Användarhandbok Spärradministration

Dokumenthistorik

Expandera...

Datum	Version	Namn	Förändring
27 Jan 2021	1.0	Okänd användare (lexhagenm)	Första version
22 Mar 2021	1.1	Okänd användare (lexhagenm)	Uppdaterat med behörighetsinformation
23 Nov 2021	1.2	Okänd användare (lexhagenm)	Lagt till information om stöd för inloggning med nya SITHS eID-metoderna
04 Apr 2023	1.3	Peter Leader Emma Fridén	Tagit bort en rad i inledningstabellen

Innehåll

- Adresser
- Inledning
- Begrepp
- Behörighet
    - Inloggning
    - Behörighetsgrundande egenskaper i HSA

Adresser

Produktion: https://sparradmin.inera.se

Test: https://sparradmin.ineratest.org (kräver särskilt SITHS-kort för testmiljöer)

Inledning

En spärr skapas för att neka åtkomst till patientuppgifter. Spärren gäller alla informationstyper men informationstyperna *Uppmärksamhetsinformation* och *L äkemedel – Ordination/förskrivning* kan undantas från spärren. Spärren kan gälla oavsett när uppgifterna registrerats eller för ett begränsat datumintervall.

Typ	Beskrivning
Läkemedelsordination/förskrivning	Information om läkemedelsordination/förskrivning och till dess kopplade administration av läkemedel som utförs inom hälso- och sjukvården. Med läkemedelsordination menas ”ordination som avser läkemedelsbehandling” [Ref 1].
Uppmärksamhetsinformation	Information som avser något som avviker från det man normalt kan förvänta sig och som påverkar handläggningen av vård eller omsorg. Uppmärksamhetsinformationen ligger till grund för en uppmärksamhetssignal [Ref 1]

En spärr innebär att patientuppgift/er på angiven vårdenhet (inre spärr) eller vårdgivare (yttre spärr) blir spärrad för de aktörer som arbetar "utanför" denna vårdenhet eller vårdgivare.

Tjänsten Spärradministration erbjuder funktionalitet för att administrera och använda spärrar i vårdsystem. Administration av spärrar genomförs av personer som innehar rollen för spärradministration.

Skapade spärrar kan användas av andra vårdsystem som vill hantera spärrar och kontrollera om vårdsystemets patientuppgifter är markerad som spärrad för vissa medarbetare.

Arbete i tjänsten Spärradministrations grafiska gränssnitt loggas enligt Patientdatalagen - PDL. Följande åtgärder/händelser loggas och utgör underlag för uppföljning:

- Registrera ny spärr
- Häva spärr permanent
- Tillfälligt häva spärr
- Makulera felregistrerad spärr

Begrepp

Tjänsten Spärradministration omfattar följande verksamhet och begrepp:

Begrepp	Beskrivning
Spärr	En spärr beskriver vissa patientuppgifter som avses vara spärrade. Spärren beskriver bland annat vilken patientinformationen gäller, när i tiden denna information registrerats etc. Informationen spärras för en viss organisation såsom en vårdgivare och/eller vårdenhet. En patient kan ha flera aktiva spärrar som alla gäller "tillsammans". En spärr kan aldrig ändras, utan den måste i så fall hävas/makuleras och registreras på nytt. En spärr är av typen inre eller yttre. En yttre spärr spärrar information för alla medarbetare/personal utanför den angivna vårdgivaren. En inre spärr spärrar information för all personal utanför den angivna vårdenheten och är en snävare spärr än den yttre.
Tillfällig hävning av spärr	En tillfällig hävning syftar till att tillfälligt åsidosätta en spärr för en viss medarbetare/personal, eller alla medarbetare på en viss vårdenhet. En spärr kan ha ett flertal tillfälliga hävningar som gäller för olika medarbetare. En tillfällig hävning har ett slutdatum då hävningen automatiskt upphör att gälla. Slutdatumet får inte vara längre fram än 7 kalenderdagar. En tillfällig hävning kan permanent återkallas och kan då aldrig bli aktiv igen.
Permanent hävning av spärr	En permanent hävning görs då en tidigare spärr inte längre skall gälla beroende på att patienten inte önskar ha sin information spärrad eller liknande orsak. En permanent hävd spärr kan aldrig bli aktiv igen.
Makulera spärr	En spärr tas bort i det fall spärren felregistrerats och markerar att spärren aldrig skulle ha existerat. En makulerad spärr kan aldrig bli aktiv igen.

En spärr kan, till exempel vid en nödsituation, tillfälligt hävas. Patientens spärrade uppgifter blir då tillgängliga för en eller flera medarbetare på specificerad vårdenhet. Den tillfälliga hävningen är tidsbegränsad och kan återkallas innan tidsbegränsningen gått ut.

Det finns två olika typer av tillfälliga hävningar av en spärr:

- Nödöppning - En tillfällig hävning av spärr som sker utan patientens samtycke, t.ex. vid en nödsituation.
- Patienten ger samtycke - En tillfällig hävning av spärr som sker med patientens samtycke till registreringen.

En spärr kan hävas permanent vilket är oåterkalleligt.

Behörighet

Behörig medarbetare kan:

- Registrera spärr
- Söka uppgifter gällande spärr
- Häva spärr permanent
- Tillfälligt häva spärr
- Ta bort tillfällig hävning
- Makulera felregistrerad spärr
- Visa alla spärrar hos egen vårdgivare
- Visa om patienten har spärrar registrerade hos andra vårdgivare

Test-miljöer kräver särskilda tjänstekort

För testmiljöer kan man inte använda sitt vanliga tjänstekort utan här krävs ett särskilt SITHS-kort för test.

Det är också viktigt att det är ett "riktigt testkort" och inte ett "reservkort" då det inte är tillåtet att administrera spärrar med reservkort.

Mer information om SITHS-kort och hur man beställer sådana finns på Ineras hemsida...

Inloggning

Inloggning sker via Ineras IdP som erbjuder tre olika sätta att identifiera sig. Dels det klassiska sättet med SITHS-kort i kortläsare och NetId installerat på datorn man loggar in ifrån.

Fr.o.m 1 december 2021 finns även möjlighet att använda de nya SITHS eID-metoderna där man kan logga in med hjälp av appar på dator eller mobiltelefon som mer liknar upplevelsen man får via inloggning m.h.a BankID.

Observera

För att det ska vara möjligt att logga in m.h.a de nya metoderna måste er Region ha anslutit sig till dessa och installerat SITHS eID-appen på din dator och/eller mobiltelefon.

-Har du inte fått någon information om detta från er Region så välj det tredje alternativet i valet av inloggningsmetod:
Legitimera dig med: Net iD på **denna** enhet med SITHS e-legitimation.



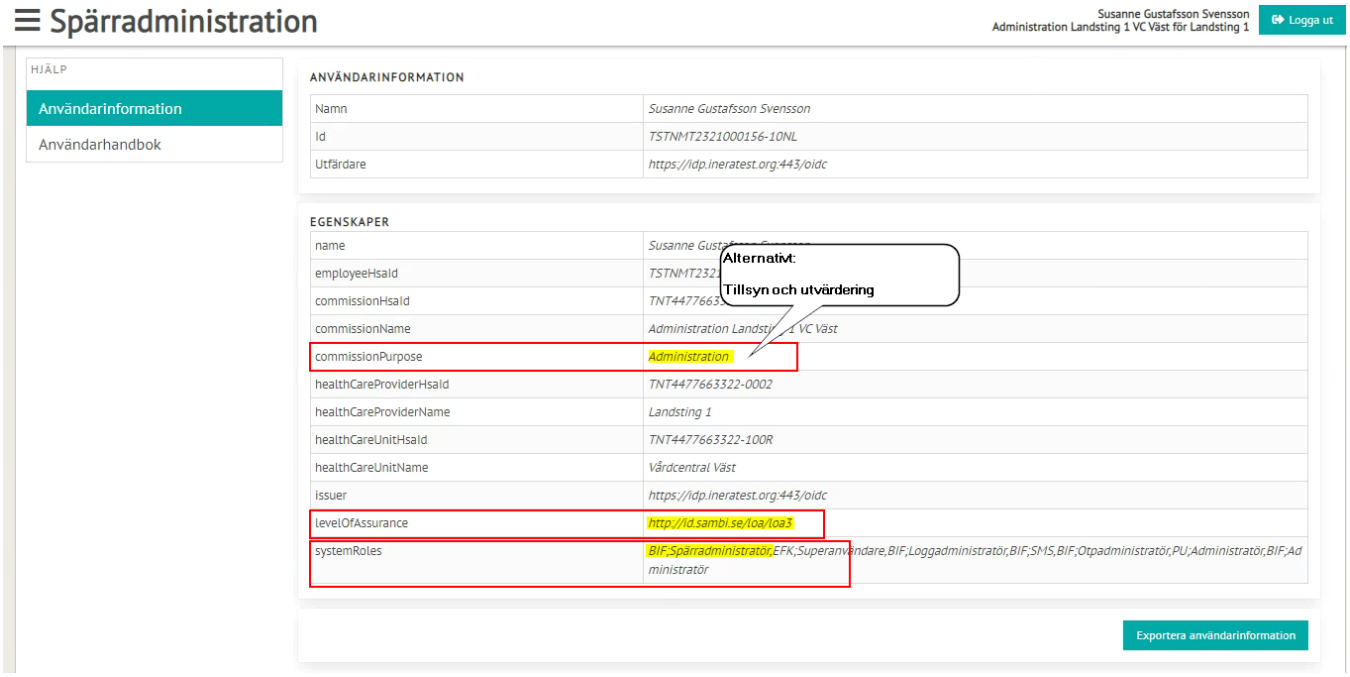
Behörighetsgrundande egenskaper i HSA

För att vara tekniskt behörig att administrera spärrar finns tre kriterium:

1. Du skall i HSA ha **Systemrollen** (*systemRoles*) "BIF;Spärradministratör".
2. Du skall logga in i tjänsten med ett medarbetaruppdrag med **Syfte** (*commissionPurpose*) "Administration" eller "Tillsyn och utvärdering". Uppdraget måste dessutom vara knutet till en vårdenhet.
3. Du skall logga in i tjänsten med ett SITHS-kort som är utgivet med **Tillitsnivå 3** (*levelOfAssurance*). Värdet visas som *http://id.sambi.se/loa/loa3* där **loa3** är ett krav för spärradministration. Bland annat blir t.ex ej uppgraderade äldre SITHS-kort samt Reservkort LoA 2 vilket betyder att dessa inte kan användas för spärradministration sedan januari 2021 - Ny LoA-hantering för SITHS-kort 2021. Mer information om vilka korttyper, eller rättare sagt certifikatstyper, som ger vilken LoA-nivå finns på IdP:ns sida Tillitsnivå (LoA)

Har man loggat in i tjänsten men inte får se några Spärr-menyer så är inte alla tre kriterier uppfyllda. Uppgifterna kommer från inloggningen via Ineras IdP som i sin tur hämtar uppgifterna om Roll och Syfte från HSA-katalogen.

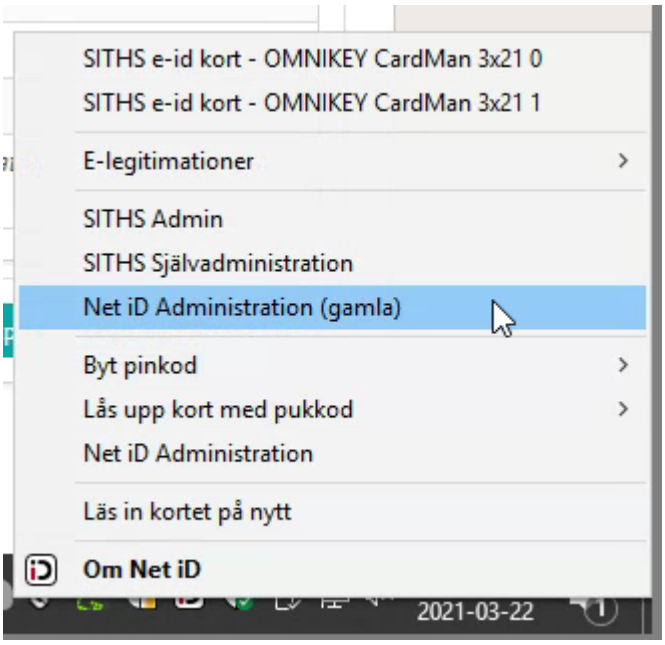
Under fliken Användarinformation kan man se vilka egenskaper man har fått efter inloggning och kan där jämföra dessa med behörighetskraven. Vid kontakt med supporten kan man ta en skärmbild av dessa eller exportera alla uppgifter till en fil med hjälp av knappen Exportera användarinformation och bifoga detta till supportärendet.



Klicka på bilden för en större version

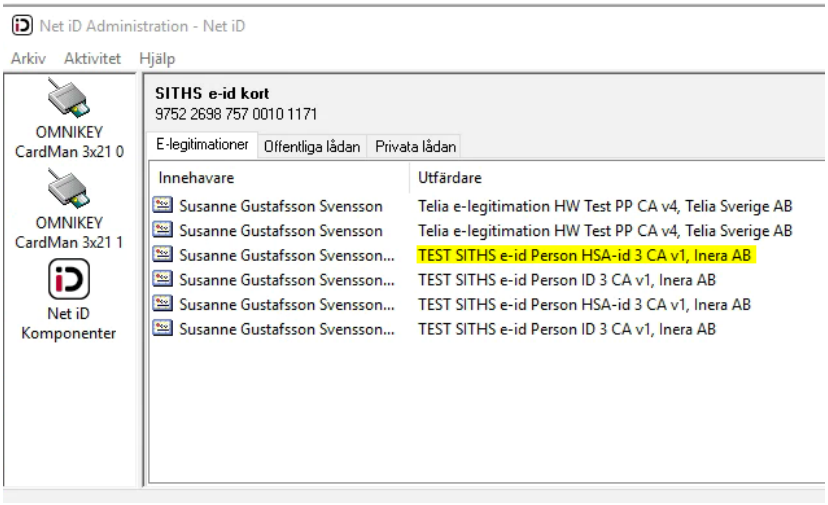
Ifall man saknar Systemroll eller Medarbetaruppdrag med rätt syfte så får man kontakta sin HSA-Administratör.

LoA-nivå kommer också från IdP-inloggningen men beror på vilken typ av kort/certifikat som använts. Ifall tillitsnivån är för låg kan man via NetId-applikationen kontrollera vilka typer av certifikat som ligger på SITHS-korten man använder. Högerklicka på NetId-symbolen och välj **Net iD Administration (gamla)**.



Nu ska de certifikat som ligger på kortet i kortläsaren listas. Kontrollera att där finns ett LoA-3-certifikat som Ineras IdP godtar.

För SITHS e-id-certifikaten ingår LoA-nivå i namnet. I certifikatsnamnet *SITHS e-id Person HSA-id **3** CA v1* säger trean att certifikatet är utgivet med tillitsnivå/LoA 3 vilket alltså är ett krav för att använda gränssnittet för Spärradministration.



Figur: I detta fall har användaren satt i ett kort för TEST-miljöer.

Läs mer om att arbeta i tjänsten Spärradministration:

- 1. Söka spärrar
- 2. Registrera spärrar
- 3. Häva spärrar
- 4. Skapa rapporter med spärrar
- 5. Kopiera spärrar