|  |  |
| --- | --- |
|  | Infrastructure:directory:authorizationmanagement  Tjänstekontraktsbeskrivning  Version 1.0\_RC6  2014-10-22 |

Innehåll

[1 Inledning 6](#_Toc401743782)

[1.1 Svenskt namn 6](#_Toc401743783)

[1.2 WEB beskrivning 6](#_Toc401743784)

[2 Versionsinformation 7](#_Toc401743785)

[2.1 Version 1.0\_RC5 7](#_Toc401743786)

[2.1.1 Oförändrade tjänstekontrakt 7](#_Toc401743787)

[2.1.2 Nya tjänstekontrakt 7](#_Toc401743788)

[2.1.3 Förändrade tjänstekontrakt 7](#_Toc401743789)

[2.1.4 Utgångna tjänstekontrakt 7](#_Toc401743790)

[2.2 Version tidigare 7](#_Toc401743791)

[3 Tjänstedomänens arkitektur 8](#_Toc401743792)

[3.1 Flöden 8](#_Toc401743793)

[3.1.1 Flöde – Hämta information om anställd/uppdragstagare 8](#_Toc401743794)

[3.1.2 Obligatoriska kontrakt 10](#_Toc401743795)

[3.2 Adressering 11](#_Toc401743796)

[3.3 Aggregering och engagemangsindex 11](#_Toc401743797)

[4 Tjänstedomänens krav och regler 11](#_Toc401743798)

[4.1 Informationssäkerhet och juridik 11](#_Toc401743799)

[4.2 Icke funktionella krav 11](#_Toc401743800)

[4.2.1 Krav på en tjänsteproducent 11](#_Toc401743801)

[4.2.2 Övriga krav 14](#_Toc401743802)

[4.2.3 Krav på en tjänstekonsument 14](#_Toc401743803)

[5 Tjänstedomänens meddelandemodeller 15](#_Toc401743804)

[5.1 V-MIM 15](#_Toc401743805)

[5.2 Formatregler 15](#_Toc401743806)

[5.2.1 RIV-specifikation 15](#_Toc401743807)

*[6](#_Toc401743808)* [Tjänstekontrakt 16](#_Toc401743808)

[6.1 GetCredentialsForPersonIncludingProtectedPerson 16](#_Toc401743809)

[6.1.1 Version 16](#_Toc401743810)

[6.1.2 Fältregler 16](#_Toc401743811)

[6.1.3 Tjänstekontraktsspecifika krav och regler 18](#_Toc401743812)

[6.1.4 SLA-krav 18](#_Toc401743813)

[6.1.5 Logiska fel 19](#_Toc401743814)

[6.1.6 Annan information om kontraktet 22](#_Toc401743815)

[6.2 GetCredentialsForPerson 22](#_Toc401743816)

[6.2.1 Version 22](#_Toc401743817)

[6.2.2 Fältregler 22](#_Toc401743818)

[6.3 GetPersonAuthorizedToSystemIncludingProtectedPerson 23](#_Toc401743819)

[6.3.1 Version 23](#_Toc401743820)

[6.3.2 Fältregler 23](#_Toc401743821)

[6.3.3 Tjänstekontraktsspecifika krav och regler 25](#_Toc401743822)

[6.3.4 SLA-krav 25](#_Toc401743823)

[6.3.5 Logiska fel 25](#_Toc401743824)

[6.3.6 Annan information om kontraktet 27](#_Toc401743825)

[6.4 GetPersonAuthorizedToSystem 28](#_Toc401743826)

[6.4.1 Version 28](#_Toc401743827)

[6.4.2 Fältregler 28](#_Toc401743828)

**Revisionshistorik**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | Revision Nr | Revision Datum | Beskrivning av ändringar | Ändringar gjorda av | Granskad av |
|  | PA1 | 2013-10-30 | * Första version, kopierad från tidigare arkitekturella beslut för infrastructure:directory:organization innan uppdelningen i flera domäner | Henrika Littorin |  |
|  | PA2 | 2014-01-23 | * Ändrat format för specialitycode och specialityName. Tagit bort kommentarer. | Robert Lundmark |  |
|  | PA3 | 2014-01-30 | * + Ändrat felkod och meddelanden | Robert Lundmark |  |
| 1.0\_RC2 |  | 2014-03-18 | Justeringar enligt avstämning med Ineras IT-arkitekt och A&R I samt efter intern genomgång:   * Infört två alternativ för hantering av flera anslutna tjänsteproducenter (katalogtjänster) med beskrivning av fördelar för respektive alternativ * Justering av hänvisning till arkitekturella beslut (nu gemensamma för tre domäner), borttag av referenser till borttagna AB:n samt justering av numrering av övriga AB:n * Justerat skrivning om styrning av åtkomst * Borttag av några exempel på krav som kan ställas på tjänstekonsument * Borttag av referens till HSA-policyn för krav på producent * Borttag av SLA-krav på antal avbrott och längd på avbrott | Henrika Littorin, Ronny Nilsson |  |
| 1.0.0.RC\_03 |  | 2014-07-22 | Justeringar enligt granskningsprotokoll VIS samt T   * Svenskt namn på domänen * Överflytt av beskrivning av alternativ för aggregering/engagemangsindex till AB * Överfört till ny mall | Henrika Littorin |  |
| 1.0\_RC4 |  | 2014-08-20 | * Justerat namnet på tjänstedomänen till endast gemener enligt besked från Sonja Kantonen * Återgått till gammal benämning av versioner enligt besked från Leo Röjerås | Henrika Littorin |  |
| 1.0\_RC5 |  | 2014-09-05 | * Tillägg av nytt avsnitt ”Svenskt namn” samt justering under rubriken WEB beskrivning enligt ny mall för TKB | Henrika Littorin, Inera AB |  |
| 1.0\_RC6 |  | 2014-10-22 | * Korrigerat felkoder och varningar. | Robert Lundmark, Cybercom AB |  |

**Referenser**

|  |  |  |  |
| --- | --- | --- | --- |
| Namn | Dokument | Kommentar | Länk |
| R1 | Arkitekturella beslut – infrastructure:directory:authorizationmanagement | Version 1.0\_RC5, 2014-09-05 | [http://rivta.se/domains/infrastructure\_directory\_authorizationmanagement.html](http://rivta.se/domains/infrastructure_directory_organization.html) |
| R2 | RIVTA flera dokument | Finns på Webben | <http://rivta.se/> |
| R3 | CeHis Råd Utlämnande av information från HSA | Version 1.0, 2013-04-25 | [www.inera.se/hsa](http://www.inera.se/hsa), under Dokument och Stödjande |
| R4 | Tillitsramverk: HSA-policy | Version 3.6, 2013-02-05 | [www.inera.se/hsa](http://www.inera.se/hsa), under Dokument och Avtal |
| R5 | RIV Informationsspecifikation HSA Struktur och innehåll | Version 4.3, 2014-04-29 | [www.inera.se/hsa](http://www.inera.se/hsa), under Dokument och Styrande |
| R6 | Behörighetsmodell för hälso- och sjukvården | Version 1.0, 2011-12-09 | [www.inera.se/hsa](http://www.inera.se/hsa), under Behörighetsmodell |

**Förkortningar**

|  |  |  |
| --- | --- | --- |
| Förkortning | Betydelse | Kommentar |
|  |  |  |

# Inledning

Detta är beskrivningen av tjänstekontrakten i tjänstedomänen **infrastructure**:**directory**:**organization**.

Den svenska benämningen är **Infrastruktur** Katalogtjänster **Organisationsuppgifter**.

Tjänstekontrakten är baserade på RIVTA 2.1 [R2] och reglerade genom arkitekturella beslut [R1].

Tjänstekontraktsbeskrivningen är en kravspecifikation. Den skall fungera som ett teknikneutralt, formellt regelverk som reglerar integrationskrav för parter (tjänstekonsumenter och tjänsteproducenter) som avser ansluta system för samverkan enligt dessa tjänstekontrakt. Tjänstekontraktsbeskrivningen är också ett viktigt underlag för skapande av de tekniska kontrakten (scheman och WSDL-filer).

Detta dokument kompletterar reglerna i de tekniska kontrakten. Tjänsteproducenter och tjänstekonsumenter ska m.a.o. följa såväl de maskintolkbara reglerna i de tekniska kontrakten, så väl som de regler som uttrycks verbalt i detta dokument.

## Svenskt namn

infrastruktur:katalogtjänster:behörighetshantering

behörighetshantering

## WEB beskrivning

Tjänstedomänens ändamål är att förse övriga tjänster med kvalitetssäkrad och aktuell behörighetsgrundande information.

Användningsområden utgörs främst av sökningar efter behörighetsgrundande egenskaper i form av information om personers uppdrag kopplade till organisation samt anställningsrelaterade och personliga egenskaper av betydelse för åtkomst till information, vilket ofta, men inte alltid, är relaterat till Patientdatalagen, PDL.

***I arbetet har följande personer deltagit:***

*Tjänstedomänansvarig*:

Henrika Littorin, Inera AB

*Projektgrupp 2013-05-07 – 2013-08-16*

Johan Zenk, Landstinget i Östergötland, ordförande HSA Förvaltningsgrupp

Henrika Littorin, Inera AB, tjänsteansvarig HSA

Ronny Nilsson, Inera AB, konsult och teknisk expert HSA

Björn Skeppner, Inera AB, IT-arkitekt

*Utveckling och test*

Robert Lundmark, Cybercom Sweden AB

Ronny Nilsson, Inera AB, konsult och teknisk expert HSA

# Versionsinformation

Denna revision av tjänstekontraktsbeskrivningen handlar om version **1**.**0**.**0**.

Observera att version för detta dokument och domänen måste vara lika. Detta för att spårbarheten inte skall brytas.

## Version 1.0\_RC5

### Oförändrade tjänstekontrakt

Inga kontrakt har tidigare varit publicerade.

### Nya tjänstekontrakt

* GetCredentialsForPersonIncludingProtectedPerson
* GetCredentialsForPerson
* GetPersonAuthorizedToSystemIncludingProtectedPerson
* GetPersonAuthorizedToSystem

Se kontraktsbeskrivningar under kap 6 Tjänstekontrakt. Se även AB-2.2 [**Error! Reference source not found.**].

### Förändrade tjänstekontrakt

Inga tjänstekontrakt har förändrats.

### Utgångna tjänstekontrakt

Inga tjänstekontrakt har utgått.

## Version tidigare

-

# Tjänstedomänens arkitektur

## Flöden

### Flöde – Hämta information om anställd/uppdragstagare

Det viktigaste syftet för tjänstedomänen är att medverka till att rätt person får åtkomst till rätt information och/eller rätt funktionalitet vid rätt tillfälle. Detta görs genom att tjänsteproducenten förser tjänstekonsumenten med relevanta personliga och uppdragsrelaterade egenskaper som sedan kan utvärderas mot ett regelverk för åtkomst i tjänsteproducentens tjänst.

En säker autentisering och auktorisering av användare är en viktig grundkomponent i både administrativa och vårdprocesser av olika slag. Genom att inhämta egenskaper för användare från en gemensam källa istället för att varje system lagrar och underhåller sin egen användardatabas får man både en säkrare hantering av behörigheter och en minskad administration. Det underlättar också för användaren som kan logga in med hjälp av sitt SITHS-kort (sin e-legitimation) och därmed slipper hålla ordning på ytterligare ett användar-id och lösenord. Slutligen är det också, i fallet vårdprocesser, ett sätt för vårdgivaren att uppfylla kraven i t.ex. Patientdatalagen.

Tjänstekontrakten som stödjer detta flöde är

* GetCredentialsForPersonIncludingProtectedPerson (se avsnitt 6.1) och GetCredentialsForPerson (se avsnitt 6.2)
  + Levererar bland annat information om medarbetaruppdrag och legitimerad yrkesgrupp.
* GetPersonAuthorizedToSystemIncludingProtectedPerson (se avsnitt 6.3) och GetPersonAuthorizedToSystem (se avsnitt 6.4)
  + Levererar bland annat information om tilldelad behörighet vid rollbaserad accesskontroll.

#### Arbetsflöde

1. Flödet startar generellt när en användare önskar åtkomst till information och/eller funktionalitet i tjänstekonsumentens tjänst (nedan kallad Tjänsten)
   1. Tjänstekonsumenten kan här antingen hämta de behörighetsgrundande egenskaperna i det ögonblick då användaren försöker få åtkomst till informationen eller i förväg genom regelbunden (ofta dygnsvis) inhämtning av behörighetsgrundande egenskaper för samtliga registrerade användare
2. Användaren loggar in i Tjänsten, oftast med SITHS-kort eller e-legitimation/bank-ID
3. Användarens HSA-id eller person-id extraheras och skickas i överenskommet tjänstekontrakt till tjänsteproducentens tjänst (nedan kallad Katalogen)
   1. Om inloggning skett med användar-id och lösenord måste en översättning till HSA-id eller person-id ske i Tjänsten
   2. Extraheringen kan göras av tjänsten själv eller i en IdP, Identity Provider
4. Katalogen verifierar om aktuellt HSA-id/person-id återfinns i Katalogen
   1. Om så inte är fallet skickas ett meddelande till Tjänsten att användaren saknas och flödet fortsätter då enligt punkt 7 nedan
5. Om användaren återfinns i Katalogen extraheras de egenskaper som specificerats i aktuellt tjänstekontrakt och skickas till Tjänsten
   1. I flera fall ompaketeras egenskaperna i en IdP till en biljett enligt nationell standard innan de skickas vidare till Tjänsten
6. Användarens egenskaper från Katalogen värderas mot det regelverk som fastställts för åtkomst till information/funktionalitet i Tjänsten
   1. För tjänster som lyder under Patientdatalagen inhämtas till värderingen även egenskaper för den information användaren önskar åtkomst till samt information om samtycke och spärr
7. Tjänsten meddelar användaren om vilken åtkomst användaren har samt ger åtkomst enligt gällande regelverk
   1. Även en användare som inte hittats i Katalogen skulle kunna ges åtkomst till information/funktionalitet som inte kräver en autentiserad användare, det är upp till den som definierar regelverket för Tjänsten
8. Tjänsten meddelar användaren resultatet av sökningen och presenterar den information som erhållits från Katalogen samt eventuella andra informationskällor

##### Roller

|  |  |
| --- | --- |
| Namn/beteckning | Beskrivning alt. referens |
| Användare | Utgörs som regel av en medarbetare inom vården (som loggar in i en tjänst/ett system/en applikation vars behörighet lyder under Patientdatalagen alternativt tillämpar rollbaserad accesskontroll och där rollen lagras i separat katalogtjänst) |
|  |  |

#### Flödesdiagram



### Obligatoriska kontrakt

|  |  |
| --- | --- |
| **Tjänstekontrakt** | **Flöde** |
| GetCredentialsForPersonIncludingProtectedPerson (se avsnitt **Error! Reference source not found.**) | Hämta behörighetsgrundande egenskaper |
| GetCredentialsForPerson (se avsnitt **Error! Reference source not found.**) | Hämta behörighetsgrundande egenskaper |
| GetPersonAuthorizedToSystemIncludingProtectedPerson (se avsnitt 6.3) | Hämta behörighetsgrundande egenskaper |
| GetPersonAuthorizedToSystem (se avsnitt 6.4) | Hämta behörighetsgrundande egenskaper |

## Adressering

Tjänstedomänen tillämpar Tjänsteplattformens systemadressering. Tjänstekonsumenten adresserar Tjänsteplattformen, Tjänsteplattformen adresserar tjänsteproducenten med HSA-id för tjänstekonsumenten.

## Aggregering och engagemangsindex

För närvarande är aggregering eller engagemangsindex ej aktuellt, då endast en tjänsteproducent är ansluten till tjänstedomänen.

I samband med att fler tjänsteproducenter ansluter till tjänstedomänen behöver sökningen från anropande tjänstekonsument realiseras mot flera tjänsteproducenter. Vilken alternativ lösning som ska tillämpas när denna situation uppstår är ännu inte beslutat, se AB-2.3 [**Error! Reference source not found.**].

# Tjänstedomänens krav och regler

Dessa gäller alla tjänstekontrakt i hela tjänstedomänen om inte undantag görs för specifika tjänstekontrakt senare i dokumentet.

## Informationssäkerhet och juridik

Informationsinnehållet i de katalogtjänster som är anslutna som tjänsteproducenter ägs och förvaltas av respektive ansluten organisation/juridisk person. Informationsägarskapet beskrivs ytterligare i utredning utförd av Arkitektur och Regelverk Säkerhet (se avsnitt 4 i [R3]). I de fall som producenten i sin katalogtjänst lagrar information för flera informationsägare är det upp till varje ansluten organisation att avgöra vilken information som ska lämnas ut till vilken mottagare.

Tjänsteproducenten ansvarar därmed för att information endast lämnas ut till de tjänstekonsumenter som respektive informationsägare godkänt. Det tydliggörs här eftersom det avviker från T-boken i det att Tjänsteplattformen då inte ansvarar för den tekniska åtkomstkontrollen (ej möjligt när systembaserad adressering tillämpas). Om informationsägaren har behov av att reglera åtkomst per tjänstekonsument, ska tjänsteproducenten filtrera svaret enligt informationsägarens önskemål. Observera att det är regionala policyer snarare än lagar och förordningar som styr i vilken grad tjänsteproducenten ska begränsa åtkomst för en viss tjänstekonsument. Kunskapen om tjänsteproducentens identitet (d.v.s. ursprunglig tjänstekonsument i anropskedjan) får bara användas för teknisk åtkomstbegränsning på så sätt att svaret blir som om de vårdgivare/vårdenheter vars verksamhetschef inte godkänner aktuell tjänsteproducent varit exkluderade i frågan.

## Icke funktionella krav

### Krav på en tjänsteproducent

Följande krav skall beaktas då ett system agerar som en tjänsteproducent för tjänstedomänens ingående tjänster.

Tjänsteproducenten ansvarar för

* att tillhandahålla tjänsten i enlighet med denna tjänstekontraktsbeskrivning med avseende på
  + tjänstedomänens arkitektur (se avsnitt **Error! Reference source not found.**)
  + informationssäkerhet och juridik (se avsnitt **Error! Reference source not found.**)
  + felhantering (se avsnitt **Error! Reference source not found.**)
  + SLA:er (se avsnitt **Error! Reference source not found.**)
  + informationsinnehåll (specificeras för resp. tjänstekontrakt under avsnitt 6)
  + tjänstedomänens meddelandemodeller (se avsnitt **Error! Reference source not found.**)
* att vid behov förmedla kontakt mellan tjänstekonsument och informationsägare, t.ex. i frågor som rör förändring av innehåll
* att (vid behov genom kravställning på anslutna organisationer/informationsägare) tillse att
  + den information som tillhandahålls vid var tid är uppdaterad och korrekt
  + den information som tillhandahålls vid var tid i möjligaste mån är säkrad mot ursprungskällor
    - minst omfattar detta kontroll av namnuppgifter mot Skatteverket samt kontroll av legitimerad yrkesgrupp mot Socialstyrelsens register minst en gång per månad
  + tillämpliga lagar och regelverk, t.ex. Personuppgiftslagen PUL, efterlevs
  + det finns ett dokumenterat regelverk för hur administratörsbehörigheter tilldelas och tas bort
  + uppgifter om koppling mellan HSA-id och individ/organisation samt mellan HSA-id och vårdgivare/vårdenhet arkiveras i minst 10 år efter det att anställning och/eller verksamhet upphört
  + HSA-id behålls då en person byter person-identitet (t.ex. från samordningsnummer till personnummer)
* att upprätthålla en organisation för administration samt för mottagande av driftstörningsinformation
* att förändringar som görs i tjänsten loggas så att det går att spåra vem som gjort en förändring och när
* att särskild hantering av personer med skyddade personuppgifter finns dokumenterad och tillämpas
* att årligen genomföra intern revision för att säkerställa att tjänsteproducenten verkligen uppfyller samtliga krav beskrivna i denna tjänstekontraktsbeskrivning

#### SLA krav

Följande generella SLA-krav gäller för alla tjänsteproducenter som tillhandahåller tjänstekontrakt inom domänen. Observera att för en konsument kan tillgängligheten bli något lägre utifrån t.ex. mellanliggande kommunikationsutrustning, kommunikationsnät och användning av regional tjänsteplattform.

|  |  |  |
| --- | --- | --- |
| **Kategori** | **Värde** | **Beskrivning** |
| Svarstid |  | Definieras per tjänstekontrakt i avsnitt 6. |
| Tillgänglighet | 24x7, 99,9% |  |
| Last |  | Definieras per tjänstekontrakt i avsnitt 6. |
| Aktualitet | 10 minuter | Vid uppdatering av information i katalogtjänsten får det maximalt ta så lång tid innan den informationen används av och returneras via tjänstekontrakten. |
| Återställningstid | 1 dygn | Vid katastrof som bortfall av driftshall |

#### Felhantering

##### Logiska fel

Vid ett **logiskt fel**, d.v.s. förutsättning för att kunna besvara anropet saknas, t ex för att visst nödvändigt objekt eller attributvärde saknas,i de uppdaterande tjänsterna levereras resultCode, resultText.  
Syftet med resultText är att tjänstekonsumenten av tjänsten ska kunna visa upp informationen för användaren.

De värden som resultCode kan returnera är:

* **OK**   
  Transaktionen har utförts enligt uppdraget i frågemeddelandet.
* **ERROR**  
  Transaktionen har INTE kunnat utföras enligt uppdrag i frågemeddelandet p.g.a. logiskt fel.

De felkoder/felmeddelanden som används och som returneras i resultText beskrivs under respektive tjänstekontrakt i kapitel 6.

I möjligaste mån ska resultatet från anropet returneras även om visst/vissa logiska fel förekommer, men då med resultCode=ERROR och en resultText som anger ”Varning”. Då kan anropande program avgöra om uppgifterna ändå kan användas eller inte och på vilket sätt en slutanvändare ska meddelas.

Om resultat inte alls kan returneras, flaggas detta med resultCode=ERROR och en resultText som anger ”Fel”.  
Exempel på fel där resultat inte kan returneras är t ex

* Om sökt identitet saknas i katalogen, eller om identiteten inte avser rätt objekttyp eller felaktigt tillhör flera olika objekt.

Exempel på mindre fel där resultat ändå kan returneras, tillsammans med en varning och utpekning av felet är:

* Då obligatoriska attribut (som skulle returnerats) saknas
* Attribut med värde som inte följer gällande värdemängd
* Värdemängdsattribut med både kod-del och klartext-del men där dessa inte matchar varandra enligt gällande värdemängd
* Attribut med felaktig syntax, t ex
  + Sammansatta attribut saknad någon del (t ex telefontider)
  + Telefonnummer med bokstäver i
  + Telefontider med tim-del med bokstäver eller utanför 0-24
  + E-postadress utan @ eller webbadress utan http://
  + Felaktigt format för datum
  + Etc. etc.

#### Tekniska fel

Vid ett tekniskt fel levereras normalt ett generellt undantag (SOAP-fault).

Exempel på tekniska fel vid anrop till någon av tjänstedomänens tjänstekontrakt där SOAP-fault returneras är:

* Katalogen (eller ev. läskopia) är inte nåbar (ur funktion, överlastad, kommunikationsmässigt eller på annat sätt onåbar)
* Katalogen returnerar att det blev ett internt fel vid sökningen
* Grundläggande information i katalogen, t ex kodtabeller, innehåller felaktig information eller felaktigt strukturerad information.

Exempel på andra tekniska fel är:

* Anslutande tjänst är inte behörig att anropa det aktuella tjänstekontraktet. För denna typ av fel returneras ”http Status 403 – Access is denied”.
* Tjänstekontraktsprogramvaran har slutat fungera. För denna typ av fel returneras ”http Status 503 – Service Temporarily Unavailable”.
* För fatala tekniska fel t ex server-fel, fel på kommunikationsutrustning, fel i webb-tjänst-systemprogramvaran, kan svar helt utebli, därför måste konsumenten ha hantering för uteblivet svar (time-out) för sådant fall.

Vid tekniska fel förmedlas inga kataloguppgifter till konsumenten.

### Övriga krav

-

### Krav på en tjänstekonsument

Följande krav skall beaktas då ett system agerar som en tjänstekonsument för tjänstedomänens ingående tjänster.

Autentisering av tjänstekonsument ska alltid ske med SITHS Funktionscertifikat.

Tjänstekonsumenten ansvarar för att ha en kontinuitetsplan för det fall att tjänsteproducentens tjänst inte skulle vara tillgänglig.

Tjänstekonsumenten skall redovisa sin belastning på tjänstedomänen (antalet anrop) till såväl tjänstedomänansvarig som till ansvarig för den/de tjänsteproducenter som tjänstekonsumenten anropar. Eventuella väsentliga ändringar av belastning ska kommuniceras i god tid före effektuering så att tillgänglighet och prestanda kan upprätthållas över tid.

Tjänstekonsumenten skall följa vid var tid gällande villkor för den/de tjänsteproducenter från vilka tjänstekonsumenten hämtar information. Ett exempel på sådana villkor är HSA-policy [R4], där informationsägarna bland annat ställer krav på

* att all användning av informationen erhållen från tjänsteproducenten ska beskrivas i godkänd HPTB, HSA-policytillämpning för brukarorganisation
* att tillämpliga lagar och regelverk, t.ex. Personuppgiftslagen PUL, efterlevs
* att information som lagras i egen applikation ska skyddas på tillfredställande sätt
* att information som lagras i egen applikation ska hållas uppdaterad mot ursprungskällan
* att intern revision genomförs årligen för kontroll av efterlevnad till HSA-policy

Anslutna tjänsteproducenter kan ha egna processer för godkännande av tjänstekonsumenter som anropar tjänsteproducentens katalogtjänst.

# Tjänstedomänens meddelandemodeller

Här beskrivs de meddelandemodeller som tjänstekontrakten bygger på. För varje meddelandemodell beskrivs hur mappning ser ut delvis mot V-TIM, här version 2.2 samt mot schema (XSD) för tjänstekontrakt.

## V-MIM

För tjänstedomänen utnyttjas befintliga strukturer inom HSA för förvaltning och vidareutveckling av informations- och meddelandemodeller, se även AB-2.4 [**Error! Reference source not found.**]. Två gånger per år införs genomarbetade och beslutade ändringar i informationsmodellen enligt särskild process.

Nuvarande informationsmodell beskrivs i RIV Informationsspecifikation HSA Struktur och Innehåll [R5]. Ingen mappning mot nationellt fackspråk är genomförd av skäl som beskrivs i AB-2.5 [**Error! Reference source not found.**].

## Formatregler

### RIV-specifikation

Formatregler för tjänstedomänen specificeras i RIV Informationsspecifikation HSA Struktur och Innehåll [R5], se även AB-2.6 [**Error! Reference source not found.**]. Ytterligare detaljer finns i även schemabeskrivningen för respektive tjänstekontrakt, se avsnitt 6.

# Tjänstekontrakt

## GetCredentialsForPersonIncludingProtectedPerson

GetCredentialsForPersonIncludingProtectedPerson används för att söka ut behörighetsgrundande egenskaper för angiven person. Informationen används som regel av e-tjänster (eventuellt via en IdP) för att auktorisera användare mot den egna tjänstens regelverk för åtkomst till information/funktionalitet, normalt i enlighet med den nationella behörighetsmodellen [R6].

De behörighetsegenskaper som returneras är

* De Medarbetaruppdrag som personen är knuten till inklusive information om vårdgivaren och vårdenheten, samt
* Personliga egenskaper: Legitimerad yrkestitel, Förskrivarkod(-er), Befattning och   
  Individuell behörighetsegenskap för IT-tjänster

Detta tjänstekontrakt skiljer sig från kontraktet beskrivet i 6.2 på så sätt att det även ger åtkomst till personer med skyddade personuppgifter. Se AB-2.7 [**Error! Reference source not found.**]. Informationsägaren avgör om tjänstekonsumenten ska beviljas åtkomst till personer med skyddade personuppgifter.

### Version

Version på detta kontrakt är 1.0\_RC5.

### Fältregler

Nedanstående tabell beskriver varje element i begäran och svar. Har namnet en \* finns ytterligare regler för detta element och beskrivs mer i detalj i stycket Regler. Attributen som levereras beskrivs mer ingående i nedan inklippta Exceldokument, med avseende på t.ex. fältlängder och krav på innehållet[[1]](#footnote-1).



|  |  |  |  |
| --- | --- | --- | --- |
| **Namn** | **Typ** | **Beskrivning** | **Kardinalitet** |
| **Begäran** |  |  |  |
| personHsaId \*1) | String | Unik identifierare för den person vars behörighetsegenskaper ska sökas ut. | 0..1 |
| personalIdentityNumber \*1) | String | Person-id för den person vars behörighetsegenskaper ska sökas ut. | 0..1 |
| searchBase | DN | Sökbas. Om ingen sökbas anges används *c=SE* som sökbas. | 0..1 |
| **Svar** |  |  |  |
| credentialInformation \*2) | CredentialInformationType | Behörighetsegenskaper för sökt person | 0..n |
| ..givenName | String | Personens Förnamn | 1..1 |
| ..middleAndSurName | String | Personens Mellannamn och efternamn. Namnen är separerade med mellanslag. | 1..1 |
| ..personHsaId | String | Personens HSA-id | 1..1 |
| ..healthCareProfessionalLicence | String | Personens Legitimerade yrkestitel(-lar). | 0..n |
| ..personalPrescriptionCode | String | Personens förskrivarkod. | 0..1 |
| ..groupPrescriptionCode | String | Gruppförskrivarkod (er) som personen tilldelats av sin arbetsgivare | 0..n |
| ..nursePrescriptionRight | NursePrescriptionRightType | Förskrivningsrätt för barnmorska/sjuksköterska | 0..n |
| .. ..healthCareProfessionalLicence | String | Personens Legitimerade yrkestitel (Barnmorska eller Sjuksköterska) | 1..1 |
| .. ..prescriptionRight | Boolean | Personen har förskrivningsrätt inom den angivna Legitimerade yrkestiteln | 1..1 |
| ..hsaSystemRole | HsaSystemRoleType | Personens Individuella behörighetsegenskaper för IT-tjänster. | 0..n |
| .. ..systemId | String | IT-tjänstens SystemId | 1..1 |
| .. ..role | String | Personens Roll inom IT-tjänsten | 1..1 |
| ..paTitleCode | String | Personens Befattningskoder | 0..n |
| ..protectedPerson | Boolean | true: om person har skyddad identitet  (om personen inte har skyddad identitet kommer inget värde att returneras) | 0..1 |
| ..commission | CommissionType | De medarbetaruppdrag som personen är kopplad till | 0..n |
| .. ..commissionName | String | Medarbetaruppdragets Namn | 1..1 |
| .. ..commissionHsaId | String | Medarbetaruppdragets HSA-id | 1..1 |
| .. ..commissionPurpose | String | Medarbetaruppdragets ändamål | 1..1 |
| .. ..commissionRight | CommissionRightType | Medarbetaruppdragets rättigheter | 0..n |
| .. .. ..activity | String | Rättighet aktivitet | 1..1 |
| .. .. ..informationClass | String | Rättighet informationstyp | 1..1 |
| .. .. ..scope | String | Rättighet omfång | 1..1 |
| .. ..healthCareUnitHsaId \*3) | String | HSA-id för vårdenhet enligt PDL | 0..1 |
| .. ..healthCareUnitName \*3) | String | Vårdenhetens namn | 0..1 |
| .. ..healthCareUnitStartDate \*3) | dateTime | Startdatum för vårdenhetens verksamhet | 0..1 |
| .. ..healthCareUnitEndDate \*3) | dateTime | Slutdatum för vårdenhetens verksamhet | 0..1 |
| .. ..healthCareProviderHsaId | String | Vårdgivarens HSA-id | 1..1 |
| .. ..healthCareProviderName | String | Vårdgivarens Namn | 1..1 |
| .. ..healthCareProviderOrgNo | String | Vårdgivarens organisationsnummer | 1..1 |
| .. ..healthCareProviderStartDate | dateTime | Startdatum för vårdgivarens verksamhet | 0..1 |
| .. ..healthCareProviderEndDate | dateTime | Slutdatum för vårdgivarens verksamhet | 0..1 |
| resultCode | String | Resultat av metodanrop (OK eller ERROR). | 1..1 |
| resultText | String | Beskrivning av fel vid resultCode=ERROR. | 0..1 |

### Tjänstekontraktsspecifika krav och regler

Till denna informationsmängd finns regler som ej uttrycks i schemafilerna och tabellen ovan. Dessa återfinns nedan.

\*1) personHsaId och personalIdentityNumber

Exakt ett av fälten personHsaId och personalIdentityNumber ska anges.

\*2) credentialInformation

En person kan ha flera olika HSA-id om personen har lagts upp i olika organisationers grenar av katalogen.

Vid sökning med person-id så kommer i sådant fall en credentialInformation returneras per HSA-id (bl.a. eftersom kopplingen mellan personobjekt och medarbetaruppdrag görs via personens HSA-id).

\*3) Vårdenhets- (healthCareUnit-) attribut

I det fall ett Medarbetaruppdrag ligger direkt under Vårdgivaren så returneras inga Vårdenhetsattribut, d.v.s. inga värden returneras för de attribut vars namn inleds med healthCareUnit.

### SLA-krav

Krav på svarstider anges under förutsättning att SSL-uppkoppling är etablerad, d.v.s. SSL-förhandlingstid tillkommer vid start av ny SSL-session. Angivna krav på svarstid utgår ifrån mätning från Tjänsteplattformen mot Katalogtjänsten, och exklusive den tid som tjänsteplattformen behöver för att förmedla fråga och svar.

Svarstid ska kunna garanteras upp till angiven last.

|  |  |  |
| --- | --- | --- |
| **Antal returnerade medarbetaruppdrag** | **Svarstider måste garanteras upp till följande last** | **Svarstid för 95 % av alla anropen ska ligga inom** |
| Person med 0-1 medarbetaruppdrag | 10 anrop/s | 150 ms |
| Person med 2-9 medarbetaruppdrag | 5 anrop/s | 300 ms |
| Person med 10-199 medarbetaruppdrag | 1 anrop/s | 2000 ms |

### Logiska fel

För alla logiska fel returneras resultCode=ERROR och en förklarande text i resultText. Följande logiska fel har identifierats för detta kontrakt:

Fel för vilka ingen information returneras.

* Angiven sökbas finns inte i katalogen.  
  resultText=”<katalog-id>;Fel;GetCredentialsForPersonIncludingProtectedPersons; 1; Angiven sökbas: <värde> kan inte hittas”.
* Sökt person finns inte i katalogen (det går inte att hitta något personobjekt med angivet HSA-id).  
  resultText=”<katalog-id>;Fel;GetCredentialsForPersonIncludingProtectedPersons; 2; Det går inte att hitta något personobjekt med angivet [HSA-id: <värde>]”.
* Sökt person finns inte i katalogen (det går inte att hitta något personobjekt med angivet person-id).  
  resultText=”<katalog-id>;Fel;GetCredentialsForPersonIncludingProtectedPersons; 3; Det går inte att hitta något personobjekt med angivet [person-id: <värde>]”.
* Personens förnamn saknas  
  resultText=”<katalog-id>;Fel;GetCredentialsForPersonIncludingProtectedPersons; 4; Personobjektet saknar obligatorisk information om personens förnamn. Gäller personobjekt <path>”
* Personens efternamn saknas  
  resultText=”<katalog-id>;Fel;GetCredentialsForPersonIncludingProtectedPersons; 5; Personobjektet saknar obligatorisk information om personens efternamn. Gäller personobjekt <path>”
* Personens HSA-id saknas  
  resultText=”<katalog-id>;Fel;GetCredentialsForPersonIncludingProtectedPersons; 5; Personobjektet saknar obligatorisk information om personens HSA-id. Gäller personobjekt <path>”

Varnande fel för vilka fullständigt svar ändå ska returneras, men där en eller flera uppgifter pekas ut som felaktiga:

* Personens Legitimerad Yrkesgrupp innehåller värde som inte följer gällande värdemängd.  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 50; Felaktig syntax för personens legitimerade yrkesgrupp: <värde>. Gäller personobjekt: <path>”
* Personens personalPrescriptionCode innehåller ett felaktigt eller icke-numeriskt värde.  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 11; Personobjektets värde för Förskrivarkod innehåller ett felaktigt eller icke-numeriskt värde: <värde>. Gäller personobjekt <path>”
* Personens groupPrescriptionCode innehåller ett felaktigt eller icke-numeriskt värde.  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 12; Personobjektets värde för Gruppförskrivarkod innehåller ett felaktigt eller icke-numeriskt värde: <värde>. Gäller personobjekt <path>”
* Personens nursePrescriptionRight innehåller felaktigt värde som inte följer gällande syntax.  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 13; Personobjektets värde för Förskrivningsrätt för barnmorska/sjuksköterska följer inte gällande syntax: <värde>. Gäller personobjekt <path>”
* Personens nursePrescriptionRight/healthCareProfessionalLicence innehåller värde som inte följer gällande värdemängd.  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 15; Personobjektets värde för Förskrivningsrätt för barnmorska/sjuksköterska följer inte gällande värdemängd för Legitimation: <värde>. Gäller personobjekt <path>”
* Personens hsaSystemRole innehåller felaktigt värde som inte följer gällande syntax.  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 14; Personobjektets värde för Individuell behörighetsegenskap för IT-tjänster följer inte gällande syntax: <värde>. Gäller personobjekt <path>”
* Ett uppdrags HSA-Id saknas  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 20; Medarbetaruppdraget med Namn: <värde> saknar obligatoriskt uppgift om HSA-Id. Gäller uppdraget <path>”
* Ett uppdrags Ändamål saknas  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 21; Medarbetaruppdraget med HSA-Id: <värde> och namn: <värde> saknar obligatoriskt uppgift om Ändamål. Gäller uppdraget <path>”
* Ett uppdrags Ändamål innehåller värde som inte följer gällande värdemängd  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 22; Medarbetaruppdraget med HSA-Id: <värde> och namn: <värde> har ett värde för Ändamål som ej följer gällande värdemängd: <värde>. Gäller uppdraget <path>”
* Ett uppdrags Rättigheter innehåller felaktigt värde som inte följer gällande syntax.  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 23; Medarbetaruppdraget med HSA-Id: <värde> och namn: <värde> följer inte gällande syntax för Rättigheter: <värde>. Gäller uppdraget <path>”
* Ett uppdrags Rättigheter/Aktivitet innehåller värde som inte följer gällande värdemängd.  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 24; Medarbetaruppdraget med HSA-Id: <värde> och namn: <värde> följer inte gällande värdemängd för Rättigheter/Aktivitet: <värde>. Gäller uppdraget <path>”
* Ett uppdrags Rättigheter/Informationstyp innehåller värde som inte följer gällande värdemängd.  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 25; Medarbetaruppdraget med HSA-Id: <värde> och namn: <värde> följer inte gällande värdemängd för Rättigheter/Informationstyp: <värde>. Gäller uppdraget <path>”
* Ett uppdrags Rättigheter/Omfattning innehåller värde som inte följer gällande värdemängd.  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 26; Medarbetaruppdraget med HSA-Id: <värde> och namn: <värde> följer inte gällande värdemängd för Rättigheter/Omfattning: <värde>. Gäller uppdraget <path>”
* ;Varning;
* Felaktig syntax för personens befattning (klartext)  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 28; Felaktig syntax för personens befattning (klartext): <värde>. Gäller personobjekt: <path>”
* Felaktig syntax för personens befattning (koden stämmer inte med klartexten)  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 29; Felaktig syntax för personens befattning (koden: <värde> stämmer inte med klartexten: <värde>). Gäller personobjekt: <path>”
* En enhet saknar HSA-Id   
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 30; En enhet saknar obligatoriskt uppgift om HSA-Id. Gäller vårdenheten <path>.
* Ett uppdrag ligger under en vårdenhet vars Start-datum inte följer gällande syntax.  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 31; Medarbetaruppdraget med HSA-Id: <värde> och namn: <värde> ligger under en vårdenhet vars Start-datum inte följer gällande syntax: <värde>. Gäller vårdenheten <path>”
* Ett uppdrag ligger under en vårdenhet vars Slut-datum inte följer gällande syntax.  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 32; Medarbetaruppdraget med HSA-Id: <värde> och namn: <värde> ligger under en vårdenhet vars Slut-datum inte följer gällande syntax: <värde>. Gäller vårdenheten <path>”
* Vårdenhet saknar obligatorisk uppgift om vårdgivartillhörighet.  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 31; Vårdenhet saknar obligatorisk uppgift om vårdgivartillhörighet. Gäller vårdenheten <path>”
* Ett uppdrag ligger under en vårdenhet som har felaktig uppgift om vårdgivartillhörighet.  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 32; Medarbetaruppdraget med HSA-Id: <värde> och namn: <värde> ligger under en vårdenhet som har felaktig uppgift om vårdgivartillhörighet: <värde>. Gäller vårdenheten <path>”
* Vårdgivare som saknar obligatorisk uppgift om organisationsnummer.  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 40; Vårdgivare saknar obligatorisk uppgift om organisationsnummer. Gäller vårdgivaren <path>”
* Vårdgivare vars uppgift om organisationsnummer inte följer gällande syntax.  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 41; Vårdgivare vars organisationsnummer inte följer gällande syntax: <värde>. Gäller vårdgivaren <path>”
* Det finns flera objekt med samma HSA-Id som en vårdgivare  
  resultText=”<katalog-id>;Varning;GetCredentialsForPersonIncludingProtectedPersons; 42; Medarbetaruppdraget med HSA-Id: <värde> och namn: <värde> tillhör en vårdgivare med samma HSA-Id som andra objekt: <värde>”
* Felaktig multiplicitet för attribut. Attribut kan endast ha ett värde.  
  resultText=”<katalog-id>;Varning;GetEmployeeIncludingProtectedPerson; 60; Attributet kan endast ha ett värde. Gäller attribut: <värde>. Gäller objekt: <path>”

### Annan information om kontraktet

-

## GetCredentialsForPerson

Metoden är identisk med GetCredentialsForPersonIncludingProtectedPerson, förutom att information om skyddade personer aldrig returneras.

Det innebär också att fältet protectedPerson aldrig kommer att returneras.

För beskrivning av metoden se kap 6.1 GetCredentialsForPersonIncludingProtectedPerson ovan.

### Version

Version på detta kontrakt är 1.0\_RC5.

### Fältregler

Eftersom att skyddade personer aldrig returneras, så innebär det att fältet protectedPerson (se 6.1.2 Fältregler) aldrig kommer att returneras.

## GetPersonAuthorizedToSystemIncludingProtectedPerson

GetPersonAuthorizedToSystemIncludingProtectedPerson kontrollerar om angiven person har ett attribut ”Individuell behörighetsegenskap för IT-tjänster” som matchar angivet SystemId, om så är fallet returneras information, som kontaktinformation samt legitimation och specialitet, för personen. Metoden kan användas av en tjänstekonsument för att verifiera behörighet där rollbaserad accesskontroll tillämpas.

Detta tjänstekontrakt skiljer sig från kontraktet beskrivet i 6.4 på så sätt att det även ger åtkomst till personer med skyddade personuppgifter. Se AB-2.7 [**Error! Reference source not found.**]. I Informationsägaren avgör om tjänstekonsumenten ska beviljas åtkomst till personer med skyddade personuppgifter.

### Version

Version på detta kontrakt är 1.0\_RC5

### Fältregler

Nedanstående tabell beskriver varje element i begäran och svar. Har namnet en \* finns ytterligare regler för detta element och beskrivs mer i detalj i stycket Regler. Attributen som levereras beskrivs mer ingående i nedan inklippta Exceldokument, med avseende på t.ex. fältlängder och krav på innehållet[[2]](#footnote-2).



|  |  |  |  |
| --- | --- | --- | --- |
| **Namn** | **Typ** | **Beskrivning** | **Kardinalitet** |
| **Begäran** |  |  |  |
| personHsaId \*) | String | Sökt persons HSA-id. | 0..1 |
| personalIdentityNumber \*) | String | Sökt persons Person-id | 0..1 |
| systemId | String | Namn på den IT-tjänst som behörighet ska kontrolleras för | 1..1 |
| searchBase | DN | Sökbas. Om ingen sökbas anges används *c=SE* som sökbas. | 0..1 |
| **Svar** |  |  |  |
| isAuthorized | Boolean | *true* om personen är behörig, d.v.s. har matchande SystemId i attributet ”Individuell behörighetsegenskap för IT-tjänster”, annars *false*. | 1..1 |
| personInformation | PersonType | Information om personen.  Om personen har flera behöriga person-objekt returneras en instans per objekt. | 0..n |
| ..personHsaId | String | Personens HSA-id. | 1..1 |
| ..givenName | String | Tilltalsnamn. | 1..1 |
| ..middleAndSurName | String | Mellan och Efternamn separerade med mellanslag | 1..1 |
| ..nickName | String | Smeknamn. Används då tilltalsnamn inte är det namn som personen vill använda/bli tilltalad med. | 0..1 |
| ..mail | String | Epostadress. | 0..1 |
| ..telephoneNumber | Telefon | Publikt direkttelefonnummer. | 0..n |
| ..switchboardNumber | Telefon | Telefonnummer till växel. | 0..1 |
| ..nonPublicTelephoneNumber | Telefon | Tjänstetelefonnummer. | 0..1 |
| ..mobileNumber | String | Mobiltelefonnummer. | 0..n |
| ..smsTelephoneNumber | Telefon | Telefonnummer för SMS-meddelanden. | 0..1 |
| ..telephoneHour | TimeSpan | Telefontider för publik telefon (telephoneNumber). | 0..n |
| .. ..fromDay | String | Från dag. Måndag (1) – Söndag (7). | 1..1 |
| .. ..fromTime | Time | Från tid. Format enligt ISO-8601. | 1..1 |
| .. ..toDay | String | Till dag. Måndag (1) – Söndag (7). | 1..1 |
| .. ..toTime | Time | Till tid. Format enligt ISO-8601. | 1..1 |
| .. ..comment | String | Information om aktuellt tidsintervall. | 0..1 |
| ..labeledUri | String | Webbadress. | 0..1 |
| ..description | String | Generell beskrivning. | 0..1 |
| ..languageKnowledgeCode | String | Kod för språk personen har tillräcklig kunskap om för att kunna ta emot patienter som talar detta språk. | 0..n |
| ..title | String | Titel i fritext | 0..1 |
| ..healthCareProfessionalLicence | String | Legitimerad yrkesgrupp | 0..n |
| ..specialityCode | String | Klassificeringskod för specialistutbildning utöver grundutbildning. | 0..n |
| ..specialityName | String | Specialistutbildning utöver grundutbildning. | 0..n |
| ..hsaSystemRole | HsaSystemRoleType |  | 0..n |
| .. ..systemId | String | Tjänstens SystemId | 1..1 |
| .. ..role | String | Personens Roll inom tjänsten | 1..1 |
| ..dn | DN | ”Distinguished Name”. Objektets placering (sökväg) i katalogen, t.ex. cn=Henrika Littorin,ou=Anställda,ou=Enhet Systemförvaltning,ou=Område e-tjänster Drift och Förvaltning,o=Inera AB,c=SE | 1..1 |
| ..protectedPerson | Boolean | true: om person har skyddad identitet  (om personen inte har skyddad identitet kommer inget värde att returneras) | 0..1 |
| resultCode | String | Resultat av metodanrop (OK eller ERROR). | 1..1 |
| resultText | String | Beskrivning av felet. | 0..1 |

### Tjänstekontraktsspecifika krav och regler

Till denna informationsmängd finns regler som ej uttrycks i schemafilerna och tabellen ovan. Dessa återfinns nedan.

\*) personHsaId och personalIdentityNumber

Exakt ett av fälten personHsaId och personalIdentityNumber ska anges.

### SLA-krav

Svarstider är specifika för respektive tjänstekontrakt.

Krav på svarstider är dock inte definierade idag, men följande svarstidsnivå uppfylls idag (förutsatt SSL-uppkoppling):

|  |  |  |
| --- | --- | --- |
| **Metod** | **Svarstider måste garanteras upp till följande last** | **Svarstid för 95 % av alla anrop ligger inom** |
| GetPersonAuthorizedToSystemIncludingProtectedPerson | 10 anrop/s | 100 ms |

### Logiska fel

För alla logiska fel returneras resultCode=ERROR och en förklarande text i resultText. Följande logiska fel har identifierats för detta kontrakt:

Fel för vilka ingen information returneras.

* Angiven sökbas finns inte i katalogen.  
  resultText=”<katalog-id>;Fel;GetPersonAuthorizedToSystemIncludingProtectedPerson; 1; Angiven sökbas: <värde> kan inte hittas”.
* Sökt person finns inte i katalogen (det går inte att hitta något objekt med angivet HSA-id eller person-id).  
  resultText=”<katalog-id>;Fel;GetPersonAuthorizedToSystemIncludingProtectedPerson; 2; Det går inte att hitta något objekt med angivet [HSA-id: <värde>][person-id: <värde>]”.
* Objektet med angivet HSA-id är inget personobjekt.  
  resultText=”<katalog-id>;Fel;GetPersonAuthorizedToSystemIncludingProtectedPerson; 3; Objektet med angivet HSA-id: <värde> är inget person objekt.”
* Det finns andra typer av objekt med angivet HSA-id  
  resultText=”<katalog-id>;Fel;GetPersonAuthorizedToSystemIncludingProtectedPerson; 4; Det finns andra typer av objekt med angivet HSA-Id: <värde>”
* Personens HSA-id saknas  
  resultText=”<katalog-id>;Fel;GetCredentialsForPersonIncludingProtectedPersons; 5; Personobjektet saknar obligatorisk information om personens HSA-id. Gäller personobjekt <path>”

Varnande fel för vilka fullständigt svar ändå ska returneras, men där en eller flera uppgifter pekas ut som felaktiga:

* Personens förnamn saknas  
  resultText=”<katalog-id>;Varning;GetPersonAuthorizedToSystemIncludingProtectedPerson; 10; Personobjektet saknar obligatorisk information om personens förnamn. Gäller personobjekt: <path>”
* Personens efternamn saknas  
  resultText=”<katalog-id>;Varning;GetPersonAuthorizedToSystemIncludingProtectedPerson; 11; Personobjektet saknar obligatorisk information om personens efternamn. Gäller personobjekt: <path>”
* Felaktig syntax för personens epostadress  
  resultText=”<katalog-id>;Varning;GetPersonAuthorizedToSystemIncludingProtectedPerson; 13; Felaktig syntax för personens epostadress: <värde>. Gäller personobjekt: <path>”
* Felaktig syntax för personens telefonnummer  
  resultText=”<katalog-id>;Varning;GetPersonAuthorizedToSystemIncludingProtectedPerson; 14; Felaktig syntax för personens telefonnummer: <värde>. Gäller personobjekt: <path>”
* Felaktig syntax för personens växeltelefonnummer  
  resultText=”<katalog-id>;Varning;GetPersonAuthorizedToSystemIncludingProtectedPerson; 15; Felaktig syntax för personens växeltelefonnummer: <värde>. Gäller personobjekt: <path>”
* Felaktig syntax för personens tjänstetelefonnummer  
  resultText=”<katalog-id>;Varning;GetPersonAuthorizedToSystemIncludingProtectedPerson; 16; Felaktig syntax för personens tjänstetelefonnummer: <värde>. Gäller personobjekt: <path>”
* Felaktig syntax för personens mobiltelefonnummer  
  resultText=”<katalog-id>;Varning;GetPersonAuthorizedToSystemIncludingProtectedPerson; 17; Felaktig syntax för personens mobiltelefonnummer: <värde>. Gäller personobjekt: <path>”
* Felaktig syntax för personens SMS-telefonnummer  
  resultText=”<katalog-id>;Varning;GetPersonAuthorizedToSystemIncludingProtectedPerson; 18; Felaktig syntax för personens SMS-telefonnummer: <värde>. Gäller personobjekt: <path>”
* Felaktig syntax för personens Telefontid  
  resultText=”<katalog-id>;Varning;GetPersonAuthorizedToSystemIncludingProtectedPerson; 19; Felaktig syntax för personens Telefontid [från-dag saknas][från-dag har felaktig syntax: <värde>][till-dag saknas][till-dag har felaktig syntax: <värde>][från-tid saknas][från-tid har felaktig syntax: <värde>][till-tid saknas][till-tid har felaktig syntax: <värde>]. Gäller personobjekt: <path>”
* Felaktig syntax för personens webadress  
  resultText=”<katalog-id>;Varning;GetPersonAuthorizedToSystemIncludingProtectedPerson; 20; Felaktig syntax för personens webadress: <värde>. Gäller personobjekt: <path>”
* Felaktig syntax för personens språkkod  
  resultText=”<katalog-id>;Varning;GetPersonAuthorizedToSystemIncludingProtectedPerson; 21; Felaktig syntax för personens språkkod: <värde>. Gäller personobjekt: <path>”
* Felaktig syntax för personens legitimerade yrkesgrupp  
  resultText=”<katalog-id>;Varning;GetPersonAuthorizedToSystemIncludingProtectedPerson; 22; Felaktig syntax för personens legitimerade yrkesgrupp: <värde>. Gäller personobjekt: <path>”
* Felaktig syntax för personens specialitetskod  
  resultText=”<katalog-id>;Varning;GetPersonAuthorizedToSystemIncludingProtectedPerson; 23; Felaktig syntax för personens specialitetskod: <värde>. Gäller personobjekt: <path>”
* Felaktig syntax för personens specialitet (klartext)  
  resultText=”<katalog-id>;Varning;GetPersonAuthorizedToSystemIncludingProtectedPerson; 24; Felaktig syntax för personens specialitet (klartext): <värde>. Gäller personobjekt: <path>”
* Felaktig syntax för personens attribut för Individuell behörighet till IT-tjänst  
  resultText=”<katalog-id>;Varning;GetPersonAuthorizedToSystemIncludingProtectedPerson; 26; Felaktig syntax för personens attribut för Individuell behörighet till IT-tjänst: [felaktig avgränsare][Roll saknas]: <värde>. Gäller personobjekt: <path>”
* Felaktig syntax för personens flagga för skyddad person  
  resultText=”<katalog-id>;Varning;GetPersonAuthorizedToSystemIncludingProtectedPerson; 27; Felaktig syntax för personens flagga för skyddad person: <värde>. Gäller personobjekt: <path>”
* Felaktig multiplicitet för attribut. Attribut kan endast ha ett värde.  
  resultText=”<katalog-id>;Varning;GetEmployeeIncludingProtectedPerson; 60; Attributet kan endast ha ett värde. Gäller attribut: <värde>. Gäller objekt: <path>”

### Annan information om kontraktet

-

## GetPersonAuthorizedToSystem

Metoden är identisk med GetPersonAuthorizedToSystemIncludingProtectedPerson, förutom att skyddade personer aldrig returneras.

Det innebär också att fältet protectedPerson aldrig kommer att returneras.

För beskrivning av metoden se kap 6.3 GetPersonAuthorizedToSystem ovan.

### Version

Version på detta kontrakt är 1.0\_RC5.

### Fältregler

Eftersom att skyddade personer aldrig returneras, så innebär det att fältet protectedPerson (se 6.3.2 Fältregler) aldrig kommer att returneras.

1. Dokumentet innehåller beskrivning av attribut/element ingående i samtliga tjänstekontrakt i tjänstedomänerna infrastructure:directory:organization, infrastructure:directory:employee och infrastructure:directory:authorizationmanagement. För att isolera de attribut som är aktuella för detta tjänstekontrakt, filtrera på kolumn R. [↑](#footnote-ref-1)
2. Dokumentet innehåller beskrivning av attribut/element ingående i samtliga tjänstekontrakt i tjänstedomänerna infrastructure:directory:organization, infrastructure:directory:employee och infrastructure:directory:authorizationmanagement. För att isolera de attribut som är aktuella för detta tjänstekontrakt, filtrera på kolumn V. [↑](#footnote-ref-2)