Instruktion för att kunna använda Säkerhetstjänsternas administrationsgränssnitt

Instruktion för att kunna utnyttja funktioner i Säkerhetstjänsterna

Denna instruktion beskriver vilka tekniska förutsättningar som gäller för att komma åt Säkerhetstjänsterna och hur man i HSA sätter upp behörigheten som behövs för att kunna utnyttja funktioner i Säkerhetstjänsterna.

Instruktionen visar hur olika administratörer får tillgång till de användargränssnitt som Säkerhetstjänsterna tillhandahåller.
Denna instruktion täcker följande roller:

- Loggadminstratör
- Spärradministratör
- Samtyckesadministratör

I dokumentet refereras dessa roller som ”Administratören” när informationen gäller alla roller.

Dokumenthistorik

Version	Författare	Kommentar
1.0	Tomas Fransson	Slutversion
1.1	Tomas Fransson	Uppdaterat länkar till 2.1-versionen av SÄK i kap 3
1.2	Tomas Fransson	Referens till Portöppnningsdokumentet för att bättre förklara förutsättningarna för 2.1
1.3	Tomas Fransson	Döpt om dokumentet, ny huvudrubrik
1.4	Tomas Fransson	Korrigerat URL till Sjunet
1.5	Tomas Fransson	Uppdaterat referens till Portförändringsdokumentet
1.6	Tomas Fransson	Uppdaterat referens till Webadmin-GUI efter produktionssättning av 2.6.1
1.7	Henrika Littorin	Uppdaterat information om HSA
1.8	Tomas Fransson	Revidering efter Henrikas kommentarer
1.9	Tomas Fransson	Överfört till Confluence
1.10	Tomas Fransson	Kompletterat med information om behörighet för samtyckesadministration
1.11	Tomas Fransson	Ändrat information i samband med att Spärrtjänsten blev en fristående tjänst.
1.12	Magnus Lexhagen	Lagt till information om krav på SITHS-kortens tillitsnivå (LoA)
1.13	Magnus Lexhagen	Lagt till info och adresser till Samtyckestjänsten samt stuvat om lite.
1.14	Magnus Lexhagen	Lagt till information om stöd för inloggning med nya SITHS eID-metoderna

1. Inledning

Administratören behöver tillgång till Säkerhetstjänsternas användargränssnitt.

För att administratören ska kunna arbeta behöver organisationen vara ansluten till Säkerhetstjänsterna.

Som administratör behöver man ha

- giltigt SITHS-kort med tillitsnivå 3* och tillhörande inloggningskoder.
- åtkomst till Säkerhetstjänsternas administratörsverktyg.
- registrerade behörighetsegenskaper i HSA.

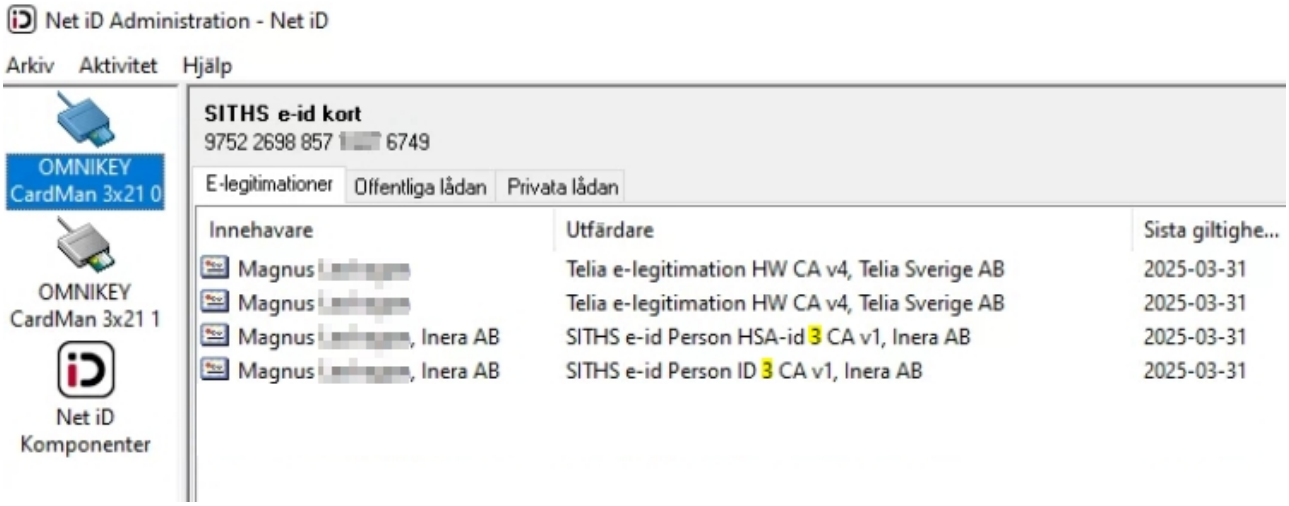
Denna instruktion ger information om hur organisationen skapar förutsättningar för att kunna agera som administratör i Säkerhetstjänsterna.

* Tillitsnivå, eller LoA-nivå från det tekniska begreppet *Level of Assurance,* beskriver tilliten till sättet som kortet har givits ut. T.ex så har "reservkort" ofta LoA 2 vilket alltså är en för låg tillitsnivå för att kunna användas för att administrera Spärrar, Loggar och Samtycken i Säkerhetstjänster.

2. SITHS-kort

Saknar administratören giltigt SITHS-kort alternativt att man inte har sina koder kontaktar man den egna enheten för utgivningen av SITHS-kort.

SITHS-kortet skall vara utgivet med minst tillitsnivå (LoA) 3. Namnet på eid-certifikatet brukar avslöja LoA-nivån. *SITHS e-id Person HSA-id **3** CA v1* ger LoA 3 medan *SITHS e-id Person HSA-id **2** CA v1* ger LoA 2.



Mer om SITHS-kort finns att läsa på Ineras webbplats: www.inera.se.

3. 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.

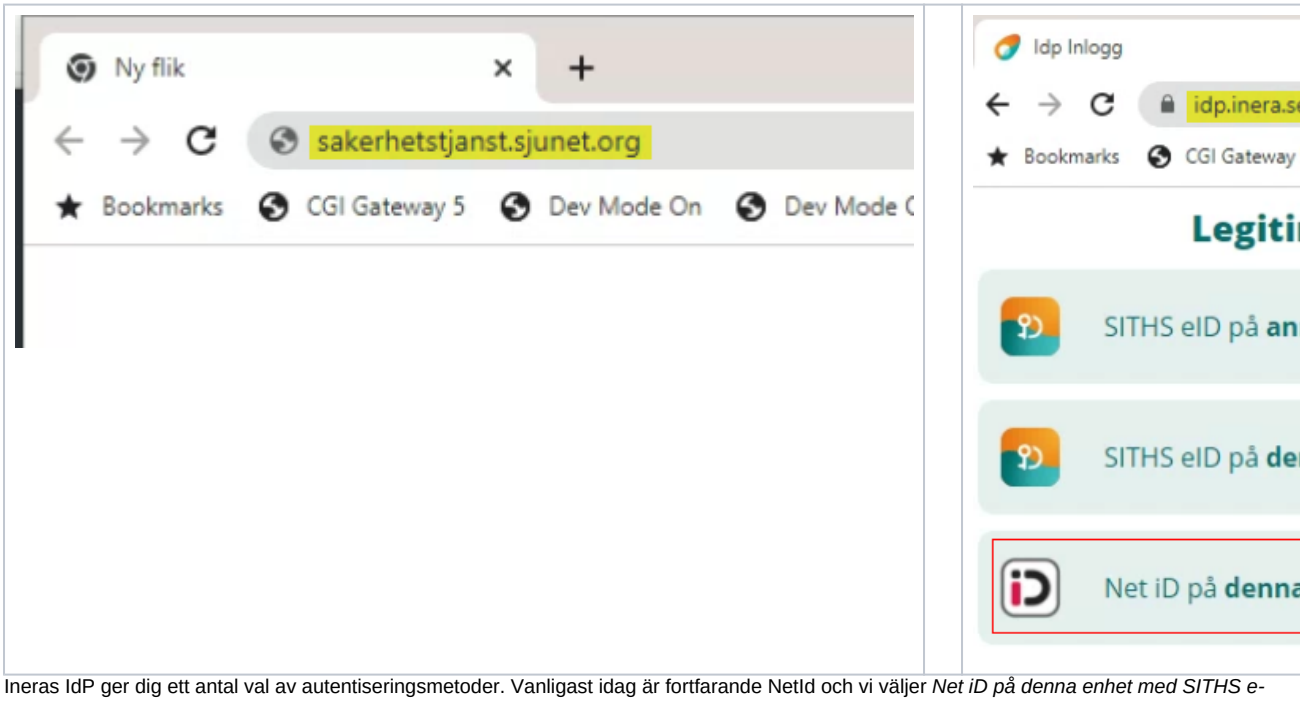
Observera

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.

3.1. Inloggningsflöde NetId

1. När du surfar in på någon av Säkerhetstjänsters adresser utan att vara inloggad så detekterar tjänsten detta och dirigerar om dig till Ineras IdP.



2. Ineras IdP ger dig ett antal val av autentiseringsmetoder. Vanligast idag är fortfarande NetId och vi väljer *Net iD på denna enhet med SITHS e-legitimation* för detta flöde.

3. När man klickar på Net iD-valet ovan så dirigeras man om till en adress som kräver att du identifierar dig med ett certifikat. Den tekniken kallas för mTLS och används av Net iD för att föra över certifikatet på ditt SITHS-kort till IdP:n.

4. När IdP:n har läst ut ditt HSA-id från certifikatet som NetID har skickat över så hämtar IdP:n dina uppgifter från HSA.

5. Har du flera medarbetaruppdrag i HSA så blir du nu omdirigerad till en sida med medarbetaruppdragsval. Har du bara ett medarbetaruppdrag väljs detta automatiskt. Säkerhetstjänster kräver att du har minst ett medarbetaruppdrag som matchar informationen i kapitlet nedan.

6. När medarbetaruppdraget är valt så kan IdP:n sätta ihop en "biljett" som berättar vem du är. Du blir nu slutligen omdirigerad till Säkerhetstjänster igen. I bakgrunden skickas din biljett från IdP:n med så att Säkerhetstjänster kan kontrollera att du är behörig.

4. Behörighetsgrundande egenskaper i HSA

Varje person som ska vara administratör måste finnas upplagd i HSA. Personen måste också ha verksamhetschefens uppdrag att få åtkomst till patientinformation i ändamålet Administration samt att vara Spärr- Logg- eller Samtyckes-administratör.

Administration i HSA görs av lokala HSA-administratörer i den egna organisationen, antingen via det nationella administrationsgränssnittet HSA Admin eller via ett administrationsgränssnitt mot den lokala HSA-katalogen. Kontakta din lokala HSA-förvaltning för att få veta vad som gäller hos er.

Informationen från HSA läses av adminstrationsgränssnitten för spärr, samtycke och logg. För att effektivisera hanteringen så cachar administrationsgränssnitten informationen. Det betyder att det kan ta upp till fem minuter innan en ändring i HSA-katalogen slår igenom. Det tillkommer dessutom tid för överföringen från den lokala HSA-katalogen till den nationella. Man måste räkna med ytterligare några minuter för denna tid, sammantaget ska ändringen slå igenom inom tio minuter.

4.1. Medarbetaruppdrag med rättigheter för spärr- samtycke- och loggadministration

Medarbetaruppdrag är den tekniska beskrivningen av verksamhetschefens individuella behörighetstilldelning i enlighet med Patientdatalagen. Verksamhetschefen för en vårdenhet beslutar att en medarbetare för att kunna utföra sitt arbete behöver åtkomst till patientdata och i vilket ändamål. För att få åtkomst till loggfunktionen krävs att administratören har verksamhetschefens tillåtelse/uppdrag att läsa patientdata i ändamålet Administration, d.v.s. **Spärr/Logg/Samtyckes-administratören är av kopplad till ett medarbetaruppdrag med ändamålet Administration**.

För mer information om hur detta hanteras i HSA, se Handbok för HSA-administratörer på www.inera.se alternativt den egna organisationens handbok för det lokala administrationsgränssnittet.

Notera att medarbetaruppdraget ska registreras på vårdenhetsnivå. Verksamhetschefen för den vårdenheten inom vårdgivaren vidtalas och står för uppdragsgivandet till de Loggadministratörer som kommer att arbeta för hela vårdgivaren. Eftersom Loggdata betraktas som patientdata måste verksamhetschefen för de medarbetare som arbetar som administratörer följa upp deras arbete. Detta möjliggöras genom den loggning som sker i administrationsgränssnittet.

4.2. Individuell egenskap för it-tjänster

Utöver medarbetaruppdraget med ändamålet Administration krävs även att ett värde läggs in i attributet ”Individuell egenskap för it-tjänster”. Följande värden ska användas:

Roll	Värde
Loggadministratör	BIF;Loggadministratör
Spärradministratör	BIF;Spärradministratör
Samtyckesadministratör	BIF;Samtyckesadministratör

För mer information om hur detta hanteras i HSA, se Handbok för HSA-administratörer på www.inera.se alternativt den egna organisationens handbok för det lokala administrationsgränssnittet.

5. Förutsättningar för åtkomst till Säkerhetstjänsterna

5.1. Adresser

5.1.1. Spärrtjänsten

Samma adress från Sjunet och Internet

Miljö	Adress
PROD	https://sparradmin.inera.se
TEST	https://sparradmin.ineratest.org

5.1.2. Loggtjänsten

Samma adress från Sjunet och Internet

Miljö	Adress
PROD	https://loggtjanst.inera.se
TEST	https://loggtjanst.ineratest.org

5.1.3. Samtyckestjänsten

Samma adress från Sjunet och Internet

Miljö	Adress
PROD	https://samtyckestjanst.inera.se
TEST	https://samtyckestjanst.ineratest.org

5.2. Brandväggsöppningar

I Guiden för Säkerhetstjänster beskrivs IP-adresser som gäller för att få åtkomst till Säkerhetstjänsterna, i produktion och test.

I Guide till Ineras Spärrlösning återfinner du motsvarande information för Spärrtjänsten och Guide till Samtyckestjänsten gäller för Samtyckestjänsten.

Alla dokument som beskriver Säkerhetstjänster finns på www.inera.se.

6. Användarhandböcker

När accessen till respektive tjänst är uppsatt korrekt kan man läsa mer om hur man arbetar i tjänsternas gränssnitt i tjänsternas användarhandböcker.

- Spärrtjänsten
- Loggtjänsten
- Samtyckestjänsten