfiguration/1/rivtab21

logQueryingService/GetInfoLogsForPatient/1/rivtabp21

logQueryingService/GetInfoLogsForCareProvider/1/rivtabp21

logQueryingService/GetAccessLogsForPatient/1/rivtabp21

logQueryingService/GetLogsForPatient/1/rivtabp21

logQueryingService/GetLogsForUser/1/rivtabp21

logQueryingService/GetLogsForCareProvider/1/rivtabp21

logQueryingService/GetLogReportsInfo/1/rivtabp21

logQueryingService/PingForConfiguration/1/rivtab21



5.3 Produktionstest

Tjänst	Adress	Kommentar
Sjunet		
Autentisering	https://idp.prodtest.sakerhetstjanst.sjunet.org:8443/idp/saml/sso/{binding}	
WEBadmin	https://prodtest.sakerhetstjanst.sjunet.org:7443/spadmin	
Metadata IdP	https://idp.prodtest.sakerhetstjanst.sjunet.org:8443/idp/saml	
Metadata SP	https://prodtest.sakerhetstjanst.sjunet.org:7443/sp/saml	
Internet		
Autentisering	https://idp.prodtest.sakerhetstjanst.inera.se:8443/idp/saml/sso/{binding}	
WEBadmin	https://prodtest.sakerhetstjanst.inera.se:7443/spadmin	
Metadata IdP	https://idp.prodtest.sakerhetstjanst.inera.se:8443/idp/saml	
Metadata SP	https://prodtest.sakerhetstjanst.inera.se:7443/sp/saml	



5.4 Produktion

Tjänst	Adress	Kommentar
Sjunet		
Autentisering	https://idp.sakerhetstjanst.sjunet.org:8443/idp/saml/sso/{binding}	
WEBadmin	https://sakerhetstjanst.sjunet.org:7443/spadmin	
Metadata IdP	https://idp.sakerhetstjanst.sjunet.org:8443/idp/saml	
Metadata SP	https://sakerhetstjanst.sjunet.org:7443/sp/saml	
Loggtjänsten StoreLog	https://sakerhetstjanst.sjunet.org:7080/logService/StoreLog/1/rivtabp21	
Internet		
Autentisering	https://idp.sakerhetstjanst.inera.se:8443/idp/saml/sso/{binding}	
WEBadmin	https://sakerhetstjanst.inera.se:7443/spadmin	
Metadata IdP	https://idp.sakerhetstjanst.inera.se:8443/idp/saml	
Metadata SP	https://sakerhetstjanst.inera.se:7443/sp/saml	



6. IP-adresser

DNS-namn	IP-adress	Kommentar
idp.sakerhetstjanst.sjunet.org	81.89.145.244	Produktionsmiljö
sakerhetstjanst.sjunet.org	81.89.145.246	
idp.sakerhetstjanst.inera.se	78.41.244.29	
sakerhetstjanst.inera.se	78.41.244.29	
idp.acctest.sakerhetstjanst.sjunet.org	81.89.145.245	Acceptanstestmiljö
acctest.sakerhetstjanst.sjunet.org	81.89.145.245	
idp.acctest.sakerhetstjanst.inera.se	78.41.244.31	
acctest.sakerhetstjanst.inera.se	78.41.244.31	
idp.prodtest.sakerhetstjanst.sjunet.org	81.89.145.252	Produktionstestmiljö
prodtest.sakerhetstjanst.sjunet.org	81.89.145.252	
idp.prodtest.sakerhetstjanst.inera.se	78.41.244.30	
prodtest.sakerhetstjanst.inera.se	78.41.244.30	
idp.utvtest.sakerhetstjanst.sjunet.org	81.89.145.251	Utvecklingstestmiljö
utvtest.sakerhetstjanst.sjunet.org	81.89.145.251	
idp.utvtest.sakerhetstjanst.inera.se	78.41.244.28	
utvtest.sakerhetstjanst.inera.se	78.41.244.28	



7. Referenser

Ref	Dokument ID	Dokument
R1	Releasenotes	Release Notes - Lokal Säkerhetstjänst
R2	Användarhandbok Lokala Säkerhetstjänster	Användarhandbok Lokala Säkerhetstjänster .pdf
R3	Installation & administration	Installation och administration - Lokala Säkerhetstjänster (linux).pdf
R4	SAD Autentiseringstjänsten	SAD Autentiseringstjänsten 2 0 V0.91.docx
R5	SAD Spärrtjänsten	SAD - Spärrtjänst PA4.docx
R6	SAD Samtycke & Patientrelation	SAD - Tjänster för Samtycke och Patientrelation 1.0.docx
R7	SAD Loggtjänsten	SAD - Tjänster för logghantering V0.7.docx
R8	Tjänstekontraktbeskrivning Spärrtjänsten	http://www.rivta.se
R9	Tjänstekontraktbeskrivning Samtyckestjänsten	http://www.rivta.se
R10	Tjänstekontraktbeskrivning Patientrelationstjänsten	http://www.rivta.se
R11	Tjänstekontraktbeskrivning Loggtjänsten	
R12	SAMBI SAML specifikation	http://www.inera.se/Documents/Infrastruktur/Infrastruktur/Sakerhetstjanster/Autentiseringstjanst/sakerhetstjanster_sambi_saml_profil_1.02.pdf
R13	RIV TA 2.1	http://www.rivta.se
R14	RIV PDLiP	http://www.cehis.se/images/uploads/dokumentarkiv/PDLiP_RIV_10_specifikation_110926.pdf
R15	HSA-katalogen	http://www.inera.se/ Befintlig koppling till HSA-tjänsten nyttjas i den webbapplikation som finns för administration av stödtjänsterna. Stödtjänsten själv nyttjar inte HSA-tjänsten. Notera att RIV TA Tjänstekontrakt för HSA är under utveckling och ska användas vid nya integrationer mot HSA, se även [B1], AB-4.
R16	Personuppgifter	Tjänstekontraktbeskrivning Personuppgiftstjänsten med tjänstedomän <code>population_residentmaster</code> . http://www.rivta.se



		<i>Tjänstekontrakt som nyttjas för att hämta personuppgifter om patienter.</i>
R17	Hämtningstjänst åtkomstloggar	Hämta loggarkiv_PA5.pdf
R18	Testrapport - Lokala Säkerhetstjänster	https://service.projectplace.com/pp/pp.cgi/d837121981/Testrapport%20-%20Lokala%20S%C3%A4kerhetstj%C3%A4nster.pdf?save_as=1
R19	Acceptanstestprotokoll	
R20	RIV TA Referensapplikation -Java	http://www.rivta.se
R21	RIV TA Referensapplikation Microsoft	http://code.google.com/p/rivta/wiki/RefAppBasicProfileWcf
R22	OpenSAML	https://wiki.shibboleth.net/confluence/display/OpenSAML/Home
R23	OIOSAML	http://www.ohloh.net/p/oiosaml



8. FAQ, exempel

Nedan följer ett exempel på typiska frågor kring anslutning till IdP'n:

Vad är det minsta som NPÖ behöver klara?

- a. Finns det någon Utility-SDK eller motsv för de funktioner som SP ska göra?
Ja det finns färdiga ramverk som man kan använda, där man enbart behöver konfigurera upp de enligt SAMBI-profilen. T.ex. opensaml eller oiosaml (som bygger på opensaml).
- b. export av SAML V2.0 Metadata dokument,
Som SP MÅSTE man på något sätt skapa metadata, antingen manuellt eller automatiskt. Publiceringen av metadata enligt "well known location" dvs på samma url som dess id (entitiy-id) är dock frivilligt. Se t.ex. säkerhetstjänsters metadata som man direkt kan hämta ifrån tjänsten på <https://acctest.sakerhetstjanst.inera.se:8443/idp/saml>
Som SP räcker det dock att man förmedla tjänstens metadata t.ex. via mail till IdP:ns förvaltningsorganisation.
- c. signera <saml2p:AuthnRequest> meddelandet
Ja det är krav enligt sambi-profilen att man som SP signerar AuthnRequest meddelandet.
- d. SP använder Identity Discovery Profile [SAML2Prof], d.v.s. common-domain cookie, för att erhålla aktörens SSO IdP
Ja det är krav enligt sambi-profilen att man ska använda sig av Identity Discovery Profile för att komma till "rätt" IdP. Dock skulle man kunna skjuta på denna implementation till ett senare tillfälle då vi ännu inte har fått den gemensamma domänen där alla tjänster ska ligga! Denna puck ligger hos Inera och vi har lyft denna till er(björn skeppner!) förut. Finns ju bara en IdP än sålänge också...
- e. SP SKALL signera begäran
Ja, samma som c.
- f. SP SKALL stödja HTTP-Post
För SSO response, ska SP stödja http-POST eller http-artifact. För SLO ska SP stödja http-Post.
- g. hantera "unsolicited responses"

Ja en SP ska stödja "unsolicited responses", om man ska prioritera så är detta något man kan implementera senare.



h. SP SKALL signera samt verifiera signaturen

Korrekt

Pkt9 Enligt sambi ska SP stödja SLO. Rent tekniskt är det ju inget måste för att få SSO att fungera,(utan konsekvensen blir ju att man som användare kan jobba med olika medarbetaruppdrag i två applikationer som bägge är anslutna till autentiseringstjänsten, vilket inte ska gå ifall bägge SP:ar har stöd för SLO.) Däremot måste man ju ha SLO för att kunna få till att göra ett uppdragsval på nytt.