Checklista

Anslutning till NPÖ som konsument

Innehållsförteckning

Revisionshistorik		
Version	Författare	Kommentar
2.0	Madeleine Marklund	Fastställd version 2.0, efter godkännande av NPÖ införande på internet.
2.1	Madeleine Marklund	Reviderade uppgifter kring funktionscertifikat av SIHTS förvaltningen
2.2	Madeleine Marklund	Reviderad adress NPÖ internet
2.3	Ronny Nilsson och Patrik Sjöberg	Uppdateringar m a p * vad gäller för organisation som har SITHS och HSA ombud, * nya krav för SITHS CA v1 och Säkerhetstjänster 2.0 * samt tabellen för godkända operativsystem och webläsare
2.4	Patrik Sjöberg	Uppdatering av portinformation punkt 3.1 och 3.2

CHECKLISTA- ANSLUTNING TILL NPÖ SOM KONSUMENT

1. Inledning

Detta dokument är en **checklista** som ska vara en hjälp till införandeansvariga i landsting, kommun och privata vårdgivare för att möjliggöra anslutning till Nationell patientöversikt som konsument. Den i dokumentet använda termen NPÖ beskriver anslutningen till det nationella webgränssnittet ”NPÖ Tillämpning”.
Anslutning till NPÖ via lokalt vårdsystem och frågetjänst beskrivs i separat dokument.

Inera har ett införandestöd till de vårdgivare som ska ansluta till Nationell Patientöversikt och som nås på npo@inera.se.

Här i beskrivs vad som ska göras, medan det i refererade dokumenten förtydligar hur man gör det. Dokumentet är enbart en checklista för den tekniska anslutningen till NPÖ och de administrativa åtgärder man behöver göra.

För att personer ska kunna använda NPÖ krävs att han/hon finns upplagd i HSA och har ett SITHS-kort. Det krävs också att personen är kopplad till ett (eller flera) medarbetarmedarbetaruppdrag, samt att vissa specifika uppgifter om person och organisation är angivna i HSA.

2. Förklaringar

2.1. Inloggning/autentisering i NPÖ

För autentisering (d.v.s. inloggning och identifiering av användaren) används:

- SITHS-kort
- PIN kod
- Kopplad till Medarbetaruppdrag i HSA

2.2. Vad är Säkerhetstjänster?

Nationella IT-lösningar för vård- och omsorg måste garantera säkerhet, integritet och sekretess. Användare måste kunna identifieras och tillgång till information anpassas efter verksamhetschefens beslut. Det är krav som Patientdatalagen ställer. Det är i det sammanhanget som Säkerhetstjänsterna kommer in. Tjänsterna hjälper till att kontrollera att rätt person får tillgång till rätt information. För åtkomst till NPÖ används SITHS-kort med PIN kod för identifiering och HSA för att tala om vad personalen får göra via tilldelat medarbetaruppdrag. Loggfunktionen finns i Säkerhetstjänster.

2.3. Vad är HSA

HSA är en elektronisk katalog som innehåller grundläggande uppgifter om anställda och deras organisatoriska tillhörighet, men också uppgifter som beskriver den anställdes roller och medarbetaruppdrag inom vård- och omsorg.

När en person behöver ta del av till exempel vårdinformation, så används uppgifterna i HSA för att kontrollera att personen i fråga är anställd inom vården eller omsorgen, samt vilket medarbetaruppdrag och roll personen har. Därefter kan personen ta del av den efterfrågade informationen som han/hon är behörig till.

Ansvaret att hålla HSA uppdaterad är vårdgivarens (VG) och utförs av lokala HSA-administratörer.

Organisationen kan ha eget HSA-avtal med Inera eller vara tredjeparts-ansluten via ett ombud (kan vara ett landsting, kommun eller privat ombud). Om er organisationen är ansluten via ett HSA-ombud är det ert ombud som ska registrera uppgifterna för er i HSA.

2.4. Vad är SITHS

SITHS är en tjänstelegitimation, i form av ett plastkort, som innehåller elektroniska certifikat som bland annat används för att logga in i olika IT-system.

Organisationen som utfärdar legitimationen kan, förutom elektronisk ID-handling, förse kortet med text och grafik (namn, personnummer, foto, namnteckning, logotyp, med mera). Certifikaten möjliggör så kallade ”två-faktors-autentisering” vilket betyder att det inte bara räcker med att ha kortet som bevis för sin identitet, kortägaren måste också känna till en PIN-kod, för att identiteten ska anses vara bevisad.

Ansvarig för den lokala SITHS-organisationen benämns RA (Registration Authority).

Organisationen kan ha eget SITHS-avtal med Inera eller vara tredjeparts-ansluten via ett ombud (kan vara ett landsting, kommun eller privat ombud). Om er organisation är ansluten via ett SITHS-ombud är det ert ombud som utfärdar certifikat år er personal samt funktionscertifikat.

2.5. På vilket sätt fungerar SITHS och HSA ihop

Det elektroniska certifikatet som finns på SITHS-kortet bygger på uppgifter som finns i HSA-katalogen. Personen kan alltså inte få ett SITHS-kort om den inte finns med i HSA. När en person “loggar in” med hjälp av SITHS-kortet så görs först en kontroll av att certifikatet är giltigt. Är det giltigt så söks personen med det aktuella certifikatet upp i HSA-

katalogen. Därefter avgör de personliga uppgifterna i HSA-katalogen om personen har behörighet att ta del av den efterfrågade informationen.

2.5.1 Funktionscertifikat

På motsvarande sätt används HSA som utgångspunkt för att skapa funktionscertifikat, vilket är nödvändigt vid TGP-alternativet on-line (för TGP-alternativ se kapitel 2.7).

För att skapa ett funktionscertifikat måste vårdgivaren (landstinget, kommunen eller privata vårdgivaren) som har eget SITHS-avtal ha:

1. En gren i service (tjänste-) trädet i HSA. Om inte gren finns ansöker en direktansluten SITHS-organisation om en sådan gren via Ineras kundservice, se http://www.inera.se/kundservice/ .
2. En HSA-administratör över grenen i tjänsteträdet.
3. En SITHS-administratör med rollen RA eller ORA för grenen
4. Bevis att vårdgivaren (kommun, landsting eller privata vårdgivaren) äger domänen man tänker använda och att den person som ska utfärda certifikatet får utfärda certifikat för domänen (en domän i detta sammanhang är t.ex. vadstena.se eller om man ska gå över Sjunet blir adressen, vadstena.sjunet.org).

Vårdgivarens RA (Registration Authority) är den som har det lokala ansvaret för kort-och certifikathantering. Det är de som kan utfärda funktionscertifikat. Kontakta vårdgivarens RA för information kring funktionscertifikat. För frågor kring HSA så kontakta vårdgivarens HSA-förvaltning.

SITHS-ombud utfärdar enklast funktionscertifikat åt en tredjeparts-ansluten organisation under ombudets egen service-gren i HSA. Organisationen behöver visa att de äger domännamnet för ombudet (jmf punkt 4 ovan).

2.6. Anslutningsavtal NPÖ och Personuppgiftsbiträdesavtal

För att påbörja ett anslutningsprojekt tecknas en intresseanmälan med Inera.
För att få tillgång till sammanhållen journalföring via NPÖ krävs att vårdgivaren tecknar ett anslutningsavtal med Inera samt tecknar ett personuppgiftsbiträdesavtal för att Inera och dess underleverantörer ska få hantera vårdgivarens personuppgifter (t.ex. loggar).

Information om detta finns på denna länk med dokument under avsnitten ***Avtal*** och ***Intresseanmälan.*** Det kan påpekas att den avgift för införandetjänst som omnämns i anslutningsavtalet endast gäller anslutning som *producent* av information till NPÖ.

2.7. Tillgänglig patient (TGP) och Tjänsteplattform (TP)

För att söka en patient i NPÖ måste vårdgivaren (VG) etablera en TGP-tjänst. Den begränsar urvalet av patienter vårdpersonal kan söka information om. Denna funktionalitet är reglerad i patientdatalagen. Regelverket för den lokala TGP-tjänsten beslutas av verksamhetschefen.

Information om Tillgänglig patient (TGP) finns på denna länk med dokument under avsnittet ***Tillgänglig Patient (TGP).*** Där finns även beskrivning av tekniska krav för att tjänsten ska fungera.

Kommunikationen med centrala delen av TGP går via Tjänsteplattformen (TP) och anmälningsförfarandet av TGP och TP beskrivs i material (ovan).

Beroende på vilken TGP tjänst man vill ha, och om man ansluter via Sjunet eller Internet, fyller man i olika blanketter vid beställning av TP enligt nedan (Blanketterna finns i hänvisat material ovan).

Innan ifyllande av blankett C – ta kontakt med er leverantör för att klara ut vem som fyller i blanketten.

Om organisationen är tredjepartsansluten via SITHS-ombud rekommenderas i god tid beställa nödvändiga funktionscertifikat för de servrar som ska anslutas till online-tjänst.

OBS 1. Att den domän som används måste Domänvalideras av Inera om detta inte redan gjorts. Om organisationens domänen t ex ”tgp.storkommunen.sjunet.org” ska användas och kommunen inte redan reserverat domänen ”storkommunen.sjunet.org” kommer Inera (eftersom Inera kontrollerar den övergripande domänen ”sjunet.org”) göra det i samband med domänvalideringen.
Domänvalideringsunderlag skickas till Ineras kundservice.

OBS 2. DNS-entry måste beställas från Inera. Domänen i exemplet ovan ”tgp.storkommunen.sjunet.org” behöver läggas upp i Sjunets DNS så att Tjänsteplattformen sedan kan slå på den adressen och få ut servern Ip-nummer. Beställs hos Ineras kundservice.

Blanketter som ska fyllas i			
Val av TGP tjänst	**Variant av aktuell TGP tjänst**	**Blankett D**	**Blankett C**
Sjunet			
TGP0	Batch	Anmälan om koppling till TGP0 på Sjunet (beställning D)_(mall_v<v>).docx	Behövs ej
TGP0	Uthopp (Condis)	Anmälan om koppling till TGP0 på Sjunet (beställning D)_(mall_v<v>).docx	Behövs ej
TGP online Sjunet	Egen TGP Sjunet	Anmälan om koppling till TGP-On-Line på Sjunet (beställning D)_(mall_v<v>).docx	Anmälan om anslutning av TGP-On-Line (beställning C)_(mall_v<v>).docx
Internet			
TGP1	Batch	Anmälan om koppling till TGP1 på Internet (beställning D)_(mall_v<v>).docx	Behövs ej
TGP1	Uthopp (Condis)	Anmälan om koppling till TGP1 på Internet (beställning D)_(mall_v<v>).docx	Behövs ej
TGP1	Webb applikation (TGP webbadmin)	Anmälan om koppling till TGP1 på Internet (beställning D)_(mall_v<v>).docx	Behövs ej
TGP online Internet	Egen TGP Internet	Anmälan om koppling till TGP-On-Line på Internet (beställning D)_(mall_v<v>).docx	Anmälan om anslutning av TGP-On-Line (beställning C)_(mall_v<v>).docx

Förtydligande angående blanketterna: Blanketterna C och D är i grunden generella för alla tjänster som ansluts via tjänsteplattformen. Vissa fält är därför förifyllda för NPÖ och TGP. Med röd text (och X) anges vad som vårdgivaren själv ska fylla i. Notera att det som i tjänsteplattformen benämns *producentsystem* är TGP-tjänsten och *konsumentsystem* är NPÖ.

3. Checklista med kommentarer för anslutning till NPÖ

Syftet med checklistan är att ge de införandeansvariga i landsting, kommun och privata vårdgivare en hjälp att kontrollera att organisationen har utfört de aktiviteter som måste genomföras för att få tillgång till NPÖ.

Till varje punkt i checklistan finns kommentarer angivna för att ge en översiktlig information om respektive punkt. Till vissa punkter finns även hänvisning till dokument som ger en mer utförlig information om punkten i fråga.

För ytterligare information om anslutning till NPÖ hänvisas till denna länk med dokument.

☐ Ansluten till HSA

Direktanslutning till HSA: Din verksamhet har ansökt om anslutning samt tecknat avtal direkt med Inera.

Tredjepartanslutning till HSA via Landsting eller kommun: Din verksamhet har ansökt om anslutning samt tecknat avtal med en organisation som har en direktanslutning till HSA.

För mer information, se Anslutning till HSA.

Tredjepartanslutning till HSA via privat ombud: Din verksamhet har ansökt om anslutning samt tecknat avtal med Svensk e-identitet. För mer information, se HSA och SITHS som tjänst.

☐ Ansluten till SITHS

Direktanslutning till SITHS: Din verksamhet har ansökt om anslutning samt tecknat avtal direkt med Inera.

Tredjepartanslutning till SITHS via Landsting eller kommun: Din verksamhet har ansökt om anslutning och tecknat avtal med en organisation som har en direktanslutning till SITHS, ett så kallat ombud för SITHS.

För mer information, se Anslutning till SITHS- steg för steg.

Tredjepartsanslutning till SITHS via privat ombud: Din verksamhet har ansökt om anslutning samt tecknat avtal med Svensk e-identitet. För mer information se, HSA och SITHS som tjänst.

☐ Vårdgivare och vårdenheter registrerade i Tjänsteplattformen (TP)

Kommunikation med TGP går via TP.

HSA-ID för vårdgivaren (VG) samt samtliga vårdenheter (VE) med medarbetaruppdrag ska registreras. Dessa kan registreras på två sätt:

1. En registrering endast Vårdgivare, vilket då innebär att samtliga vårdenheter inkluderas.
2. En registrering per kombination av Vårdgivare och specifik vårdenhet. Dessa registreras dock

på en och samma blankett. Detta sätt behöver bara användas om det finns flera TGP-tjänster inom samma vårdgivare.

Vårdgivaren väljer själva det sätt som bäst passar deras verksamhet. Dessa kopplas sedan till den TGP tjänst som ska användas. Anmälan görs på blanketter C och D enligt tabell som visas i kapitel 2.7.

Blanketterna finns i en Zip fil som finns under http://www.inera.se/Vardtjanster/NPO/Dokument/ . Zip filen heter Material om tillgänglig patient, TGP.

☐ Tillgängliga patienter registrerade i TGP-Tjänsten

Vill du ha ytterligare en övergripande information om TGP kan du läsa ”Checklista TGP” som du också hittar på http://www.inera.se/Vardtjanster/NPO/Dokument/.

Gäller endast TGP Off-line metoden eller TGP webb-admin.

Beskrivning av TGP-tjänst och information om införande o förvaltning.

☐ SITHS-kort och kortläsare

Om medarbetarna inte har SIHTS kort, måste kort beställas. Läs mer här http://www.inera.se/Infrastrukturtjanster/SITHS/Anslutning/ Kommuner och landsting har ofta en etablerad SIHTS förvaltning. Tillbehör, så som kortläsare kan beställas via blankett Bilaga 1.1.1 Beställning 110328.doc av behörig beställare.

Om ni är tredjepartsanslutna till SITHS kontakta ert ombud.

☐ Systemkrav

Systemkraven beskrivs i separata punkter nedan.

☐ Krav på operativsystem och webbläsare uppfyllda

Javascript och Cookies ska vara påslaget (enable) i webbläsarna nedan.

Följande kombinationer (X) av operativsystem, webbläsare och Net iD stöds och supportas av Inera och Secmaker.

Operativsystem och webbläsare	Net iD				
	5.3	5.5	5.6.1	5.6.2	5.6.3
Windows XP (SP3)					
IE 7	X	X	X	ESK	X
IE 8	X	X	X	ESK	X
Firefox 3.6.24	ESK	X	X	ESK	X
Windows 7 (SP1) – 32-bit					
IE 7	ESK	X	X	ESK	X
IE 8	ESK	ESK	X	ESK	X
IE 9	ESK	ESK	ESK	ESK	ESK
Firefox 3.6.24	ESK	X	X	ESK	X
IE 10	ESK	ESK	ESK	ESK	ESK
Windows 7 (SP1) – 64-bit					
IE 7 -32-bit	ESK	X	X	ESK	X
IE 8 -32-bit	ESK	ESK	X	ESK	X
IE 9 -32-bit	ESK	ESK	ESK	ESK	ESK
IE 8 -64-bit	ESK	ESK	ESK	ESK	ESK
IE 10	ESK	ESK	ESK	ESK	ESK

ESK = Ej Supportad/Stödd Kombination, T= Under test

Andra kombinationer än ovan kan fungera, men stöds och supporteras inte av Inera och Secmaker. Om man har en annan kombination så ska man testa så att nedstängning av sessionen sker på ett korrekt sätt när SITHS-kortet rycks ur kortläsaren. Om så inte sker ska man uppdatera sin konfiguration enligt matrisen ovan.

☐	Krav på konfiguration vid blockering av ”popup-fönster”	Om webbläsarna konfigurerats med ”Aktivera blockering av popup-fönster” ska följande platser tillåtas: www.npo.se (medger åtkomst via internet) npo.sjunet.org (medger åtkomst via Sjunet)
☐	Krav på Net iD uppfyllda, Net iD installerat på arbetsstationer som ska nå NPÖ	Net iD installerad som CSP-programvara (programvara för att läsa SITHS-kort). Använd Net iD version enligt matris ovan. Rekommendationen är att man använder senaste version av Net iD enligt matris. Om organisationen har en direktanslutning till SITHS (har avtal med Inera) så finns det på SITHS projektplats installationspaket att ladda ner som innehåller rätt inställningar i Net iD (enbart RA-organisationen, Registration Authority har tillgång till detta). I vissa fall kan man ha gjort lokala anpassningar av Net iD. Den information som behöver finnas i **Net iD:s konfigurationsfil (iid.cfg) under C:/program/Net iD** för att automatisk nedstängning av webbläsaren ska fungera är: [NetControl] Applications=iexplore.exe;firefox.exe; iidxweb.exe Ask=0 Enable=1

3.1. **Sjunet** – Brandväggsöppningar åtkomst till NPÖ

☐ Brandväggar öppnade

För att komma åt **NPÖ** via Sjunet krävs att följande brandväggar är öppna:

NPÖ:
utgående (till NPÖ)
https://npo.sjunet.org
Port: **443**
IP: **81.89.147.11**

Säkerhetstjänsterna:

Till och med 2013-04-20: utgående (till Säkerhetstjänsterna)
https://cluster.bif.sjunet.org

Port: **8443** och **8444**

IP: **81.89.145.244**

Från och med 2013-04-20 då Säkerhetstjänster 2.1 tas i drift: utgående (till Säkerhetstjänsterna)

https://sakerhetstjanst.sjunet.org

Port: **7443, 7444, 7445 och 7446**

IP: **81.89.145.246**

https://idp.sakerhetstjanst.sjunet.org

Port: **8443** och **8444**

IP: **81.89.145.244**

Verifiera autentiseringen i den nya produktionsmiljön:
Sjunet
http://sakerhetstjanst.sjunet.org:7443/spadmin/
(IP: **81.89.145.246**)

Används TGP tjänsten med uthoppsfunktion skall även följande öppnas

TGP uthopp (endast om uthopp används)
utgående (till TGP)
http://tgp.npo.sjunet.org

Port: **80 och 443**

IP: **81.89.148.60**

TGP-tjänst (endast om lokal TGP-tjänst, on-line, används)
från tjänsteplattformen:

port **443**
IP: **82.136.149.61**

till lokal TGP-tjänst:
enlig TGP-leverantörens anvisningar***.

Se även:
http://code.google.com/p/skltp/wiki/FAQTeknik

För revokeringskontroll behöver både kommunikationsvägar finnas för kontroll av både nya och gamla SITHS-certifikat.

För SITHS v3 behöver någon av följande **revokeringsadresser** ska vara öppna:

Sjunet
URL=ldap://sithscrl.carelink.sjunet.org/cn=SITHS%20CA%20ver%203,o=SITHS%20CA,c=SE?certificateRevocationList;binary?
82.136.149.44 port 389

eller

URL=http://sithsocsp.trust.telia.com
194.237.208.174 port 80

Internet
URL=http://www.carelink.se/siths-ca/ca003.crl
80.76.157.219 port 80

För Siths CA v1 behöver någon av följande **revokeringsadresser** ska vara öppna:

Internet
http://crl1.siths.se/sithstype1cav1.crl
80.76.157.219 port 80

http://ocsp1.siths.se
194.237.208.174 port 80

Sjunet

http://crl2.siths.sjunet.org/sithstype1cav1.crl
82.136.163.164 port 80

http://ocsp2.siths.sjunet.org
82.136.160.42 port 80

Brandväggar måste också öppnas för att HSA- och SITHS-organisationen ska komma åt HSA Admin och SITHS Admin. Detta görs av nätverkstekniker i samband

med tjänsternas införande.

”OBS” kontrollera att dessa adresser inte spärras i någon generell produkt för internetfiltrering (typ Bluecoat).

3.2. **Internet** - Brandväggsöppningar för åtkomst till NPÖ

☐ Brandväggar öppnade

För att komma åt **NPÖ** via Internet krävs att följande brandväggar är öppna:

NPÖ:
utgående (till NPÖ)
https://www.npo.se
Port: **443**
IP: **194.14.70.123**

Säkerhetstjänsterna:

Till och med 2013-04-20: utgående (till Säkerhetstjänsterna)
https://sakerhetstjanst.inera.se

Port: **8443** och **8444**

IP: **78.41.244.29**

Från och med 2013-04-20 då Säkerhetstjänster 2.1 tas i drift: utgående (till Säkerhetstjänsterna)
https://sakerhetstjanst.inera.se

Port: **7443, 7444, 7445 och 7446**

IP: **78.41.244.29**
https://idp.sakerhetstjanst.inera.se

Port: **8443** och **8444**

IP: **78.41.244.29**

Verifiera autentiseringen i den nya produktionsmiljön:
Internet
https://sakerhetstjanst.inera.se:7443/spadmin/
(IP: **78.41.244.29**)

Används webb applikation för att administrera TGP (sk TGP webbadmin) så gäller:
Applikationen startas med länken:
https://tgp.npo.se/TGPadmin/ssl/default.aspx
Port: 80 och 443
IP: 88.131.57.137

Används TGP tjänsten med uthoppsfunktion ska även följande öppnas

TGP uthopp (endast om uthopp används)
utgående (till TGP)
http://tgp.npo.se
Port: **80 och 443**
IP: **88.131.57.137**

TGP-tjänst (endast om lokal TGP-tjänst, on-line, används)
från tjänsteplattformen:
port **443**
IP: **193.108.43.179**

till lokal TGP-tjänst:
enlig TGP-leverantörens anvisningar***.

Se även:
http://code.google.com/p/skltp/wiki/FAQTeknik

För revokeringskontroll behöver både kommunikationsvägar finnas för kontroll av både nya och gamla SITHS-certifikat.

För Siths v3 behöver följande **revokeringsadress** ska vara öppen:

Internet

URL=http://www.carelink.se/siths-ca/ca003.crl
80.76.157.219 port 80

För Siths CA v1 behöver någon av följande **revokeringsadresser** ska vara öppna:
http://crl1.siths.se/sithstype1cav1.crl
80.76.157.219 port 80

http://ocsp1.siths.se
194.237.208.174 port 80

”OBS” kontrollera att dessa adresser inte spärras i någon generell produkt för internetfiltrering (typ Bluecoat).

☐ Krav på Kortläsare och drivrutin uppfyllda

Vissa kortläsares drivrutin kan ibland inte registrera att SITHS-kortet har ryckts ur kortläsaren. Det innebär att Net iD inte upptäcker att något har hänt och följaktligen inte stänger ner sessionen.

Vi rekommenderar därför att ni utgår från Cygates eller Secmakers kortläsarbroschyr, som innehåller kortläsare som fungerar bra. Det är också viktigt att man använder den senaste drivrutinsversionen från tillverkaren. Använd **inte** Microsofts generiska drivrutin från 2006.

Andra läsare kan också fungera bra men var noga med dess drivrutiner.

I båda dessa fall så bör man testa så att kortläsaren och dess drivrutin fungerar korrekt, se stycket om funktionstest av SITHS-kort och dess kortläsare nedan.

☐ CA och Rotcertifikat fungerar korrekt

SITHS Rotcertifikat är vitlistat hos Microsoft Internet Explorer, vilket innebär att en användare slipper få upp varningsmeddelande vid anslutning till en webbsida identifierad med ett vitlistat certifikat.

Om man trots detta får upp följande varningsmeddelande **”Ett problem har uppstått vid den här webbplatsens säkerhetscertifikat”** vid anslutning till NPÖ så behöver ansvarig för klientinstallationen aktivt välja att lita på CA, vilket görs enligt följande:

Rotcertifikat finns på Ineras hemsida Infrastrukturtjänst SITHS.

Välj aktuella rotcertifikat (SITHS CA v3.cer och SITHS Type 1 CA v1.crt och SITHS Root CA v1.crt). Se till att rotcertifikatet installeras under **Betrodda rotcertifikatutfärdare** (Trusted Root Certification Authorities) under aktuell webbläsare.

☐ Funktionstest av SITHS/kortläsare utförd

Funktionstest av SITHS-kort och dess kortläsare kan ske på följande sätt:

1. Anslut kortläsare till datorn och sätt i SITHS-kortet i kortläsaren.
2. Leta upp Net iD genom att klicka på **Start** och därefter **Alla Program**. Klicka på **Net iD-mappen** och därefter på **Administration** eller
   Högerklicka på **Net iD-ikonen** och därefter på **Administration** om den finns på datorns skrivbord.
   Då visas ett Net iD-fönster där alla certifikat som finns på SITHS-kortet visas.
3. Ryck ur SITHS-kortet ur kortläsaren.
   Då ska alla certifikat som finns på SITHS-kortet försvinna från Net iD-fönstret. Om så inte sker så är det fel på kortläsaren och/eller dess drivrutin.

☐ Användare registrerad i HSA

För en mer utförlig beskrivning hur man lägger in attributen i HSA hänvisas till dokumentet HSA Admin Handbok.

☐ Vårdgivare (VG) och vårdenhet (VE) registrerad

I HSA Admin får endast Huvudansvarig och Central admin markera att en enhet är **vårdgivare** (hsaHealthCareProvider) eller **vårdenhet** (hsaHealthCareUnit)
samt ange vem som är **verksamhetschef** (hsaHealthCareUnitManager) för den aktuella vårdenheten.
Likaså är det endast Huvudansvarig och Central admin som får ange vilka enheter som tillhör en vårdenhet.

☐ Registrerat organisationsnummer för aktuell vårdgivare	Organisationsnummer behöver finnas registrerat på de objekt som ska definieras som vårdgivare. Definieras i attributet **Org.nummer** (orgNo) i formuläret Enhet i HSA Admin.
☐ Registrerad adressinformation för aktuell vårdenhet	Det är postadressen och postnummer där verksamheten bedrivs som måste registreras. Detta görs i attributet **Postadress** (postalAddress) i formuläret Adresser i HSA Admin och i attributet **Postnummer där verksamheten bedrivs** (postalCode) i formuläret Kontakt i HSA Admin. Vårdgivare och vårdenhet kan i vissa fall ligga på samma nivå.
☐ Registrerat telefonnummer för aktuell vårdenhet	Telefonnummer till vårdenheten där verksamheten bedrivs, vilket definieras i attributet **Direkttelefon** (telephoneNumber) i formuläret Adresser i HSA Admin.
☐ Medarbetaruppdrag definierat	Medarbetaruppdrag ska definieras och tilldelas via beslut av verksamhetschefen. Medarbetaruppdraget ska ha syfte ”hsaCommissionPurpose”=**Vård och behandling**. Samma medarbetaruppdrag kan användas för flera olika tjänster och det är önskvärt att man återanvänder redan befintliga medarbetaruppdrag där så är möjligt. Om vårdenheten saknar ett medarbetaruppdrag med syfte ”Vård och behandling” måste ett nytt sådant skapas.
☐ Medarbetaruppdrag rättigheter	**hsaCommissionRight=Värde1;Värde2;Värde3** **Ex. hsaCommisssionRight=LÄSA;Alla;SJF** **Värde 1** Anger vad man ska få göra. I dagsläget går det endast att välja LÄSA **Standardvärde för NPÖ:** LÄSA **Värde 2** Anger vilka informationstyper (t.ex. kontakt, utlämnade läkemedel och diagnos) medarbetarna ska få se. Giltiga värden utöver Alla hittar du i ”Kodverk_och_OIDer_i_NPÖ_version_X.X.xls” som finns i ”Anslutningsanvisningar NPÖ YYYY-MM-DD.zip”, under teknisk dokumentation på Inera.se. Man kan bara välja informationstyperna på toppnivån (de utan bindessträck i

		sig). Ex. **Alla** **Standardvärde för NPÖ:** Alla **<u>Värde 3</u>** Anger från vilka ställen medarbetaren ska få se information. Giltiga värden är: **SJF**=Information från Sammanhållen journalföring. **VG**=Information från alla enheter inom Vårdgivaren **VE**=Information bara från den egna Vårdenheten
☐	Användare registrerad	**Standardvärde för NPÖ:** , Sammanhållen journalföring, SJF Registreras med: **Tilltalsnamn** (givenName, gn) **Mellannamn** (middlename) **Efternamn** (sn, surName)
☐	Användare kopplad till medarbetaruppdrag	Användare måste vara kopplade till ett **Medarbetaruppdrag** (hsaCommissionMember), definierat enligt ovan. Registreras i formuläret Tilldela medarbetaruppdrag i HSA Admin.
☐	Legitimerad yrkesgrupp angiven*	Registreras i attributet **Leg yrkesgrupp** (hsaTitle) i formuläret Anställning/medarbetaruppdrag i HSA Admin.
☐	Befattning angiven (i NPÖ behövs detta enbart registreras för personer med förskrivningsrätt och utan legitimerad yrkesgrupp)*	Registreras i attributet **Befattning** (paTitleName), (paTitleCode) i formuläret Anställning/ medarbetaruppdrag i HSA Admin.
☐	Arbetsplatskod angiven**	Registreras i attributet **Arbetsplatskod** (unitPrescriptionCode) Attributet används för vårdenheten (VE) eller vårdgivaren (VG) och ger tillgång till Läkemedelsförteckningen via NPÖ.

☐	Förskrivarkod angiven**	Registreras i attributet **Förskrivarkod** (personalPrescriptionCode) i formuläret Anställning/medarbetaruppdrag. Attributet används för personlig förskrivarkod och ger tillgång till Läkemedelsförteckningen via NPÖ.

***** Är obligatoriskt i samband med att anslutningen till Läkemedelsförteckningen sker via Tjänsteplattformen.***
***Observera** att uppgift om ”Legitimerad yrkesgrupp” och ”Förskrivarkod”, samt uppgift om ”Specialitet”, som registreras i HSA måste överensstämma med uppgifterna om personen i Socialstyrelsens register över hälso- och sjukvårdspersonal, HOSP.*

***** Är obligatoriskt***
***Observera** arbetsplattskod och förskrivarkod används för att identifiera användaren i Läkemedelsförteckningen hos Apoteken Service AB.*

**** Notera att vissa TGP-leverantörer (t.ex. Treserva) inte använder standardporten (443) för https-trafik.*

☐	TGP webbadmin	*Används webb applikation för att administrera TGP (sk TGP webbadmin) så gäller följande:* Användarna ska ha attributet ”hsaSystemRole”=**TGP;Administratör** och vara kopplade till ett medarbetaruppdrag (hsaCommissionMember). Medarbetaruppdraget ska ha syfte ”hsaCommissionPurpose”=**Administration**.

☐	SITHS-kort beställda	SITHS-kort beställs av vårdgivarens lokala SITHS-organisation.

☐ Lokal support etablerad

Lokalt kunskapsstöd för NPÖ ska finnas tillgängligt. Det lokala kunskapsstödet (supporten) kan vid behov vända sig till Nationell Kundservice vid Inera, servicedesk@inera.se . Krav från Nationell Kundservice erhålls när Intresseanmälan tecknats.

4. Verksamhetsaktiviteter vid ett konsument införande

Förutom de aktiviteter som finns ovan, behöver anslutande vårdgivare även göra följande aktiviteter.

☐ Avtal

- ☐ Teckna Intresseanmälan med Inera inför projektstart
- ☐ Teckna Anslutningsavtal NPÖ med Inera
- ☐ Teckna Personuppgiftsbiträdesavtal med Inera

☐ TGP-tjänst etablerad

- ☐ Regelverk beslutat
- ☐ Tjänst etablerad
- ☐ Tillgängliga patienter registrerade

☐ Lokal support etablerad

- ☐ Funktionsbrevlåda anmäld till Inera
- ☐ Kontakperson anmäld till Inera

☐ Riktlinjer och rutiner

- ☐ Ta fram och besluta om Riktlinjer för inhämtande av samtycke
- ☐ Ta fram och besluta om Rutinbeskrivning för användning (”När använder man NPÖ”) av Nationell Patientöversikt
- ☐ Rutiner för logguppföljning etablerade

☐ Utbildning

- ☐ Gränssnitt, Nationell Patientöversikt
- ☐ Patientdatalagen
- ☐ Rutinbeskrivning för användning
- ☐ Loggуppföljning
- ☐ Utbildning av Supportorganisation