# Fördjupad analys RPA

Fördjupad analys av identitet och åtkomststyrning för robotar

Version 1.0

inera

## Innehåll

**Sammanfattning** ..... **3**

**1. Inledning** ..... **4**

1.1 Syfte ..... 4

1.2 Avgränsning ..... 4

1.3 Deltagare ..... 4

1.4 Tillvägagångssätt ..... 5

**2. Översikt RPA** ..... **6**

2.1 Definition av RPA ..... 6

2.2 Juridisk översikt ..... 6

**3. Säker identitetshantering för Robotar** ..... **8**

3.1 Generella informationssäkerhetskrav ..... 8

3.2 Informationsmängder som beskriver robotar ..... 8

3.3 Säker identitet för Robotar ..... 10

**4. Processer kring identitetshantering och åtkomststyrning av Robotar** ..... **13**

4.1 Processer för livcykelhantering av robotar ..... 13

4.2 Användning av robotar ..... 16

**5. Nästa steg** ..... **17**

5.1 Utvecklingsbehov ..... 17

5.2 Tidplan för utveckling och införande ..... 18

5.3 Kostnadsestimat ..... 18

**Referenser** ..... **20**

**Bilaga 1 Juridisk Översikt** ..... **21**

**Bilaga 2 Informationsmängder i HSA** ..... **25**

# Revisionshistorik

| Version | Datum | Författare | Kommentar |
|---|---|---|---|
| 1.0 | 2020-04-21 | Ulrika Nilsson | Rapport fastställd |

# Sammanfattning

Denna fördjupade analys kring RPA har tittat närmare på möjligheten att använda den nationella infrastrukturen för vård och omsorg för att säkra identitet och åtkomststyrning för robotar. Analysen har skett genom två workshops med ämnes- och verksamhetsexperter samt genom rättslig översikt. I arbetet har det dels gjorts analyser av vilka grundläggande generella krav som bör gälla för säker identitetshantering och åtkomststyrning av robotar, dels har det gjorts en analys av hur den nationella säkerhetsinfrastrukturen för vård och omsorg, kan anpassas för att möjliggöra implementering av RPA.

Resultatet av analysen visar att det finns centrala informationsmängder som behöver hanteras för att säkra identiteter för robotar. Dessa presenteras i rapporten tillsammans med en vägledning för certifikatshantering av robotar. En slutsats är att den nationella infrastrukturen för SITHS och HSA inte går att använda i sin nuvarande utformning för att hantera identiteter för robotar. Det beror på att några viktiga informationsmängder saknas i HSA. Det finns inte heller någon certifikatstyp inom SITHS som kan användas för robotar. Att använda personliga tjänstelegitimationer till robotar bryter mot regelverket inom SITHS och Svensk e-legitimation och det är inte heller praktiskt möjligt att använda SITHS servercertifikat för robotar i och med att robotar utgörs av processer som agerar i olika användargränssnitt snarare än i en och samma server.

Analysen har kommit fram till att det är möjligt och relativt enkelt att anpassa den nationella infrastrukturen så att även identiteter och åtkomststyrning kan hanteras för robotar. Inom HSA innebär utvecklingen att HSA-schemat behöver utökas med några ytterligare informationsmängder och att gränssnitt anpassas för att kunna administrera information om robotar. SITHS kan också, inom ramen för nuvarande upphandling, utveckla en ny certifikatstyp, ”RPA-certifikat”, som kan lagras på kort liknande de nuvarande SITHS-certifikaten för personer.

Sist i rapporten presenteras en tidplan för utveckling av den nationella infrastrukturen för att kunna införa stöd för säker identitetshantering och åtkomststyrning av robotar. Kopplat till denna finns även ett kostnadsestimat för genomförandet av utvecklingen.

# 1. Inledning

RPA används i allt större utsträckning inom kommuner och regioner. Används de på rätt sätt kan de förbättra både effektivitet och säkerhet genom resurs- och kostnadsbesparingar, kortare handläggningstider och öka riktighet och kvalitet. Den stora framgångsfaktorn för användningen av RPA är att det inte kräver någon ombyggnad av system, utan nuvarande system kan användas utan förändringar. Robotarna använder befintliga användargränssnitt i befintligt skick.

I dagsläget fungerar inte säker identitetshantering och åtkomststyrning av robotar inom vård och omsorg. Det finns inte etablerade rutiner och regelverk för hur robotars identiteter och åtkomststyrning ska hanteras på ett säkert sätt. Roboten agerar som en människa, men kan inte ha ett personligt ansvar.

Hanteringen av robotar skiljer sig åt mellan olika organisationer i vård och omsorg, och det går därmed inte att använda robotar på ett säkert sätt över organisationsgränser.

## 1.1 Syfte

Detta uppdrag innebär genomförande av en fördjupad analys av hur regelverk och praktisk hantering av identiteter och åtkomststyrning för robotar skulle kunna fungera samt utvecklas i nuvarande säkerhetsinfrastruktur för vård och omsorg.

## 1.2 Avgränsning

Uppdragets inriktning är att analysera vilken utveckling som behöver ske i den nuvarande säkerhetsinfrastrukturen för vård och omsorg för säker identitets- och åtkomststyrning inom HSA och SITHS. Arbetet har avgränsats till att den nationella IdP:n endast ska kunna hantera robotcertifikat.

Arbetet har avgränsat sig från processer som utförs under övervakning av en människa, så kallad *attended RPA*, t.ex. användning av makron.

## 1.3 Deltagare

Följande personer har deltagit i arbetet med fördjupad analys för RPA:

| | |
|---|---|
| Ulrika Nilsson | Secure State Cyber (Uppdragsledare) |
| Johan Zenk | Region Östergötland |
| Christer Allskog | Inera |
| Christoffer Johansson | Inera |
| Ronny Nilsson | Inera |
| Fredrik Ljunggren | Kirei |
| Annika Bärgård | Västerås stad |
| Stefan Bäckström | Region Halland |
| Andi Kravljaca | Nacka kommun |
| Tomas Gustafsson Nielsen | Västra Götalandsregionen |

| | |
|---|---|
| Manolis Nymark | Inera |

## 1.4 Tillvägagångssätt

Uppdraget genomfördes på följande sätt:

- Workshops med verksamhetsexperter från kommuner och regioner samt experter inom HSA, SITHS, Säkerhetstjänster och svensk e-legitimation.
- Genomgång av rättsliga förutsättningar och utmaningar samt regelverk inom nationell säkerhetsinfrastruktur för vård och omsorg.

# 2. Översikt RPA

## 2.1 Definition av RPA

Vid starten av arbetet var det viktigt att enas om en definition av RPA och Robot för att säkerställa att alla hade samma syn på det i det fortsatta arbetet. Nedan presenteras den definition av robot/RPA som togs fram av arbetsgruppen:

> *En robot, eller RPA, definieras som en process med ett visst ändamål. Roboten agerar i ett användargränssnitt avsett för människor utan mänsklig inblandning.*
>
> *En process är en serie instruktioner, eller aktiviteter, som utförs sekventiellt eller parallellt. Processen har ett antal behörigheter för att stödja det aktuella ändamålet.*

Det finns ingen tydlig definitionsskillnad mellan ”robot” och ”RPA”, men i diskussioner med terminolog beskrivs att begreppet ”robot” bör användas när fokus är själva subjektet, dvs. den entitet som agerar eller ”den digitala medarbetaren”. Begreppet RPA, som står för *Robotic Process Automation*, bör användas när man vill fokusera beskrivningen mer på själva tekniken som används och processen som utförs. I arbetet med denna analys har vi har försökt använda de båda begreppen parallellt på detta sätt för att lyfta de olika aspekterna, men i vissa fall har det varit svårt att välja varför begreppen kan ses som synonymer i dokumentet.

## 2.2 Juridisk översikt

En del av uppdraget har varit att översiktligt redogöra för de rättsliga förutsättningarna avseende identiteter och åtkomststyrning av RPA. Nedan följer en sammanfattning av denna redogörelse. För detaljerad information om de rättsliga förutsättningarna för RPA och juridiska områden som behöver vidareutvecklas kopplat till RPA, se bilaga 1 Juridisk Översikt.

### 2.2.1 Patientdatalagen

Avseende patientdatalagen har inga hinder hittats kring att använda automatiserade processer i sig. Två viktiga områden som lyfts fram är att tydligt koppla ansvaret för bearbetningen till en fysisk individ och behovet av samtycke från patient när information ska användas från olika vårdgivare vid sammanhållen journalföring.

### 2.2.2 Underskrifter

När det gäller underskrifter regleras detta igenom eIDAS-förordningen och det konstateras att det inte föreligger något hinder för elektroniska underskrifter, men en enskild bedömning behövs av underskriftskravets innebörd.

### 2.2.3 Förvaltningslagen och kommunallagen

Av förvaltningslagen framgår att automatiserade beslut kan användas av statliga myndigheter, men inte i kommunal verksamhet enligt kommunallagen. Regeringen har tillsatt en utredning för översyn av denna skillnad.

### 2.2.4 Dataskyddsförordningen och socialtjänstlagen

Avseende personuppgifter är det generellt inte tillåtet med automatiserade beslut som inbegriper profilering[1] enligt dataskyddsförordningen, dvs. att behandla personuppgifter för att bedöma personliga egenskaper hos en individ. Undantag finns i förordningen. Inom hälso- och sjukvården råder osäkerhet om undantagen är tillämpliga på medvetslösa patienter vars vård innefattar automatiserade beslut som inbegriper profilering.

Även när det gäller socialtjänstlagen finns vissa begränsningar då det finns krav på att utförandet av vissa uppgifter sker av personal med tillräcklig utbildning och avlagd examen eller motsvarande. Därmed kan RPA i kommunal verksamhet idag främst användas som ett avancerat beslutsstöd, utan möjlighet till automatiserade beslut.

### 2.2.5 Utrednings- och påverkansområden

Den rättsliga översikten pekar på följande områden som behöver utredas vidare:

- *Ansvarsfrågor* – exempel vad gäller mjukvara, innehåll och hantering av algoritmer, t.ex. vad som får utföras, hur det ska presenteras för berörda och hur de berörda kan påverka hanteringen.
- *Profilering* - exempelvis kring hälso- och sjukvårdsinsatser enligt artikel 22 i GDPR och även kring personuppgifter i socialtjänsten.

Regioner och kommuner skulle också behöva arbeta för förändringar inom följande områden:

- *Generell översyn* - Det behöver förtydligas i svensk lag vilka beslut som kan fattas automatiserat eller inte inom hälso- och sjukvården. PDL är främst utformad för en reaktiv vård och lagen behöver förändras för att hantera mer preventiv vård (förebyggande hälso- och sjukvård). För området socialtjänst behöver kraven på personals utbildning och kompetens bedömas utifrån möjligheten till automatiserat beslutsfattande.
- *Komplettering av föreskrifter* - Socialstyrelsens föreskrifter bör kompletteras med beskrivningar av hur RPA ska hanteras inom hälso- och sjukvården.

[1] Profilering handlar om att behandla personuppgifter för att bedöma personliga egenskaper hos en individ. Det definieras i art. 4.1 i GDPR: " profilering: varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar".

# 3. Säker identitetshantering för Robotar

## 3.1 Generella informationssäkerhetskrav

Organisationer som hanterar RPA behöver se till att det finns ett systematiskt säkerhetsarbete i organisationen som uppfyller ISO 27001 och som inkluderar riskhantering, regler, processer kring hantering av RPA. Framförallt handlar det om att det ska finnas dokumenterade och kvalitetssäkrade processer för livscykelhantering och åtkomststyrning för robotar samt säkerställd förändringshantering. Lämpliga tekniska och organisatoriska åtgärder behöver vidtas för att säkerställa att säkerhetsnivån är tillräcklig i förhållande till risken med användningen av RPA.

Den fysiska och logiska säkerheten kring den tekniska miljön som roboten agerar i är mycket viktig. Riskerna för att RPA utnyttjas på ett felaktigt sätt eller av obehöriga måste hanteras.

Skapandet av identiteter för robotar och installation behöver hanteras på så vis att ingen enskild individ på egen hand kan skapa, modifiera eller installera en identitet utan inblandning av annan befattningshavare (*Separation av arbetsuppgifter*).

Rutiner och processer för uppföljning av säkerheten behöver också ske kontinuerligt för att verifiera att regelverk, instruktioner och rutiner efterlevs. Det kan t.ex. ske genom återkommande internrevisioner som omfattar hanteringen av RPA.

## 3.2 Informationsmängder som beskriver robotar

### 3.2.1 Generell vägledning kring informationsmängder som beskriver robotar

För att kunna utfärda tillförlitliga identiteter/certifikat till robotar och hantera robotar över tid behöver det finnas kvalitetssäkrad och uppdaterad information om robotens identitet, ändamål och vem som ansvarar för roboten. Det är grunden för säker identitetshantering och åtkomststyrning för robotar.

Analysen har kommit fram till att följande grundläggande informationsmängder behöver finnas för en robot.


*Figur 1. Grundläggande informationsmängder om robotar.*

Nedan presenteras informationen i form av attribut och beskrivningar:

| | |
|---|---|
| ***Unikt id*** | En unik identitet. |
| ***Namn*** | Namn som används för roboten. För att visuellt kunna identifiera en robot i olika sammanhang är det lämpligt att det av namnet framgår att det är en robot. |
| ***Beskrivning*** | Beskrivning av robotens ändamål i form av process som den utför. En robots identitet är unikt kopplad till vad den gör. Därför är beskrivningen av robotens ändamål och den process som utförs mycket viktig. |
| ***Startdatum*** | Datum då roboten startades, dvs. fick sin identitet. |
| ***Slutdatum*** | Datum då giltighetstiden för robotens identitet upphör, dvs. det datum då robotens identitet måste förnyas eller att processen inte längre ska finnas kvar. |
| ***Organisations-tillhörighet*** | Organisation som roboten tillhör. |
| ***Ansvarig person*** | Identitet på den person i organisationen som är verksamhetsmässigt ansvarig för robotens användning. |

Utöver den grundläggande informationen behöver roboten även tilldelas behörigheter och rättigheter på ett säkert sätt för att kunna utföra aktuella processer i olika användargränssnitt.

Behörigheter för robotar ska alltid utgå ifrån *least privilege*-principen, så att den inte kan nyttjas till annat än det den är ämnad för. Processen för behörighetstilldelning behöver också regleras genom tydliga och säkra rutiner som utgår från undertecknade beställningsunderlag av den som ansvarar för roboten (ansvarig person).

### 3.2.2 Information om robotar i HSA Katalogtjänst

HSA Katalogtjänst är utformad för att registrera och hantera kvalitetssäkrad information om personer, organisationer och funktioner för anslutna organisationer. Regelverket är utformat så att informationen kan nyttjas i användning över organisationsgränser (tillit mellan organisationerna i en federation).

Utöver objekt för personer, organisationer och funktioner finns i HSA även medarbetaruppdrag, t.ex. vårdmedarbetaruppdrag som används för att styra behörigheter i enlighet med patientdatalagen, bl.a. genom koppling till vårdenhet och definierade ändamål för åtkomststyrningen. HSA är också källa för utfärdande av SITHS-certifikat och utgör lagringsplats för information om SITHS-certifikat och SITHS-kort.

HSA-konceptet utgår från ett gemensamt regelverk, HSA-policyn, med fastställda regler och rutiner för att säkerställa att information som registreras i alla organisationer är korrekt och aktuell. Det finns även definierade administratörsroller och säker åtkomststyrning för de administratörer som hanterar olika objekt i HSA och en process för uppföljning av informationssäkerheten.

I dagsläget går det inte att registrera robotar i HSA eftersom informationsmängder och objekt för robotar saknas. Det bedöms dock vara relativt enkelt att uppdatera HSA så att även robotar kan hanteras i den ordinarie infrastrukturen.

Den grundläggande informationen som presenterades i avsnittet ovan skulle relativt enkelt kunna läggas in i HSA för robotar och några av HSA:s ordinarie informationsmängder skulle kunna nyttjas även för robotar. Gränssnitt och regelverk kan också anpassas som en del i den ordinarie schemauppdateringsprocessen för att hantera robotar.

I bilaga 2, Informationsmängder för robotar i HSA, finns information om vilka objekt och attribut som skulle behöva kompletteras eller hanteras i det nuvarande HSA-schemat.

## 3.3 Säker identitet för Robotar

### 3.3.1 Generell vägledning då SITHS-certifikat inte kan användas

Om en organisation vill ta steg för att införa säkra identiteter för robotar innan den nationella infrastrukturen är anpassad för detta finns några rekommendationer att följa.

- Det behöver vara tydligt och spårbart vem som är ansvarig för roboten, se beskrivning av grundläggande informationsmängder tidigare.
- Använd endast robotar för processer inom den egna organisationen.
- Ha kontroll på vilka risker som finns med roboten, se till att organisationen har ett systematiskt informationssäkerhetsarbete med genomförda riskanalyser och informationsklassningar.

Om certifikat utfärdas till roboten, se till att:

- certifikatet minst innehåller unik identitet (unikt id) och ett namn
- det finns ett slutdatum på certifikatet som är max 2 år från utfärdandet
- det är ordning och reda i rutiner för utfärdande och administration av certifikaten så att certifikatet inte kan missbrukas

- eventuella mjuka certifikat inte dupliceras
- skydda privata nyckelmaterial från att röjas.

Det är inte tillåtet att:

- använda en personlig e-legitimation eller ett person-id som identitet för en robot (inte heller tjänstelegitimation för personer eller HSA-id för en person)
- tillföra personliga attribut till en robot som inte är korrekta, till exempel legitimerad yrkesgrupp och förskrivningskod.

### 3.3.2 Möjlig utveckling av SITHS-certifikat för robotar

I dagsläget är det inte möjligt att utfärda SITHS-certifikat till robotar. Det beror på att det inte finns någon information i HSA om robotar och inte heller någon certifikatstyp inom SITHS som kan användas för robotar. Att använda personliga tjänstelegitimationer till robotar bryter mot regelverket eftersom de endast får utfärdas till fysiska personer.[2]

SITHS servercertifikat[3] skapas utifrån information som lagras i en separat del av HSA, HSA Tjänsteträd. Den delen av HSA saknar viktiga informationsmängder samt åtkomststyrningsmöjligheter. Dessutom sätter regelverket kring namnsättning i SITHS funktionscertifikat begränsningar då det enda tillåtna namnet är DNS-namn. Det är heller inte praktiskt att utfärda servercertifikat till robotar i och med att robotar utgörs av processer som agerar i olika användargränssnitt snarare än på en och samma server.

Analysen visar att det finns möjlighet att utveckla SITHS med en ny certifikatstyp avsedd för robotar inom ramen för nuvarande avtal. Ett sådant certifikat behöver definieras beträffande tillitsnivå[4] och minst innehålla HSA-id, namn på roboten samt namn på ansvarig organisation utöver ordinarie tekniska informationsmängder för certifikat. Certifikatet bör inte ha en längre maximal giltighetstid än 2 år och information om roboten som ska ingå i certifikatet behöver hämtas ifrån HSA vid skapandetillfället för att säkerställa kvalitet och för att nuvarande integrationer för utfärdande och administration av certifikat inte ska behöva förändras.

Mjuka certifikat för robotar kan kopieras och installeras på flera ställen vilket gör att ansvarig person har en sämre kontroll på användningen av certifikatet. Arbetsgruppen har därför bedömt att certifikat för robotar bör hanteras på en hård bärare för att tillföra tillräckligt värde i verksamheten. Det är också en förutsättning för att befintliga gränssnitt ska kunna användas.

För att möjliggöra utfärdande och administration av certifikat för robotar inom ramen för nuvarande SITHS behöver bäraren vara ett aktivt kort (motsvarande reservkort). Det bör dock påpekas att användning av traditionella kort som bärare kan innebära en problematik om flera robotar ska agera på en och samma enhet. Troligen kan nya hårda bärare utvecklas senare inom ramen för SITHS, men det innebär i så fall nya upphandlingar. För mer storskaligt användande

[2] DIGG, Myndigheten för digital förvaltning, granskar och godkänner svenska e-legitimationer utifrån nationella och internationella säkerhetskriterier. Tillitsramverket för Svensk e-legitimation innehåller gemensamma krav på utfärdare som behöver efterlevas av SITHS e-id. Svensk e-legitimation får endast utfärdas till fysiska personer. Även tillitsramverket för SITHS förbjuder sådan användning.
[3] Även kallat funktionscertifikat eller HCC Funktion.
[4] LoA (Level of Assurance) som bygger på internationell standard (ISO/IEC 29115).

är det rimligt att överväga enklare hårdvarumoduler, HSM[5], som kan lagra ett större antal certifikat för ändamålet.

Oavsett vilken typ av bärare som används behöver ett aktiveringsförfarande för roboten utformas. Helst ska aktiveringen göras av ansvarig person eller ansvarig förvaltare. Sådana rutiner behöver utformas så att det dels inte uppstår kritiska nyckelpersonberoenden, dels att robotens privata nyckel och certifikat inte enkelt kan missbrukas.

[5] HSM (Hardware Security Module).

# 4. Processer kring identitetshantering och åtkomststyrning av Robotar

Detta avsnitt beskriver hur processer för livscykelhantering och användning av robotar skulle kunna utformas i den nationella säkerhetsinfrastrukturen HSA och SITHS.

## 4.1 Processer för livcykelhantering av robotar

### 4.1.1 Utfärdande av identitet och certifikat för robotar

Processen för upprättande av identitet och utfärdande av certifikat för robotar utgår ifrån definiering av robotens identitet och registrering av information om roboten i HSA.


*Figur 2. Process för upprättande av identitet och utfärdande av certifikat för robotar.*

Processen för upprättande av identitet och utfärdande av certifikat för robotar startar med en initiering där behov av RPA identifieras. Processen definieras och fastställs i PDD, *Process Design Document*[6] och en SDD, *Solution Design Document*[7], beskriver processens lösningsdesign. Ansvarig person utses och den ansvarige beställer därefter en identitet för roboten genom en signerad beställning innehållande beskrivning av roboten och dess informationsmängder.

[6] PDD, *Process Design Document,* är beskrivning av processens design ur ett verksamhetsperspektiv som beskriver aktiviteter som ingår i processen steg-för-steg, samt regler och villkor som gäller för processen. Dokumentet innehåller även förändringshantering (versionshantering).
[7] SDD, *Solution Design Document,* beskriver processens lösningsdesign.

Information registreras i HSA utifrån signerad beställning i enlighet med rutiner och regelverk för kvalitetssäkring. Ansvarig person, förvaltare och organisationstillhörighet för roboten registreras.

Ansvarig person beställer ett certifikat från SITHS-administratör med särskild behörighet genom signerad beställning. Certifikat utfärdas utifrån informationsmängder registrerade i HSA, och kvitteras ut tillsammans med certifikatets bärare av utsedd förvaltare. Certifikatet installeras och aktiveras av förvaltaren.

Ansvarig person beställer behörigheter för roboten, t.ex. individuella egenskaper för it-tjänster, medarbetaruppdrag[8] samt eventuella behörigheter i andra system. RPA implementeras så att den process som roboten ska utföra kan utföras.

### 4.1.2 Förändring av robotens process

Nedan beskrivs vilka förändringar som kan ske under en robots livstid och hur de bör hanteras ur ett identitetshanterings- och åtkomststyrningsperspektiv.

Nedan beskrivs hur processen bör se ut då en RPA-process förändras utan att ändamålet för processen ändras.


*Figur 3. Process för ändring av RPA-process utan att ändamål med processen ändras.*

Om processen som roboten utför förändras utan att ändamålet för processen ändras behövs en ny SDD som beskriver förändringen. Eventuella förändringar i beskrivningen i HSA uppdateras efter det att SDD har uppdaterats.

### 4.1.3 Förändring av ändamål med robotens process

Om ändamålet med processen förändras behöver roboten avslutas och en ny robot skapas med ny identitet och nytt certifikat (ny PDD). Se 4.1.6. Process för avslut av robotar respektive 4.1.1 Process för utfärdande av identitet och certifikat för robotar.

### 4.1.4 Förändring av ansvarig person eller förvaltare

Nedan beskrivs hur processen bör se ut då ansvarig person eller förvaltare förändras för en robot.

[8] Det finns två typer av medarbetaruppdrag; vårdmedarbetaruppdrag och administrativa uppdrag.


*Figur 4. Process för förändring av ansvarig person eller förvaltare för roboten.*

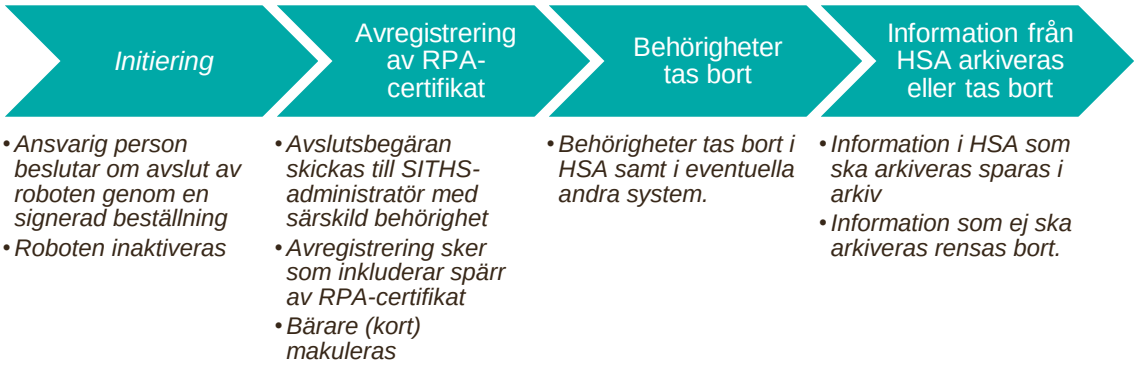
Då ansvarig person eller förvaltare förändras behöver information om detta uppdateras i HSA. En ny skriftlig beställning innehållande information om förändringarna behöver finnas som underlag.

### 4.1.5 Kontroll av att information om robot är aktuell

För att kontrollera att uppgifterna hålls uppdaterade över tid behöver det finnas en regel som beskriver att riktigheten i uppgifter om robotar ska verifieras minst kvartalsvis, på liknande sätt som anställningsuppgifter för personer registrerade i HSA kontrolleras.

### 4.1.6 Process för avslut för robotar

Nedan beskrivs hur processen bör se ut vid avslut av identitet/certifikat och behörigheter för robotar.




*Figur 5. Process för avslut av robotar.*

Processen för avslut av robotar startar med ett undertecknat beställningsunderlag från ansvarig person som beskriver att roboten ska avslutas. Roboten inaktiveras därefter i sin plattform.

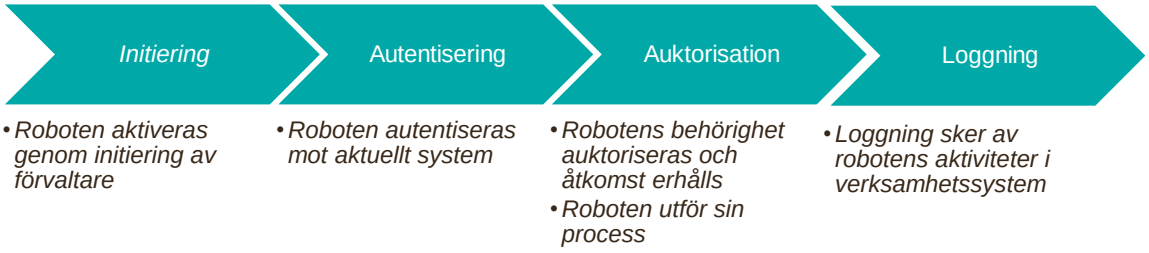
Avslutsbegäran skickas därefter till SITHS-administratör med särskild behörighet som avregistrerar kort och spärrar certifikat för roboten. Kortet makuleras genom att klippas i bitar genom chipet.

Behörigheter tas bort i HSA och i andra tjänster som eventuellt tilldelat behörigheter till roboten.

Information som ska arkiveras om robotarna sparas i arkiv och övrig information renas bort.

## 4.2 Användning av robotar

Nedan beskrivs hur processen ser ut vid användning av robotar.




*Figur 6. Process för användning av robotar.*

Processen för robotens användning startar genom att förvaltaren aktiverar roboten. Det sker både vid uppstart och vid omstart av roboten.

Vid användning av roboten autentiseras den mot det aktuella systemet (t.ex. genom IdP med SAML-biljett eller OIDC[9] när det är lämpligt). Robotens behörighet auktoriseras, t.ex. genom kontroll i HSA och åtkomst erhålls till aktuell applikation och moduler. Roboten utför sin process.

Loggning sker av robotens aktiviteter i verksamhetssystem i enlighet med samma loggfunktionalitet som för övriga användare.

[9] OpenID Connect.

# 5. Nästa steg

Det är möjligt och bedöms relativt enkelt att utveckla SITHS och HSA för att möjliggöra identitetshantering och åtkomststyrning av robotar inom den nationella säkerhetsinfrastrukturen för vård och omsorg.

I detta avsnitt presenteras utvecklingsbehovet tillsammans med en tidplan för utveckling och införande och en kostnadsuppskattning presenteras för genomförandet.

## 5.1 Utvecklingsbehov

### 5.1.1 Utvecklingsbehov HSA

Utvecklingsbehovet i HSA för att hantera robotars informationsmängder och behörigheter är följande:

- *Objekt och attribut* - Införande av objekt och attribut i enlighet med bilaga 1 i detta dokument i samband med ordinarie schemauppdateringsprocess
- *Regelverk, rutiner och processer* - Uppdatera regler, rutiner och processer i styrande och stödjande dokument
- *Administrations- och integrationsgränssnitt* - Utveckla administrationsgränssnitt (HSA Admin och SOP Admin) samt integrationsgränssnitt för tjänster som behöver hantera informationsmängder om robotar
- *Administratörsroller* - Eventuellt utveckla ny administratörsroll i HSA Admin för hantering av robotar.

### 5.1.2 Utvecklingsbehov SITHS

Utvecklingsbehovet i SITHS för att hantera certifikat för robotar är följande:

- *Ny certifikatstyp för robotar* – Utveckla ny certifikatstyp (sekundärcertifikat) för robotar som kan lagras på kort (reservkort)
- *Regelverk, rutiner och processer* - Uppdatera regler, rutiner och processer i styrande och stödjande dokument
- *Administrations- och användargränssnitt* – Utveckla SITHS Admin och Mina Sidor så att robotcertifikat kan hanteras
- *Administratörsroller* - Eventuellt utveckla ny administratörsroll i SITHS Admin för id-administratör för robotar

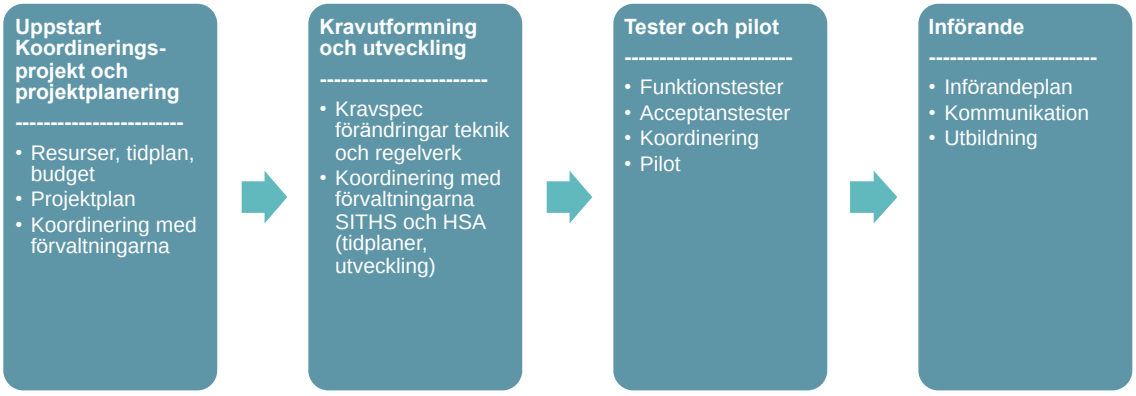
### 5.1.3 Övrig utveckling

Analysen har utgått ifrån att ingen teknisk utveckling ska behöva genomföras inom nationella säkerhetstjänster utöver användning av ett nytt certifikat för robotar och tillhörande dokumentationsförändringar.

En fördjupad rättslig utredning kan behöva genomföras för att beskriva användningen av certifikat för robotar och möjligheten att nyttja olika typer av behörigheter för robotar.

## 5.2 Tidplan för utveckling och införande

Nedan presenteras den tidplan för genomförandet av utveckling och implementering av identiteter och certifikat för robotar inom HSA och SITHS. Arbetet behöver ske i projektform och projektet beräknas ta ca 15–18 månader att genomföra i kalendertid.




*Figur 7. Tidplan för utveckling och införande av identiteter och åtkomst för Robotar.*

Vid uppstart av projektet behöver projektet planeras med en projektplan, resurser, tidplan och budget. I uppstartsfasen behöver även koordinering ske mellan förvaltningarna för HSA och SITHS för att säkerställa att beroenden mellan tjänsterna är omhändertagna.

Kravutformning- och utvecklingsfasen består av kravformuleringsarbete kring förändringar av teknik, regelverk och rutiner både för bastjänsterna och gränssnitt som agerar med tjänsterna. Även i denna fas behöver koordinering ske mellan förvaltningarna SITHS och HSA eftersom kravställning även sker mellan förvaltningarna. Utvecklingsarbetet sker även i denna fas.

I fasen för tester och pilot genomförs funktions- och acceptanstester och när de är godkända genomförs en pilot för att verifiera att utveckling och implementation fungerar korrekt.

Införandefasen utgår ifrån en införandeplan. Anslutna organisationer informeras enligt en kommunikationsplan, nödvändig dokumentation och användarhandledning tas fram och utbildningar skapas om det bedöms behövas.

## 5.3 Kostnadsestimat

Nedan presenteras de kostnader som uppskattats för genomförande av utveckling och införande av förändringarna.

| | |
|---|---|
| **Projekt-kostnader** | **Resurser**:<br>Projektledare ca 700-900 timmar: Planering, kravspecificering, styrning/koordinering (paraplyprojekt), utveckling och test med förvaltningarna, pilot<br>- Rättslig fördjupning 100-200 timmar<br>- Resurser från HSA och SITHS (se nedan)<br>- Externa kontakter |
| **Förvaltnings-kostnader** | **HSA:** Införande krav och utveckling (100-300 timmar), Tester ca 100-200 timmar, kommunikation och införande (ca 100 timmar), support |
| | **SITHS**: Införande krav och utveckling (300 - 500 timmar), Tester ca (100-300 timmar), kommunikation och införande (ca 150 timmar) |
| | **Säkerhetstjänster**: 100-200 timmar |
| **Teknisk utveckling** | **HSA**: 300-500 tkr (Schema, gränssnitt, integrationer) |
| | **SITHS**: 3-5 mkr (nytt certifikat och hård bärare, anpassa nuvarande gränssnitt) |

*Tabell 1. Kostnadsestimat/budget för utveckling och införande för identiteter och åtkomst för robotar.*

# Referenser

Dataskyddsförordningen (EU) 2016/679 (GDPR)

Förvaltningslagen (2017:900)

HSA-policy, version 4.1, 2018-03-13

Identitetsaspekter på Robotic Process Automation (workshop), version 1.0, 2019-05-03

Kommunallagen (2017:725)

Lag (2001:454) om behandling av personuppgifter inom socialtjänsten

Patientdatalagen (2008:355) (PDL)

Referensarkitektur för Identitet och Åtkomst, Rev A, 2017-08-16

Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (SOSFS 2016:40)

Socialtjänstlagen *2001:453*

Tillitsramverk Identifieringstjänst SITHS, 2019-05-15

Tillitsramverket för Svensk e-legitimation, version 2019-09-19

# Bilaga 1 Juridisk Översikt

I denna bilaga beskrivs de rättsliga förutsättningarna och juridiska områden som behöver vidareutvecklas kopplat till RPA.

## Rättsliga förutsättningar

I detta avsnitt presenteras en övergripande genomgång av de rättsliga förutsättningarna för identiteter och åtkomststyrning av RPA inom vård och omsorg.

*Patientdatalag (2008:355) (PDL)*
Det finns inga hinder i patientdatalagen för att använda automatiserade processer vid hantering av journaldata. Det finns heller inga hinder för robotar att få åtkomst till journaluppgifter, varken inom den egna vårdgivaren eller inom ramen för sammanhållen journalföring.

Roboten behöver sannolikt ha en tydlig koppling till en fysisk individ som är ansvarig för den bearbetning som utförs. Denna individ ska ha egenskaper som skulle möjliggöra att den tilldelas samma behörighet som roboten. Om journaldata från flera vårdgivare ska hanteras genom direktåtkomst (sammanhållen journalföring) behöver det även finnas ett samtycke från patienten för åtkomst. I dagsläget är det normala att samtycket registreras vid själva vårdmötet och för den aktuella vårdenheten, men det skulle kunna samlas in i förväg och även gälla på vårdgivarnivå så länge patienten kan överblicka vårdprocessen och involverade vårdgivare.

Den individuella behörighetstilldelningen, med behovs- och riskanalys, behöver precis som för fysiska personer genomföras av en verksamhetschef.

*Underskrifter*

I de fall en elektronisk underskrift ska utföras (egenhändig underskrift) ska det utföras av en fysisk person. Krav på underskrift kan följa av interna rutiner eller av författning. I författningar betecknas ett underskriftskrav med ett antal olika termer och uttryck, såsom underskriven, undertecknad eller namnteckning. Ibland kompletteras de olika termerna med termen egenhändig. De olika beteckningarna har sannolikt samma innebörd, nämligen att verifiera utställaren av handlingen och ge skydd mot förfalskning och förnekande.

Underskriftskrav har på senare tid i vissa författningar fått en teknikoberoende innebörd och kan uppfyllas såväl genom undertecknande på papper som med elektroniska medel. Det är i linje med EU:s strävan är att få bort nationella formkrav på underskrifter för att främja den inre marknaden i form av digitala tjänster och handel. Det främsta instrumentet är eIDAS-förordningen[10]. Den gäller som lag i Sverige.

Av förordningen framgår att en elektronisk underskrift inte får förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att underskriften har elektronisk form eller inte uppfyller kraven för kvalificerade elektroniska underskrifter. En kvalificerad elektronisk underskrift ska ha motsvarande rättsliga verkan som en handskriven underskrift.

[10] Nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

När det gäller underskriftskrav i äldre författningar är det inte självklart att denna kan ersättas av elektroniska signaturer. I eIDAS-förordningen finns ett förbehåll för sådana situationer.

Förordningen påverkar inte nationell rätt eller unionsrätt som avser ingående av avtal och deras giltighet eller andra rättsliga eller förfarandemässiga skyldigheter avseende formkrav. En enskild bedömning av underskriftskravets innebörd måste därför göras där det förekommer i äldre författningar. Bedömningen ska göras mot bakgrund av samtliga relevanta omständigheter såsom bestämmelsens rättsliga miljö och hur kravet tidigare har bedömts.

*Förvaltningslagen (2017:900)*

Förvaltningslagen tillåter automatiserade beslut för statliga myndigheter men inte för kommunala (beslut som har någon typ av rättsverkan för individen). Enligt 28 § Förvaltningslagen får ett beslut fattas av en befattningshavare ensam eller av flera gemensamt ”eller automatiserat”. En robot får således fatta beslut på en statlig myndighets vägnar utan någon inblandning av en mänsklig hand. Det är dock inte tillåtet inom kommunal förvaltning. Förvaltningslagen är nämligen subsidiär i förhållande till annan lag eller en förordning, dvs. om en bestämmelse i annan lag eller förordning avviker från förvaltningslagen, har bestämmelsen företräde framför förvaltningslagen (4 §). Sådana avvikande bestämmelser om beslutanderätt finns i kommunallagen. Regeringen har tillsatt en kommitté för att se över frågan om automatiserade beslut i kommunal förvaltning.[11]

*Dataskyddsförordningen (EU) 2016/679 (GDPR)*

GDPR tillåter inte automatiserade beslut som inbegriper profilering[12] av känsliga personuppgifter (art. 22).[13] Det finns två undantag; samtycke och ”viktigt allmänt intresse”. Medvetslösa patienter som är föremål för någon form av automatiserad vård och behandling som innefattar automatiserade beslut och profilering kan rimligen inte samtycka till automatiserade beslut och profilering. Oklarhet råder om undantaget ”viktigt allmänt intresse” är tillämpligt i denna situation. I förarbetena nämns bl.a. socialtjänst och Rättsmedicinalverket som viktiga allmänna intressen, men inte hälso- och sjukvård.

*Lag (2001:454) om behandling av personuppgifter inom socialtjänsten*

Denna lag innehåller bestämmelser om hur personuppgifter får behandlas inom socialtjänsten och är en kompletterande lag till GDPR. Lagstiftningen gör klart att personuppgifter får behandlas inom socialtjänsten oavsett vad den registrerade har för uppfattning därom men sätter ett antal vissa begräsningar, till exempel kring vilka sammanställningar som kan göras. Inget i lagstiftningen bedöms dock direkt hindra möjligheten att använda sig av RPA inom

[11] Se regeringens direktiv 2020:10
[12] Profilering handlar om att behandla personuppgifter för att bedöma personliga egenskaper hos en individ. Det definieras i art. 4.1 i GDPR: " profilering: varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar".
[13] Tolkningen av vad som faktiskt är ett automatiserat beslut behöver man dock borra lite djupare i. Om själva beslutet faktiskt tas av en människa i slutänden så kan det troligen inte ses som ett automatiserat beslut att verkställa detta.

Socialtjänsten för handläggning av ärende och beslutsfattande av en fysisk person. Rättsläget är dock oklart om historiska uppgifter kan hanteras av en RPA på grund av bestämmelserna i lagen om sammanställningar.

*Socialtjänstlag (2001:453) (SOL)*

SOL anger både kommunens skyldigheter och den enskildes rättigheter när det gäller den enskildes rätt till bistånd och kommunens insats av åtgärder. Där SOL framförallt påverkar möjligheten att använda sig av RPA inom Socialtjänsten torde vara de krav som ställs på beslutsfattare.

När det gäller handläggning av vissa uppgifter inom socialtjänsten ställer nämligen 3 kap SOL krav på att utförandet av uppgifterna sker av personal med tillräcklig utbildning och avlagd examen eller motsvarande. Detta gäller särskilt utförande av uppgifter som riktar sig mot barn och unga (se 3 kap § 3a SOL). I praktiken innebär detta att alla uppgifter som faller inom dessa domäner inte kan utföras enbart av ickemänsklig personal såsom robotar. Vidare framgår generellt att utförande av uppgifter inom socialtjänsten ska ske av personal med lämplig utbildning och erfarenhet. Detta allmänna krav torde innebära att en hantering som sker av RPA måste vara tillräckligt nära knuten och möjliggöra en insyn från en ansvarig handläggare i sammanhanget. Detta kan uppnås i praktiken genom att roboten inte själv kan fatta beslut i ett enskilt ärende utan detta beslut de facto måste fattas av en ansvarig handläggare och RPA ses mer som ett beslutstöd. Det ska dock särskilt understrykas att SOL:s krav inte gäller enbart själva beslutsfattandet utan själva utförandet av uppgifterna. Eventuell framtida förändringar av möjligheten att använda sig av automatiserade beslut inom socialtjänsten måste beakta och omhänderta kraven kring lämplig personal i SOL.

*Kommunallag (2017:725)*

Alla myndighetsbeslut är ett utflöde från myndighetens ledning. Inom den kommunala sfären är en nämnd ”myndigheten”. Nämnden kan emellertid enligt kommunallagen (2017:725) överföra sin beslutanderätt genom delegering till antingen ett nämndpresidium, ett utskott i nämnden, en ledamot eller ersättare i nämnden eller till en anställd i kommunen. Anställda i en kommun eller ett landsting har alltså inte någon självständig beslutanderätt utan den måste ges från nämnden.

Beslut som fattas med stöd av delegering, av ett presidium, en förtroendevald eller en anställd, avses särskilt och ska, i den omfattning nämnden bestämmer, anmälas till nämnden. Beslutet fattas av delegaten på nämndens vägnar. Beslut som inte behöver anmälas ska protokollföras särskilt om beslutet kan överklagas med laglighetsprövning enligt 13 kap kommunallagen. Inte heller för utskott, presidium, förtroendevalda eller anställa lämnas något utrymme i kommunallagen för automatiserat beslutsfattande. Därmed kan inte robotar fatta beslut automatiskt inom kommunal verksamhet, så robotar bör snarare ses som en möjlighet till avancerat beslutsstöd.

Frågan kring delegation och om delegat får använda automatiserat beslutsstöd kan behöva förtydligas i samband med varje nämnds beslut om delegation, även om det inte finns ett formellt lagkrav för det.

## Rättsliga områden som behöver vidareutvecklas

Det finns ett behov av att se över det juridiska regelverket kopplat till RPA. Ansvarsfrågor behöver förtydligas vad gäller mjukvara, innehåll och hantering av algoritmer, t.ex. vad som får

utföras, hur det ska presenteras för berörda och hur de berörda kan påverka hanteringen. En utmaning är hur medborgare ska kunna få en klar och tydlig information om den logik som ligger bakom automatiserade beslut. GDPR ställer enbart krav på ”meningsfull” information om logiken (art. 13.1 f), vilket kanske är ett för lågt ställt krav för att möta behovet av förståelse och transparens kring sådana beslut.

Som beskrivet ovan är det oklart om GDPR förbjuder automatiserade beslut som inbegriper profilering kring hälso- och sjukvårdsinsatser (artikel 22) och Regeringen har, vid en översyn av registerförfattningar inom Socialdepartements ansvarsområde med anledning av GDPR, sett ett behov av att frågan utreds, men detta har inte genomförts än (prop. 2017/18:171). Det behöver även ses över hur frågan förhåller sig till SOL.

Det behöver förtydligas i svensk lag vilka beslut som kan fattas automatiserat eller inte inom hälso- och sjukvården. PDL är främst utformad för en reaktiv vård och lagen behöver förändras för att hantera mer preventiv vård (förebyggande hälso- och sjukvård).

Socialstyrelsens föreskrifter skulle vinna på att kompletteras med beskrivning av hur RPA kan användas i Hälso- och sjukvården.

Vad gäller SOL behöver kraven på personals utbildning och kompetens bedömas utifrån möjligheten till automatiserat beslutsfattande och hur dessa krav kring kvalitetssäkerhet i ärenden och besluten bäst kan tillvaratas.

# Bilaga 2 Informationsmängder i HSA

I denna bilaga beskrivs vilka objekt och attribut som behöver kompletteras eller hanteras i HSA-schemat för att kunna hantera identiteter och åtkomststyrning för robotar. Specificeringen är en första version som behöver bearbetas i enlighet med de ordinarie schemauppdaterings-processerna innan de fastställs i HSA Policygrupp. Namn, LDAP-namn och innehållsbeskrivningar som beskrivs nedan ska ses som ett första förslag att vidarebearbeta i den ordinarie processen.

Observera att det i inom ramen för alla HSA-schemaförändringar behöver genomföras analyser av vilka dokument, gränssnitt och tjänster som påverkas. Till exempel påverkas nästan alltid det administrativa gränssnittet för HSA, HSA Admin, samt webservices. Även HSA:s styrande och stödjande dokument kan påverkas då regelverk och rutiner för RPA inte beskrivs i dagsläget.

## Nytt objekt för robotar i HSA

En ny objekttyp föreslås i HSA om robotar ska hanteras.

| **Benämning, *LDAP-namn*** | **Innehållsbeskrivning** |
|---|---|
| Robot, *hsaRPA* | En objektklass som innehåller information om robotar. |

En robot ska kunna identifieras på flera sätt som just en robot. En unik objektsklass är den grundläggande tekniska markeringen. Objektklassen bör i detta fall vara en tilläggsobjektsklass till grundobjektsklassen som lämpligen är ett personobjekt eftersom roboten behöver kunna agera som en människa i olika applikationer.

## Attribut för robotar i HSA

Nedan presenteras vilka attribut som är viktiga för robotar. Några finns redan i HSA och kan användas, medan några är nya attribut som behöver införas.

| **Benämning, *LDAP-namn*** | **Innehållsbeskrivning** | **Kommentar** |
|---|---|---|
| HSA-id, *hsaIdentity* | Obligatorisk, unik identifierare för objekt i HSA. | |
| Tilltalsnamn, *givenName (gn)* | Robotens tilltalsnamn. | Vissa kan eventuellt få problem om det bara finns ett efternamn och inte ett fullständigt namn för roboten. |
| Efternamn, *sn (surName)* | Robotens efternamn ska alltid vara ”Robot”. | För att visuellt kunna identifiera en robot i olika sammanhang är det lämpligt att det i namnet framgår att det är en robot. |

| Benämning, *LDAP-namn* | Innehållsbeskrivning | Kommentar |
|---|---|---|
| Beskrivning, *description* | Beskrivning av robotens process. | En robots identitet är unikt kopplad till vad den gör. Därför blir beskrivningen mycket viktigare för robotar än för andra objekt i HSA och behöver vara obligatorisk att ange.<br>Det är oklart om ett särskilt beskrivningsfält behövs för robotens beskrivning eller om ordinarie attribut som beskrivs här kan användas. |
| e-postadress, *mail (rfc822Mailbox)* | Uppgift om e-postadress. | En robot kan behöva en e-postadress om processen som utförs innefattar hantering av e-post.<br>Frivilligt attribut. |
| Domäninloggningsnamn | Inloggningsnamn i AD-domän som skrivs in i SITHS-certifikatet. Domäninloggningsnamnet ska vara unikt. | En robot kan behöva ett domäninloggningsnamn om processen som utförs innefattar samverkan med AD.<br>Frivilligt attribut. |
| Robottyp | Typ av robot. | Troligen kan robotar med tiden behöva delas in i olika typer (eller kategorier). Om så görs behöver det vara ett definierat kodverk inom HSA.<br>Frågan om vilka typer av robotar som finns behöver i så fall utredas vidare.<br>Frivilligt attribut. |
| Titel | Titel för roboten som beskriver robotens uppgift. | Titel önskas ibland i vissa applikationer och |

| Benämning, *LDAP-namn* | Innehållsbeskrivning | Kommentar |
|---|---|---|
| | | möjligheten att sätta en titel på en robot ger ytterligare ett sätt att beskriva att det är en robot som avses. Till exempel kan titel användas för att göra loggar om robotens aktiviteter mer lättläst.<br>Frivilligt attribut. |
| Organisatorisk hemvist | HSA-id för enheten som roboten tillhör. | Utöver organisatorisk hemvist kan även *distinguishedName* (DN) användas för att peka ut var i katalogen som roboten finns. |
| Startdatum, *startDate* | Startdatum då en robot startas upp. | Datum då roboten erhåller sitt HSA-id.<br>Frivilligt attribut. |
| Slutdatum, *endDate* | Slutdatum då roboten avslutas. | Obligatoriskt attribut. |
| Robotansvarig | HSA-id för den personen som är verksamhetsmässigt ansvarig för robotens användning. | Den ansvarige personen behöver vara anställd i aktuell organisation i HSA.<br>Obligatoriskt attribut. |
| Robotförvaltare | HSA-id för den personen som förvaltar roboten, dvs. aktiverar roboten och sköter driften av roboten. | Förvaltaren behöver finnas i aktuell organisation i HSA.<br>Eventuellt kan det behöva finnas mer än en förvaltare.<br>Obligatoriskt attribut. |

De attribut som redan finns i HSA som ska användas av robotar behöver eventuellt införa nya innehållsbeskrivningar om dessa påverkas av att de även kan användas för robotar. Översyn behöver göras i samband med införande av ny schemaversion.

När det gäller slutdatum för roboten behöver det finnas någon typ av regel kring maximal tid som en robot får läggas upp för. Därför blir slutdatum obligatoriskt att ange till skillnad från personobjekt som kan ha fältet tomt med betydelsen tillsvidare.

Det behöver finnas någon typ av regel kring intervall för verifiering av robotobjektets data så att det är korrekt. Troligen kan samma intervall användas för robotar som intervallet för kontroll av personposters aktualitet, dvs. minst kvartalsvis. Kontrollen är viktig för att säkerställa att förändringar och avslut av robotar hanteras och uppdateras korrekt över tid.

Förändringar av roboten behöver arkiveras, men huvudkällan för förändringarna är lämpligen i SDD.

Information om ett robotobjekt bör arkiveras minst 5 år i HSA efter avslut. Av attributen som registreras om en robot behöver minst följande arkiveras i samband med avslutet:

- HSA-id
- Tilltalsnamn
- Efternamn
- Ansvarig person
- Beskrivning
- Robottyp

## Behörighetshantering av robotar i HSA

För att kunna utföra aktuella processer behöver robotar ha korrekt behörighet i olika användargränssnitt. Eftersom roboten agerar som en människa behöver det finnas möjlighet till samma typ av behörighetsfunktioner som det finns för personer. Inom vård och omsorgs nationella tjänster behöver det ibland finnas medarbetaruppdrag[14] för att nå vissa tjänster.

Observera att varje systemägare/informationsägare måste styra vilka funktioner som får vara åtkomliga för robotar. Det kan styras t.ex. genom att endast tillåta vissa certifikatstyper vid inloggning i tjänsten.

Nedan beskrivs vilken behörighetsinformation ifrån HSA som *kan* vara aktuell att nyttja för robotar och som därmed behöver göras möjlig att koppla till en robot:

| **Benämning, *LDAP-namn*** | **Innehållsbeskrivning** | **Kommentar** |
|---|---|---|
| medarbetaruppdragets medlemmar (vårdmedarbetaruppdragets medlemmar) | HSA-id för de som har vårdmedarbetaruppdraget samt eventuellt start- och slutdatum för hur länge uppdraget gäller. | |
| Administrativa uppdragets medlemmar, personer | HSA-id för de som har det administrativa medarbetaruppdraget samt eventuellt start- och slutdatum för hur länge uppdraget gäller. | |

[14] Det finns två typer av medarbetaruppdrag; vårdmedarbetaruppdrag och administrativa uppdrag.

| Benämning, *LDAP-namn* | Innehållsbeskrivning | Kommentar |
|---|---|---|
| Individuell egenskap för it-tjänster, *hsaSystemRole* | Beskriver en tilldelad individuell egenskap för roboten i ett visst system utan koppling till organisation. | Finns redan i HSA. |

## Certifikatsinformation för robotar i HSA

Om SITHS-certifikat användas för robotar behöver certifikats- och kortinformation finnas i HSA enligt de ordinarie rutinerna för integrationer mellan SITHS och HSA.

Se tabell nedan för översikt över SITHS-information som behöver hanteras för robotar i detta fall:

| Benämning, *LDAP-namn* | Innehållsbeskrivning | Kommentar |
|---|---|---|
| Certifikatsnummer, *serialNumber* | SITHS-certifikatets serienummer. Denna information finns endast i HSA om det finns giltiga SITHS-certifikat. | |
| Giltigt fr.o.m., *validNotBefore* | Det datum som SITHS-certifikatet är giltigt från och med. | |
| Giltigt t.o.m., *validNotAfter* | Det datum som SITHS-certifikatet är giltigt till och med. | |
| HCC, *userCertificate* | Giltiga SITHS-certifikat | |
| Kortnummer, *cardNumber* | Kortnummer för SITHS-kortet. Denna information finns endast i HSA om det finns giltiga SITHS-certifikat kopplade till kortet. | |

Utöver ovanstående behöver en del teknisk information finnas kring robotar på samma sätt som för andra objekt, t.ex. senast ändrad av, senaste förändringstidpunkt, pekare och internt UUID för objektet finnas för att nämna några exempel. Även detta behöver utredas vidare i samband med den ordinarie schemauppdateringsprocessen.