Förstudierapport

Identitets- och behörighetsfederation för eHälsa

Innehåll

Utgåvehistorik för dokumentet

Utgåva	Datum	Kommentar
Version 0.1	2012-04-16	Bakgrund, syfte, vision och delar förvaltning adderat till dokumentet
Version 0.2	2012-04-17	Definition och begrepp
Version 0.3	2012-04-17	Vidareutvecklat kapitel tre efter avstämningar
Version 0.4	2012-04-19	Vidareutvecklat kapitel tre, litet kring granskning, kostnader & finansieringsmodell, bruttolista med ”förslag till beslut-punkter”
Version 0.5	2012-04-20	Kapitel tre uppdaterat efter projektmöte 2012-04-20
Version 0.6	2012-04-24	Kapitel ett och fem inlagda
Version 0.7	2012-04-24	Ny version efter avbrott som genererat ny version 0.6_1
Version 0.8	2012-04-25	Tillitsramverk och teknisk lösning adderat
Version 0.81	2012-04-25	Mindre korrigeringar gällande stavning och disposition
Version 0.82	2012-04-30	Mindre korrigeringar gällande språk och stavning
Version 0.83	2012-04-30	SWOT-analys adderad
Version 0.85	2012-05-03	Uppdateringar efter projektmöte
Version 0.9	2012-05-11	Uppdateringar efter remissrunda
Version 1.0	2012-06-15	Fastställd efter styrgruppsmöte den 11 juni 2012

1 Sammanfattning & förslag till beslut

1.1 Sammanfattning

Uppdraget har varit att ta fram en tjänstebeskrivning avseende en identitets- och behörighetsfederation för vård och omsorg. Förstudierapporten har strukturerats kapitelmässigt utifrån de specifikationer som fastställts i uppdragsdirektivet.

Visionen är att ”Federationen skall fungera som en nationell mötesplats för säkra e-tjänster genom att vara det infrastrukturella navet som sammanlänkar e-tjänster och användarorganisationer i en lösning som bygger på tillit och skydd för den personliga integriteten”.

I samband med utformning och implementation av federationslösningen bör utgångspunkten att federationen skall vara nationell ges hög prioritet. Den grundläggande idén är att alla privata och offentliga aktörer som bedriver verksamhet inom vård och omsorg, aktörer inom hälsa och livsmedel samt myndigheter skall kunna använda sig av federationens infrastruktur. I stället för att överväga egna mer avgränsade och mindre initiativ kring federationslösningar kan dessa organisationer då istället allokera egna resurser till utveckling av nya e-tjänster och anpassningar av befintliga e-tjänster för att dessa skall kunna fungera i en federativ lösning. Detta torde vara optimalt ur ett samhällsekonomiskt perspektiv likväl som ur den enskilda organisationens synvinkel.

I kapitel tre ges en översiktlig beskrivning av federationen. Dessutom redovisas ett antal centrala hörnstenar, som till exempel mål, nytta, ägarskap och finansieringsmodell. Bedömningen av juridiska aspekter på federationslösningen återfinns i kapitel fyra ”Legal analys”.

För att möta visionen beskriver förstudierapporten hur en teknisk lösning och ett så kallat tillitsramverk som reglerar medverkan i federationen kan utformas på det som kallas Level of Assurance 3 (LoA3). Denna benämning refererar till en viss nivå på säkerhetsskyddet och är baserat på ett flertal internationella standarder inom området. I kapitel fem ”Tillitsramverk” och kapitel sex ”Teknisk infrastruktur” återfinns en principinriktning för hur federationslösningen bör realiseras baserat på LoA3.

Hur federationslösningen bör förvaltas framgår av kapitel sju ”Förvaltning”. Resultatet av en analys av styrkor, svagheter, möjligheter och hot (SWOT) framgår av kapitel åtta. I kapitel nio ges en redovisning av underlag till projektdirektiv för nästa fas (informationsfrågor, framtagande av tillitsramverk, realisering av pilotlösning och plan för anslutning av e-tjänster). Slutligen återfinns referenser och definitioner i kapitel tio.

1.2 Förslag till beslut

Baserat på det samlade resultatet i förstudierapporten har ett underlag med huvudsakligt innehåll för ett projektdirektiv tagits fram som redovisar föreslagna aktiviteter i nästa steg – utformning och implementation av federationslösningen.

I enlighet med underlaget till projektdirektiv lämnas följande förslag till beslut:

a. Framtagande av kommunikationsplan omfattande aktiviteter som webbplats, informationsmaterial (informationsblad, presentationer, ev. profilmaterial etc.), varumärkesarbete, seminarium.

b. Road map för anslutning av e-tjänster tas fram genom överenskommelser med ett antal centrala organisationer inom vård- och omsorgssektorn.

c. Tillitsramverk utformas om möjligt baserat på/eller i direkt samverkan med e-legitimationsnämnden som kommer att lämna förslag kring tillitsramverk (helt nyligen aviserats till oktober 2012) och de första e-tjänster där överenskommelse om anslutning träffas.

d. Teknisk etablering av en identitets- och behörighetsfederation för vård och omsorg i enlighet med avsnitt 6.2. Tillitsramverket (punkt c ovan) måste först utformas men med mycket kort varsel kan redan från start en teknisk miljö användas för tester och verifiering av SAML-förmågor. När sedan tillitsramverket finns på plats, något senare under andra halvan av 2012, kan en pilotmiljö etableras med avsikt att försörja de e-tjänster som har behov av en identitets- och behörighetsfederation för vård och omsorg.

e. Federationen centrala funktioner skall förvaltas och vidareutvecklas utan vinstintressen och ägarskapet av dessa skall baseras på en bred representation från organisationer inom vård- och omsorgssektorn. Förslaget är att formerna för ägarskap och finansiering klarläggs genom en särskild aktivitet i inledningen av nästa steg

f. Arbetet med att realisera ovanstående aktiviteter föreslås att bedrivas i projektform fram till att ägarfrågan är beslutad och ett antal e-tjänster implementerats inom federationen

g. För att säkerställa om ett personuppgiftsbiträdesavtal behövs eller inte för denna Identitets- och behörighetsfederationen bör Datainspektionen rådfrågas för att få saken bedömd av dem i ett samrådsyttrande

2 Bakgrund

2.1 Motiv för projektet

Inom vård och omsorg, dit även läkemedelsdistribution, apotek och socialtjänst räknas, finns ett behov av infrastrukturlösningar som garanterar en patientsäker, kostnadseffektiv och praktiskt enkel åtkomst av e-tjänster för användarorganisationer inom och mellan olika organisationer. Det finns även en förbättringspotential när det gäller säkerhetsfrågor som autentisering och behörighetshantering inom branschen. Detta samtidigt som stora mängder integritetskänslig information hanteras.

För att realisera en mer ändamålsenlig, gemensam lösning som bättre tillgodoser krav och behov inom vård och omsorg har .SE och CeHis tillsammans med Apotekens Service AB genomfört ett projekt i syfte att utvärdera möjligheterna med och effekterna av att utforma en identitets- och behörighetsfederation för eHälsa.

I förstudierapporten kommer Federationen genomgående att refereras till som federationen och federationslösningen.

2.2 Medverkande

I arbetet har nedanstående personer medverkat:

Roll	Namn	Tel/E-postadress
Styrgrupp	Ylva Hambraeus Björling	ylva.hambreus.bjorling@apotekensservice.se
	Peter Alvinsson	peter.alvinsson@ltkalmar.se
	Danny Aerts	danny.aerts@iis.se
	Lennart Jonasson	lennart.jonasson@skl.se
Projektledning	Håkan Josefsson	hakan.josefsson@apotekensservice.se
Ref.grupp	Lennart Eriksson	lennart.eriksson@cehis.se
	Elisabeth Ekstrand	elisabeth.ekstrand@iis.se
Arbetsgrupp	Stefan Larsson	stefan.larsson@apotekensservice.se
	Kerstin Andres	kerstin.andres@apotekensservice.se
	Manne Andersson	manne.andersson@apotekensservice.se
	Thomas Nilsson	thomas@certezza.net
	Staffan Hagnell	staffan.hagnell@iis.se
	Michael Winberg	michael.winberg@iis.se
	Anette Hall	anette.hall@iis.se
	Filippa Murath	filippa.murath@iis.se
	Ewa Jerilgård	ewa.jerilgard@inera.se
	Pål Resare	pal.resare@skl.se
	Ulf Palmgren	ulf.palmgren@skl.se

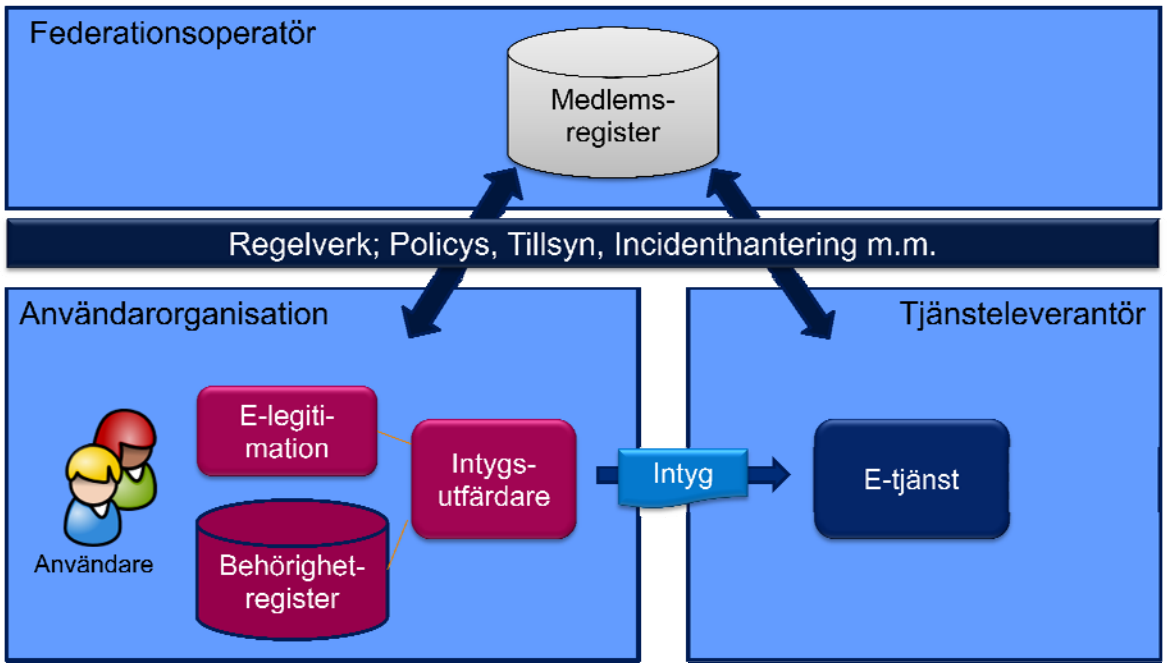
3 Federationen

3.1 Översikt

Federationen skall utvecklas för alla organisationer, privata såväl som offentliga, som bedriver verksamhet inom vård och omsorg. Den gemensamma bärande grunden är den samlade författningsreglering som reglerar verksamheterna inom vård och omsorg och som i huvudsak kan sägas ha det primära målet att fungera till skydd för den personliga integriteten och patientsäkerheten.

Federationen kan förenklat beskrivas som en sammanhållen teknisk infrastruktur där hanteringen av identiteter och åtkomsträttigheter knyts samman med ett obegränsat antal olika e-tjänster. Användarna får på så sätt åtkomst till många olika e-tjänster på ett enkelt och användarvänligt sätt.

I bilden nedan ges en konceptuell översikt av federationslösningen.



Användarorganisation kan vara en statlig myndighet, landsting, kommun eller annan juridisk person eller enskild näringsidkare som bedriver vård och omsorg i Sverige. Användarorganisationen ansvarar för att användare har giltiga elektroniska identiteter och respektive behörighetsstyrande attribut för att kunna nyttja e-tjänster inom Federationen. Attributtjänster kan i olika omfattning köpas av marknaden eller tillhandahållas i egen regi.

Tjänsteleverantör är den som tillhandahåller e-tjänster till en eller flera Användarorganisationer inom Federationen.

Federationsoperatörens roll är att sköta federationens löpande verksamhet, däribland att förvalta tillitsregelverket och federationens gemensamma funktioner. Attributtjänster och e-legitimationer kan i olika omfattning köpas på marknaden eller tillhandahållas i egen regi.

3.2 Vision

Federationen skall fungera som en nationell mötesplats för säkra e-tjänster genom att vara det infrastrukturella navet som sammanlänkar e-tjänster och användarorganisationer i en lösning som bygger på tillit och skydd för den personliga integriteten.

3.3 Mål

Målen för federationslösningen är att:

- tillhandahålla **en** infrastrukturlösning för säker åtkomst av e-tjänster för **hela** sektorn eHälsa
- vara det självklara valet för organisationer som vill uppnå en optimerad nivå på hanteringen av identiteter och behörigheter samt skyddet av den personliga integriteten i sina verksamheter
- underlätta för informationsägare att fullgöra de skyldigheter som bland annat följer av personuppgiftsansvaret
- vara ett självklart alternativ till att utforma separata lösningar för hanteringen av identiteter och behörigheter, separat för varje enskilt system, i varje enskild organisation
- tillhandahålla en gemensam och tydlig infrastruktur, baserad på standard, som erbjuder marknaden en tydlig bas för tillhandahållande av effektiva e-tjänster
- fungera som ett forum som verkar för medlemmarnas gemensamma intressen, verkar för samverkan, kunskapsutveckling, erfarenhetsutbyte och där spridning av goda exempel möjliggörs

3.4 Nytta

Nyttoeffekterna av att realisera federationen uppnås i huvudsak inom områdena:

- Personlig integritet
- Stöd för fullgörande av de skyldigheter som följer med personuppgiftsansvar
- Patientsäkerhet
- Kostnadseffektivitet
- Praktisk enkelhet/användarvänlighet
- Teknik- och leverantörsoberoende

Beträffande den personaliga integriteten innebär federationslösningen positiva effekter ur två aspekter. Dels genom en generell höjning av säkerhetsskyddet och dels genom en likformning/likabehandling av säkerhetsskyddet för känsliga personuppgifter. Båda dessa aspekter tillgodoses genom att de aktörer som ingår i federationen kommer att tillämpa samma tekniska och administrativa säkerhetsnivåer vilka också kommer att ligga på högre säkerhetsnivåer än vad som är fallet i flertalet av dagens tillämpningar. På samma grunder kan man hävda att federationslösningen bidrar till att stödja det arbete och de skyldigheter som följer med personuppgiftsansvaret.

Något mer utförligt kan sägas att den personliga integriteten, arbetet utifrån personuppgiftsansvaret samt patientsäkerheten tillgodoses inom federationen genom att ha gemensamma kravnivåer utifrån säkerhetsrelaterade och rättsliga frågor, t.ex. hantering av identiteter och behörigheter, autentisering, spårbarhet samt en mängd andra IT- och informationssäkerhetsfrågor. Dessa kravnivåer definieras och beskrivs detaljerat i det gemensamma tillitsramverket. De aktörer som ingår i federationen förbinder sig att följa tillitsramverket. Dessutom skall återkommande granskning av efterlevnaden av tillitsramverket genomföras, enligt gemensamt fastställda principer. Federationen kommer även att förvaltas av en oberoende part.

Kostnadseffektiviteten för e-tjänsteleverantören uppnås genom att man via federationslösningen tillhandahåller en gemensam skalbar infrastruktur där man över tiden kan tillföra en mängd nya tjänster som är av intresse för användarna i federationen. Nya e-tjänsteleverantörer har möjlighet att utveckla och tillhandahålla tjänster utifrån federationens kända krav, gränssnitt, regler och rutiner.

Federationslösningens samlade potential för positiva kostnadseffekter och generella nyttoeffekter i daglig verksamhet, t.ex. i form av effektivare inloggningsförfaranden, är med största sannolikhet väldigt stor men varierar med antalet tjänsteanvändande organisationer och antalet tjänster. Det är därför av avgörande betydelse att vidta åtgärder och agera så att vi syftet att tillhandahålla **en** infrastrukturlösning för **hela** sektorn vård och omsorg uppnås.

Två exempel på positiva konstadseffekter redovisas översiktligt i det följande. Resultaten är baserade på en så kallad ”PENG-analys” som genomförts avseende en federativ lösning för identifiering och behörighetshantering. Analysen har genomfört på uppdrag av Sveriges kommuner och landsting (SKL) och omfattade fyra processer med tillhörande IT-stöd hos Stockholms stad, Lidingö Stad och Stockholms läns landsting.

Kommunernas verksamhet
Analysen visar att genom en federativ lösning kan behörighetsadministrationen genomföras i en central punkt varför den samlade tidsåtgången kan reduceras med 33 % genom en federativ lösning.

Landstingets verksamhet
Analysen visar att genom en federativ lösning kan behörighetsadministrationen genomföras i en central punkt varför den samlade tidsåtgången blir 42 % lägre genom en federativ lösning.

Federationslösningen bidrar till praktisk enkelhet ur ett IT-arkitekturperspektiv genom att tillhandahålla en infrastruktur baserad på breda standarder där e-tjänsteleverantörer och Användarorganisationer kan mötas/integrera via en generell och relativ liten kontaktyta.

För användaren bidrar federationslösningen till ökad användarvänlighet, till exempel genom möjlighet till single sign on (SSO) till många olika tjänster. Storleken på denna nyttoeffekt varierar mellan olika användarorganisationer/organisationer och beror på verksamhetens inriktning, hur många tjänster en användare nyttjar löpande under normala arbetsförhållanden.

3.5 Målgrupp

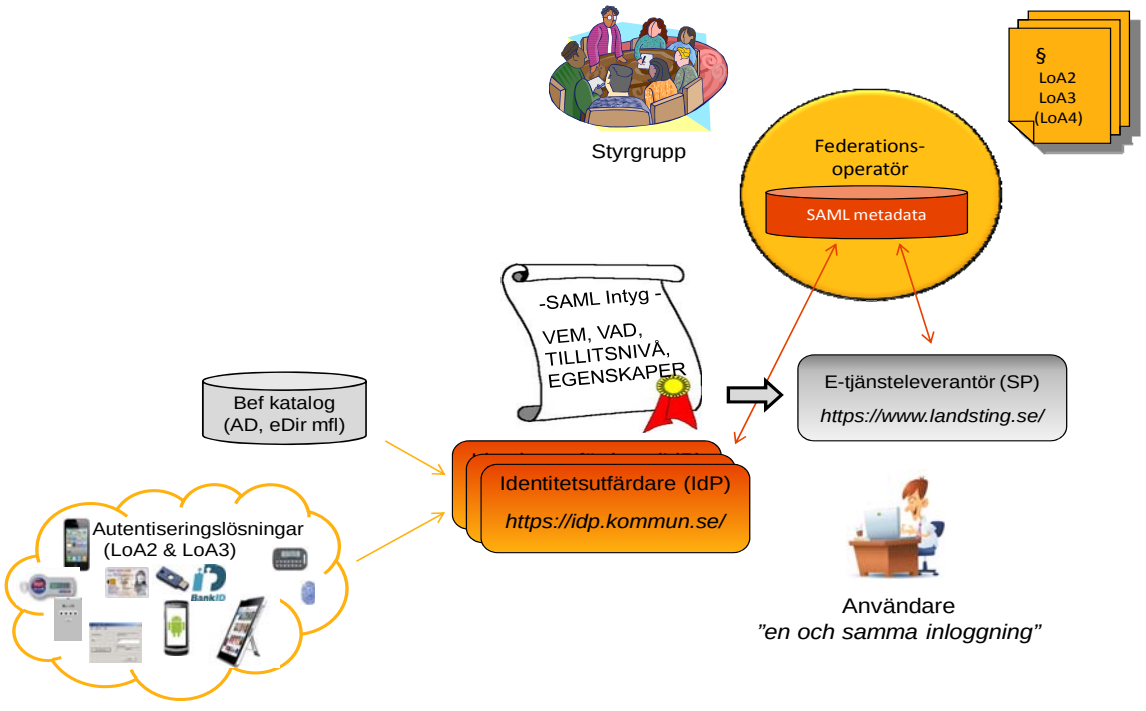
Federationens målgrupp är privata såväl som offentliga aktörer som bedriver verksamhet inom eHälsa.

Exempel på privata och offentliga organisationer som tillhör målgruppen för denna federationslösning är:

- Kommuner
- Landsting
- Apoteksaktörer
- Tandläkare
- Övriga privata vård- och omsorgsgivare
- Övriga offentliga vård- och omsorgsgivare
- Invånare
- Veterinärer

3.6 Aktörer och huvudkomponenter

I kapitel elva ”Referenser och definitioner” ges exakta definitioner av de begrepp som förekommer i hela rapporten. I detta avsnitt ges en beskrivning av Federationens aktörer och huvudkomponenter och deras roll, ansvar och funktion.



Federationens organisation.

Aktörer och huvudkomponenter i federationen:

- Användare
- Användarorganisationer
- Styrgrupp
- Federationsoperatör
- Tillitsramverk
- Intygsutfärdare
- E-tjänsteleverantör
- Granskning

Användare inom federationen ges åtkomst till de e-tjänster som anses nödvändiga utifrån den egna rollen. Detta beslutas inom den egna organisationen där också behörighetstilldelning och behörighetsadministration hanteras.

Användarorganisationer syftar på den organisation där användaren har sin anställning. Denna organisation kan vara en privatägd eller offentlig aktör som bedriver verksamhet inom vård och omsorg. Användarorganisationer har valt att ingå i federationen för att kunna använda olika e-tjänster. Användarorganisationer svarar för de egna användarnas identitets- och behörighetshantering. Samma organisation kan samtidigt även fungera som e-tjänsteleverantör och tillhandahålla e-tjänster till andra användarorganisationer inom federationen.

Styrgruppen fungerar som medlemmarnas representanter och beslutar om federationens organisation och förvaltning. Styrgruppen ansvarar för strategiska beslut som rör finansieringsmodell, tillitsramverk samt principer för hur revisioner och granskningar skall genomföras. Det dagliga operativa arbetet sköts av Federationsoperatören, som också rapporterar till styrgruppen. Federationsoperatören kan eskalera frågor till styrgruppen. Styrgruppen skall genom sin sammansättning representera breda intressen inom vård och omsorg – branschorganisationer eller motsvarande bör ingå i styrgruppen för att på så sätt säkerställa nationell representation för olika användargrupper.

Federationsoperatören ansvarar för det dagliga operativa arbetet och driver arbetet enligt den förvaltningsmodell som beskrivs i detalj i kapitel åtta ”Förvaltning”. .SE skall fungera som federationsoperatör. Drift av teknisk lösning samt förvaltning av medlemsregistret och tillitsramverket är huvuduppgifter för federationsoperatören.

Tillitsramverket redovisar den samlade kravbilden/fastställd tillitsnivå inom federationen. Den fastställda tillitsnivån omfattar kravnivåer inom områdena teknisk implementation, administration och operationella rutiner.

Intygsutfärdaren utfärdar ett tekniskt intyg. Detta intyg innehåller uppgifter om en användares identitet och de egenskaper som är förknippade med användaren – exempelvis användarens roll och, enkelt uttryckt, beslutade åtkomsträttigheter.

E-tjänstleverantören tillhandahåller e-tjänster till användarna inom federationen. Tjänsterna tillgängliggörs genom att e-tjänstleverantörens lösningar kan tolka federationens tekniska intyg.

Granskningen fyller en viktig funktion eftersom grunden inom federationen är tillit – tillit till ingående parters efterlevnad av tillitsregelverket, gällande tillitsnivåer, parternas hantering av autentisering och behörigheter - och ytterst tillit till utställda tekniska intyg.

3.7 Ägarskap

Federationen skall fungera som en nationell mötesplats för säkra e-tjänster genom att vara det infrastrukturella navet som sammanlänkar e-tjänster och användarorganisationer i en lösning som bygger på tillit och skydd för den personliga integriteten. Federationen skall förvaltas och vidareutvecklas utan vinstintressen.

Principiellt kan vi därför inom ramen för förstudien fastslå att:

- Ägarskapet för federationen skall baseras på en bred representation inom vård- och omsorgssektorn.

Förslaget är att formerna för ägarskapet klarläggs genom en särskild aktivitet under ett nästa steg, samtidigt som en testmiljö för federationslösningen byggs upp.

Fram till att ägarfrågan är beslutad föreslås att det vidare arbetet med testmiljö och utformning av federationen bedrivs i projektform.

3.8 Kostnader & finansieringsmodell

I samband med planering och utformning av projektets projektdirektiv fastslogs att projektet skall uppskatta resursbehov, aktiviteter och tidplan för:

- genomförande av pilotdrift under 2012
- uppbyggnad och införande av federationslösningen

3.8.1 Kostnader för pilotmiljö

Genomförande av pilotdrift under 2012:

- Kostnader för att realisera en mer begränsad teknisk miljö för pilotdrift uppskattas omfatta 150-200 timmar

- Investeringskostnaden för att realisera en mer begränsad teknisk miljö för pilotdrift under 2012 uppskattas till 200.000 SEK

- Initial årlig förvaltningskostnad för en mer begränsad pilotlösning under 2012 uppskattas till 0 – 0,5 heltidsresurser, helt beroende på omfattning av tillkommande e-tjänster

3.8.2 Kostnader för fullskalig lösning

Baserat på erfarenheter från Swedish Academic Identity (SWAMID) och beräkningar gjorda för den planerade Skolfederationen kan det uppskattas att:

- Investeringskostnaden för att realisera en fullskalig teknisk lösning för federationen uppskattas grovt inom projektet till 3 Mkr.

- Årlig förvaltningskostnad för en fullskalig lösning beräknas omfatta tre heltidsresurser.

Med en fullskalig lösning avses en federationslösning som ska klara cirka 300 e-tjänster och intygsutfärdare.

3.8.3 Finansieringsmodell

Federationen skall förvaltas och vidareutvecklas med full kostnadstäckning, genom en avgift från användarorganisationerna, men utan vinstintressen.

Användarorganisationerna föreslås erlägga en fast årlig medlemsavgift.

Förslag till beslut
Förslaget från projektgruppen är därför att en detaljerad avgiftsmodell fastställs genom en samordnad aktivitet kring ägarskap, ägarformer och avgiftsmodell, i nästa fas.

3.9 Införande av e-tjänster

Förslaget är att det i nästa fas genomförs en dialog med centrala organisationer inom vård och omsorg i Sverige för att klarlägga förutsättningar kring specifika e-tjänster och fastställa en Road map för anslutning av e-tjänster till federationen.

Ovanstående bör genomföras baserat på den sammantagna nationella lägesbilden avseende användarorganisationer och e-tjänster som tillhör målgruppen för federationen.

Inledande samtal har genomförts med Kommunförbudet Stockholms Län (KSL), Stockholms Stad och Stockholms Läns Landsting (SLL). Detta har resulterat i ett antal tänkbara tillämpningar som kan bli aktuella för anslutning till federationen.

De önskade tillämpningarna är:

- Beställningsportalen och andra likartade e-tjänster för förskrivningsstöd
- Försäkringskassans LEFI Online och andra likartade tjänster
- Kvalitetsregister, såsom Demensregistret, Palliativregistret och SeniorAlert, som vänder sig till målgruppen
- Nationell Patientöversikt (NPÖ)
- Elektroniskt Expertstöd (EES)
- Pascal eller motsvarande gränssnitt för dosapotek som vänder sig till målgruppen
- Nationell Ordinationsdatabas (NOD)
- Pulsen Combine eller motsvarande socialtjänstsystem som kan kategorisera sig som ”molntjänster”
- Sekund, färdtjänsten kundadministrativa system, i Stockholmsregionen eller motsvarande e-tjänst för andra regioner
- SLL’s Mina Vårdkontakter eller motsvarande e-tjänst i andra regioner
- Stockholms stads Paraplysystemet (Stockholmsstads samlingsnamn för socialsystemen) eller motsvarande e-tjänst hos andra kommuner där privata utförare är intressenter.
- E-tjänster för samordnad vårdplanering likt Webcare som vänder sig till kommuner och privata vårdgivare
- CeHis/Ineras tjänsteplattform
- Hälsotjänster kopplade till vård och omsorg (t.ex. Uppsala Sustains)

4 Legal analys

Utmärkande för de organisationer som är avsedda att ingå i federationslösningen är att de behandlar känsliga personuppgifter i sin verksamhet. (Med känsliga personuppgifter avses enligt personuppgiftslagen (PuL) uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening. Det är också uppgifter som rör hälsa eller sexualliv.) Hanteringen av dessa register styrs ofta av speciallagar s.k. registerförfattningar som gäller före PuL, t ex patientdatalagen, apoteksdatalagen, lagen om receptregister. Nämnda lagar ställer i regel krav på behörighetstilldelning och åtkomstkontroll och innehåller ofta bestämmelser om tystnadsplikt.

Den samlade bedömningen är att federationslösningen tillhandahåller ett kraftfullt stöd för att uppfylla de skyldigheter som följer med personuppgiftsansvaret.

4.1 Författningsreglering

Federationen ska hantera de personuppgifter som behövs för att avgöra om viss personal är behörig att få tillträde till ett system. I person-uppgiftslagen (1998:204) finns regler som ska skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Lagen gäller för behandling av personuppgifter i hela samhället för verksamhet som bedrivs av såväl myndigheter som enskilda. Den är således även tillämplig på en identitets- och behörighetsfederation för området eHälsa.

Enligt 3 § personuppgiftslagen (PuL) är en *personuppgift* all slags information som direkt eller indirekt kan knytas till en fysisk person som är i livet är enligt personuppgiftslagen en personuppgift. Det gäller även krypterade uppgifter och olika slags elektroniska identiteter, som exempelvis IP-nummer, som också räknas som personuppgifter om de kan kopplas till fysiska personer.

En avgörande fråga är vad som avses med "*behandling av personuppgifter*". Enligt 3 § PuL avses allt man gör med personuppgifter, vare sig det sker med en dators hjälp eller inte. Exempel på behandling av personuppgifter är *insamling, registrering, lagring och bearbetning, organisering, lagring, bearbetning, ändring, återvinning, inhämtande, användning, utlämnade genom översändning, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring*. Så snart personuppgifter på något sätt hanteras är det fråga om en behandling som faller under PuL om behandlingen är helt, eller delvis automatiserad eller avser ett manuellt personregister som är sökbart enligt särskilda kriterier.

Federationens uppgift är att behandla personuppgifter och det är sannolikt att flera av de exempel som nämns ovan kommer att utföras av federationen även om behandlingen inte är avsedd att vara särskilt omfattande.

Sådana personuppgifter som följer av medlemskap, anställningsförhållanden, kundförhållanden, eller något därmed jämförligt förhållande anses inte som känsliga.

Personuppgifterna som ska behandlas av federationen hänför endast sig till anställning hos en huvudman eller vårdgivare och torde därmed inte kunna betecknas som känsliga.

Det är normalt att den personuppgiftsansvarige, den juridiska person (till exempel aktiebolag, stiftelse eller förening) eller den myndighet som behandlar personuppgifter i sin verksamhet och som bestämmer vilka uppgifter som ska behandlas och vad uppgifterna ska användas till, allt under förutsättning att behandlingen är tillåten enligt PuL. Om *flera juridiska personer* bestämmer över en viss behandling kan de vara gemensamt personuppgiftsansvariga. Detsamma gäller för

databaser som myndigheter använder gemensamt (om inte något annat anges i lag eller förordning).

Enligt 22 § PuL får personnummer eller samordningsnummer behandlas utan samtycke bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering, eller något annat beaktansvärt skäl. Då syftet med hela federationen är en *säker identifiering av användarna* och behandlingen av personnummer eller samordningsnummer kan därför detta göras utan de anställdas samtycke.

4.2 Avtal

Medlemmarna i denna federation ska vara organisationer inom hälso- och sjukvård samt omsorg som behandlar känsliga personuppgifter inom sin verksamhet. Enligt PuL ska den personuppgiftsansvarige se till att personuppgifter som behandlas i verksamheten skyddas.

Olika typer av avtal kommer att behöva upprättas för att reglera federationens, i första hand kommer dessa vara civilrättsliga affärsavtal mellan parterna. Men även frågan hur personuppgifterna får behandlas inom ramen för federationen kan behöva regleras i avtal mellan parterna.

Det är inte ovanligt att den personuppgiftsansvarige får hjälp med ”databearbetningen” av någon annan, datadriften sköts i praktiken av någon som inte är anställd i organisationen, vanligen en ”driftoperatör” som också blir personuppgiftsbiträde. I detta fall kan möjligen federationsoperatörens roll likställas med en driftoperatörs.

Enligt PuL får ett personuppgiftsbiträde bara behandla personuppgifter enligt instruktioner från den personuppgiftsansvarige och ska finnas ett skriftligt avtal som reglerar hur biträdet ska behandla uppgifterna och vilka säkerhetsåtgärder som ska vidtas. Personuppgiftsbiträdet kan vara en fysisk eller juridisk person (företag, stiftelse, myndighet, etc.), en anställd i den personuppgiftsansvariges organisation eller någon annan som behandlar personuppgifter under den personuppgiftsansvariges direkta ansvar är inte personuppgiftsbiträde.

5 Tillitsramverk

5.1 Allmänt om åtkomst

Åtkomst är flödet av information mellan ett subjekt och ett objekt. Ett subjekt är en aktiv enhet som begär åtkomst till ett objekt eller data i objektet. Ett subjekt kan vara en användare, ett program, eller en process som behöver åtkomst till ett objekt för att utföra en uppgift. När en applikation öppnar en fil så är applikationen ett subjekt och filen är ett objekt. Ett objekt är en passiv enhet som innehåller information. Ett objekt kan vara en dator, databas, fil, applikation, katalog eller ett fält i en tabell i en databas. När du söker information i en databas, så är du det aktiva subjektet och databasen det passiva objektet.

Åtkomstkontroll är en bred term som omfattar flera olika typer av mekanismer som upprätthåller åtkomstkontroll som exempel egenskaper i datorsystem, nätverk och information. Åtkomstkontroll är extremt viktigt och grundläggande ur säkerhetssynpunkt för att förhindra otillåtet användande av en verksamhets resurser. När en användare ombeds att ange användarnamn och lösenord vid användande av sin dator så är det en form av åtkomstkontroll. När användaren loggat in och senare försöker öppna en fil så finns det troligtvis en lista för den filen med användare, grupper och behörigheter. Om användaren inte finns på listan så nekas åtkomst. Detta är en annan form av åtkomstkontroll.

En användares behörighet och rättigheter kan baseras på exempelvis identitet, tillstånd, uppdrag, roll, gruppmedlemskap etc. Åtkomstkontroll ger verksamheten möjlighet att kontrollera, begränsa, övervaka och skydda resursers integritet och sekretess.

5.2 Allmänt om registrering, identifiering och autentisering

För att ett subjekt, exempelvis en användare, skall kunna använda en e-tjänst eller annan elektronisk resurs, så måste subjektet ha en digital identitet. Själva ansökan eller registreringen för att få en identitet kan se olika ut. I sin enklaste form kan en användare klicka på ”Ny Användare” på en webbsida för att själv skapa en identitet genom att registrera ett användarnamn och lösenord. I en mer avancerad form så krävs ett personligt möte och legitimering med ID-kort för att användaruppgifter skall registreras och en identitet skapas.

För att använda en e-tjänst eller elektronisk resurs så måste subjektet först bevisa att den är den som den utger sig för att vara. I vissa fall, exempelvis författningskrav, så måste man i efterhand även kunna se hur subjektet har använt resursen och till vad.

Subjektet börjar med att uppge sin identitet, den digitala representationen av användaren. Identiteten kan t.ex. vara i form av ett användarnamn eller användarnummer. Hela förfarandet kan liknas med att en användare talar om vad han eller hon heter.

För att ett subjekt skall kunna bevisa att den verkligen är den som den utger sig för att vara så måste subjektet ange ytterligare en del av identitetsinformationen, en identitetshandling. En identitetshandling kan vara ett lösenord, kryptologisk nyckel, PIN kod, biometriskt attribut eller annan information. Detta kan liknas med ett körkort eller pass.

Ett subjekts identitet verifieras i en autentiseringsprocess. Autentisering är oftast en 2-stegs process: angivande av publik information (identitet) plus angivande av privat information (identitetshandling). Intygsutfärdaren (IdP) jämför angiven identitet och identitetshandling med information som sparades vid registrering och skapandet av subjektets digitala identitet. Om dessa överensstämmer med den sparade informationen så blir subjektet autentiserat.

En lyckad identifiering och autentisering medför att intygsutfärdaren ställer ut ett intyg. Detta intyg konsumeras, eller används, av e-tjänsteleverantören (SP) för auktorisation till e-tjänsten.

Registrering och skapande av identiteter, identifiering, autentisering och distribution av intyg kan hanteras på olika sätt. Detta medför att tilliten kan variera till att ett subjekt faktiskt är det som det utger sig för att vara. För att säkerställa att alla ingående kriterier hanteras i nivå med skyddsvärdet för ett objekt så sammanställs samtliga ingående kriteriers förväntade egenskaper i ett tillitsramverk.

5.3 Allmänt om tillitsramverk

Tillitsramverk avses utgöra en central del i det regelverk som ska vara styrande för en identitets- och behörighetsfederation. De flesta av de internationella ansträngningar som gjorts för att definiera nivåer av tillit har sin grund i publikationen SP800-63-1[1] från det amerikanska National Institute of Standards and Technology (NIST). Ett betydelsefullt arbete för att skapa ett tillitsramverk har genomförts inom Kantara Initiative[2].

Arbeten pågår också inom International Organization for Standardization och International Electro technical Commission (ISO/IEC) som väntas leda till en standard på området, ISO/IEC 29115[3]. Den befinner sig för närvarande i status Draft International Standard (DIS) och enligt uppgift kommer SIS (Swedish Institute of Standards) att rösta nej till den presenterade draften mot bakgrund att den är långt från redo att se dagens ljus.

Arbeten har också bedrivits inom Europeiska unionen, där det storskaliga så kallade STORK-projektet, Secure Identity Across Borders Linked, behandlat ämnet i sitt ramverk Quality Authentication Assurance (QAA)[4] .

Gemensamt för de omnämnda initiativen är att de definierar fyra tillitsnivåer (*Level of Assurance*, LoA). Något förenklat kan tillitsnivåerna beskrivas som en måttstock, där en lägre indikering på skalan motsvarar enklare användning och utgivning, lägre kostnader men också en lägre skyddsnivå. Högre klassificering medför högre kostnader för såväl utgivande som användande men leder till att en högre grad av tillit kan fästas vid identifieringen.

5.3.1 Beskrivning av de olika tillitsnivåerna

De fyra tillitsnivåerna beskriver olika grader av tillit till utställda intyg enligt nedan:

- LoA1 – Låg tillit till ett intygs äkthet och innehåll
- LoA2 – Viss tillit till ett intygs äkthet och innehåll
- LoA3 – Hög tillit till ett intygs äkthet och innehåll
- LoA4 – Mycket hög tillit till ett intygs äkthet och innehåll

Tillitsnivå 1 (LoA1) representeras vanligtvis av en självregistrerad användare utan några egentliga krav på vare sig registrerings eller identifieringsprocessen. Vidare sker autentiseringen utan några egentliga krav.

Tillitsnivå 2 (LoA2) representeras vanligtvis av en eller flera kontroller i samband med registrerings och identifieringsprocessen i syfte att få viss tillit till det som sedermera representeras i ett intyg. Det ställs vissa krav med avseende på autentisering, men inom rimliga gränser tillåts lösenord.

[1] NIST SP800-63-1 http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf
[2] Kantara Initiative Identity Assurance Framework (IAF) http://kantarainitiative.org
[3] ISO http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45138
[4] STORK D2.1 - Framework Mapping of Technical/Organisational Issues to a Quality Scheme

Tillitsnivå 3 (LoA3) representeras vanligtvis av flera kontroller, inklusive någon form av legitimering, i samband med registrerings- och identifieringsprocessen i syfte att få hög tillit till det som sedermera representeras i ett intyg. Det ställs höga krav på autentisering där bland annat 2-faktors autentisering är ett grundkrav. Därmed inte sagt att alla 2-faktorslösningar accepteras.

Tillitsnivå 4 (LoA4) representeras vanligtvis av rikligt med kontroller, inklusive legitimering och personligt besök, i samband med registrerings- och identifieringsprocessen i syfte att få mycket hög tillit till det som sedermera representeras i ett intyg. Det ställs höga krav på autentisering där bland annat hårda bärare av nyckelmaterialet är ett grundkrav.

För att kunna fastställa lägsta acceptabla tillitsnivå för en e-tjänst, bör följande beaktas med avseende på risker och konsekvenser som ett felaktigt innehåll i ett intyg kan medföra:

- Obehag, oro eller ryktesskada
- Finansiell skada
- Skada för organisationens rykte
- Civilt- eller straffrättsligt brott
- Personsäkerhet

5.3.2 En e-tjänsts val av tillitsnivå

För höga krav på tillit till ett intygs äkthet och innehåll kan medföra högre kostnader, men också resultera i mindre flexibilitet och användbarhet för användaren. Den högre kostnaden uppstår på grund av att det vanligen är dyrare att etablera och underhålla ett system med höga krav på tillit till ett intygs äkthet och innehåll. Den minskade flexibiliteten för användaren visar sig exempelvis genom att användaren enbart kan använda viss utrustning eller viss programvara för att nå e-tjänsten eller att identiteten i praktiken enbart kan utfärdas till och användas av vissa kategorier av personer.

Vid val av lägsta acceptabla tillitsnivå för en e-tjänst så måste även hänsyn tas till berörd författningsreglering. Till exempel gör Datainspektionen tolkningen av 31 § i personuppgiftslagen (PUL) att åtkomst till en e-tjänst över öppna nät, såsom Sjunet och Internet, som innehåller känsliga personuppgifter, skall föregås av stark autentisering - alltså minst tillitsnivå 3 (LoA3). Vidare följer av 2 kap. 5 § Socialstyrelsens författningssamling (SOSFS 2008:14) bland annat att en vårdgivare som använder öppna nät för att hantera patientuppgifter har ansvar för att det finns rutiner som säkerställer att åtkomst till patientuppgifter föregås av stark autentisering - alltså minst den autentisering som föreskrivs på tillitsnivå 3 (LoA3).

5.4 Mjuka certifikat ogillas i tillitsnivå 3 (LoA3)

Initiativtagarna till identitets- och behörighetsfederationen för vård och omsorg har tydligt deklarerat att mjuka certifikat inte kan accepteras inom ramen för tillitsnivå 3 (LoA3) med anledning av enkelheten att exempelvis kopiera BankID's PKCS#12-filer.

Mot bakgrund av den kravställningen har följande alternativa tillvägagångssätt diskuterats i förstudien och redogörs mer i detalj i separata avsnitt nedan:

- Särskilt anpassa tillitsramverket för identitets- och behörighetsfederationen för vård och omsorg och där diskvalificera mjuka certifikat för tillitsnivå 3 (LoA3). Se avsnitt 5.4.1.
- Kravställning av tillitsnivå 4 (LoA4) i stället för tillitsnivå 3 (LoA3) i de sammanhang där stark autentisering erfordras. Se avsnitt 5.4.2.
- Tydligt deklarera i intyget vilken autentiseringsmetod som använts vid autentiseringen vilket ger e-tjänsten möjlighet att diskvalificera oönskade autentiseringsmetoder. Se avsnitt 5.4.3.
- Strikt tolkning av tillitsnivå 3 (LoA3) där kravställningen för mjuka certifikat diskvalificerar flertalet lösningar. Se avsnitt 5.4.4.

5.4.1 Särskild anpassning av tillitsramverk för att exkludera mjuka certifikat

En mjuk hållning, som inte kräver några tekniska anpassningar är att göra särskilda anpassningar i tillitsramverket för federationen. Här är det möjligt att exempelvis skärpa skrivningen ytterligare utöver vad som anges nedan i avsnitt 5.4.4. Det är också möjligt att helt diskvalificera mjuka certifikat från tillitsnivå 3 (LoA3). Noterbart är att samtliga omnämnda ramverk i förstudien behöver hanteras.

Exempel på referenser som behöver hanteras:

- I NIST SP800-63-1 är ”Multi Factor Software Cryptographic Token” klassad för tillitsnivå 3 (LoA3).
- I Kantara Initiative IAF SAC AL3_CM_CRN#060 anges “Software cryptographic token strength” för tillitsnivå 3 (LoA3)
- I Stork QAA anges ” Soft certificates or one-time password device token.” samt “Qualified Soft certificates according to Annex I of Directive 1999/93/EC.” för tillitsnivå 3 (LoA3)
- I ISO/IEC 29115 (DIS) är det mjuka certifikatet lika tydligt hanterat. Men det finns en kontroll (C. HardwareOnly) som endast är kravställd för tillitsnivå 4 (LoA4).

Stora ändringar bör undvikas då samverkan med andra federationer och andra aktörer som tillämpar tillitsramverken försvåras. Den eventuella granskningen/revideringen kommer inte att kunna ske utan anpassningar vilket kommer att vara kostnadsdrivande. Det bör också noteras att de fyra ramverken som studerats är relativt samstämmiga i detta avseende varför det inte rör sig om en avvikelse utan flera.

5.4.2 Tillitsnivå 4 (LoA4) i jämförelse med tillitsnivå 3 (LoA3)

I såväl tillitsnivå 3 (LoA3) som tillitsnivå 4 (LoA4) inryms det ofta återkommande begreppet ”stark autentisering” (se exempel i avsnitt 5.3.2). Det finns dock flera skillnader mellan tillitsnivå 3 (LoA3) och tillitsnivå 4 (LoA4) som bör beaktas, särskilt i de fall där kravställaren enbart uttryckt ”stark autentisering”. Nedan är en handfull krav för tillitsnivå 4 (LoA4) från NIST, Kantara och ISO för att exemplifiera vilka ytterligare krav som ställs i tillitsnivå 4(LoA) i jämförelse med tillitsnivå 3 (LoA3).

Under rubriceringen ”organisation och styrning” kräver tillitsnivå 4 (LoA4) bland annat att:

- Intygsutfärdare (IdP) ska ha blivit godkänd i en utvärdering av efterlevnad enligt ISO/IEC 27001.

Under rubriceringen ”registrering” kräver tillitsnivå 4 (LoA4) bland annat att:

- Intygsutfärdare (IdP) måste säkerställa att identitetsinformationen som registreras tillhör ett existerande subjekt (användare) vilket endast kan ske via ett personligt möte och legitimering med godkänd traditionell identitetshandling såsom SiS märkt ID-kort, nationellt ID-kort utfärdat av svensk polis, svenskt körkort, svenskt EU-pass, nationellt ID-kort utfärdat i annat EU-land eller utländskt pass.

Under rubriceringen ”identitetshantering” kräver tillitsnivå 4 (LoA4) bland annat att:

- Vid utlämnande av identitetshandling tillse att användaren skriver under ett avtal där denne bekräftar och accepterar sitt ansvar att skydda identitetshandlingen.
- Alla ingående aktörer bevarar loggar av alla säkerhetsrelaterade händelser som kan hänföras federationen med en exakt tidsangivelse från en betrodd källa spårbar till den svenska nationella tidsskalan UTC(SP) där SP avser Sveriges Tekniska Forskningsinstitut.

Under rubriceringen ”autentisering” kräver tillitsnivå 4 (LoA4) bland annat att:

- Autentisering grundas på hårda certifikat, lagrade på kryptografisk enhet certifierad enligt Federal Information Processing Standard (FIPS) Security Standard For Cryptographic Modules (140-2)[5] level 3 vilken i sin tur ställer krav på att:
  - Nyckeldata raderas vid intrång
  - Transport av aktiveringsdata måste ske krypterat, annars måste två kanaler användas
  - Operativsystem eller motsvarande möter Common Criteria (CC) Evaluation Assurance Level 3 (EAL3)[6]
- Starka skydd mot man-in-the-middle attacker etableras
- *SAML V2.0 Holder-of-Key Web Browser SSO Profile*[7] används
- Alla led skall autentiseras och alla kanaler skall krypteras

Slutligen kan det inte nog poängteras att ingen kedja är starkare än dess svagaste länk. Varje ingående komponent i federationen minst måste leva upp till de krav som är förenat med den valda tillitsnivån.

Vår bedömning är att tillitsnivå 4 (LoA4) ställer krav som gör merparten av dagens lösningar oanvändbara. Det krävs ny design, nya skyddsmekanismer, nya autentiseringslösningar, nya utgivningsprocesser etc. som sammantaget ger en kostnad som idag sannolikt är svår att motivera. Tiden talar dock för tillitsnivå 4 (LoA4) och på sikt blir det sannolikt enklare och billigare när gapet mellan kravbilden och nuläget successivt minskar förutsatt att kravställningen redan från start är den rätta.

5.4.3 Deklaration av autentiseringsmetod i intyg

Initiativtagarna till identitets- och behörighetsfederationen för vård och omsorg har diskuterat om möjligheten att medlemmarna i federationen följer en given tillitsnivå, exempelvis tillitsnivå 3 (LoA3), men överlåter till respektive e-tjänst att diskvalificera en autentiseringsmetod.

I mitten av 2000-talet, innan begreppet tillitsnivå (*Level of Assurance*, LoA) hade blivit ett vedertaget begrepp, arbetades det fram en specifikation med ambitionen att kommunicera bland annat autentiseringsmetod. Totalt är 25 autentiseringsmetoder identifierade och det som avser någon form av certifikat kan relateras till följande:

- Public Key – X.509
- Public Key – PGP
- Public Key – SPKI
- Public Key - XML Digital Signature
- Smartcard
- SmartcardPKI
- SoftwarePKI
- SSL/TLS Certificate-Based Client Authentication

[5] FIPS 140-2 http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
[6] Common Criteria (CC) http://www.commoncriteriaportal.org/cc/
[7] http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-holder-of-key-browser-sso-cd-01.pdf

Specifikationen benämns *Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0*[8]. Den gör det möjligt att förutom autentiseringsmetod även kommunicera karaktäristik såsom:

- Registreringsprocess
- Identifieringsprocess
- Tekniska skydd
- Operativa skydd
- Legala aspekter

Ovanstående karaktäristik är vad som vanligtvis återfinns i ett tillitsramverk idag. Tillitsramverken är betydligt bättre med avseende på kravställning än vad själva specifikationen är. Överlåter man till förlitande part, exempelvis en e-tjänst, att själv göra kravställningen utifrån denna specifikation är risken stor för tolkningssvårigheter. För identitetsleverantören blir det ett omfattande arbete att leva upp till varje kravställning. Möjligheten att för användaren visa vilka identitetsleverantörer som uppfyller e-tjänstens kravställning i exempelvis en anvisningstjänst omöjliggörs eftersom SAML-metadata av naturliga orsaker inte kan förses med denna information. Exempelvis kan olika användare knutna till en och samma intygsutfärdare (IdP) ha olika karaktäristik.

Den eventuella granskning/revidering som skall ske kommer att ske individuellt med utgångspunkt från varje kravställares kravbild vilket leder till omfattande granskning/revideringskostnader.

Vår bedömning är att tillitsnivåerna kanske inte är helt perfekta för varje enskilt fall, men att kostnaden för att tillåta avvikelser inte står i paritet till nyttan.

5.4.4 Strikt tolkning av tillitsnivå 3 (LoA3) med avseende på mjuka certifikat

Såväl NIST som Kantara kräver att mjuka certfikat skall leva upp till minst FIPS 140-2. Det finns en skillnad i krav mellan NIST SP800-63-1 och Kantara IAF Service Assessment Criteria (SAC). Enligt NIST räcker det med FIPS 140-2 level 1, medan Kantara kravställer FIPS 140-2 level 2. Efter dialog med Richard G. Wilsher, CEO Zygma LLC, editor av Kantara IAF SAC, så kan det antas att SAC i större utsträckning anpassas till den nyligen publicerade uppdateringen av SP800-63, benämnd SP800-63-1.

FIPS 140-2 level 1 ställer inte några särskilda krav utöver de generella kraven i FIPS 140-2.

FIPS 140-2 level 2 ställer, utöver de generella kraven i FIPS 140-2, bland annat krav på att:

- Det finns manipuleringsbevis (epoxy, säkerhetstejp eller liknande försegling)
- Operativsystem eller motsvarande möter Common Criteria EAL2

Vår bedömning är att oavsett om det är FIPS 140-2 level 1 eller level 2 som krävs för mjuka certifikat så är de på svenska marknaden vanligaste förekommande lösningarna såsom BankID på fil med Nexus Personal som Certificate Service Provider (CSP) inte FIPS 140-2 certifierade. Därmed är de i sin nuvarande form inte att betrakta som en godkänd autentiseringslösning inom ramen för tillitsnivå 3 (LoA3). Sett ur perspektivet att användaren i vård- och omsorgsfederationen vanligtvis är en fysisk person som agerar i tjänsten (där denne representerar eller verkar hos en juridisk person) så torde detta vara till fylles.

[8] http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

5.5 Tillitsramverk för identitets- och behörighetsfederationen för vård och omsorg

5.5.1 Kravbild

Under denna förstudie har det konstaterats att vård- och omsorgsfederationens initiativtagare i huvudsak har efterfrågat tillitsnivå 3 (LoA3) vilket uppfattas ligga i linje med dagens lösningar. På sikt kan antas att högre skyddsnivåer kan erfordras vilket kan ställa krav på en högre tillitsnivå, exempelvis tillitsnivå 4 (LoA4).

För att möta det långsiktiga behovet av tillitsnivå 4 (LoA4) bör varje kravställning som rör en komponent eller beståndsdel med direkt beröring till tillitsnivån kravställas i god tid innan. Det rör dels mjuka företeelser som registreringsprocess, utfärdandeprocess osv, dels hårda ting som design skyddsmekanismer, autentiseringslösningar osv. Exempelvis bör SITHS[9] och andra autentiseringslösningar som kan bli aktuella för tillitsnivå 4 (LoA4) redan nu kravställas mot den samma.

En intygsutfärdare (IdP) använder flera källor för att utfärda ett intyg. Det är viktigt att tillitsramverket struktureras så att hela eller delar av lösningen kan granskas. Detta mot bakgrund att en komponent som exempelvis en och samma CSP (*Credential Service Provider*) kan förekomma hos flera intygsutfärdare (IdP) och rimligen inte bör granskas mer än en gång. Bland andra komponenter som kan förekomma hos flera intygsutfärdare bör nämnas källan till attribut, vanligtvis en katalog. Här kan HSA-katalogen[10] exemplifiera en källa till attribut som kan användas av flera intygsutfärdare.

Tillitsramverket bör i möjligaste mån harmoniseras med det tillitsramverk som arbetas fram i andra nationella federativa initiativ såsom E-legitimationsnämndens, Skolfederation.se och SWAMID. Detta för att undvika att exempelvis en intygsutfärdare (IdP) som verkar i flera federationer inte får en försvårande kravbild. Exempelvis en privat vårdgivare, kommun eller friskola.

Tillitsramverket skall särskilt beakta all nyckelhantering som en federation är förenat med, allt från federationsoperatörens nycklar, till varje ingående aktörs nycklar. Tillitsramverket skall belysa så väl kravställning på nycklar som hantering av nycklar såsom förvaring, utbyte, destruktion etc.

Tillitsramverket bör också så långt det är möjligt följa goda förebilder som NIST SP800-63-1 och Kantara Initiative IAF. Det senare förenklar granskning/revidering avsevärt där exempelvis Kantara Initiative Identity Assurance Framework (IAF) Service Assessment Criteria (SAC) kan ligga till grund för en granskning/revidering. ISO/IEC 29115 är i ett icke användbart skick och STORK QAA har inte en struktur som möjliggör granskning/revidering. Bilaga 9 i E-Legitimationsutredningen (SOU 2010:104) är ett exempel på ett tillitsramverk för tillitnivå 3 (LoA) där goda förebilder anpassats till de svenska förhållandena. Bilaga 9 skall dock inte ses som något färdigt och helt genomarbetat material.

Tillitsramverket skall slutligen presentera sina tillitsnivåer på ett sådant sätt att de kan utgöra grund för användningen av *SAML V2.0 Identity Assurance Profiles*[11] för att kunna kommunicera tillitsnivåer i federationen parterna i mellan.

[9] Säker IT i Hälso- och Sjukvård (SITHS) är en tjänstelegitimation med certifikat utgivna av Inera AB (Health Care Certificate (HCC)) och Telia AB (Telia eID2008).
[10] Hälso- och Sjukvårdens Adresskatalog (HSA)
[11] http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.pdf

5.6 Förslag till beslut

Vi föreslår att ett arbete inleds med att arbeta fram ett tillitsramverk för tillitsnivå 3 (LoA3) med utgångspunkt från NIST SP800-63-1, Kantara Initiative Identity Assurance Framework och E-legitimationsutredningen (SOU 2010:104) bilaga 9. Arbetet bör ske i nära samverkan med E-legitimationsnämnden, Skolfederation.se och SWAMID samt berörda informationsägare som kan antas ansluta sig till federationen i närtid.

Tillitsramverket skall särskilt beakta att tillit till intyg bygger på flera samverkande komponenter där varje enskilt komponent skall kunna granskas/revideras (ex autentiseringslösning, *CSP credential service provider*) för att minimera risken för dubbel granskning/revidering.

Vidare behöver en aktiv ställning tas till huruvida identitets- och behörighetsfederationen för vård och omsorg skall sträva mot tillitsnivå 4 (LoA4). Detta blir i sin tur vägledande för så väl kringkomponenter som administrativa rutiner hur dessa framöver skall utvecklas och kravställas.

6 Teknisk infrastruktur

6.1 Aktörer

6.1.1 Användare

Den som använder federationens tekniska infrastruktur benämns ofta för subjekt. Det kan vara en fysisk person, ett program eller en process. I vård- och omsorgsfederationen är en användare vanligtvis en fysisk person som agerar i tjänsten där denne representerar eller verkar hos en juridisk person samt privatpersoner.

6.1.2 e-tjänsteleverantör (SP)

Den aktör som erbjuder tjänster och som har förmågan att konsumera utfärdade intyg är att betrakta som e-tjänsteleverantör (*SP, Service Provider*).

e-tjänsteleverantören är att betrakta som kravställare med avseende på tillitsnivå, (LoA), identifieringsbegrepp och eventuella erfordrade attribut inom ramen för vad som överenskommits i federationen. Det är av största vikt att e-tjänsteleverantören inte överkonsumerar attribut, att den personliga integriteten inte åsidosätts och självklart skall tillämpningsbar författningsreglering följas.

6.1.3 Intygsutfärdare (IdP)

Den aktör som har förmågan identifiera och autentisera en användare (*subject*) är att betrakta som intygsutfärdare (*IdP, identity provider*). En lyckad identifiering och autentisering medför att intygsutfärdaren ställer ut ett intyg.

Det bör beaktas att i rollen som intygsutfärdare måste vederbörande också ha tillgång till erforderliga källor för att kunna bidra med de eventuella attribut som efterfrågas av e-tjänsteleverantören. Attribut kan vara allt från personliga egenskaper till behörigheter. Det kan inte nog poängteras att ett intyg inte nödvändigtvis behöver innehålla någon information som knyter an till en personuppgift.

6.1.4 Federationsoperatör

Basfunktionen för en federationsoperatör är att tillhandahåll grundläggande tjänster. En av federationsoperatörens viktigaste uppgifter är att tillhandahålla digitalt signerat aggregerat SAML-metadata (se avsnitt 8.2.2) vilket kan anses vara federationens kärna, den grundläggande tilliten. Utöver den grundläggande tilliten har federationsoperatören ingen egentlig funktion i den enskildes användning av federationen.

6.2 Kravbild

Vård- och omsorgsfederationen bör likt andra federativa initiativ ha en ambition att använda följande SAML 2.0[12]-profiler:

- eGov2[13] - Implementations profil som beskriver vilka SAML-förmågor som erfordras
- saml2int[14] - Deployment profil som beskriver hur SAML-förmågorna skall användas

De SAML-förmågor, där merparten är en del av implementationsprofilen Gov2, och hur SAML-förmågor påverkas av deploymentprofilen saml2int, redovisas i den fortsatta beskrivningen av den tekniska kravbilden nedan.

6.2.1 Krypteringsnycklar

Samtliga parter i federationen skall hantera och förvara sina krypteringsnycklar i enlighet med de krav som ställs i federationens tillitsramverk. Om inte tillitsramverket ställer högre krav så skall samtliga krypteringsnycklar uppfylla följande krav:

- Nyckellängd minimum på 2048 bitar
- Livslängd max 18 månader (vid nyckellängd 4096 bitar tillåts 24 månader)
- Parallellpublicering vid nyckelbyte minimum 2 veckor

6.2.2 SAML-metadata (MD)

För att aktörerna (*entity*) i federationen skall kunna lita på varandras intyg krävs ett utbyte av de publika nycklarna i varje aktörs nyckelpar och därigenom kan intygets signatur verifieras. Tillitsramverket förutsätts reglera nyckelhanteringen mer i detalj än vad som anges i denna tekniska beskrivning.

Utbytet sker genom att lokalt SAML-metadata (MD), vilket beskriver en aktörs egenskaper, förmågor och publika nycklar, aggregeras till federationsoperatören vilken digitalt signerar och publicerar det aggregerade SAML-metadatat. Det aggregerade och signerade SAML-metadata som publiceras av federationsoperatören är således den samlade bilden av federationens samtliga aktörers egenskaper, förmågor och publika nycklar.

Federationens aggregerade och signerade SAML-metadata publiceras lämpligen på en för federationen central URL. Exempelvis http://md.domain.tld/md/federation-v.r.xml. Där v.r är en versionsbeteckning.

Federationsoperatörens publika nyckel som används för verifiering av SAML-metadata publiceras lämpligen på en för federationen central URL. Exempelvis https://md.domain.tld/md/federation.crt.

En checksumma (hash) av den publika nyckeln bör med fördel tillgängliggöras över ytterligare en kanal. Exempelvis via DNS och med fördel i en domän som är DNSSEC-signerad. I förlängningen kan publiceringen sannolikt ske inom ramen för DANE och därmed också automatisera såväl publicering som verifiering.

Varje ingående aktör skall signaturverifiera SAML-metadata vid varje förändring mot minst en nyckelkälla.

Federationen föreslås använda saml2int som *deployment profil* vilken tydligt beskriver hur SAML-metadata skall presenteras. Utformningen av SAML-metadata regleras i OASIS *SAML V2.0 metadata specification* [SAML2Meta] och hantering av SAML-metadata regleras i OASIS

[12] Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML)

[13] Kantara Initiative eGov 2.0 profile

[14] Interoperable SAML 2.0 Web SSO deployment profile

Metadata Interoperability Profile [MetaIOP]. Samtliga ingående aktörer i federationen skall stödja dessa.

6.2.3 Autentiseringsförfrågan

I grundscenariot där en användare önskar använda en e-tjänst (SP), men är oidentifierad så blir denne ombedd att autentisera sig. Den förfrågan som e-tjänsten (SP) skapar i detta scenario är en autentiseringsförfrågan vilken användaren tar med sig till intygsutfärdaren (IdP).

Federationen föreslås använda saml2int som *deployment profil* vilken tydligt beskriver hur *SAML V2.0 Web Browser SSO Profile* [SAML2Prof[15]] skall användas vilket i sin tur återspeglar sig på autentiseringsförfrågan. Där återfinns bland annat att:

- Kommunikationen skall skyddas med TLS/SSL på transportnivå
- Det inte är något krav att signera autentiseringsförfrågan

6.2.4 Autentiseringssvar

Autentiseringssvaret kan vara en följd av en autentiseringsförfrågan, men det kan också vara ett autentiseringssvar utan någon föregående autentiseringsförfråga.

Federationen föreslås använda saml2int som *deployment profil* vilken tydligt beskriver hur *SAML V2.0 Web Browser SSO Profile* [SAML2Prof] skall användas vilket i sin tur återspeglar sig på autentiseringssvaret. Där återfinns bland annat:

- Kommunikationen skall skyddas med TLS/SSL på transportnivå
    - om TLS/SSL inte kan tillämpas skall autentiseringssvaret krypteras i sin helhet
- Autentiseringssvaret skall signeras
- e-tjänster (SP) skall acceptera icke ombedda intyg (unsolicited respons)

6.2.5 Pseudonymiserade identitetsbegrepp (NameID)

I sammanhang där användarens personliga integritet är av stor vikt kan pseudonymer användas som identifieringsbegrepp (NameID). Det finns två typer av pseudonymer. Dels persistenta pseudonymer vilka har egenskapen att de alltid mappar en användare till samma pseudonym per e-tjänst, dels transienta pseudonymer vilka aldrig mappar en användare till samma pseudonym. Vid användning av persistenta pseudonymer presenteras olika pseudonymer för olika e-tjänster. Vid användning av transienta pseudonymer presenteras en ny pseudonym vid varje nytt tillfälle och för varje e-tjänst.

Pseudonymer är en del av SAML2Core[16] och följande bör stödjas:

- urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- urn:oasis:names:tc:SAML:2.0:nameid-format:transient

I fall där pseudonymiserade identitetsbegrepp inte används önskar initiativtagarna till vård- och omsorgsfederationen att identitetsbegrepp som personnummer och HSAid används som NameID.

6.2.6 Hantering av olika tillitsnivåer (LoA)

Initiativtagarna till vård- och omsorgsfederationen ser en federation med flera tillitsnivåer. Detta behöver kunna kommuniceras parterna i mellan. Dels kan man addera information i SAML-metadata dels kan man hantera detta inom ramen för en autentiseringsfråga och ett autentiseringssvar.

Metadata ger flera fördelar. Exempelvis kan anvisningstjänsten, som använder SAML-metadata för att presentera för användare lämpliga intygsutfärdare (IdP), begränsa presentationen till

[15] Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0

[16] Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0

användare till att enbart presentera de intygsutfärdare (IdP) som minst uppfyller den efterfrågade tillitsnivån. I SAML-metadata representeras tillitsnivån av ett attribut. Samtliga ingående parter måste hantera utökat SAML-metadata som tillåter presentation av attribut i enlighet med *SAML V2.0 Metadata Extension for Entity Attributes*[17]*.* Attributen för tillitsnivå skall presenteras i enlighet med *SAML V2.0 Identity Assurance Profiles.*

Utbytet av informationen inom ramen för en autentiseringsfråga och ett autentiseringssvar ger möjlighet att hantera det faktum att en intygsutfärdare (IdP) kan representeras av olika kategorier av användare där det inte är självklart att alla användare representerar samma tillitsnivå. Vidare kan en användare ha tillgång till olika autentiseringsmetoder som i sin tur kan representera olika tillitsnivåer. Utbytet av information sker inom ramen för *Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0*. Där specifikationen anpassas i enlighet med *SAML V2.0 Identity Assurance Profiles*.

I vård- och omsorgsfederationen bör båda metoderna användas. Det tillitsramverk som används i federationen måste presenteras sina tillitsnivåer på ett sådant sätt att det kan utgöra grund för användningen av *SAML V2.0 Identity Assurance Profiles.*

6.2.7 Anvisningstjänst (DS)

I grundscenariot där en användare önskar använda en e-tjänst (SP) men är oidentifierad så blir denne ombedd att autentisera sig.

I en tvåpartsrelation så vet e-tjänsten vilken intygsutfärdare (IdP) som denne skall anvisa användaren till. I en federation likt vård- och omsorgsfederationen med kanske 100-talet intygsutfärdare krävs sålunda en generisk funktion för att anvisa användaren till ”sin” intygsutfärdare. Funktionen benämns anvisningstjänst (*DS, discovery services*).

Anvisningstjänsten använder SAML-metadata för att visa användaren de i federationen ingående identitetsintygsutfärdarna (IdP). I en federation med ett 10-tal intygsutfärdare så löses detta enklast med en lista där användaren väljer ”sin” intygsutfärdare. Valet kan exempelvis lagras i en kaka (*cookie*) så att användaren därefter alltid får sitt sista val som förvalt.

I en federation med 100-talet intygsutfärdare krävs en bättre logik där listan som presenteras kan prioriteras utifrån geografisk tillhörighet, käll IP-adress eller annan igenkänning som gör valet för användaren smidigare.

Federationens centrala anvisningstjänst publiceras lämpligen på en för federationen central URL. Exempelvis https://ds.domain.tld/anvisning.

Det bör poängteras att en central anvisningstjänst (DS) inte är en nödvändighet utan e-tjänsteleverantören (SP) kan själv välja att implementera en funktion för lokal anvisning baserat på SAML-metadata.

Det bör också poängteras att det finns möjlighet till ett scenario med icke ombedda intyg (*unsolicited respons*). Där ansluter användaren först till sin intygsutfärdare (IdP) med en parameter i anropet som sedan används för att anvisa användaren till rätt e-tjänst (SP).
Hantering av anvisning regleras av OASIS *Identity Provider Discovery Service Protocol Profile* [IdPDisco]. Samtliga ingående aktörer i federationen bör stödja detta.

6.2.8 Single-logout (SLO)

Initiativtagarna till vård- och omsorgsfederationen ställer inledningsvis inget krav på att ingående aktörer skall stödja single-logout. Federationen sätter dock inte några infrastrukturella hinder att implementera single-logout.

[17] http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.pdf

Implementationen av single-logout är inte sällan en del i den sessionshantering som är ett resultat av ett lyckat autentiseringssvar (se avsnitt 8.2.4 ovan). Själva sessionshanteringen är inte något som hanteras inom ramen för SAML viket gör frågan större än att bara vara en del i en teknisk specifikation.

Den tekniska specifikationen för att hantera single-logout inryms i *Single-logout Profile*[18]. Målbilden är att en e-tjänst (SP) skall kunna skicka en signal <LogoutRequest> till intygsutfärdare (IdP) som i sin tur skickar <LogoutRequest> till övriga e-tjänster (SP) som intygsutfärdaren (IdP) tror sig hålla session till. Varje e-tjänst (SP) måste svara med en <LogoutResponse> till intygsutfärdaren (IdP) som slutligen svarar den e-tjänst (SP) som initerade single-logout med en <LogoutResponse> som är ett kvitto på en lyckad single-logout.

När en e-tjänst (SP) implementerar funktionen är det viktigt att det framgår i användargränssnittet att den är en single-logout som utförs och att det innebär en användare loggas ur från alla e-tjänster (SP) där denna är inloggad.

6.2.9 Attributstjänst (AA)

Initiativtagarna till vård- och omsorgsfederationen har inte inledningsvis pekat på några för federationen gemensamma attributstjänster (*AA, Attribute Authority*). Federationen sätter dock inte några infrastrukturella hinder att implementera attributstjänster.

En attributsförfråga ställs ofta av en e-tjänsteleverantör (SP) som ett resultat av avsaknade attribut i det intyg som en intygsutfärdare (IdP) utfärdat i form av ett autentiseringssvar. En attributstjänst använder innehållet i subjekt-fältet som grund för en attributsförfrågan. Attributssvaret levereras i form av ett intyg där attribut relaterade till attributsförfrågan presenteras.

Skatteverket/Navet skulle kunna etablera en attributstjänst där en attributsförfrågan innehållande ett personnummer som subjekt resulterar i ett attributssvar innehållande folkbokföringsadressen.

6.3 Attribut

De för federationen gemensamma attributen kan med fördel samordnas. Det ger en tydlig kravbild för de källor som skall användas för attributen, exempelvis kataloger. En samordning kan också minska risken att likartade attribut förekommer i flera olika varianter och kanske med olika tolkningar.

Den tekniska infrastrukturen utgör inte några hinder för att använda andra attribut än de som eventuellt överenskommits mellan de enskilda aktörerna.

6.3.1 Exempel på generella attribut

Följande är att se som exempel på generella attribut i federationen:

[18] Profiles for the OASIS SAML V2 0http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

Attribut	SAML Attribute @Name	Beskrivning
sn	urn:oid:2.5.4.4	Efternamn
givenName	urn:oid:2.5.4.42	Förnamn
mail	urn:oid:0.9.2342.19200300.100.1.3	Epostadress
personalIdentityNumber	urn:oid:1.2.752.29.4.13	Personnummer eller samordningsnummer enligt SKV 704 respektive SKV 707.
hsaIdentity	urn:oid:1.2.752.29.4.19	Unik identifierare för personer, enheter, funktioner, uppdrag och organisationer inom vård och omsorg
postalAddress	urn:oid:2.5.4.16	Nåbarhetsadress
street	urn:oid:2.5.4.9	Gatuadress
postOfficeBox	urn:oid:2.5.4.18	Box
postalCode	urn:oid:2.5.4.17	Postnummer
l	urn:oid:2.5.4.7	Postort
c	urn:oid:2.5.4.6	Land
telephoneNumber	urn:oid:2.5.4.20	Telefonnummer
mobile	urn:oid:0.9.2342.19200300.100.1.41	Mobilnummer

6.3.2 Exempel på behörighetsstyrande attribut

Följande är att se som exempel på behörighetsstyrande attribut för federationen.

De tre inledande exemplen är relaterade till de anpassningar som gjordes av de behörighetsgrundande attributen för att harmonisera med Patientdatalagen (PDL, 2008:355). Bland de behörighetsgrundande attributen återfinns bland annat begreppet medarbetare i uppdrag (MiU, *hsaCommission*) för att ange syfte och rättigheter.

De fem avslutande exemplen är behörighetsstyrande attribut kopplade till rättighet, befattning, titel och/eller roll som kan användas av de intressenter i vård- och omsorgsfederationen som av en eller annan anledning inte kan anamma begreppet medarbetare i uppdrag.

Attribut	SAML Attribute @Name	Beskrivning
hsaCommissionRight	urn:oid:1.2.752.29.4.124	Rättighetstyp för aktuell medarbetare i uppdrag. Anges som <aktivitet>;<informationstyp>;<organisationsomfång>. Ex *Läsa;dia;SJF*)
hsaCommissionPurpose	urn:oid:1.2.752.29.4.125	Syftesbeskrivning för aktuell medarbetare i uppdrag. Ex *Vård och behandling*.
hsaCommissionMember	urn:oid:1.2.752.29.4.123	Medarbetaruppdragets medlemmar. Anges som <Personens HSAid>;(<startdatum>);(<slutdatum>).
personalPrescriptionCode	urn:oid:1.2.752.29.4.24	Förskrivarkod som identifierar en förskrivare eller en grupp av förskrivare.
paTitleCode	urn:oid:1.2.752.29.4.41	Kod för personens befattning enligt AID-etikett
paTitleName	urn:oid:1.2.752.29.4.50	Uppgift om vad personen är anställd som enligt AID-etikett. Klartext för personens befattning.
hsaTitle	urn:oid:1.2.752.29.4.40	Klartext för legitimerad yrkesgrupp, enligt Socialstyrelsens förteckning, som personen tillhör.
hsaSystemRole	urn:oid:1.2.752.29.4.95	Beskriver behörighet för person eller funktion i ett visst system.

6.4 Andra tillämpningar

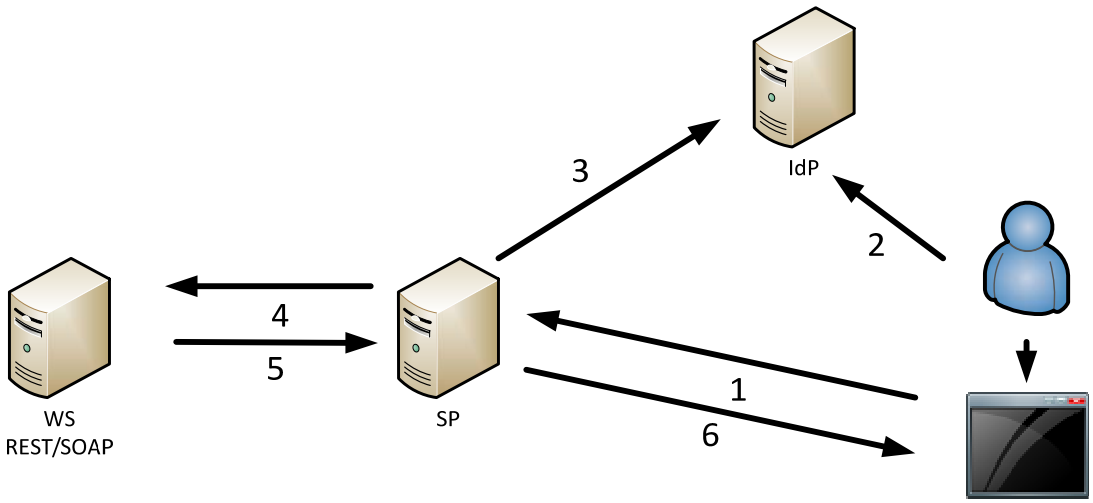
En federation baserad på SAML vänder sig i första hand till ett scenario med en användare med en webbläsare som använder en webbapplikation. Initiativtagarna till vård- och omsorgsfederationen ser fler scenarios där exempelvis webservices och andra typer av klienter än webbläsare förekommer.

6.4.1 Annan klient än en klassisk webbläsare

Inom ramen för SAML finns ytterligare en profil, utöver WEB SSO profilen, som kan vara av intresse. Den heter *SAML V2.0 Enhanced Client or Proxy Profile (ECP)*[19] Denna profil medför att andra klienter än webbklienter får en naturlig plats i en federation. Det bör noteras att profilen i dagsläget är i status ”working draft”.

Handskakningen är jämförbar med WEB SSO profilen med ECP tillämpar intygsflöde med reverse-soap samt eventuellt ett proxy-förfarande mellan klient och e-tjänst (SP). En tänkbar klient här kan vara en ”app”, en ”platta” och även en traditionell Windows-applikation.

[19] ECP http://www.oasis-open.org/committees/download.php/41209/sstc-saml-ecp-v2.0-wd02.pdf



Klienttillämpning gör ett anrop i aktörsystemet som kräver att ett bakomliggande webservice-anrop behövs exekveras (1). Den bakomliggande tjänsten kräver ett eller flera intyg för att tillåta access. För att utföra det initiala anropet krävs då att ett intyg tas fram som representerar slutanvändaren. e-tjänsten (SP) i detta fall har en eller flera fördefinierade intygsutfärdare (IdP) och låter klienten autentisera (2) sig varpå intygsutfärdare (IdP) lagrar intyget tills e-tjänsten (SP) hämtat den (reverse soap-anrop). När intyget är hämtat (3) av e-tjänsten (SP) formateras ett webserviceanrop och intyget adderas på i anropet mot webservicen (4).

När den bakomliggande tjänsten tar emot anropet sker följande

- Intyget packas upp och inspekteras (4)
  - Verifieras (signatur, tillitsnivå etc).
  - Avstämning mot SAML-metadata att intygsutfärdare (IdP) är betrodd
  - Fler kontroller om ytterligare behov finns (ex behörighet)
- Om alla kontroller passeras godkänt ges access till funktionen och/eller data (5 och 6).

Den bakomliggande tjänsten (WS) kan vara SOAP- eller REST-baserad alternativt en reverse proxy för ett tjänstelager.

6.4.2 Kombination av SAML och OAuth 2.0

Grundinfrastrukturen med SAML hanterar de flesta fall när användaren har en webbläsare och ansluter sig till en e-tjänst som förstår att hantera SAML. Sannolikt är det inte tillräckligt. Inte minst i en värld där man vill dela och aggregera data mellan olika tjänster och ”appar” där kanske ingående aktörer själva inte kan kontrollera alla ingående delar. Här kan en kombination av SAML och OAuth 2.0[20] vara lösningen där OAuth som ett öppet auktorisationsprotokoll tillför delar som SAML inte omfamnar. Exempelvis tillför OAuth 2.0 ett delegerat synsätt som möjliggör tillämpningar att agera företrädare för ett givet subjekt och därmed ges åtkomst till objekt baserat på en autentisering som ett subjekt gjort i en tillämpning vilken länkats till den/de OAuth 2.0 Token Providers som berörs av de involverade aktörer som verkar inom informationsflödet.

Bakrunden till OAuth finns i integration mellan diverse system som Twitter, Facebook, Google, Yahoo mfl och OAuth 1.0 (RFC5849) togs fram baserat på dessa erfarenheter. Denna första version kom dock att bli lite av ett fiasko som standard betraktat och det startades ett nytt arbete att ta tag i den fraktionering som uppstått och standardisera runt OAuth 2.0. RFC status är att vänta i slutet av 2012[21]. OAuth 2.0 är i vissa avseenden en förenkling samtidigt som det är en

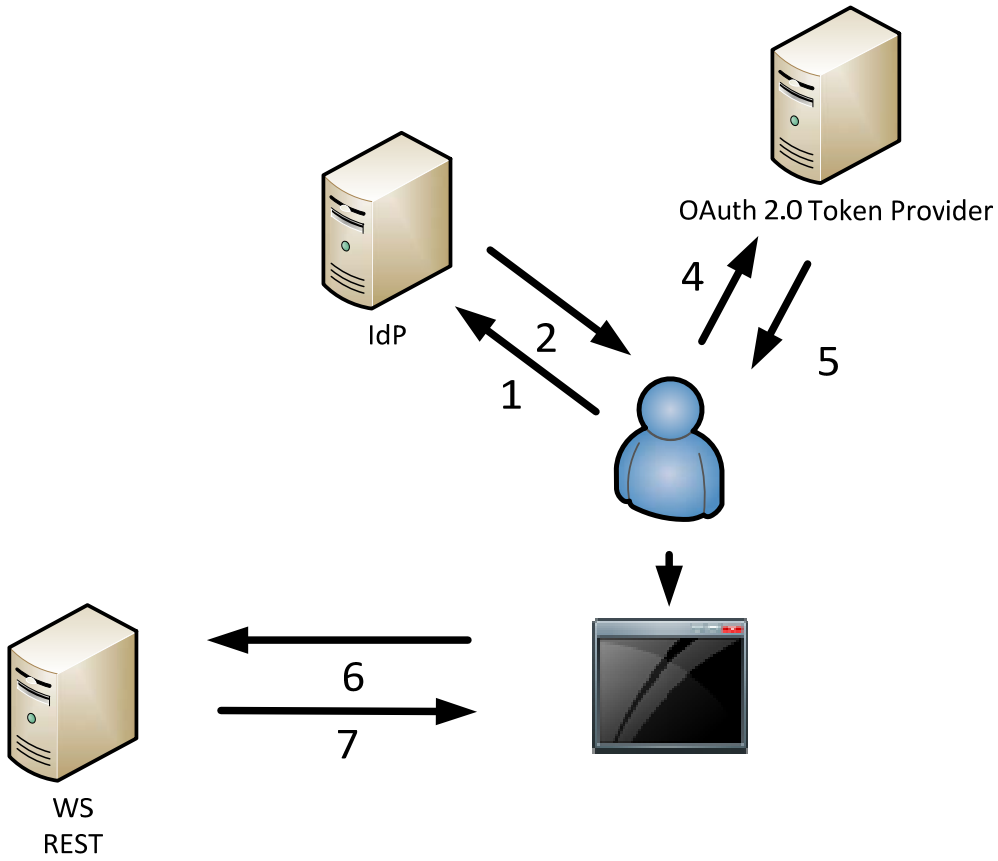
[20] Open Authentication 2.0 http://oauth.net/2/
[21] IETF OAuth Draft http://tools.ietf.org/html/draft-ietf-oauth-v2-25

anpassning till lite mer generella behov. OAuth 1.0 och OAuth 2.0 är inte kompatibla men grunden i funktionen och hur flödena mellan användare och tjänster ser ut är desamma.

Det är i sammanhanget viktigt att notera att OAuth 2.0 använder sig av motsvarigheter till SAML profiler, så kallade OAuth 2.0 User Agent Flows, vilka styr interaktionen mellan:

- User Agent (klient/tillämpning)
- OAuth 2.0 Token Provider
- OAuth 2.0 Token Consumer

OAuth 2.0 kombineras kanske bäst med REST-API:er men kan i förekommande fall även integreras inom ramarna för SOAP-baserade Web Service-miljöer. Det senare sker genom att infoga utfärdade OAuth 2.0 Tokens inom ramarna för SOAP-headern som medföljer respektive SOAP-anrop. Dock är det viktigt att notera att SOAP-endpointen som agerar mottagare på tjänstesidan måste kunna konsumera OAuth 2.0 Tokens för att kunna identifiera och auktorisera inkommande subjekt i detta scenario.

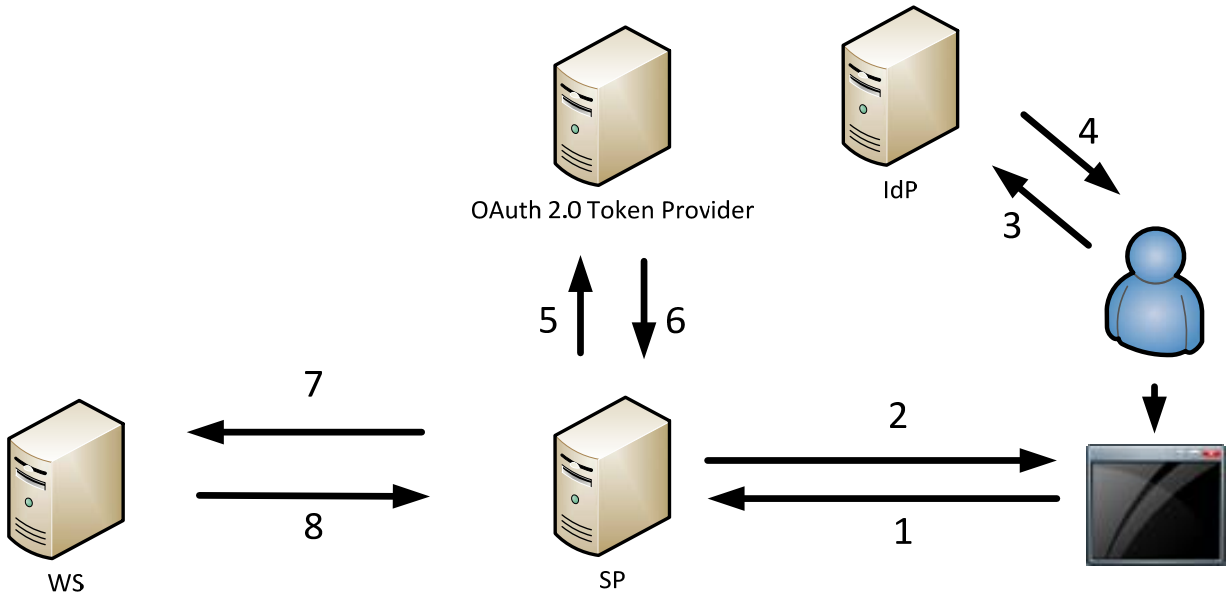


Ovan är ett exempel på hur OAuth 2.0 och SAML 2.0 kan samverka inom ramarna för en identitetsfederation:

1. Tillämpningen som önskar åtkomst till information som tillhandahålls av en Web Service med ett REST-API initierar någon av de SAML-profiler som används inom den/de federation(er) som man verkar inom.
2. Tillämpningen kvitterar ut ett eller flera SAML-intyg efter att aktuell användare autentiserat sig i enlighet med de krav som aktuell intygsutfärdare (IdP) och dess tillitsnivå(er) ställer.
3. Tillämpningen konstruerar ett OAuth 2.0 Request via ett OAuth 2.0 SAML Bearer Flow, där tidigare utkvitterade SAML-intyget agerar som underlag för autentisering mot OAuth 2.0 Token Providern.

4. OUath 2.0 Token Providern validerar SAML-intyget och skickar tillbaka ett OAuth 2.0 Response med en OAuth 2.0 Access Token förutsatt attSAML-intyget passerar samtliga verifieringsmekanismer samt att subjektet har behörighet att kvittera ut Access Token.
5. Tillämpningen exekverar ett anrop mot det REST-API som tillhandahåller åtkomst till informationen som efterfrågas. I detta anrop skickas utfärdad OAuth 2.0 Access Token med till REST-API:et.
6. Tjänstegränssnittet för REST-API:et tar emot och verifierar den OAuth 2.0 Access Token som uppvisas, om verifieringen passerar samtliga kontrollmekanismer samt att subjektet har behörighet till objektet som efterfrågas medges åtkomst.

Det är också viktigt att notera att OAuth 2.0 kan agera inom ramarna för en SAML-profils interaktionsflöde i de fall en e-tjänst (SP) med stöd för både SAML och OAuth 2.0 används. I detta fall döljs OAuth 2.0 för klienter och tillämpningar på det sätt att OAuth 2.0 används mellan en e-tjänst (SP) och den resurs som en klienttillämpning begär åtkomst till. Nedanstående bild visar detta scenario:



6.5 Elektroniska underskrifter

En identitets- och behörighetsfederation baserad på SAML har inte någon självklar lösning vad gäller elektroniska underskrifter (signaturer). Vanligtvis är det en PKI (*Public Key Infratructure*) som är den självklara infrastrukturen för elektroniska underskrifter.

Det skall i sammanhanget klart sägas att lagrummet inte är helt tydligt vad gäller det faktiska behovet av elektroniska underskrifter. Lag (2000:832) om kvalificerade elektroniska signaturer, som är ett direkt resultat av signaturdirektivet (1999/93/EG), reglerar egentligen bara det faktum att underskrifter framställda med kvalificerade certifikat inte kan diskvalificeras. Lagen gäller dessutom enbart certifikatutfärdare som är etablerade i Sverige och som utfärdar kvalificerade certifikat till allmänheten. Den närmsta kravställning på en elektronisk signatur som går att finna juridiskt beskrivet är: ”ett elektroniskt dokument vars innehåll och utställare kan verifieras genom ett visst tekniskt förfarande”.

I Sverige finns per idag en anmäld utfärdare av kvalificerade certifika, SignGuard, och de kan anses stå för en icke mätbar andel av den totala mängd av de signeringar som idag utförs. Här är lösningar från BankID, Nordea och Telia, alla inom ramen för ramavtal eID2008, klart dominerande. Noterbart att ingen av dessa utfärdare utfärdar kvalificerade certifikat.

E-legitimationsutredningen (SOU 2010:104) drev tesen att en signeringstjänst, likt en e-tjänst (SP), etableras för att säkerställa de behov som finns av en lösning för elektroniska underskrifter. E-legitimationsnämnden arbetar vidare enligt utredningens förslag och en eller flera signeringstjänster är att vänta inom ramen för den federation som E-legitimationsnämnden realiserar under 2013/2014.

Så vitt förstudien har kunnat se finns det ingen författningsreglering där krav på en kvalificerad elektronisk signatur föreligger för de organisationer som kan antas ha ett intresse av identitets- och behörighetsfederationen för vård och omsorg varför ingen särskild hänsyn behöver tas. Uppstår behovet kan det antas vara möjligt att använda E-legitimationsnämndens lösning alternativt lösningsförslag.

6.6 Förslag till beslut

Vi föreslår en teknisk etablering av en identitets- och behörighetsfederationen för vård och omsorg i enlighet med avsnitt 8.2. I första steget etableras en teknisk miljö som i mitten av 2012 kan användas för tester och verifiering av SAML-förmågor. I ett andra steg, i senare halvan av 2012, etableras en pilotmiljö, med hänsyn tagen till tillitsramverket, med avsikt att försörja de e-tjänster som har behov av en identitets- och behörighetsfederation för eHälsa.

7 Förvaltning

7.1 Förvaltningsmodell

Tanken är att .SE skall vara federationsoperatör och driva förvaltningsorganisationen. I detta kapitel har därför ett lösningsförslag för förvaltning av tjänsten utarbetats utgående från .SE:s tjänstekoncept.

I .SE konceptet utses en tjänsteägare (TÄ) som är ytterst ansvarig för tjänsten och rapporterar till .SE:s VD och ledningsgrupp. Om så är lämpligt kan tjänsteägaren delegera en del av ansvaret till en operativ tjänsteägare. Till tjänsten knyts också tjänstemedarbetare på hel- eller deltid. En tjänst har ett eget kostnadsställe för ekonomisk uppföljning. Budget och tjänsteplan tas fram årligen av tjänsteägaren och godkänns av .SE:s VD/ledningsgrupp.

Ovanstående lösning behöver troligen kompletteras med någon form av styrgrupp eller liknande där lämpliga parter i federationen ingår. Till denna är det naturligt att .SE:s tjänsteägare rapporterar – se separat avsnitt i tjänsteförstudien om organisation.

7.2 Tjänstens Processer

De levererande processerna är (i .SE:s modell) som skall hanteras när tjänsten övergår till förvaltning anges i bilden nedan.

Utöver ovanstående finns behov av stödprocesser bl.a. juridik och ekonomi.

7.2.1 Utvecklingsprocessen

I denna process hanteras förändringar av tjänsten i syfte att förbättra den. Det finns en mer långsiktig hantering på 1-3 års basis som hanteras årligen i form av att tjänsteplaner och budget tas fram för det närmaste året. I tjänsteplanen finns också de planerade förändringar man vill göra till tjänsten. Dessa kan vara införandet av nya tekniska funktioner, förändringar av regelverk, hur tjänsten skall finansieras, uppdatering av avtal och andra dokument etc.

Utöver dessa ”planerade” förändringar så uppstår behov av oförutsedda ändringar och det hanteras då i utvecklingsprocessen och en prioritering görs kontinuerligt av oförutsedda och planerade ändringar.

En tjänstebeskrivning tas fram som också fungerar som underlag till kommande medlemmar, eventuellt omgjort till mer marknadsorienterat format.

7.2.1.1 Tjänstebeskrivning

Beskriver tjänsten och dess innehåll. Finansiell beskrivning av tjänsten är nödvändig för att kunna prissätta/debitera.

7.2.1.2 Tjänsteplan

När tjänsten utvecklas tas en årlig tjänsteplan fram som gäller till nästa revidering. I tjänsteplanen finns styrkor och svagheter samlad, konkurrensanalys, tjänstemål på kort och lång sikt (strategi), möjliga förbättringar etc. samt en budget fram till nästa revidering. I planen finns också de aktiviteter som förväntas genomföras under det kommande året.

7.2.1.3 Dokumenthantering

Dessa dokument tas fram i samband med utvecklingen av federationen och måste underhållas i förvaltningen:

- Avtal
- Tillitsramverk och informationssäkerhet
- Administrativa rutiner (inkl Hantering av metadata)
- Tekniska rutiner
- Tekniska specifikationer och krav
- Rutiner för test
- Legala krav
- Attributpolicy
- Tvistlösning
- Granskning och kontroll av efterlevnad
- Rutiner för avstängning, nedgradering i samband med incidenter

7.2.2 Försäljningsprocessen

Denna process hanterar hur nya medlemmar tillkommer (ansökan om medlemskap). Här finns också hanteringen av godkännande av den nya medlemmen tills den är upplagd i metadataregistren hos Federationsoperatören.

7.2.2.1 Administration

7.2.2.1.1 Kundtjänst

7.2.2.1.2 Nya medlemmar/granskningar

Hantering av nya medlemmars ansökningar administreras av Kundtjänst. Detta innebär att man tar emot dessa, granskar att all information är med och skickar dem därefter till utsedd ”granskningsgrupp” för godkännande. Efter godkännande hanterar Kundtjänst de vidare kontakterna med den nya medlemmen tills de registrerat sina metadata, godkänd ansökan arkiverats och de kan börja använda systemet. I detta sammanhang kan t.ex. också erbjudas nedanstående:

- Testsystem för att nya medlemmar skall kunna göra funktionsprov.
- Hänvisning till externa konsulter för tekniskt stöd i införandet i medlemmens egna system.

7.2.2.2 Försäljning

Specificeras i nästa steg av projektet.

7.2.3 Leveransprocessen

Processen hanterar metadata registren så att anvisningstjänsten (hänvisningstjänsten) som är det tekniska och administrativa stöd som federationsoperatören tillhandahåller så att användare skall kunna välja sin intygsutfärdare (IdP) och underliggande teknisk infrastruktur. Här ligger också debitering av tjänsten samt (årliga) omprövningar av tidigare godkända medlemmar.

7.2.3.1 Teknik

Den tekniska lösningen är inte i detalj beslutad men det är ingen komplicerad teknik och det finns ett antal lösningar i drift både i Sverige och i världen. Det finns tydliga likheter med den drift .SE har av den svenska toppdomänen .se.

Ett krav som noterats är att den tekniska driftens tillgänglighet är extremt viktig. Detta gäller också för toppdomänen .se men här är det inte bara att Internet stannar utan också om ”liv och död”. Initialt antas att tillgänglighetskraven är på en avsevärt lägre nivå, då hänvisningstjänsten inte är en single point of failure utan metadata återfinns primärt lokalt hos partnerna.

7.2.3.1.1 Teknisk lösning

Den tekniska lösningen kan delas upp i följande olika delar:

- Metadataregister som innehåller information om intygsutfärdare, tjänsteleverantörer och attributsutfärdare.
- Anvisningstjänst som är den del där användare får välja sin intygsutfärdare och efter valet identifiera sig.
- Testmiljö används för att kunna erbjuda nya ”medlemmar” till federationen att verifiera att deras applikationer fungerar med federationen hos intygsutfärdaren.
- Övervakningsfunktion för att kunna se att ”medlemmarnas” system i federationen är tillgängliga.
- HSM (Hardware Security Model) – vi avser att använda HSM för vår privata nyckel.
- Webbplats med allmän information om federationen men också annat t.ex. driftinformation.
- Utöver detta behövs system och hjälpmedel för att underhålla detta i drift i form av system för backup, incidenthanteringssystem etc. Ett loggsystem för spårbarhet krävs också.

7.2.3.1.2 Metadata-register

Dessa register är grunden till anvisningstjänsten och uppdateringsfrekvensen är mycket begränsad men de är dock mycket viktiga varför en redundant driftlösning är ett måste. Drift behöver göras på två separata platser och med minst en koppling mellan dem och eventuellt ytterligare en i separat kanalisation. Kopplingar mot internet/(distributionspunkter – nedan) behövs från varje driftställe. Det är inte klart om det behövs en ”hot” standby lösning (med samtidig uppdatering och omedelbart driftövertagande vid en nedgång av den ena driftsplatsen) eller om det räcker med en ”warm” standby lösning (med ett övertagande inom x antal timmar).

Bedömningen så här långt indikerar att en ”warm” standby lösning skulle räcka. I jämförelse med driften av toppdomänen .se så använder vi en ”warm” för domännamnsregistren.

Oaktat standby lösning så skall detta hanteras i en helt separat driftmiljö avgränsad från övrig verksamhet med mycket begränsad tillgång utåt.

I etapp 1 räcker det med en ”warm” standby lösning.

7.2.3.1.3 Anvisningstjänst

Inledningsvis förutses en låg volym och att endast en enklare lösning behövs.

På sikt kommer tjänsten troligen att ha en hög transaktionsvolym och därigenom behöva vara tillgänglig 100 % (denna del är en form av ”single point of failure” för hela federationen varför den måste minst dubbleras). Den tekniska lösningen är relativt enkel genom att den hämtar data från metadata registren ovan och skickar vidare en användare till rätt mottagare utifrån dessa. Om det inte räcker eller att man vill skydda sig mot det fall att Internets infrastruktur slås ut lokalt kan det även bli aktuellt med ett stort antal replikerade servrat inom Sverige.

I jämförelsen med driften av toppdomänen .se så finns knappt 200 servrar spridda över världen som fungerar på ett liknande sätt (svarar på DNS-anrop). I denna lösning finns också en distributionslösning med några olika distributionspunkter där dessa servrar hämtar information från motsvarigheten till metadata registren för DNS-anropen med lite olika tidsintervall. En motsvarande lösning skulle säkert kunna användas för Anvisningstjänsten.

Ytterligare en lösning skulle kunna vara att lagra lokalt i minnet (”cacha”) i tjänsteleverantörens system lämpligt data för att kunna hantera att Anvisningstjänsten inte svarar på förfrågningar (avbrott eller för hög transaktionsvolym). Detta är ett sätt att ytterligare stärka tillgängligheten. Utformningen av en sådan lösning behöver undersökas närmare.

Lösningen för Anvisningstjänsten måste vara tillgänglig på Internet, dock med en relevant säkerhet.

7.2.3.1.4 Testmiljö

Nya medlemmar behöver kunna testa sina system mot ett testsystem innan de startar ”på riktigt” i federationen för att förvissa sig om att allt fungerar som det är tänkt. Här kan det vara lämpligt att lägga in någon form av funktionsprov som måste godkännas innan de släpps in. Testmiljön skall vara helt separerad från produktionssystemet och det får inte finnas några tvivel i vilket man är. Systemet måste vara tillgängligt på internet. Tillgänglighetsbehoven är oklara i dagsläget men troligen behövs dygnet runt drift fast en 100 % tillgänglighet är nog inte nödvändig. .SE har en liknande lösning för toppdomänen .se där återförsäljarna (webbhotell etc.) testar sina nya system (EPP-test) innan de får köra mot produktionsmiljön.

I etapp 1 behövs inte denna testmiljö men den som nämns nedan behövs dock om än i begränsad omfattning.

Utöver ovanstående testmiljö kommer det också att behövas någon form av intern testmiljö för att verifiera tekniska uppdateringar av federationen.

7.2.3.1.5 Övervakningsfunktion

Federationsoperatörens egna system kommer att behöva övervakas med övervakningshjälpmedel som informerar när någonting inte fungerar och sådana system har .SE sedan tidigare. Det är troligt att Federationsoperatören också kommer att behöva övervaka ”medlemmarnas” system på ett enklare sätt för att se att de är i drift (ping el. liknande) eftersom Federationsoperatören förväntas hantera en kundtjänst och hantera incidenter. Utöver detta kommer Federationsoperatören behöva reda ut de incidenter/problem som medlemmarna inte klarar.

7.2.3.1.6 Webbplats

En webbplats med information om federationstjänsten kommer att behövas. En lösning med en webbplats i drift och en som ”warm” standby förutses behövas.

7.2.3.1.7 Övriga drifthjälpmedel

För att kunna lösa incidenter kommer Federationsoperatören att behöva ha kontaktvägar till både sina egna tekniker och till andra Medlemmarnas tekniker. Krav på ett system för att hantera incidenter, problem, förändringar (”change”) och större uppdateringar av programvara (”release management”) förväntas. .SE har detta på plats, dock enbart internt i dagsläget. En hantering av loggfiler kommer att krävas för att kunna ”spåra” förändringar av metadata-registren.

7.2.3.2 Kundtjänst

7.2.3.2.1 Incidenthantering

En kundtjänst som kan hantera de incidenter som uppstår i leveransprocessen. Den normala kundtjänst som användaren vänder sig till (”first line”) är troligen hos identitetsutfärdaren eller hos tjänsteleverantören medan federationsoperatören blir ”second line” - se Bilden nedan på det tänkta flödet i Federationsoperatörens Kundtjänst.

Vid mycket allvarliga incidenter kan en krisorganisation behöva kallas in. .SE har idag en organisation och rutin men den kommer att behöva kompletteras med de som ansvarar för federationslösningen.

Inledningsvis kommer Kundtjänsthanteringen att bli begränsad under förutsättning att användare primärt vänder sig till befintliga kundtjänster och eventuellt på sikt en ”Nationell Kundtjänst”. Federationsoperatörens roll för incidenthantering blir då mer av teknisk art (tillgång till beredskap och krishantering).

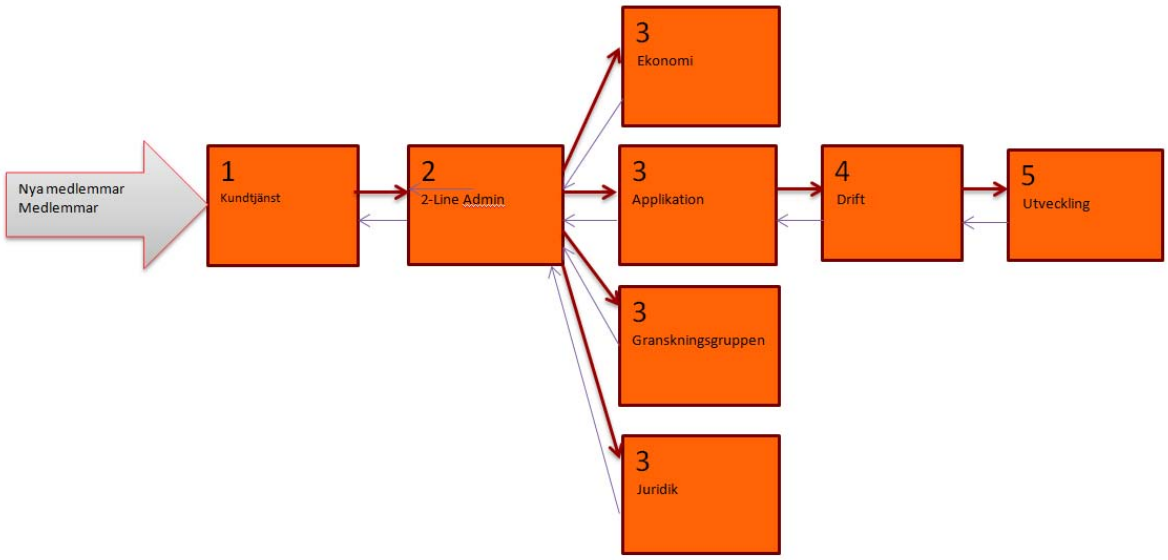
7.2.3.2.2 Ändring av uppgifter

Medlemmar kommer att ändra/ta bort uppgifter i metadata registren. Dessa administreras av Federationsoperatörens. Kundtjänst.

7.2.3.2.3 Granskning/efterlevnad

En initial granskning görs inom försäljningsprocessen i samband med att ”Medlemmen” ansluter sig. Hur granskningen går till är oklart i dagsläget mer än att det utförs i en separat grupp som administreras av Federationsoperatörens Kundtjänst.

En regelmässig uppföljning över att ”Medlemmarna” sköter sina åtaganden förväntas och den kommer att hanteras som den initiala genom Federationsoperatörens Kundtjänst.



Figur - Tänkt flöde i Federationsoperatörens Kundtjänst

7.2.3.2.4 Ärendehanteringssystem

Kundtjänst förutsätts hantera alla ärenden genom ett administrativt system (.SE använder BMC´s Service Desk Express) med full spårbarhet av alla ärenden och vad som gjorts och av vem.

7.2.3.2.5 Kontaktmöjligheter till Federationsoperatörens Kundtjänst

Kundtjänst nås normalt under kontorstid (8-17) vardagar på telefon, via e-post eller fax.

7.2.4 Kundvårdsprocessen

Denna del hanterar primärt uppföljningen av medlemmarnas/kundernas behov för att se att Federationsoperatörens tillfredsställer dem.

7.2.4.1 Arbetsmetod för förbättringsarbete

Federationsoperatören bör ha ett strukturerat kvalitetsarbete för att fånga upp och lösa kunders krav och önskemål.

7.2.4.1.1 Uppföljning av kundnöjdhet

Federationsoperatören bör mäta och hur nöjda Medlemmarna är över tiden med tjänsten. Detta kan göras t.ex. genom:

- Medlemsundersökningar - Fakta om medlemmarnas förväntningar, önskemål, behov och krav samlas in med hjälp av medlemsundersökningar.
- Slutkundsundersökningar – motsvarande för slutkunder (NKI)

7.2.4.1.2 Klagomål/synpunkter

Federationsoperatören bör kunna hantera klagomål/synpunkter från Medlemmar och allmänheten. Ärendena ska dokumenteras i ärendehanteringssystemet och redovisas regelbundet för tjänsteägaren.

7.2.4.1.3 Nyhetsbrev

Federationsoperatören bör åta sig att via e-post skicka ut nyhetsbrev till alla Medlemmar, regelmässigt eller vid behov, för att sprida aktuell information, förbättringsåtgärder eller allmänt om vad som pågår.

7.2.4.2 Mål och resultat

Federationsoperatören bör åta sig att följa upp långsiktiga mål, så som t.ex. kundnöjdhet. Mål kan exempelvis vara:

- Nöjda medlemmar = NMI 75
- Nöjda kunder = NKI 80
- Tillgänglighet kundtjänst via telefon = 90 procent
- E-posthantering = besvara 90 procent inom 8 timmar
- Nöjda med Kundtjänst service, betyg 4 av 5

Federationsoperatören ska kunna genom möten, kundundersökningar och resultatuppföljningar av mätningar också säkerställer att förändringar leder till önskat resultat.

7.3 Ekonomi

7.3.1 Personal

7.3.1.1 Kompetenser/Behov

En tjänsteägare, med både en teknisk och en marknadsmässig kunskap behövs för att hålla ihop tjänsten. Detta är troligen en heltidssysselsättning, åtminstone efter en tid men inledningsvis bedöms det räcka med en halvtid. Utöver det behövs primärt tekniker för att hantera systemen och ev. kundtjänstpersonal.

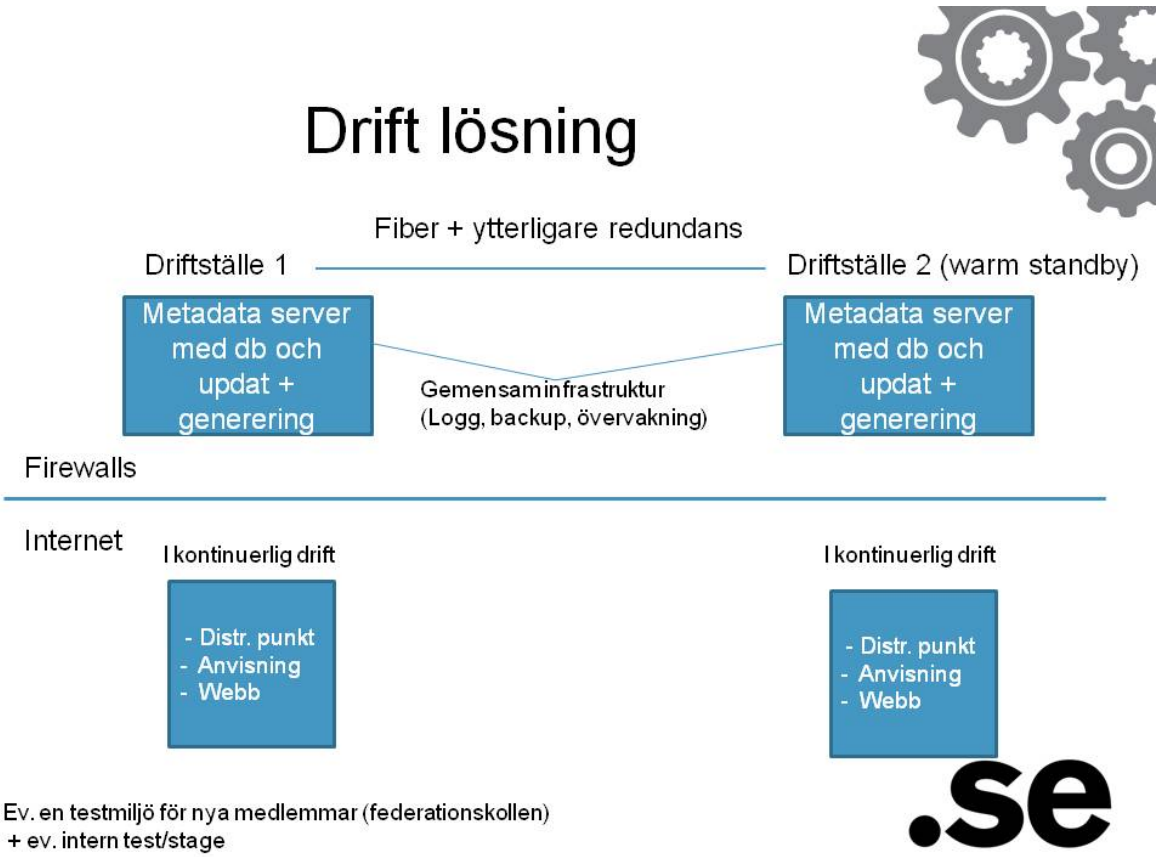
För den tekniska driften behövs troligtvis en 24 timmars beredskap bli nödvändig. Kundtjänst förutsätts kunna hanteras under kontorstid under förutsättning att ”Medlemmarna” i federationen kan nå beredskapen utanför kontorstid.

7.3.2 Debitering

Debitering av medlemskapet i federationen görs i Leveransprocessen.

7.4 Övrigt

7.4.1 Översiktlig driftlösning.



8 Risker

8.1 SWOT-analys för den rekommenderad lösning

Som en del i förstudien har projektgruppen analyserat vilka styrkor (*strengths)*, svagheter (*weaknesses*), möjligheter (*opportunities*) och hot (*threats*) som finns för den föreslagna lösningen i denna rapport.

I uppgiften ingick att identifiera de troliga alternativ som i nuläget finns inom respektive kategori och sedan göra sannolikhetsbedömning och prioritering av dessa.

8.1.1 Styrkor

Bland de styrkor som den föreslagna lösning har, så har följande identifierats som de tre de mest signifikanta:

- Kostnadseffektiv
- Nationell och neutral
- Säker lösning

Den föreslagna lösningen innebär möjligheter till kostnadseffektiv administration och utnyttjande av infrastruktur. Minskade kostnader för administration och infrastruktur vid en federationsanslutning, innebär frigörande av andra resurser och bör därmed kunna ses som ett samhällsekonomiskt bra alternativ.

Federationen innebär *en* nationell lösning och *en* neutral part gällande granskning och kravställning av anslutande parter, vilket förenklar förhållningssättet för anslutande parter.

Generellt sett, så innebär federationen att säkerheten kring hantering av känslig information stärks. Ett enhetligt sätt att hantera t.ex. personuppgifter innebär att den personliga integriteten stärks för individen.

8.1.2 Svagheter

Bland de svagheter som den föreslagna lösning kan ha, så har följande identifierats som de tre de mest signifikanta:

- Stor teknikfokusering
- Lösningen delvis oprövad
- Oklart ägande och oklar finansieringsmodell

Kring den föreslagna lösningen har det lagts ett förhållandevis stort fokus på den tekniska lösningen. Det finns dock fler aspekter, som t.ex. granskningsförfarande, som behöver utredas ytterligare innan en fullt utbyggd federation finns på plats.

Den föreslagna lösning kan anses som en oprövad lösning, då det inte finns riktigt jämförbara befintliga lösningar att förhålla sig till. Den tekniska realiseringen är känd, men de administrativa aspekterna har inte riktigt prövats i jämförbara sammanhang.

I nuläget är det oklart vilken ägarkonstellation federationslösningen kommer att ha och vilken finansieringsmodell som kommer att användas. Detta kan vara en svaghet för snabb etablering av federationen.

8.1.3 Möjligheter

Bland de tänkta möjligheter som finns inom den föreslagna lösning, så har följande identifierats som de tre de mest signifikanta:

- Bättre stöd för mobila tillämpningar
- Kostnadseffektivisering
- Bättre stöd för samverkan och nya relationer

Den föreslagna lösning innebär möjligheter för tjänster som använder andra lösningar än traditionella webbläsare för interaktion att medverka i federationen. Detta borde i förlängningen också innebära att mobila lösningar och tillämpningar, på ett enklare sätt kan medverka i federationen.

Som tidigare nämnts, så innebär federationen en stor möjlighet till kostnadseffektivisering. Kostnader för administration och infrastruktur bör kunna reduceras för anslutande tjänsteleverantörer, både på kort och längre sikt.

Den sedan tidigare nämnda enhetligheten inom förslagna lösningen, ger naturligtvis också möjligheter till ett vidgat samarbete inom och mellan befintliga konstellationer inom eHälsa.

8.1.4 Hot

Bland de möjliga hot som den föreslagna lösning kan ha, så har följande identifierats som de tre de mest signifikanta:

- Revirtänk
- E-legitimationsnämndens arbete försenas
- Federationen förblir okänd

Idag finns ett flertal fungerande ”tvåpartsfederation” på marknaden där investering gjorts under både längre och kortare tidsperspektiv. Dessa ”tvåpartsfederationer” kan möjligen ha svårt att motivera nya investeringar för att ingå i federationen, i alla fall på kort sikt, utan fortsätter att använda och förvalta sina befintliga lösningar.

Detta federationsinitiativ är på inget sätt en isolerad aktivitet. Hänsyn har tagits till liknande pågående initiativ och därmed finns ett beroende till och från andra aktiviteter. Skulle t.ex. E-legitimationsnämndens arbete försenas eller förändra inriktning, kan detta påverka och bromsa en etablering av federationen.

För att nå de önskade effekterna gällande t.ex. kostnadseffektivisering och ökad samverkan, krävs det att federationen hittar medlemmar som är beredda att ansluta utnyttja av federationen. Därför är det av väsentlighet att existensen av detta initiativ kommuniceras till alla tänkbara intressenter.

8.2 Projektrisker

Riskanalys för nästa fas i projektet genomförs efter att detaljerat Projektdirektiv tagits fram och nästa fas i projektet startar.

9 Underlag till projektdirektiv – utformning & implementation

Nedan listas förslag till huvudsakliga aktiviteter till projektdirektiv för nästa steg – utformning och implementation av federationslösningen.

1. Framtagande av kommunikationsplan omfattande aktiviteter som:

- Webbplats
- Informationsmaterial (informationsblad, presentationer, ev. profilmaterial etc.)
- Varumärkesarbete
- Seminarium
- Lansering i media

2. Road map för anslutning av e-tjänster tas fram genom överenskommelser med ett antal centrala organisationer inom eHälsa.

3. Utformning av tillitsramverk

- Baserat på/eller i direkt samverkan med e-legitimationsnämnden som kommer att lämna förslag kring tillitsramverk (helt nyligen aviserats till oktober 2012) och de första e-tjänster där överenskommelse om anslutning träffas

4. Teknisk etablering av en federation baserat på föreslagna kravnivåer i avsnitt 6.2.
- Initialt kan med kort varsel en teknisk miljö användas för tester och verifiering av SAML-förmågor i olika tillämpningar
- När tillitsramverket finns på plats kan en pilotmiljö etableras med avsikt att försörja de e-tjänster som initialt ansluts till federationen.

5. Formerna för ägarskap och finansiering klarläggs baserat på principerna att:
- Federationen skall förvaltas och vidareutvecklas utan vinstintressen
- Ägarskapet av federationen skall baseras på en bred representation från organisationer inom vård- och omsorgssektorn. Förslaget är att formerna för ägarskap och finansiering klarläggs genom en särkskild aktivitet omgående i nästa steg.

6. Former för det fortsatta arbetet:

- Arbetet med att realisera ovanstående aktiviteter föreslås att bedrivas i projektform fram till att ägarfrågan är beslutad och ett antal e-tjänster implementerats inom federationen, dvs. pilotprojekt genomfört och överlämnat till förvaltning

10 Referenser och definitioner

10.1 Referenser

Personer och dokument som har mer info.

Ref.	Dokumentnamn, beteckning och namn	Utgåveid, datum
1	Begreppsmodellvy, Begreppsmodeller 110220.pdf	Version 1.0, 2011-02-18
2	RIV-SPECIFIKATION, PDLiP RIV 10 specifikation 110926.pdf	Version 1.0, 2011-09-23
3	PDL Infomodell, PDLiP VDIM 110328.pdf	2011-03-28
4	Electronic Authentication Guideline, NIST Special Publication 800-63-1	800-63-1, December 2011
5	Identity Assurance Framework:Service Assessment Criteria, Kantara IAF-1400-Service Assessment Criteria.doc	Version 2.0, 2010-04-24
6	STORK D2.1 - Framework Mapping of Technical/Organisational Issues to a Quality Scheme	Version 1.5, 2008-10-13
7	ISO/IEC 29115	Draft
8	SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, FIPS PUB 140-2.pdf	2001-05-25
9	Authentication Context for the OASIS Security Assertion Markup Language (SAML), saml-authn-context-2.0-os	Version 2.0, 2005-03-15

10.2 Definitioner

Ord/förkortning/akronym	Förklaring
Anvisningstjänsten	Det tekniska och administrativa stöd som Federationsoperatören tillhandahåller för att Användare ska kunna välja sin intygsutfärdare. *Engelska; Discovery Service eller WAYF (Where Are You From).*
Användare	Den fysiska person som har tilldelats en Identitet i *Federationen*.
Användarorganisation	Organisation med Användare som är ansluten till federationen. Användarorganisation kan vara en statlig myndighet, landsting, kommun eller annan juridisk person eller enskild näringsidkare som bedriver vård och omsorg i Sverige. Användarorganisationen ansvarar för att dess Användares har giltiga elektroniska identiteter och Attribut.

Attributsutfärdare	Den som utfärdar attributsintyg inom *Federationen*. Engelska: Attribute authority (AA)
Biljett	Se Intyg
e-tjänsteleverantör	Den som tillhandahåller e-tjänster inom *Federationen*. Engelska: Service Provider (SP)
Federationsoperatör	Den som sköter *Federationen*s löpande verksamhet och förvaltar Regelverket och Gemensamma funktioner för *Federationen* på uppdrag av Styrgruppen
Identitet	En unik beteckning för en Användare i *Federationen*.
Identitetsutfärdare	Den organisation som tilldelar Användare identiteter och utfärdar Identitetsintyg inom *Federationen*. Engelska: Identity Providers (IdP)
Intyg	Ett av en intygsutfärdare utställt intyg i elektronisk form med uppgifter om en Användares identitet och/eller attribut. Engelska; Assertion.
Medlem	Medlem i *Federationen* kan vara Användarorganisation och e-tjänsteleverantör.
Metadata	Den tekniska informationen om *Federationen*:s Medlemmar.
Metadataregistret	Det för *Federationen* gemensamma register med Medlemmarnas Metadata.
Regelverket för *Federationen*	Det regelverk som styr samverkan för parterna i *Federationen*.
Federationen	Ett samarbete mellan Användarorganisationer, verksamma som Identitets- och/eller Attributsutfärdare, samt av e-tjänsteleverantörer.
Styrgruppen	Styrgruppen för *Federationen* ansvarar för den strategiska inriktningen och för övergripande policyfrågor för *Federationen* samt utövar tillsyn över Federationsoperatörens förvaltningsarbete.
Tillitsnivå (LoA)	Grad av tillit till en identitet som kan tillmätas enligt ett givet Tillitsramverk. *Engelska: Levels of assurance (LoA)*

Tillitsramverk	Den del av Regelverket för *Federationen* som behandlar tillit de i federationen utfärdade identitets- och attributsintygen. Engelska: Trust Framework:
Tjänsteleverantör	Se e-tjänsteleverantör

11 Projektet

11.1 Uppdragsgivare och uppdragstagare

Beställare/Projektägare:

.....

<Nnnn Nnnn>

Projektledare:

.....

<Nnnn Nnnn>