Användarhandbok Loggtjänsten

Dokumenthistorik

Expandera...

Datum	Version	Namn	Förändring
05 May 2022	1.0	Unknown User (lexhagenm)	Första version
14 Apr 2023	1.1	Unknown User (engstromf)	Korrigerat QA adress

Innehåll

Adresser

Produktion: https://loggtjanst.inera.se/

QA: https://loggtjanst.ineraqa.org

Test: https://loggtjanst.ineratest.org

Inledning

Syftet med Loggrapporttjänsten är att söka fram och presentera logginformation för att möjliggöra uppföljning av vad som gjorts i verksamheten.

En loggrapport skapas antingen som ett PDF-dokument eller som en XML datafil. PDF-dokumentet är tänkt att läsas direkt av en logg-administratör medan XML-formatet är tänkt att kunna läsas av annan mjukvara såsom kalkylprogram.

Flera loggrapporter kan beställas samtidigt. Ett statusfält indikerar ungefärlig tid till när loggrapporterna är klar. När statusfältet är grönt kan loggrapporten hämtas i webbgränssnittet. Behörig medarbetare kan:

- Hämta ny loggrapport
- Se lista och hämta beställda loggrapporter

En loggrapport ligger kvar i systemet 96 timmar efter det att den har beställts innan den automatiskt rensas bort

Följande åtgärder/händelser kan loggas i vårdsystem:

- Läsa
- Skriva
- Signera
- Radera
- Nödöppning
- Utskrift
- Vidimera

Behörighet

Behörighetsgrundande egenskaper i HSA

Behörig medarbetare kan beställa loggrapport innehållandes loggar som tillhör den vårdgivare medarbetaren loggat in för. Vårdgivaren ges av valt medarbetaruppdrag.

För att vara behörig krävs följande:

- Du skall i HSA ha den personliga **Systemrollen** (*systemRoles*) "BIF;Loggadministratör".
- 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.
- 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 loggadministration 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)

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.

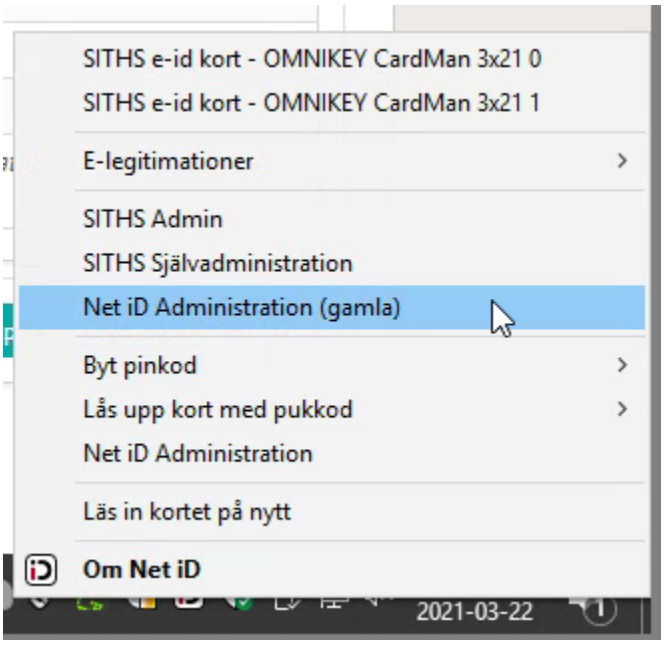
-Har du inte fått någon information om detta från er Region så välj det tredje alternativet i valet av inloggningsmetod:
Legitimera dig med: Net iD på **denna** enhet med SITHS e-legitimation.

Har man loggat in i tjänsten men inte får se några Logg-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.

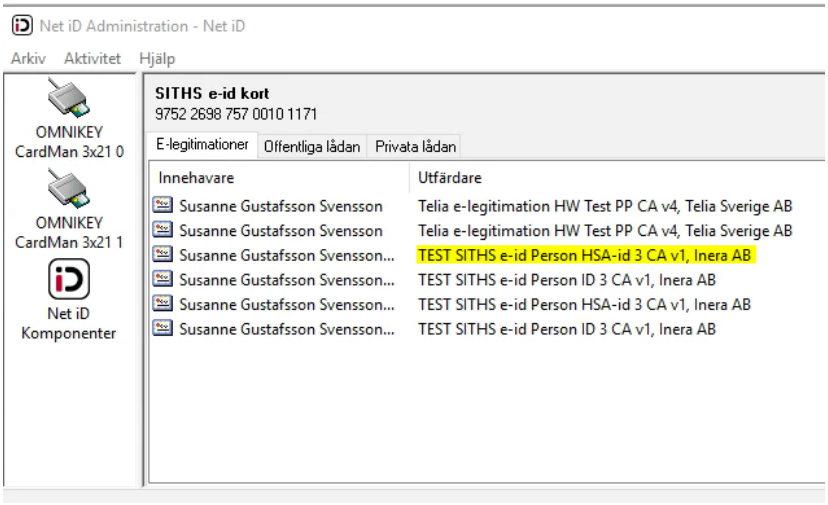
Ifall man saknar Systemroll eller Medarbetaruppdrag med rätt syfte så får man kontakta sin HSA-Administratör.

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 Loggadministration.



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