JUNI 2021

Utredningsrapport

Analys av potentiella lösningar för anslutning av tredjepartsprodukter

Förord

Den här rapporten är resultatet av en utredning som genomfördes på Inera hösten 2020 och våren 2021. Tre rapporter från utredningen om möjligheterna till anslutning av tredjepartsprodukter för invånare till Ineras infrastruktur och tjänster, daterade den 21 juni 2021, har nu publicerats:

- Huvudrapport anslutning av tredjepartsprodukter
- Kortversion anslutning av tredjepartsprodukter, samt
- Analys av potentiella lösningar för anslutning av tredjepartsprodukter

Det är ett stort och komplext område och utredningens resultat kommer behöva diskuteras vidare, framför allt med regionerna. Troligtvis behövs en gemensam satsning för att få den infrastruktur och regelverk på plats som kan möjliggöra anslutning av tredjepartsprodukter för invånare till Ineras tjänster och infrastruktur.

Troligtvis behövs även mer dialog med fler intressenter för att bottna alla perspektiv och hitta vägar framåt. Om det finns inspel från Ineras styrelse, regioner, kommuner, leverantörer eller andra intressenter på områden som behöver fördjupas eller om det finns förslag på hur konkreta behov kan lösas och vägen framåt kan se ut, tas det tacksamt emot.

Ett sätt att komma vidare skulle kunna vara att fokusera på ett konkret behov, förstå det spelrum som finns för att lösa behovet, och sedan driva frågan vidare i nära samverkan med en eller ett fåtal pilotregioner tillsammans med berörda leverantörer.

Sara Meunier

CTO och Analyschef

Innehåll

1. Inledning

Detta dokument analyserar potentiella lösningar och lösningsmönster som svar på de behov som lyfts i huvudrapport för uppdraget ”Utredning om möjligheterna till anslutning av tredjepartsprodukter för invånare till Ineras tjänster och infrastruktur”.

Analyserna kan i vissa fall ge svar på om en potentiell lösning går att använda för att ansluta tredjepartsprodukter, men i andra fall kan analysen endast peka ut de områden där mer djupgående utredningar behöver göras innan en färdig lösning kan presenteras.

De potentiella lösningarna utgår från den infrastruktur som erbjuds av Inera i nuläget för att ansluta tjänsteproducenter och tjänstekonsumenter samt ger förslag på områden där infrastrukturen behöver förändras eller utökas för att kunna erbjuda anslutning av tredjepartsprodukter riktade direkt till patienter.

Potentiella lösningar baserade på den framtida samverkansarkitektur som Inera håller på att utveckla, och som ännu inte är realiserade, analyseras *inte* i detta dokument.

De lösningar och lösningsmönster som presenteras ska därför inte betraktas som färdiga förslag utan endast som en analys av mönster och lösningar som används inom Inera idag och de konsekvenser som blir följden om de tillämpas för anslutning av tredjepartsprodukter riktade till patienter.

Alla lösningar och lösningsmönster beskrivs under respektive behovsscenario som de svarar mot. Alla behovsscenarion är hämtade från huvudrapporten.

1.1 Förutsättningar och antaganden för alla lösningsmönster

Alla lösningsmönster utgår från följande förutsättningar:

- Patientapplikationen kan vara en mobilapplikation eller en webbapplikation.
- Patientapplikationen består av två delar, en klient och en server
- Patientapplikationens serverdel kan vara fristående eller en del av ett verksamhetssystem.
- Patientapplikationen är upphandlad av den vårdgivare som erbjuder applikationen till sina patienter

Alla flödespilar i diagrammen utgår från den som initierar anropet, vilket kan skilja sig från riktningen för det huvudsakliga informationsflödet.

2. Behovsscenario ”Hämta patientinformation”

2.1 Generell beskrivning

En vårdgivare erbjuder en **applikation för sina patienter för att kunna visa patientens information** som stöd i behandling hos vårdgivare. Applikationen med patientens vy erbjuds antingen genom att vårdgivaren har upphandlat en applikation av extern leverantör eller genom

vårdgivarens journalsystemleverantör som har en patientingång där funktioner möjliggör visning av patientinformation. Den huvudsakliga digitala kommunikationen i behandlingen sker via lokal integration till vårdgivarens system.

För att applikationen ska kunna ge avsett stöd behöver den få tillgång till **vissa delar av patientens vårdrelaterad dokumentation,** såsom journalinformation eller annan information om patienten som exempelvis högkostnadsinformation som finnas förvarad hos andra vårdgivare och deras upphandlade produkter. Denna informationen vill vårdgivaren tillgängliggöra via appen för invånare genom **Ineras infrastruktur**.

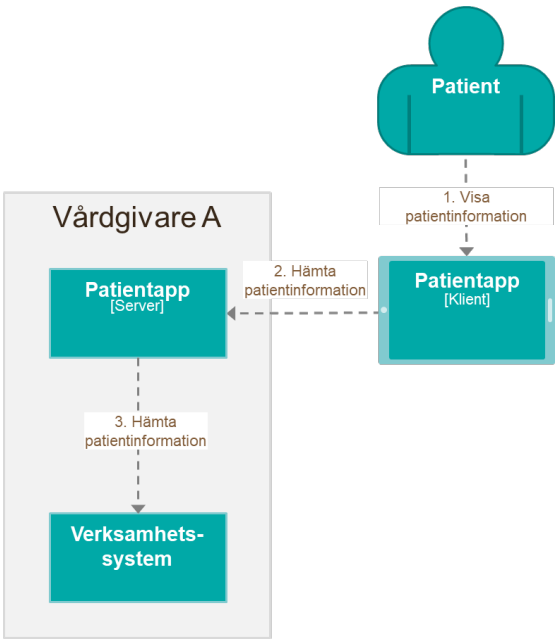
2.2 Lösningsmönster ”Hämta lokal patientinformation”

2.2.1 Behov

En vårdgivare erbjuder en **applikation för sina patienter för att kunna visa patientens information** som stöd i behandling hos vårdgivare. Den huvudsakliga digitala kommunikationen i behandlingen sker via lokal integration till vårdgivarens system.

2.2.2 Lösningsbeskrivning

Vårdgivaren nyttjar i detta scenario inte Ineras infrastruktur varför detta lösningsmönster inte beskrivs närmare här. Lösningsmönstret kan kombineras med olika stödtjänster från Inera.



2.3 Lösningsmönster ”Hämta samlad patientinformation 1a”

2.3.1 Behov

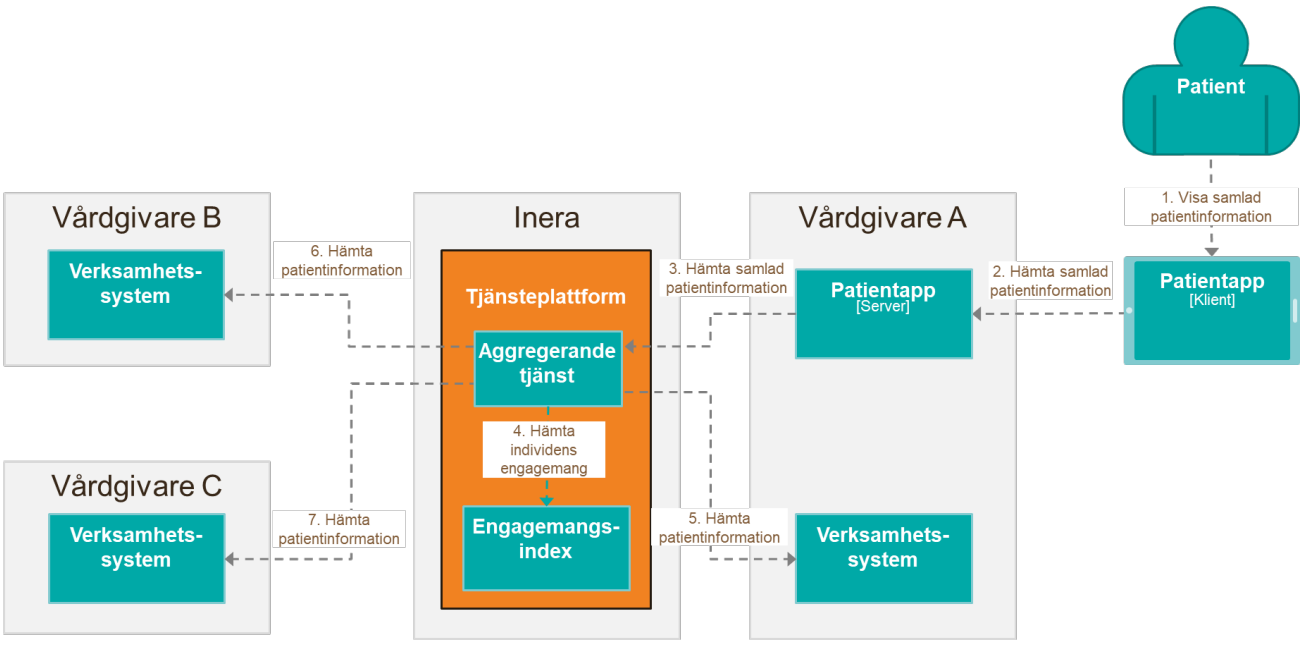
En vårdgivare erbjuder en **applikation för sina patienter för att kunna visa patientens information** som stöd i behandling hos vårdgivare.

För att applikationen ska kunna ge avsett stöd behöver den få tillgång till **vissa delar av patientens vårdrelaterad dokumentation,** såsom journalinformation eller annan information om patienten som exempelvis högkostnadsinformation som finnas förvarad hos andra vårdgivare och deras upphandlade produkter. Denna informationen vill vårdgivaren tillgängliggöra via appen för invånare genom **Ineras infrastruktur**.

2.3.2 Lösningsbeskrivning

Använd en eller flera aggregerande tjänster. En aggregerande tjänst är en tjänst i den nationella tjänsteplattformen (NTjP) som för en viss individ sammanställer en nationell vy av den informationen som specificeras i det valda tjänstekontraktet.

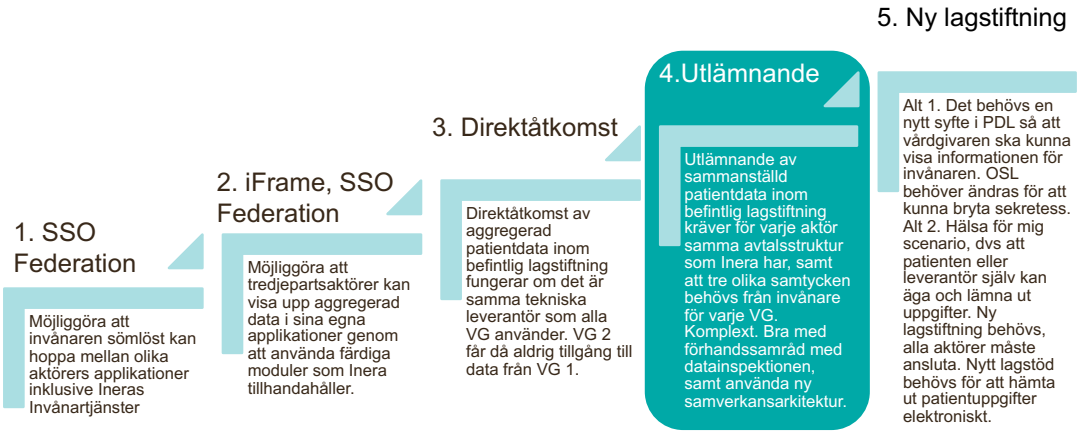
En aggregerande tjänst är beroende av stödtjänsten Engagemangsindex som håller uppdaterad information över vilka informationsägare som har information av en viss typ gällande en given invånare.



2.3.3 Trappstegsmodell

Trappstegsmodellen beskrivs i huvudrapporten och används för att rangordna de olika lösningsmönstren utifrån svårighetsgrad där fem anger den högsta svårighetsgraden. Detta

mönster har placerats på trappa fyra:



2.3.4 Förutsättningar

För att mönstret ska kunna tillämpas krävs att följande förutsättningar är uppfyllda:

- Det finns en aggregerande tjänst för den efterfrågade informationsmängden
- Tillräckligt många vårdgivare är anslutna som producenter till det aktuella tjänstekontraktet för att aggregeringen ska vara meningsfull för användaren
- Varje tjänsteproducent tillåter vårdgivarens tjänstekonsument åtkomst till informationen
- Tjänstekontrakten och tjänsteproducenterna stödjer automatiserad menprövning.
- Tjänstekonsumenten filtrerar bort poster som inte ska visas för patienten
- Det finns ett överenskommet, gemensamt regelverk som stödjer tjänstekonsumentens avsedda användning

2.3.5 Tillämpning

Mönstret är användbart när en tjänstekonsument efterfrågar en nationell vy av patientens information och har behov av att bearbeta informationen för att skapa ett skräddarsytt grafiskt användargränssnitt för användarna.

2.3.6 Kända användningsområden

Idag används detta mönster främst inom sammanhållen journalföring med applikationen NPÖ, som riktar sig till vårdmedarbetare, samt för att ge invånarna möjlighet att ta del av sin journalinformation genom tjänsten Journalen som finns på 1177.se.

Utveckling av en aggregerande tjänst för högkostnadsskydd sker under 2020.

Följande tjänstedomäner använder detta mönster:

- Aktivitetshantering
- Basuppgifter tillstånd (observationer och mätvärden)
- Ordinationsutfall (exempelvis ordination, förskrivningar och vaccinationer)

- Remisstatus
- Resurssamordning (vårdkontakter, vårdplaner och användande av vårdtjänster)
- Tillståndsbeskrivning (patientens hälsotillstånd)
- Utfall av aktiviteter (exempelvis EKG, laboratoriesvar och bilddiagnostik)

2.3.7 Varianter

Lösningsmönstret är i första hand tänkt att användas för direktåtkomst, men kan även användas då de samlade patientuppgifterna behöver lagras hos vårdgivaren, i ett eget utrymmer för patienten eller i patientapplikationen. **De juridiska konsekvenserna blir olika beroende på vilken variant som väljs och måste beaktas vid val av implementation.** De juridiska konsekvenserna beskrivs i en bilaga till huvudrapporten

2.3.8 Konsekvenser – Juridik

De juridiska konsekvenserna beskrivs i en bilaga till huvudrapporten. Här ges en kort sammanfattning:

Juridisk lösning 1

En individ kan hämta ut patientinformation eller administrativ information från en vårdgivare (privat eller offentlig) enligt Patientdatalagen (PDL). Då man ska hämta ut informationen från Vårdgivare B (eller C) med hjälp av Vårdgivare A krävs flera samtycken från invånaren:

1. Samtycke för att bryta sekretess hos Vårdgivare B (eller C)
2. Samtycke för att föra över uppgifterna från Vårdgivare B (eller C) till Vårdgivare A och därefter till individen
3. Samtycke för att Vårdgivare A ska få lov att behandla uppgifterna

Notera att informationen inte ska innehålla uppgifter om andra än invånaren. Det krävs även personuppgiftsbiträdesavtal mellan Vårdgivare A och aktörer som tillhandahåller de tekniska lösningarna i enlighet med dataskyddsförordningens bestämmelser.

Juridisk lösning 2

Lösningen bygger på att Vårdgivare A agerar som personuppgiftsbiträde åt Vårdgivare B (eller C) samt att Inera agerar som underbiträde. I ett sådant scenario övertar inte Vårdgivare A personuppgiftsanvaret och invånaren begär därmed utlämnande av uppgifter från Vårdgivare B (eller C) med stöd av 5 kap Patientdatalagen (PDL). Problemet med denna tolkning är att PDL enligt 2 kap 6 § stadgar ett personuppgiftsansvar för vårdgivare.

Det är även troligt att behandlingen hos Vårdgivare A strider mot den grundläggande principen om uppgiftsminimering. En kedja med flera parter, avtal och ”databaser” som upprättas med syfte att individen ska få tillgång till sin information på ett ”nytt” tillvägagångssätt får anses vara i strid med principen om uppgiftsminimering.

Juridisk lösning 3

Denna lösning är endast på idéstadiet. Lösningen bygger på att enskilds direktåtkomst borde kunna tillämpas om vårdgivarna har samma leverantör av patientapplikationen.

Patientapplikationen måste då tydligt skilja på informationsmängder som kommer från olika vårdgivare.

För att lösningen ska kunna hämta upp och visa patientinformation från alla vårdgivare så måste alla vårdgivare upphandla alla patientapplikationer som används av någon vårdgivare, oavsett om de själva använder patientapplikationen. Detta styrs bl.a. av lagen om offentlig upphandling.

Det är inte klarlagt om någon av ovanstående juridiska lösningar är praktiskt framkomliga och det är därför oklart om lösningsmönstret går att använda utifrån ett juridiskt perspektiv.

2.3.9 Konsekvenser – Avtal

2.3.10 Konsekvenser – IT-säkerhet

Konsekvenser gällande IT-säkerhet beskrivs översiktligt i huvudrapportens kapitel om säkerhet, test och kvalitetssäkring.

Enligt huvudrapporten behövs det utökade säkerhetslösningar i infrastrukturen för att minska skadan vid ett dataintrång i en tredjepartsprodukt där angriparen får kontroll över produkten och kan styra informationsflödet. Dessa begränsningar kan implementeras på flera olika nivåer. Här beskrivs kortfattat begränsningar som redan är implementerade samt förslag till mekanismer som eventuellt kan implementeras i Ineras infrastruktur. Förslagen kräver ytterligare utredningar.

Begränsa de informationstyper som tredjepartsprodukten kan hämta

All kommunikation som sker via tjänstekontrakt begränsas per automatik till de informationstyper som tjänstekontraktet definierar.

Begränsa vilka individer som tredjepartsprodukten kan hämta information om

Begränsa till individer som vårdgivaren har patientrelation med

En extern mekanism liknande TGP (tillgänglig patient) som idag används för att säkerställa att en vårdgivare endast kan hämta patientuppgifter för patienter som vårdgivaren har en patientrelation till skulle kunna införas. Mekanismen skulle i det här fallet kontrollera att vårdgivaren som har upphandlat patientapplikationen har en patientrelation till den patient vars information efterfrågas. Skadan vid ett intrång begränsas därmed till att omfatta de patienter som den aktuella vårdgivaren har en patientrelation till.

Begränsa till individer som har gett samtycke

Om det krävs samtycke för att hämta informationen så bör mekanismen utformas så att den även kan användas för att begränsa skadan vid intrång.

Begränsa till den/de användare som tillgång till en unik instans av en tredjepartsprodukt

Skadan vid ett eventuellt intrång kan minimeras om det går att unikt identifiera en applikation och knyta varje patientapplikation till en specifik individ. I detta scenario tillåts en patientapplikation endast att hämta information om en specifik patient (eller åtminstone en i förväg bestämd begränsad mängd patienter) som man via ett externt register har knutit till en

eller flera patientapplikationer. Förfrågningar om information rörande andra patienter från den registrerade applikationen godkänns inte.

Förslaget bygger på att det går att med relativt god precision identifiera en unik instans av en webbapplikation eller mobilapplikation. Detta är en teknik som används av t.ex. Facebook och Google för att öka säkerheten vid inloggning till deras tjänster. Om man byter dator, webbläsare eller geografisk plats så finns det en god chans att Facebook eller Google skickar ett mejl och upplyser om att en misstänkt inloggning har gjort. Tekniken är inte beroende av cookies utan bygger på attribut som alla webbläsare och mobilapplikationer skickar med i ett anrop till en server. Genom att nyttja en liknande teknik och knyta patientapplikationernas unika identiteter till en specifik individ kan man avsevärt minska riskerna vid ett intrång.

Lösningen kräver utökning av Ineras infrastruktur samt införande av en ny http-header som innehåller den unika identifieraren. Struktur och format för den unika identifieraren måste standardiseras av Inera och implementeras av tredjepartsprodukten. Tekniken för identifiering går ofta under benämningen ”device fingerprint”, [11].

Nyttja en säkerhetsinfrastruktur som bygger på identitetsintyg och åtkomstintyg istället för organisatorisk tillit

Detta alternativ kräver att hela säkerhetsinfrastrukturen för Inera och regionerna förändras. Förändringen skulle dock minska risken vid intrång eftersom det inte räcker att få kontroll över en applikation. Varje anrop från applikationen måste åtföljas av ett signerat identitetsintyg som kan användas för att hämta ett åtkomstintyg som i sin tur används för att hämta information från andra personuppgiftsansvarigas källsystem.

2.3.11 Personuppgiftsansvarigs behov av att kontrollera sin information

Behörighetskontroll av tjänstekonsumenter

Konfigurering och upprätthållande av den behörighetskontroll som bestämmer vilken tjänstekonsument som får anropa en viss logisk adress görs vid verksamhetsbaserad adressering i tjänsteplattformen. Vid källsystemsbaserad adressering, vilket är den vanligaste adresseringsmodellen när tjänstedomäner använder aggregerade tjänster, så görs åtkomstkontrollen i regel i ”anslutningsfilter” som tjänsteproducenterna själva konfigurerar och upprätthåller. Användning av den centrala behörighetsmekanism som finns i Ineras tjänsteplattform är frivillig vid källsystemsbaserad adressering eftersom den endast kan kontrollera behörighet på källsystemsnivå och inte för enskilda vårdenheter.

Den åtkomstkontroll som görs i dessa ”anslutningsfilter” benämns ibland ”vitlistning” eftersom filtrering görs på godkända tjänstekonsumenters HSA-Id. Med tjänstekonsument avses här den ursprungliga tjänstekonsumenten, t.ex. HSA-Id för NPÖ eller Journalen. Skälet till att ”anslutningsfilter” används är att vårdgivaren är personuppgiftsansvarig och har enligt PDL ansvar för vilka som får åtkomst till informationen.

Detta innebär att tjänsteproducenten via sitt ”anslutningsfilter” kan neka åtkomst till tjänstekonsumenter som informationsägaren inte har godkänt. Det kan därför vara en lång process att få en ny tjänstekonsument godkänd hos alla tjänsteproducenter. Detta är framför allt ett hinder i de fall tjänstekonsumenten inte förvaltas av Inera.

Dagens manuella process som används för att konfigurera de filter hos tjänsteproducenterna som upprätthåller kontrollen av vilka tjänstekonsumenter som är godkända skulle behöva automatiseras och kopplas till en överenskommen process för att godkänna och certifiera tjänstekonsumenter, oavsett om det är tredjepartsprodukter eller tjänster som förvaltas av Inera.

Inera har tidigare försökt att adressera detta problem genom att införa en tjänst som tillhandahåller en lista av godkända tjänstekonsumenter som tjänsteproducenterna kan ladda ner och använda för att automatiskt uppdatera sina vitlistor. En handlingsplan kallad ”Handlingsplan Nationella vitlistan för Sammanhållen Journalföring v 2.0” togs fram i början av 2019, men intresset för en nationell vitlista har varit lågt bland aktörerna och initiativet har inte resulterat i någon faktisk realisering.

Vid införande av en certifieringsprocess som även omfattar appar bör man tänka på att både apparna och deras operativsystem uppdateras relativt ofta. Detta kan kräva frekventa, nya certifieringar vilket ställer stora krav både på leverantörerna och den certifierande organisationen.

Automatiserad menprövning

Automatiserad menprövning görs genom att tjänstekontrakten innehåller en flagga kallad ApprovedForPatient som tjänsteproducenter kan använda för att ange om en journalpost ska visas för en patient. Alla regioner använder inte denna flagga utan vissa regioner använder istället en filterfunktion i 1177 Journal som kan filtrera bort viss information innan den visas för patienten. Filterfunktion består av tre olika filter och är mer grovkornig än ovan nämnda flagga. Tredjepartsprodukter behöver antingen implementera motsvarande filterfunktion eller så måste alla regioner använda flaggan för automatiserad menprövning

2.3.12 Individens behov av att kontrollera sin information

Individen vill hämta sin egen information och behöver i det enklast fallet inte några samtycken för att kontrollera detta. Beroende på hur implementation görs rent tekniskt kan det dock krävas samtycken. Detta gäller specifikt i det fall att patientapplikationen tillhandahålls av en vårdgivare och patienten vill hämta information från en annan vårdgivare. Samtyckestjänsten hos Inera hanterar i dagsläget endast samtycken för Sammanhållen Journalföring.

Ett annat scenario är när individen har behov av ett ombud. Ineras ombudsfunktioner används idag endast av Journalen och behöver utökas för att även stödja tredjepartsprodukter.

2.3.13 Styrkor och svagheter

Övriga styrkor och svagheter som inte redan har beskrivits som en konsekvens:

Styrkor:

- Enkelt att använda för en tjänstekonsument. En konsument får ett svar som innehåller samlad patientinformation från alla tjänsteproducenter som har information om patienten.

Svagheter:

- Alla tjänsteproducenter måste uppdatera engagemangsindex med förändring av patientinformation

- Tjänstekonsumenten får inte tillbaka något svar förrän den aggregerande tjänsten har fått svar från alla tjänsteproducenter eller om time-out tiden har uppnåtts (27 sekunder för närvarande) varvid den aggregerande tjänsten returnerar ett svar innehållande information från de tjänsteproducenter som har svarat inom detta tidsintervall.

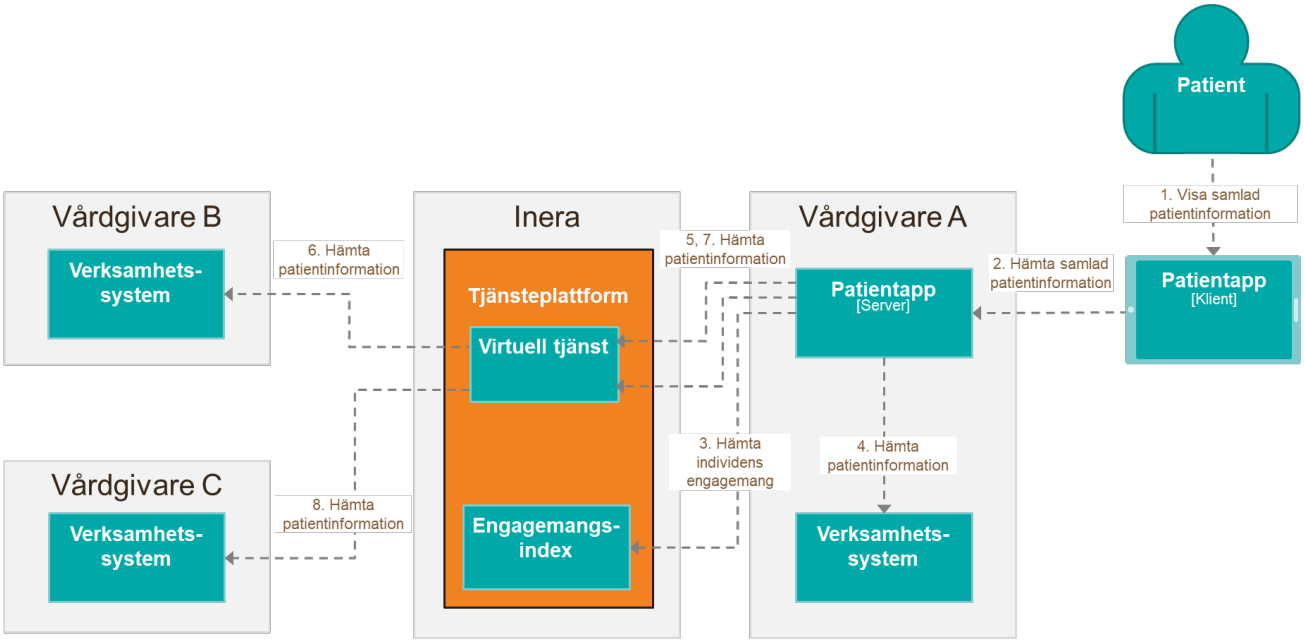
2.4 Lösningsmönster ”Hämta samlad patientinformation 1b”

2.4.1 Behov

Samma som ”Hämta samlad patientinformation 1a”

2.4.2 Lösningsbeskrivning

Låt tjänstekonsumenten använda engagemangsindex. Tjänstekonsumenten anropar engagemangsindex och får på så vis uppdaterad information över vilka informationsägare som har information av en viss typ gällande en given invånare. Med hjälp av informationen i engagemangsindex kan tjänstekonsumenten därefter anropa de aktuella tjänsteproducenterna och sammanställa en nationell vy av information som specificeras i det valda tjänstekontraktet.



2.4.3 Trappstegsmodell

Trappstegsmodellen beskrivs i huvudrapporten och används för att rangordna de olika lösningsmönstren utifrån svårighetsgrad där fem anger den högsta svårighetsgraden. Detta mönster har placerats på trappa fyra:

2.4.4 Förutsättningar

- Samma som ”Hämta samlad patientinformation 1a”
- Mönstret förutsätter även att tjänstekonsumenter ges åtkomst till engagemangsindex, vilket för närvarande inte är tillåtet annat än för aggregerande tjänster på Tjänsteplattformen. Utredningen ”AOR-1915 – Konsumentåtkomst till engagemangsindex” [1] bereder detta ärende.

2.4.5 Tillämpning

Samma som ”Hämta samlad patientinformation 1a”

2.4.6 Kända användningsområden

Detta lösningsmönster används inte idag

2.4.7 Varianter

Samma som ”Hämta samlad patientinformation 1a”

2.4.8 Konsekvenser – Juridik

Samma som ”Hämta samlad patientinformation 1a”

2.4.9 Konsekvenser – Avtal

Samma som ”Hämta samlad patientinformation 1a”

2.4.10 Konsekvenser – IT-säkerhet

Samma som ”Hämta samlad patientinformation 1a”

2.4.11 Personuppgiftsansvarigs behov av att kontrollera sin information

Samma som ”Hämta samlad patientinformation 1a”

2.4.12 Individens behov av att kontrollera sin information

Samma som ”Hämta samlad patientinformation 1a”

2.4.13 Styrkor och svagheter

Övriga styrkor och svagheter som inte redan har beskrivits som en konsekvens:

Styrkor:

- Jämfört med lösningsmönster 1a så binds inte centrala resurser upp för att invänta svar från alla producenter och aggregera ihop ett svar
- Tjänstekonsumenten kan själva bestämma hur man vill anropa tjänsteproducenterna, hantera svaren samt eventuella fel.
- Det krävs ingen centralt driftsatt aggregerande tjänst

Svagheter:

- Alla tjänsteproducenter måste uppdatera engagemangsindex med förändring av patientinformation

2.5 Lösningsmönster ”Hämta samlad patientinformation 1c”

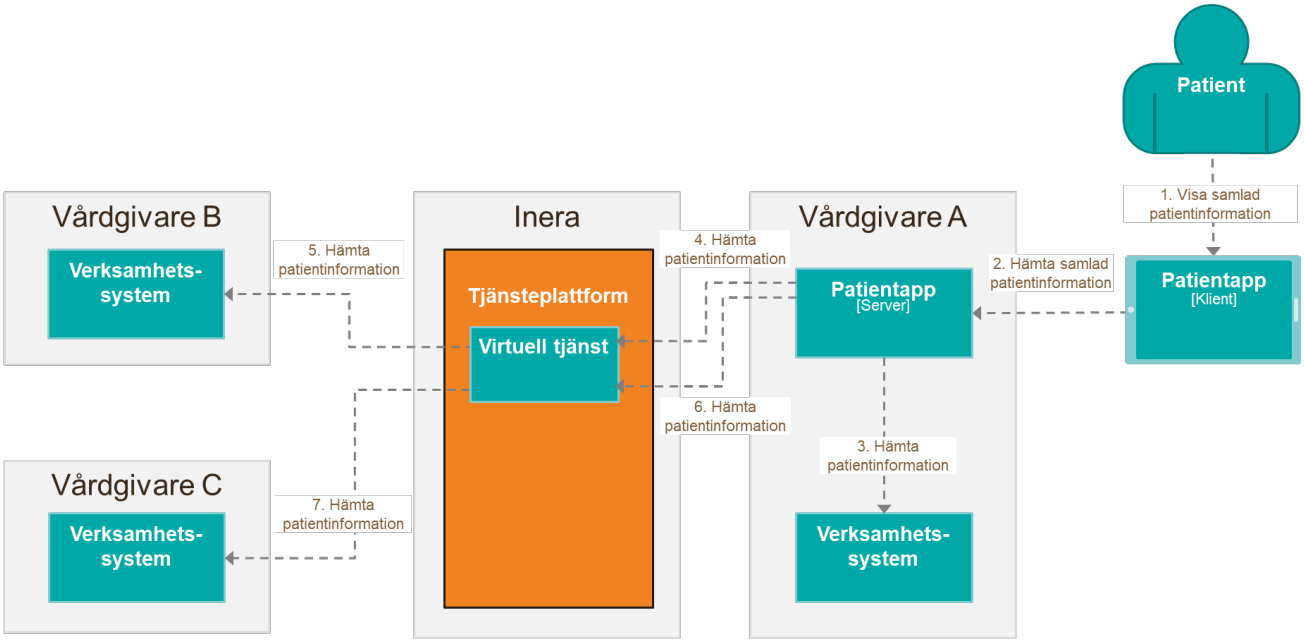
2.5.1 Behov

En vårdgivare erbjuder en applikation för sina patienter för att kunna visa patientens information som stöd i behandling hos vårdgivare. Applikationen ska även kunna visa patientens information från andra vårdgivare än den som är ansvarig för behandlingen. Det förväntas att patienten vet vilka mottagningar som är aktuella att hämta information från.

2.5.2 Lösningsbeskrivning

Lösningen kräver inga aggregerande tjänster men kan behöva stödtjänster där användaren kan välja vilka mottagningar som information ska hämtas ifrån. Stödtjänsterna visas inte i nedanstående lösningsmönster.

Lösningsmönstret kan även användas i de fall där varje region tillhandahåller en regional tjänst, exempel på detta är listningsdomänen.



2.5.3 Trappstegsmodell

Trappstegsmodellen beskrivs i huvudrapporten och används för att rangordna de olika lösningsmönstren utifrån svårighetsgrad där fem anger den högsta svårighetsgraden. Detta mönster har placerats på trappa fyra:

2.5.4 Förutsättningar

För att mönstret ska kunna tillämpas krävs att följande förutsättningar är uppfyllda:

- Det kan förutsättas att patienten vet eller kan välja ut från en lista vilka mottagningar som information ska hämtas ifrån eller att det finns en tjänst för varje region.
- Varje tjänsteproducent tillåter vårdgivarens tjänstekonsument åtkomst till informationen
- Beroende på typen av information som överförs så kan det finnas krav på att tjänstekontrakten och tjänsteproducenterna stödjer automatiserad menprövning, vilket i det här fallet innebär att varje överförd post har en markering som anger om posten är tillåten att visas för patienten.
- I fallet med automatiserad menprövning måste tjänstekonsumenten filtrerar bort poster som inte ska visas för patienten
- Det finns ett överenskommet, gemensamt regelverk som stödjer tjänstekonsumentens avsedda användning

2.5.5 Tillämpning

Mönstret är användbart när en tjänstekonsument efterfrågar en nationell vy av patientens information och har behov av att skapa ett skräddarsytt grafiskt användargränssnitt för användarna samt att patienten kan förutsättas veta vilka mottagningar informationen ska hämtas ifrån eller att det finns en tjänst för varje region.

2.5.6 Kända användningsområden

Tidbokningstjänsten hos 1177 använder detta mönster i kombination med att användaren har möjlighet att välja vilka mottagningars tider som ska hämtas.

Listningstjänsten hos 1177 använder detta mönster genom att hämta en patients listningar från aktuell regions listningstjänst.

2.5.7 Varianter

2.5.8 Konsekvenser – Juridik

Samma som ”Hämta samlad patientinformation 1a”

2.5.9 Konsekvenser – Avtal

Samma som ”Hämta samlad patientinformation 1a”

2.5.10 Konsekvenser – IT-säkerhet

Informationen som finns i motsvarande kapitel för mönstret ”Hämta samlad patientinformation 1a” är i stora drag relevant även för detta mönster, men exakt vilka av förslagen som är tillämpbara beror på vilken tjänstedomän som mönstret tillämpas inom.

2.5.11 Personuppgiftsansvarigs behov av att kontrollera sin information

Informationen som finns i motsvarande kapitel för mönstret ”Hämta samlad patientinformation 1a” är relevant även för detta mönster, men de tjänster som är aktuella för detta mönster använder i regel verksamhetsbaserad adressering vilket medför att behörighetskontrollen görs i

tjänsteplattformen och det finns inte samma behov hos tjänsteproducenterna att använda eller konfigurera ”anslutningsfilter”.

2.5.12 Individens behov av att kontrollera sin information

Samma som ”Hämta samlad patientinformation 1a”

2.5.13 Styrkor och svagheter

Övriga styrkor och svagheter som inte redan har beskrivits som en konsekvens:

Styrkor:

- Inget behov av en aggregerad tjänst

Svagheter:

- Förutsätter att patienten vet eller kan välja ut från en lista vilka mottagningar som information ska hämtas ifrån eller att det finns en tjänst för varje region.

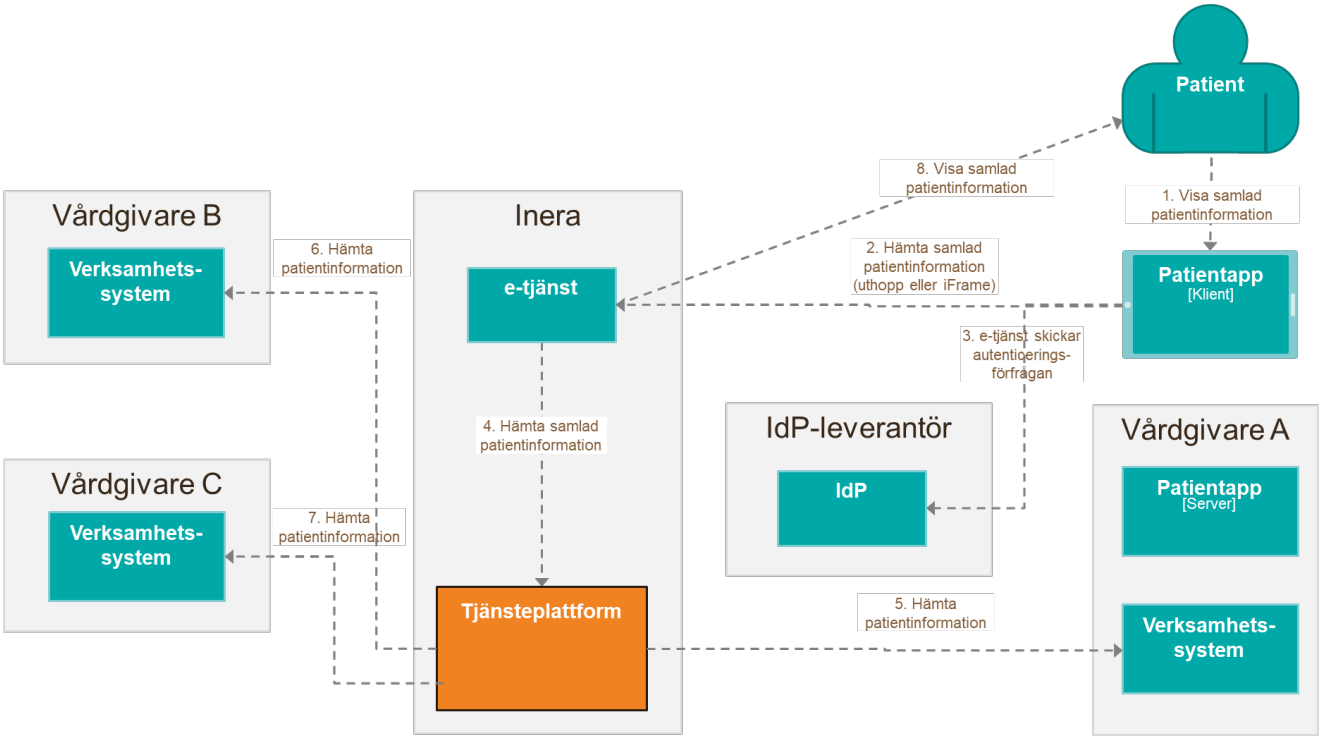
2.6 Lösningsmönster ”Hämta samlad patientinformation 1d”

2.6.1 Behov

En vårdgivare erbjuder en applikation för sina patienter för att kunna visa patientens information som stöd i behandling hos vårdgivare. Applikationen ska även kunna visa patientens information från andra vårdgivare än den som är ansvarig för behandlingen.

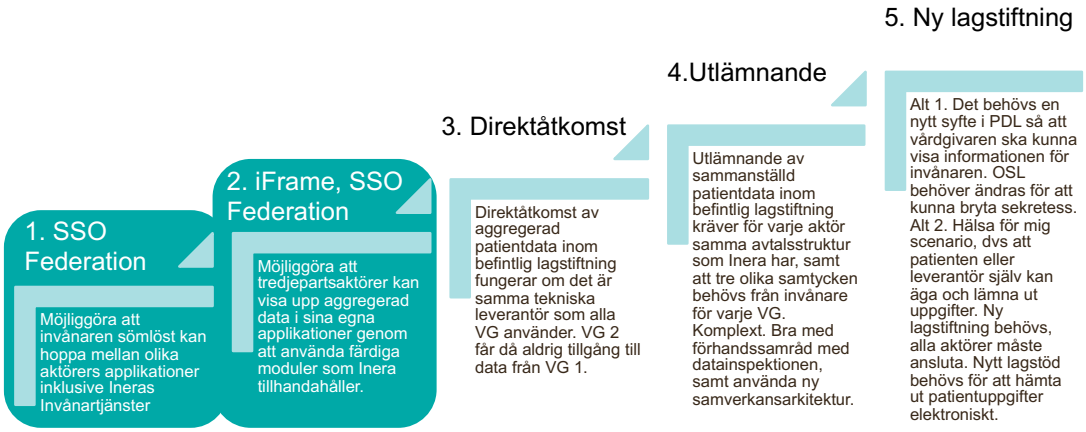
2.6.2 Lösningsbeskrivning

Använd en gemensam IdP eller en säkerhetsfederation tillsammans med en nationell e-tjänst som tillhandahåller en nationell vy av patientinformationen. När användaren av patientapplikationen vill se sin samlade patientinformation från alla vårdgivare så gör patientapplikationen ett uthopp till en nationell e-tjänst där användaren automatiskt loggas in och kan se sin information.



2.6.3 Trappstegsmodell

Trappstegsmodellen beskrivs i huvudrapporten och används för att rangordna de olika lösningsmönstren utifrån svårighetsgrad där fem anger den högsta svårighetsgraden. Detta mönster har placerats på trappa ett eller två:



2.6.4 Förutsättningar

- Mönstret förutsätter att patientapplikationen och e-tjänsten använder samma IdP eller att två olika IdP används som tillhör samma federation. E-tjänsten måste lita på den IdP som patienten använde för att logga in i patientapplikationen.
- Om en lösning med iFrame används eller en mobilapplikation av typen hybrid-app nyttjas så måste cookies från den nationella tjänstens vara markerade med `SameSite=None` och `Secure`, se appendix ”Analys av iFrame-lösning” för en detaljerade förklaring.

2.6.5 Tillämpning

Mönstret är användbart när en tjänstekonsument efterfrågar en nationell vy av patientens information och samtidigt inte har en egen skräddarsydd vy som högsta prioritet utan kan accepterar en färdig nationell vy.

Mönstret är även användbart för en patientapplikation där det inte finns tid och/eller resurs för att uppfylla alla krav och regler som ställs på en applikation som ska sammanställa en nationell vy av patientens information.

2.6.6 Kända användningsområden

Inera använder Läkemedelskollen från eHälsomyndigheten enligt detta mönster när den visas upp via 1177.se. Lösningsmönstret används även vid uthopp från 1177.se till regionala tjänster, även om syftet i det fallet är att tillgängliggöra regionala tjänster och inte en nationell vy av patientinformationen.

2.6.7 Varianter

Patientapplikationen kan välja att implementera mönstret genom att låta den nationella e-tjänsten öppna ett eget fönster (via uthopp) eller genom att visa e-tjänsten i en del av patientapplikationens fönster (via en iFrame). Se appendix ”Analys av iFrame-lösning”.

2.6.8 Konsekvenser – Juridik

Den juridiska bedömningen utgår från beskrivningen i appendix ”Analys av iFrame-lösning” och speciellt kapitel 7.2 ”Jämförelse av lösningsalternativ”.

En viktig fråga i sammanhanget är i vilken utsträckning den personuppgiftsansvarige vårdgivarens webbsida kan påverka eller kontrollera innehållet i en iFrame som visar invånarens vårddokumentation som finns presenterad i Journalen (1177). Vilka möjligheter har JavaScriptet att läsa eller ändra i s.k.Windows-objekt och deras tillhörande Document-objekt?

Alla moderna webbläsare följer ett protokoll benämnt Same-origin policy. Webbläsare som följer detta protokoll ger endast JavaScript från ett webbläsarfönster (t.ex. en flik) full åtkomst till ett Window-objekt i ett annat webbläsarfönster (t.ex. en iFrame eller en annan flik) om dokumentet i respektive fönster har laddats från samma plats.

Det innebär att HTML-koden i kapitel 7.2, som exemplifierar en minimal prototyp av en patientapplikation, måste laddas från samma webbserver som 1177 vårdguiden, för att eventuella JavaScript i dessa HTML-dokument ska få tillgång till data från 1177, oavsett om patientöversikten från 1177 visas i en iFrame eller en ny flik.

Eventuella JavaScript i dessa HTML-dokument har dock en begränsad tillgång till Window-objekten i den iFrame eller den flik som har laddats från https://e-tjanster.1177.se, men det handlar om funktioner och attribut som inte anses vara direkt relaterat till informations-innehållet,

Det sagda innebär att den vårdgivare som erbjuder en iFrame-lösning i sina digitala tjänster eller appar som på invånares kommando visar innehållet i Journalen via 1177 för den specifika invånaren inte bestämmer över målet med personuppgiftsbehandlingen. Det gör ju i stället de personuppgiftsansvariga vårdgivare som genom direktåtkomst via Journalen tillgängliggör uppgifter för invånaren i en iFrame, Inte heller är det så att vårdgivaren som erbjuder en iFrame styr över medlen. Oavsett det kan personuppgiftsansvar endast föreligga om kontroll över mål och medel föreligger. Det har de vårdgivare som genom enskilds direktåtkomst via 1177 tillgängliggör sina uppgifter om en specifik invånare i en iFrame. Någon överföring av personuppgifter mellan vårdgivare förekommer således inte i dessa fall. Behandlingen är därmed en tillåten behandling.

2.6.9 Konsekvenser – Avtal

Ej analyserat

2.6.10 Konsekvenser – IT-säkerhet

I denna lösning är det inte patientapplikationen som hanterar den nationella vyn av patientinformationen och behöver därför inte certifieras eller granskas ur den aspekten.

2.6.11 Personuppgiftsansvarigs behov av att kontrollera sin information

I denna lösning är det inte patientapplikationen som hanterar den nationella vyn av patientinformationen. Patientapplikationen möjliggör endast för användaren att sömlöst logga in till en befintlig nationell tjänst som Inera redan tillhandahåller och medför därför inte några nya behov för personuppgiftsansvariga.

2.6.12 Individens behov av att kontrollera sin information

I denna lösning är det inte patientapplikationen som hanterar den nationella vyn av patientinformationen. Patientapplikationen möjliggör endast för användaren att sömlöst logga in till en befintlig nationell tjänst som Inera redan tillhandahåller och medför därför inte några nya behov för individen.

2.6.13 Styrkor och svagheter

Övriga styrkor och svagheter som inte redan har beskrivits som en konsekvens:

Styrkor:

- Patientapplikationen behöver inte ansluta sig som tjänstekonsument eller aggregera information för att visa upp en nationell vy av patientinformationen
- Patientapplikationen behöver inte certifieras eller granskas ur aspekten att den ska sammanställa en nationell vy
- Tjänsteproducenterna behöver inte godkänna en ny tjänstekonsument

- Patientapplikationen behöver inte hantera den kedja av samtycken som annars hade varit fallet om informationen för den nationella vyn hade förmedlats av patientapplikationen.

Svagheter:

- Patientapplikationen kan inte påverka hur den nationella vyn av patientinformation utformas och visas för användaren.
- Den nationella vyn måste tillåta tredjepartscookies för att kunna visas upp i en iFrame (se Appendix)
- Användaren kan behöva logga in i den nationella vyn om patientapplikationen och den nationella tjänsten inte använder samma IdP eller olika IdP som inte tillhör samma säkerhetsfederation.

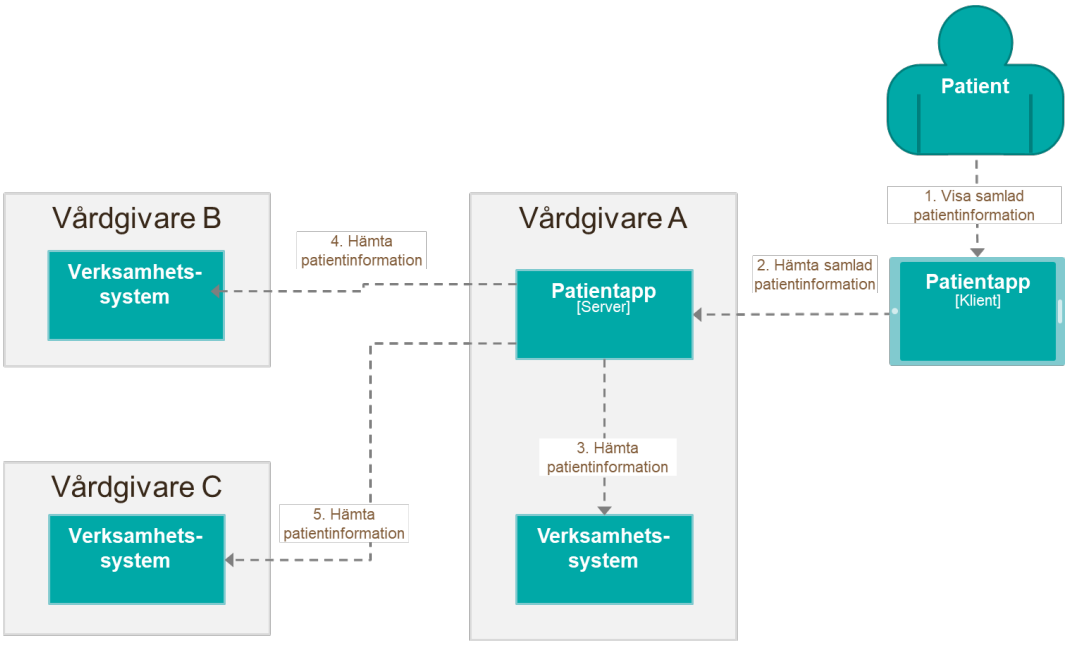
2.7 Lösningsmönster ”Hämta samlad patientinformation 1e”

2.7.1 Behov

En vårdgivare erbjuder en applikation för sina patienter för att kunna visa patientens information som stöd i behandling hos vårdgivare. Applikationen ska även kunna visa patientens information från andra vårdgivare än den som är ansvarig för behandlingen.

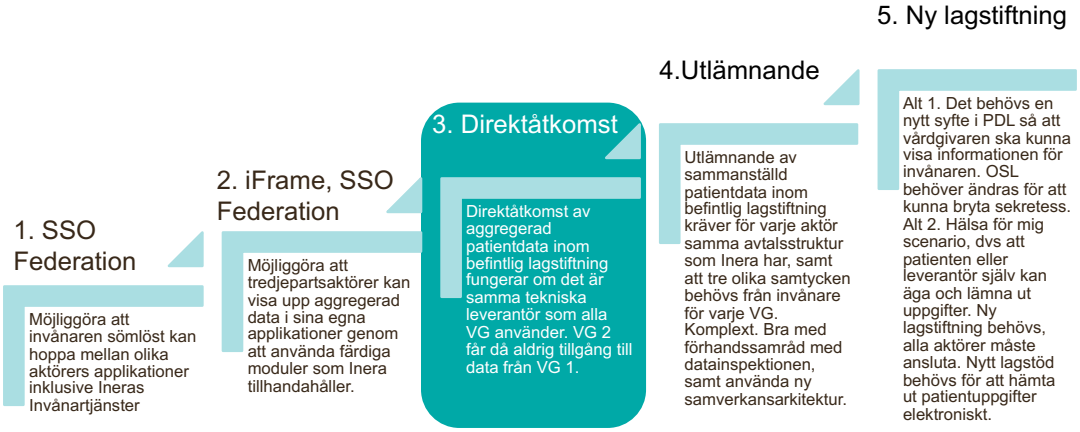
2.7.2 Lösningsbeskrivning

Vårdgivaren tillhandahåller i detta scenario en applikation som hämtar samlad patientinformation från andra vårdgivare utan att nyttja Ineras infrastruktur. Inera kan i detta scenario bidra med standardiserade tjänstekontrakt för att hämta informationen. Eftersom vårdgivaren inte nyttjar Ineras infrastruktur beskrivs detta lösningsmönster inte närmare här. Lösningsmönstret kan dock kombineras med olika stödtjänster från Inera.



2.7.3 Trappstegsmodell

Trappstegsmodellen beskrivs i huvudrapporten och används för att rangordna de olika lösningsmönstren utifrån svårighetsgrad där fem anger den högsta svårighetsgraden. Detta mönster har placerats på trappa tre:



3. Behovsscenario ”Hämta brukarinformation”

3.1 Generell beskrivning

En kommun erbjuder en **applikation för sina brukare för att kunna visa brukarens information** som stöd och insatser i äldreomsorgen. Applikationen med brukarens vy erbjuds antingen genom att kommunen har upphandlat en applikation av extern leverantör eller genom kommunens systemleverantör som har en invånaringång där funktioner möjliggör visning av brukarinformation.

För att applikationen ska kunna ge avsett stöd behöver den få tillgång till **vissa delar av brukarens personakt eller annan information** om brukaren, exempelvis information om utförd hemtjänst där den privata utföraren äger sin information, eller information om antal genomförda resor med färdtjänst och annan administrativ information från andra organisationer än kommunen. Denna informationen vill kommunen få tillgång till via **Ineras infrastruktur**.

3.2 Lösningsmönster ”Hämta brukarinformation”

Samma lösningsmönster som för regionerna borde kunna användas inom den kommunala hälso- och sjukvården, däremot så är förutsättningarna annorlunda inom socialtjänsten. Lösningsmönster för socialtjänsten har ej analyserats närmare i denna utredning.

4. Behovsscenario ”Hämta grunddata”

4.1 Generell beskrivning

En vårdgivare har av extern leverantör upphandlat en applikation som den erbjuder sina patienter. Den huvudsakliga digitala kommunikationen i behandlingen sker via lokal integration till vårdgivarens system. För att applikationen ska kunna ge avsett stöd till patienten behöver den få tillgång till **grund/katalogdata** som finns i **Ineras kataloginfrastruktur** exempelvis adresser från HSA eller utbudsinformation från utbudstjänsten.

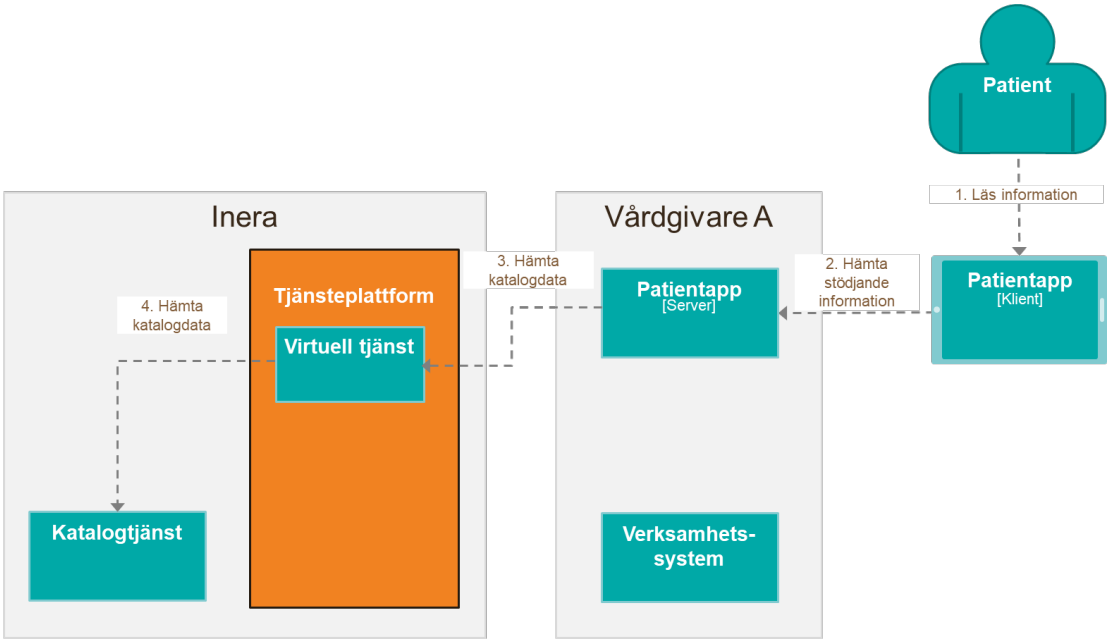
4.2 Lösningsmönster ”Hämta grunddata via tjänstekontrakt”

4.2.1 Behov

Enligt den generella beskrivningen

4.2.2 Lösningsbeskrivning

Grunddata måste först skapas eller samlas in för att därefter distribueras för användning. Mönstret visar inte hur grunddata samlas in utan enbart hur grunddata distribueras. I nedanstående lösningsmönster distribueras grunddata via tjänstekontrakt och virtuella tjänster i tjänsteplattformen. Lägg märke till att även om tjänsten som distribuerar grunddata förvaltas av Inera så är det inte Inera som äger informationen.



4.2.3 Förutsättningar

För att mönstret ska kunna tillämpas krävs att följande förutsättningar är uppfyllda:

- Det finns avtal mellan informationsägare, Inera, vårdgivare (kund) och eventuell leverantör som medger att vald grunddata får delas

Utökat resonemang

DIGG definierar grunddata som uppgifter, inom offentlig förvaltning, som flera aktörer har behov av och som är viktiga i samhället. Mer allmänt brukar man definiera grunddata som viktig information som är gemensam för en verksamhet och som delas av flera intressenter och system.

Grunddata är således ett ganska brett begrepp vilket medför att det inte går att göra en generell juridisk tolkning som gäller all grunddata. På samma sätt är det troligen svårt att hitta en generell avtalsmodell som täcker alla typer av grunddata. En lösning är att definiera juridik och avtal specifikt för varje tjänst eller informationsmängd, men det vore bättre om man kunde gruppera olika typer av grunddata i kategorier som kan nyttja samma juridiska tolkning och affärsavtal.

En informationsmängd är journalinformation som redan behandlats i kapitlet om patientinformation. Journalinformation använder i regel andra lösningsmönster än den grunddata som behandlas i detta kapitel.

Vårddokumentation som inte är journalinformation, t.ex. listning, högkostnadsskydd och eventuellt spärrinformation (ej klarlagt) bör gå att gruppera ihop ur en juridisk synvinkel, men använder inte nödvändigtvis det föreslagna mönstret för grunddata.

Informationsmängder som innehåller personuppgifter och faller under GDPR är också en informationsmängd som eventuellt går att behandla på likartat sätt ur ett juridiskt och avtalsmässigt perspektiv.

Utifrån ovanstående resonemang kan man eventuellt tänka sig följande gruppering:

- Journalinformation
- Vårddokumentation som inte är journalinformation
- Personuppgifter som faller under GDPR
- Öppen data
  - Kan nyttjas fritt av alla aktörer och kräver minimalt med kontroller vid anslutning. API är helt öppet
  - Tänkbart exempel på tjänst är Utbud
- Data med kostnad som får spridas fritt
  - Informationen är inte känslig ur ett juridiskt perspektiv eller har någon typ av upphovsrätt, men de som vill nyttja informationen för att t.ex. bygga egna tjänster får betala för förvaltningen av de tekniska tjänsterna.
  - Exempel är Hitta och jämför vård (HJV)/adresser till mottagningar, adressregister för Säker Digital Kommunikation m.m.
- Data som ej får spridas fritt
  - Detta kan omfatta upphovsskyddad data eller annan data som inte får spridas fritt
  - Informationen kan nyttjas av alla aktörer om man köper tjänsten, d.v.s. betalar för förvaltning av informationen och tekniken.
  - Exempel är beslutsstöd för rådgivning, kunskapsdatabaser.

Detta är dock endast en tänkbar ansats av många. Varje tjänst måste bedömas för sig, men förhoppningsvis går det över tid att hitta användbara kategoriseringar.

4.2.4 Tillämpning

Mönstret är användbart för grunddata som efterfrågas av tjänstekonsumenter i mängder som inte överskrider den kapacitet som kan hanteras via en Tjänsteplattform. Meddelanden på flera tiotals megabyte är inte lämpliga att skicka via en Tjänsteplattform.

4.2.5 Kända användningsområden

PU-tjänsten, Utbudstjänsten, HSA-katalogen m.fl. Notera att detta är exempel på tjänster där interaktionsmönstret används och inte exempel på tjänster som används av tredjepartsprodukter.

4.2.6 Varianter

Lösningsmönstret är i första hand tänkt att användas för direktåtkomst, men kan även användas då grunddata behöver lagras hos vårdgivaren eller i patientapplikationen för att förbättra prestanda.

HSA-katalogen använder även en variant där information synkroniseras mellan den centrala HSA-katalogen och de regionala HSA-katalogerna. Lokala tjänster ansluter därefter i första hand till den regionala katalogen.

HSA-katalogen har även äldre tjänster där tjänstekonsumenterna ansluter direkt till HSA-katalogen utan att nyttja Tjänsteplattformens virtuella tjänster.

4.2.7 Konsekvenser – Juridik

Termen grunddata omfattar data inom olika juridiska lagrum. Det är därför svårt att ge en enhetlig bedömning av de juridiska konsekvenserna för alla grunddatatjänster. Bedömningen måste istället göras för varje enskild tjänst. Exempelvis så är GDPR det huvudsakliga lagrummet för PU-tjänsten till skillnad mot Hjälpmedelstjänsten som inte innehåller någon persondata.

4.2.8 Konsekvenser – Avtal

Ej analyserat

4.2.9 Konsekvenser – IT-säkerhet

Termen grunddata omfattar många olika domäner där det kan vara stor skillnad när det gäller behovet av tillgänglighet, riktighet och konfidentialitet. Exempelvis skulle ett intrång i en tredjepartsprodukt som har tillgång till grunddata från Hjälpmedelstjänsten inte betraktas som allvarligt eftersom grunddata från Hjälpmedelstjänsten redan publiceras öppet på 1177.se. Motsvarande intrång i en tredjepartsprodukt som har tillgång till PU-tjänsten (Personuppgiftstjänsten) skulle orsaka betydligt större skada eftersom PU-tjänsten innehåller personuppgifter.

Grunddata som innehåller känsliga uppgifter behöver mekanismer för att minimera skadan vid ett dataintrång i en tredjepartsprodukt där angriparen får kontroll över produkten och kan styra informationsflödet. Precis som när det gäller patientuppgifter kan dessa begränsningar implementeras på flera olika nivåer, men förutsättningar och möjligheter skiljer sig något från fallet med patientuppgifter.

Här beskrivs kortfattat begränsningar som redan är implementerade samt förslag till mekanismer som eventuellt kan implementeras i Ineras infrastruktur. Förslagen kräver ytterligare utredningar.

Begränsa de informationstyper som tredjepartsprodukten kan hämta

All kommunikation som sker via tjänstekontrakt begränsas per automatik till de informationstyper som tjänstekontraktet definierar. Ett exempel på detta är tjänstekontrakten inom domänen personuppgifter där det finns olika tjänstekontrakt för att hämta personuppgifter som är skyddade respektive inte skyddade.

Begränsa vilka individer som tredjepartsprodukten kan hämta information om

Detta är en möjlighet som erbjuds i användningsfallet för att hämta patientuppgifter, men det är inte relevant när det gäller grunddata eftersom grunddata i de allra flesta fall inte förväntas hämtas av en viss individ eller på uppdrag av en viss individ.

Nyttja en säkerhetsinfrastruktur som bygger på identitetsintyg och åtkomstintyg istället för organisatorisk tillit

Detta alternativ kräver att hela säkerhetsinfrastrukturen för Inera och regionerna förändras. Förändringen skulle dock minska risken vid intrång eftersom det inte räcker att få kontroll över en applikation. Varje anrop från applikationen måste åtföljas av ett signerat identitetsintyg som kan användas för att hämta ett åtkomstintyg som i sin tur används för att hämta information från systemet som tillhandahåller grunddata.

4.2.10 Personuppgiftsansvarigs behov av att kontrollera sin information

Grunddata som innehåller persondata har också Personuppgiftsansvariga. Exempel på grunddatatjänster med personuppgiftsansvariga är PU-tjänsten och HSA-katalogen. Till skillnad mot användningsfallet ”Hämta samlad patientinformation” så tillhandahålls oftast grunddata från en samlad katalog och inte i olika källsystem hos personuppgiftsansvariga producenter. Detta medför att den tekniska behörighetskontrollen görs via Tjänsteplattformens centrala behörighetskontroll och inte i lokala ”anslutningsfilter” hos källsystemen.

Menprövning

Åtkomst till uppgifter via Personuppgiftstjänstens tjänstekontrakt sker primärt med stöd av ett elektroniskt utlämnande i form av ett s.k. automatiserat *ADB-utlämnande*. Utlämnandet bygger på att personuppgiftsansvarig har gjort en prövning av varje enskilt fall baserat på ett i förväg fattat schablonmässigt menprövningsbeslut. Menprövningsbeslutet ska inkludera vad som kan lämnas ut för uppgift som är skyddad (sekretessmarkerad)

4.2.11 Individens behov av att kontrollera sin information

Samtycke är främst något som berör PU-tjänsten där en individ kan ange samtycke till att en verksamhet kan skicka meddelande till personen via en ”digital aviseringsväg” (mejl, mobilnummer, etc.)

4.2.12 Styrkor och svagheter

Övriga styrkor och svagheter som inte redan har beskrivits som en konsekvens:

Styrkor:

- Enkelt att använda för en tjänstekonsument som kan använda sig av den etablerade infrastrukturen runt den nationella tjänsteplattformen

Svagheter:

- Det finns begränsningar i storleken på meddelanden som kan skickas över tjänsteplattformen

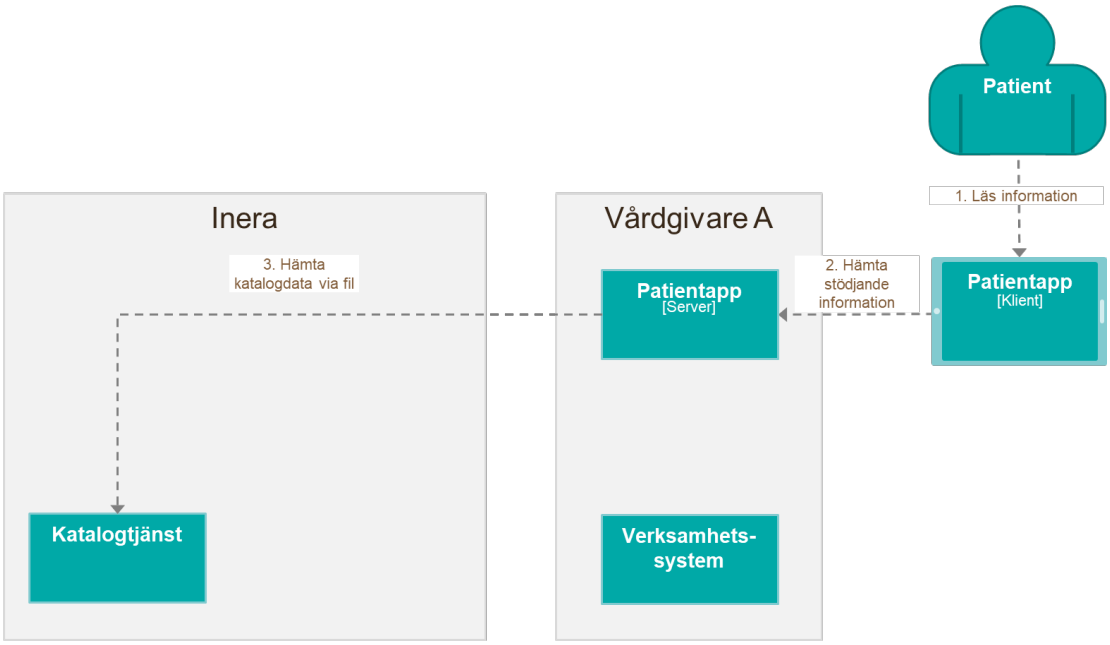
4.3 Lösningsmönster ”Hämta grunddata via fil”

4.3.1 Behov

Enligt den generella beskrivningen

4.3.2 Lösningsbeskrivning

Grunddata måste först skapas eller samlas in för att därefter distribueras för användning. Mönstret visar inte hur grunddata samlas in utan enbart hur grunddata distribueras. I nedanstående lösningsmönster distribueras grunddata via filöverföring direkt till klienten. Lägg märke till att även om tjänsten som distribuerar grunddata förvaltas av Inera så är det inte Inera som äger informationen.



4.3.3 Förutsättningar

För att mönstret ska kunna tillämpas krävs att följande förutsättningar är uppfyllda:

- Det finns avtal mellan informationsägare, Inera, vårdgivare (kund) och eventuell leverantör som medger att vald grunddata får delas

4.3.4 Tillämpning
Mönstret är användbart för grunddata som efterfrågas av tjänstekonsumenter i mängder som överskrider den kapacitet som kan hanteras via en Tjänsteplattform. Meddelanden på flera tiotals megabyte är inte lämpliga att skicka via en Tjänsteplattform.

4.3.5 Kända användningsområden
HSA-katalogen

4.3.6 Varianter
Lösningsmönstret är tänkt att användas då stora mängder grunddata behöver hämtas och lagras hos vårdgivaren eller i patientapplikationen. Vanligtvis sker detta via något filöverföringsprotokoll, men man kan även tänka sig andra varianter, exempelvis ett REST-baserat gränssnitt.

4.3.7 Konsekvenser – Juridik
Samma som ”Hämta grunddata via tjänstekontrakt”

4.3.8 Konsekvenser – Avtal
Samma som ”Hämta grunddata via tjänstekontrakt”

4.3.9 Konsekvenser – IT-säkerhet
Samma som ”Hämta grunddata via tjänstekontrakt”. De beskrivna lösningarna och förslagen går att översätta till motsvarande konstruktioner för filöverföring.

4.3.10 Personuppgiftsansvarigs behov av att kontrollera sin information
Samma som ”Hämta grunddata via tjänstekontrakt”.

4.3.11 Individens behov av att kontrollera sin information
Samma som ”Hämta grunddata via tjänstekontrakt”.

4.3.12 Styrkor och svagheter
Övriga styrkor och svagheter som inte redan har beskrivits som en konsekvens:

Styrkor:

- Går att skicka stora mängder data vid filöverföring.

Svagheter:

- Den etablerade infrastrukturen runt den nationella tjänsteplattformen går inte att använda.

- Tjänstekonsumenter behöver göra nya brandväggsöppningar.

5. Behovsscenario ”Skriva information”

5.1 Generell beskrivning

En invånare vill välja vårdgivare att lista sig på och vänder sig till en vårdgivare som har en applikation som är upphandlad eller utvecklad i vårdgivarens regi för detta ändamål. Invånaren har också beviljats hemtjänst och vill också välja kommunal utförare för sin hemtjänst och vänder sig till kommunen som också erbjuder en applikation som är upphandlad eller utvecklad för detta ändamål.

Invånaren använder också en del utrustning i hemmet för att övervaka sin hälsa, såsom blodtryck, puls och vikt. Dessa mätvärden behöver både vårdgivaren och kommunen få tillgång till.

OBS! Endast scenariot där en invånare vill välja vårdgivare att lista sig på beskrivs i denna rapport.

5.2 Lösningsmönster ”Listning”

5.2.1 Behov

En invånare vill välja vårdgivare att lista sig på och vänder sig till en vårdgivare som har en applikation som är upphandlad eller utvecklad i vårdgivarens regi för detta ändamål.

5.2.2 Lösningsbeskrivning

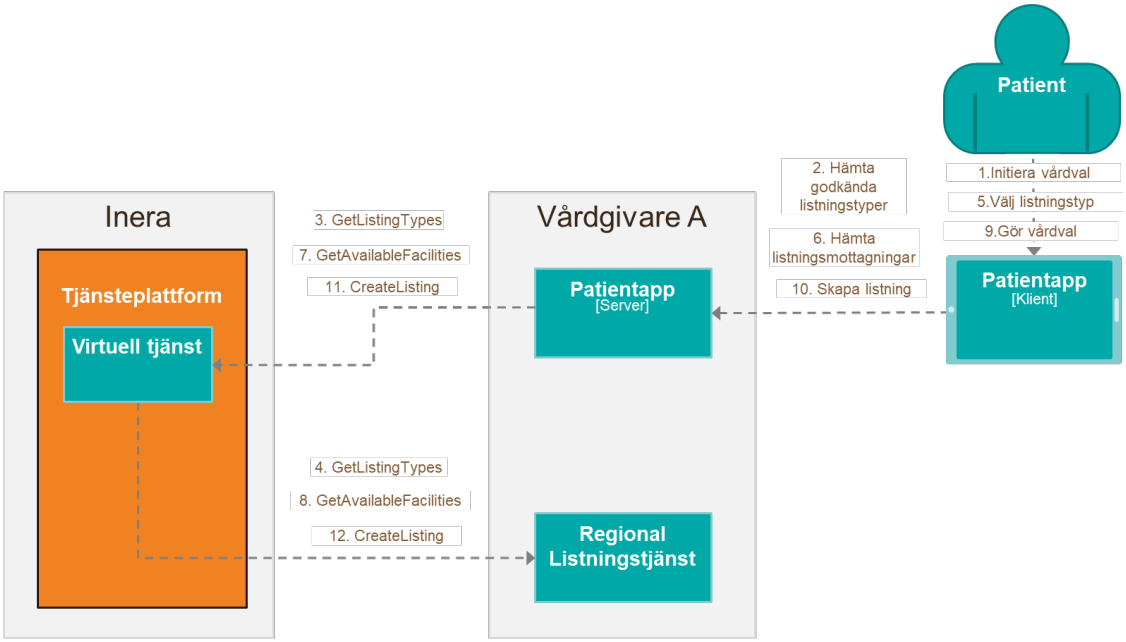
Lösningen använder tjänstekontrakten som ingår i den Nationella listningstjänsten (crm:carelisting). Bilden över flödet visar endast nödvändiga interaktioner inom listningsdomänen, men för att genomföra flödet behövs även grunddatatjänster. Varje regions listningstjänst är ansluten till den Nationella listningstjänsten, med undantag för Gotland (endast ansluten med tjänstekontraktet ”GetListing”), Uppsala och Värmland

Normalflöde för att ändra vårdval (baserat på listningstjänsten hos 1177):

1. Hämta godkända listningstyper för invånaren i aktuell region (tjänstekontrakt ”GetListingTypes”). Man kan lägga märke till att listningstyperna inte används på exakt samma sätt av alla regioner (vissa använder t.ex. Husläkarteam, HLT, istället för Husläkarmottagning, HLM) och att koden för listningstyp som skickas tillbaka behöver översättas till klartext. Varje region väljer själv i 1177 hur översättningen till klartext ska göras. I detta steg kan även grunddata behöva hämtas från PU-tjänsten för att veta vilken region användaren tillhör.
2. Användaren väljer listningstyp (om fler än en listningstyp returneras)
3. Hämta och visa listningsmottagningar som erbjuder vald listningstyp (tjänstekontrakt ”GetAvailableFacilities”)

4. Användaren väljer mottagning. Innan detta steg bör grunddata från katalogtjänst HSA hämtas för att kunna visa upp mer information om varje vårdenhet än enbart dess namn samt erbjuda filtrering på t.ex. kommun. Lägg märke till att enhetens namn inte är obligatoriskt enligt tjänstekontraktet och att det därför behövs en anslutning till katalogtjänst HSA för att säkerställa att denna information kan visas.
5. I listningstjänsten för 1177 finns möjlighet för användaren att skriva in listningsönskemål för den valda mottagningen i det fall att regionen har bestämt att detta ska vara möjligt. Listningsönskemålet hanteras via ärendehanteringssystemet i 1177 och personalen på den valda mottagningen aviseras via mejl. Det finns inget nationellt tjänstekontrakt för denna interaktion.
6. Skapa listning hos den valda mottagningen (tjänstekontrakt ”CreateListing”)

Utöver ovanstående steg stödjer listningstjänsten i 1177 även en ombudsfunktion, men detta är inget som listningstjänsten är medveten om. Listningstjänsten agerar som att barnet var användaren.



Om listning endast ska stödja inom regionen så är det inte nödvändigt att gå via Ineras tjänsteplattform. I det fallet kan patientapplikationen kommunicera direkt med den regionala listningstjänsten via de standardiserade tjänstekontrakten.

För enkelhetens skull så tillhandahålls den regionala listningstjänsten i ovanstående bild av samma vårdgivare som tillhandahåller patientappen, men detta är inte nödvändigt. Under vissa förutsättningar kan även andra regioners listningstjänster anropas. Den juridiska utredningen har kommit fram till att delning av listningsinformation är möjligt för vårdcentraler som driftas av regionerna själva.

För delning av listningsinformation mellan regioner och privata vårdgivare samt mellan privata vårdgivare krävs samtycke på samma sätt som i kapitel 2.5 och lösningsmönster ”Hämta samlad patientinformation 1c”, men endast ett samtycke krävas för att app-ansvarig vårdgivare ska kunna förmedla informationen till pålistad respektive avlistad vårdgivare eftersom båda har och får en vårdrelation med patienten.

Om patientappen endast ska visa listningsinformation så är den enklast och säkraste lösningen att använda lösningsmönster ”Hämta samlad patientinformation 1d” från kapitel 2.6, d.v.s. iFrame-lösningen.

5.2.3 Förutsättningar

För att mönstret ska kunna tillämpas krävs att följande förutsättningar är uppfyllda:

- Det kan förutsättas att det finns en tjänst för varje region.
- Regionerna tillåter patienter till andra vårdaktörer att hämta och skriva listningsinformation

5.2.4 Tillämpning

Mönstret är användbart när en tjänstekonsument efterfrågar en nationell vy av patientens information som dessutom ska vara möjlig att uppdatera.

Lösningsmönstret är även användbart när det finns behov av att skapa ett skräddarsytt grafiskt användargränssnitt i patientappen.

5.2.5 Kända användningsområden

Listningstjänsten hos 1177 använder detta mönster.

5.2.6 Varianter

5.2.7 Konsekvenser – Juridik

Vad gäller frågan om en patient via en vårdaktör kan hämta listningsinformation från andra vårdaktörer via en patientapp blir den juridiska bedömningen densamma som i appendix ”Analys av iFrame-lösning” och speciellt kapitel 7.2 ”Jämförelse av lösningsalternativ”. Det innebär att en vårdgivare genom enskilds direktåtkomst via 1177 kan tillgängliggör sina uppgifter om listning för en specifik invånare i en iFrame som finns i en patientapp. Någon överföring av personuppgifter mellan vårdgivare förekommer således inte i dessa fall. Behandlingen är därmed en tillåten behandling.

Däremot kan inte en patient via en vårdaktör skriva listningsinformation till andra vårdaktörer via en patientapp. Enskilds direktåtkomst innefattar inte en rätt att skriva, bara läsa. iFrame-lösningen kan således inte fungera som en skrivyta utan patienten nödgas registrera sina önskemål om listning hos den vårdgivare som är personuppgiftsansvarig för patientappen.

Frågan är om förmedling av listningsuppgifter från en vårdgivare till en annan (pålistning och avlistning) skulle kunna tänkas ske genom sammanhållen journalföring. Det förutsätter att arbetsuppgiften att lista patienter är en sådan behandling av personuppgifter som ryms inom ramen för sammanhållen journalföring.

Enligt 6 kap. 1 § PDL får en vårdgivare ha direktåtkomst till personuppgifter som behandlas av andra vårdgivare för ändamål som anges i 2 kap. 4 § första stycket 1 (journalföring) och 2 (administration). Med administration i 2 kap. 4 § första stycket 2 avses såväl patientrelaterad ekonomiadministration som annan administration som behövs för eller föranleds av vård i enskilda fall (prop. 2007/08:126 s. 228). Listning behövs inte för att en patient ska få vård och behandling hos en vårdgivare. Och det är inte heller nödvändigtvis så att listning alltid föranleds av ett vårdbesök; kanske patienten är på semester och uppsöker en vårdgivare på semesterorten och har ingen önskan om att lista om sig.

Sammanhållen journalföring rymmer således sannolikt inte behandling av uppgifter om listning. I stället återstår delning av listningsuppgifter genom på ADB-utlämnande mellan app-vårdgivaren och pålistade respektive avlistade vårdgivare.

Rättsläget blir detsamma som i lösningsmönster ”Hämta samlad patientinformation 1a” och de lösningar som presenteras där för informationsdelning mellan vårdgivare, bl.a. samtycke från invånaren.

Undantaget är delning av listningsinformation mellan vårdcentraler som driftas av regionerna själva. Enligt 25 kap. 11 § 5 p. OSL hindrar inte hälso- och sjukvårdssekretessen att uppgift lämnas från en myndighet som bedriver hälso- och sjukvårdsverksamhet inom en kommun eller en region till annan sådan myndighet för forskning och framställning av statistik eller för administration på verksamhetsområdet, om det inte kan antas att den enskilde eller någon närstående till den enskilde lider men om uppgiften röjs.

Bestämmelsen är tillämplig på utlämnande av uppgifter både inom en region eller inom en kommun och mellan kommuner eller regioner.

Skaderekvisitet är rakt. Presumtionen är alltså att en uppgift får lämnas ut för de angivna ändamålen, bl.a. administration. I propositionen till den aktuella bestämmelsen anför departementschefen att med administration avses ”rent administrativa ändamål som t.ex. beräkning av antalet vårdplatser och utsändande av fakturor. I den nationella tjänsten Utomlänsfakturering bygger informationsdelningen på denna sekretessbrytande bestämmelse. Som konstaterats är listningsinformation en rent administrativ uppgift som därför lämpar sig väl för att delas mellan regioner med stöd av denna bestämmelse. Något samtycke behövs inte.

För delning av listningsinformation mellan regioner och privata vårdgivare samt mellan privata vårdgivare krävs samtycke. Dock torde endast ett samtycke krävas för att app-ansvarig vårdgivare ska kunna förmedla informationen till pålistad respektive avlistad vårdgivare eftersom båda har och får en vårdrelation med patienten.

5.2.8 Konsekvens – Avtal

Lösningsmönstret förutsätter att regionerna tillåter att patienter till andra vårdaktörer hämtar och/eller skriver listningsinformation som hör till regionerna. Detta är en förutsättning som kräver vidare utredning och som regleras genom affärsmässiga avtal.

5.2.9 Konsekvenser – IT-säkerhet

5.2.10 Personuppgiftsansvarigs behov av att kontrollera sin information

Konfigurering och upprätthållande av den behörighetskontroll som bestämmer vilken tjänstekonsument som får anropa en viss logisk adress görs vid verksamhetsbaserad adressering i tjänsteplattformen.

5.2.11 Individens behov av att kontrollera sin information

Individen vill hämta sin egen information och behöver i det enklast fallet inte några samtycken för att kontrollera detta. Beroende på hur implementation görs rent tekniskt kan det dock krävas samtycken. Detta gäller specifikt i det fall att patientapplikationen tillhandahålls av en vårdgivare och patienten vill hämta information från en annan vårdgivare. Samtyckestjänsten hos Inera hanterar i dagsläget endast samtycken för Sammanhållen Journalföring.

Ett annat scenario är när individen har behov av ett ombud. Ineras ombudsfunktioner används idag endast av Journalen och behöver utökas för att även stödja tredjepartsprodukter.

5.2.12 Styrkor och svagheter

Övriga styrkor och svagheter som inte redan har beskrivits som en konsekvens:

Styrkor:

- Inget behov av en aggregerad tjänst

Svagheter:

- Förutsätter att det finns en tjänst för varje region.

6. Sammansatt behovsscenario

6.1 Generell beskrivning

Detta scenario är ett sammansatt scenario där det både ingår att hämta och registrera information av både administrativ karaktär såväl som patient- eller brukarinformation. Både kommunal omsorg och regional sjukvård inkluderas.

En invånare har nyligen skrivits ut från sluten hälso- och sjukvård. Invånaren vill ha tillgång till sin samlade planering på 1177 Vårdguiden, med planering menas vem kommer till mig när och vad ska de göra. Här involveras hemtjänst, hemsjukvård och regional hälso- och sjukvård. Invånaren vill kunna återkoppla när hen inte kan, vill kunna ändra tid eller återkoppla att hen inte behöver planerad hjälp. Även invånarens närstående vill kunna se och meddela detta.

Informationen finns i hemtjänstens planeringssystem, kommunens hälso- och sjukvårdsjournal och i regionens journalsystem samt i systemstöd för utskrivningsprocess från slutenvård och SIP (Sammanhållen Individuell Plan).

6.2 Lösningsmönster

Inga lösningsmönster har analyserats i denna utredning

7. Appendix – Analys av iFrame-lösning

7.1 Inledning

Detta appendix innehåller en djupare analys av lösningsmönstret i kapitel 2.6 ”Hämta samlad patientinformation 1d”.

Lösningsmönstrets idé är att använda en gemensam IdP eller en säkerhetsfederation tillsammans med en nationell e-tjänst som tillhandahåller en nationell vy av patientinformationen. När användaren av patientapplikationen vill se sin samlade patientinformation från alla vårdgivare så erbjuder patientapplikationen denna möjlighet genom en hyperlänk som leder till den nationella e-tjänsten (en tjänst med ett grafiskt användargränssnitt som kan nås via Internet) där användaren automatiskt loggas in och kan se sin information.

Även utan en gemensam IdP eller säkerhetsfederation är lösningen intressant p.g.a. de fördelar som mönstret medför ur ett juridiskt och IT-säkerhetsmässigt perspektiv. Nackdelen är att användaren måste manuellt logga in i den nationella e-tjänsten om en säkerhetsfederation saknas.

Lösningsförslaget har fått klartecken ur ett juridiskt perspektiv när det gäller en traditionell uthoppslösning, d.v.s. när användaren klickar på en länk för att se sin samlade patientöversikt så öppnas en ny flik eller ett nytt fönster i webbläsaren där användaren, efter implicit eller explicit inloggning, kan se sin samlade patientinformation.

Däremot så har det funnits frågetecken om samma juridiska tolkning kan göras om den nationella e-tjänsten istället visas i en iFrame. Detta appendix har därför som avsikt att beskriva de tekniska skillnaderna mellan att använda en iFrame kontra en ny webbläsarflik för att visa patientinformation från en e-tjänst samt om något av dessa alternativ medför någon skillnad med avseende på patientapplikationens möjligheter att läsa, förändra eller på andra sätt bearbeta informationen som e-tjänsten erbjuder till användaren.

Appendixet beskriver även hur valet mellan att visa e-tjänsten i en iFrame eller en webbläsarflik påverkar webbläsarens hantering av s.k. cookies, eftersom det kan begränsa den tekniska lösningens möjligheter. Detta är dock inget som har någon påverkan på patientapplikationens begränsningar när det gäller att läsa, förändra eller på andra sätt bearbeta informationen som e-tjänsten erbjuder till användaren och bör därför inte påverka den juridiska bedömningen.

Sist i appendixet ges även en kortfattad översikt gällande användning av den föreslagna lösningen i en mobilapplikation samt konsekvenser för de olika implementationsalternativen i en mobilapplikation.

7.2 Jämförelse av lösningsalternativ

7.2.1 Minimal prototyp av en patientapplikation

Nedanstående bilder visar en minimal prototyp av en patientapplikation i form av en webbapplikation. En patientapplikation i form av en nerladdningsbar mobilapplikation beskrivs inte i detta kapitel. Syftet med prototypen är att belysa skillnaden mellan att låta användaren logga in i en nationell e-tjänst via en iFrame eller att göra motsvarande inloggning i en ny webbläsarflik.

Analysen av skillnaden mellan iFrame och en ny webbläsarflik blir densamma även om en gemensam IdP eller en säkerhetsfederation används av den nationella e-tjänsten och patientapplikationen, med den skillnaden att användaren kommer att loggas in automatiskt i den nationella e-tjänsten när användaren klickar på länken till e-tjänsten.

Nedan visas användargränssnittet för en minimal patientapplikation som i stort sett endast erbjuder en länk att klicka på för att visa användarens patientöversikt på 1177.

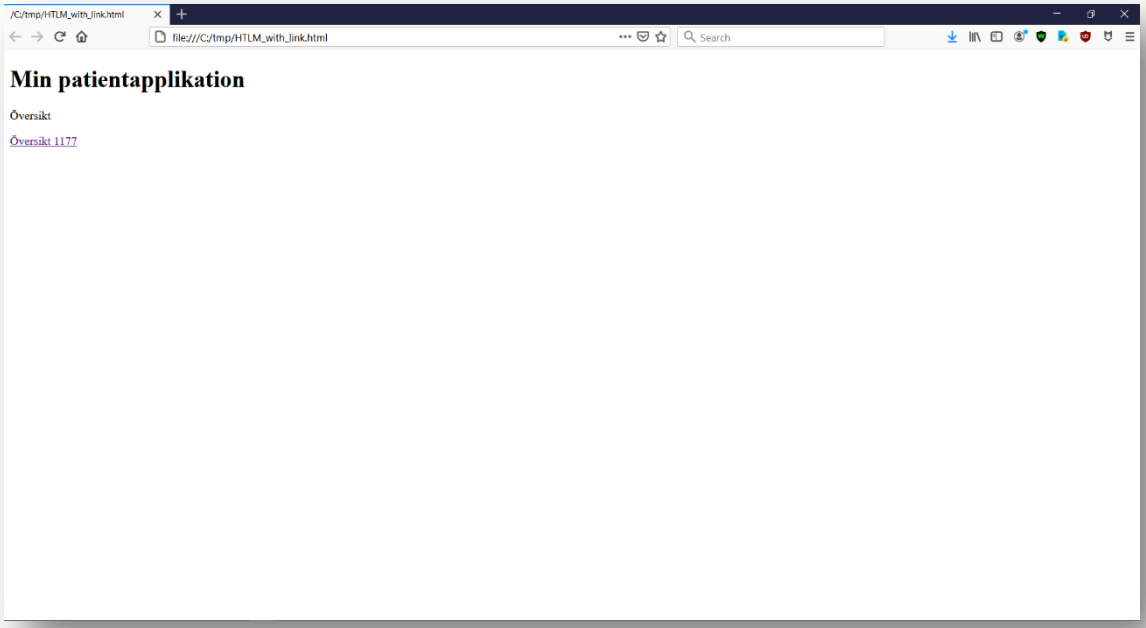


BILD 1

När användaren klickar på länken så öppnas 1177 Vårdguiden i en ny webbläsarflik enligt nedanstående bild:

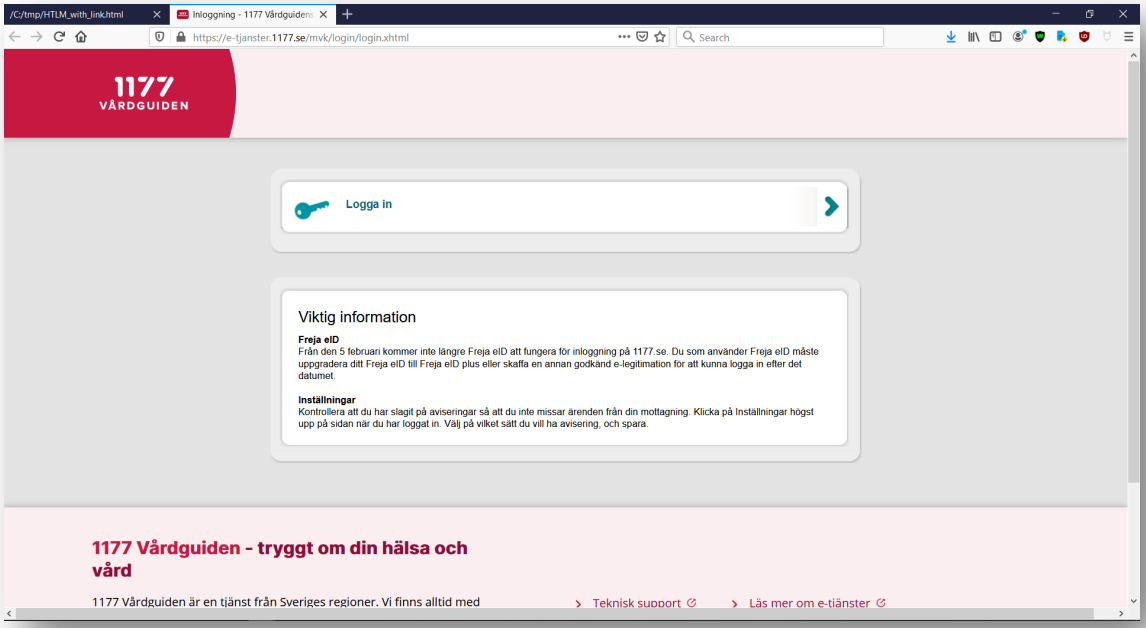


BILD 2

Näst bildsekvens visar användargränssnittet för en minimal patientapplikation med en iFrame och en klickbar länk för att visa användarens patientöversikt på 1177:

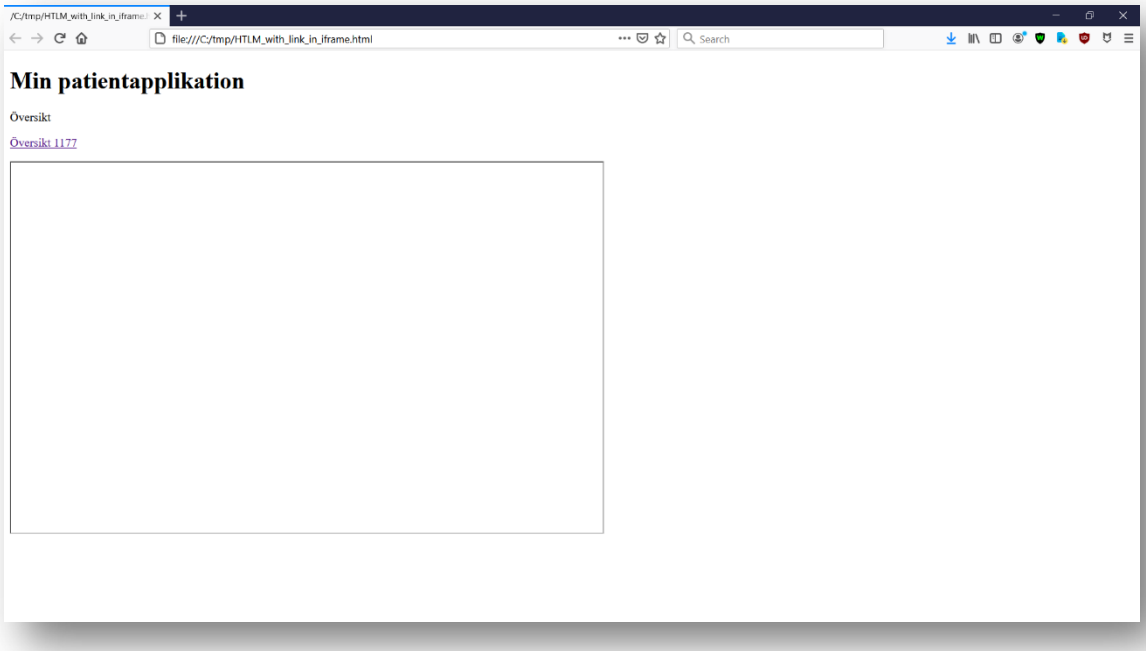


BILD 3

När användaren klickar på länken så öppnas 1177 Vårdguiden i webbapplikationens iFrame enligt nedanstående bild:

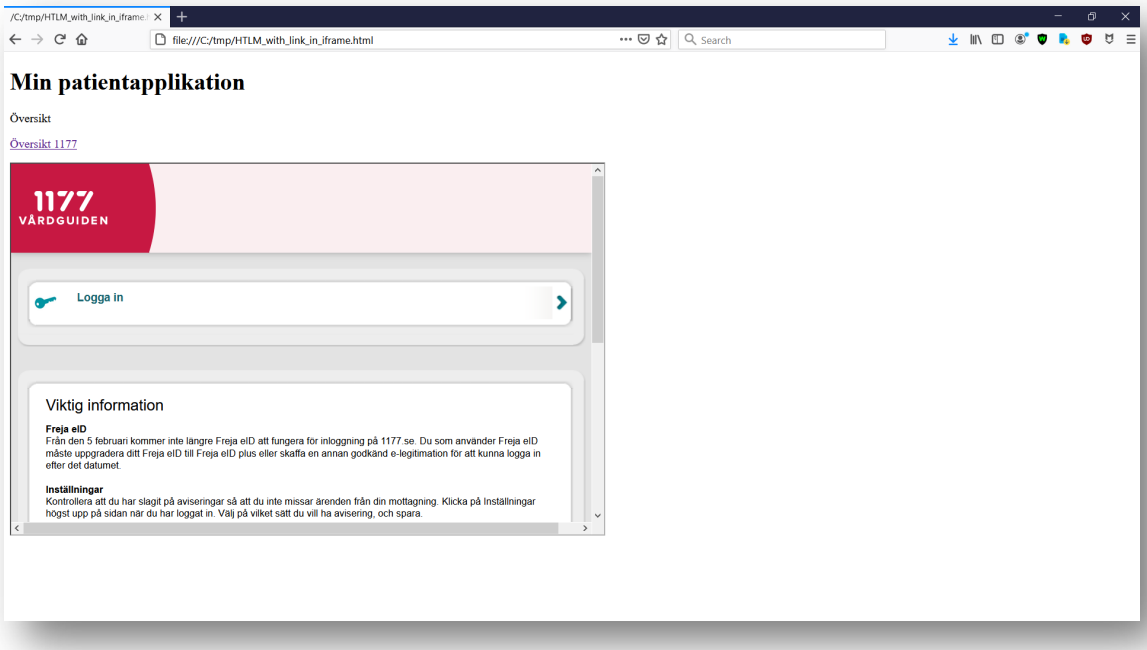


BILD 4

Det finns således en utseendemässig skillnad mellan dessa två utformningar av webbapplikationen, men finns det någon skillnad med avseende på patientapplikationens möjligheter att läsa, förändra eller på andra sätt bearbeta informationen som 1177 Vårdguiden erbjuder till användaren?

För att besvara den frågan så kommer dels den bakomliggande HTML-koden att analyseras och dels de möjligheter som patientapplikationen har att använda JavaScript för att kontrollera en iFrame eller en ny webbläsarflik.

7.2.2 HTML-kod för prototyperna

Patientapplikationen kan skapa ovanstående användargränssnitt genom att ladda upp färdiga HTML-dokument till användarens webbläsare eller genom att ladda upp JavaScript som dynamiskt skapar motsvarande HTML-dokument.

Följande HTML-kod användes för att skapa användargränssnittet som öppnar 1177 Vårdguiden i en ny webbläsarflik:

```
<!DOCTYPE html>
<html>
  <body>
    <h1>Min patientapplikation</h1>
    <p>Översikt</p>
    <a href="https://e-tjanster.1177.se/" target="_blank">Översikt 1177</a>
  </body>
</html>
```

BILD 5

Länken till 1177 skapas av `<a>`-taggen. Attributet `target="_blank"` medför att länken öppnas i en ny webbläsarflik.

Nedan visas HTML-koden som användes för att skapa användargränssnittet som öppnar 1177 Vårdguiden i en iFrame:

```
<!DOCTYPE html>
<html>
  <body>
    <h1>Min patientapplikation</h1>
    <p>Översikt</p>
    <p><a href="https://e-tjanster.1177.se/" target="iframe_a">Översikt 1177</a></p>
    <iframe src="" name="iframe_a" title="Iframe Example" width="800px" height="500px"></iframe>
  </body>
</html>
```

BILD 6

Även här används en `<a>`-tagg för att skapa länken till 1177, där attributet `target="iframe_a"` medför att länken öppnas i en iFrame med namnet `"iframe_a"`.

Det kan vara värt att nämna att detta endast är ett exempel och det finns fler sätt att öppna en ny webbläsarflik eller att ladda en iFrame med innehåll. Exempelvis kan man använda JavaScript för att skapa en ny webbläsarflik istället för statisk HTML-kod. I det fallet får patientapplikationens JavaScript en referens till den flik som 1177 Vårdguiden visas i, på samma sätt som att JavaScript alltid kan få en referens till den iFrames som 1177 visas i.

Det finns således mycket små skillnader mellan HTML-koden för att öppna länken i en ny flik eller att öppna den i en iFrame. Av särskilt intresse är dock att HTML-koden endast kan tillhandahålla en länk till 1177 Vårdguiden och att informationen från 1177 levereras direkt till användarens webbläsare utan att passera patientapplikationens server.

Frågan är dock vilka möjligheter som patientapplikationen har att använda JavaScript i webbläsaren för att skapa, läsa eller ändra information på en webbsida som den har länkat till, samt om det är några skillnader i JavaScript-kodens möjligheter eller begränsningar med avseende på om innehållet visas i en iFrame eller i en ny webbläsarflik.

7.2.3 JavaScript i webbläsare

JavaScript är ett scriptspråk som alla webbläsare kan förstå och exekvera. All JavaScript-kod som är skriven mellan två `<script>`-taggar i ett HTML-dokument kommer att exekveras i webbläsaren enligt det regelverk som finns för JavaScript och webbläsare.

Modellen för JavaScript bygger på att det finns ett globalt objekt kallat `Window`, som representerar det webbläsarfönster som scriptet körs i. `Window`-objektet tillhandahåller funktioner och attribut som behöver vara globalt tillgängliga för ett JavaScript, [2]. Framför allt

så tillhandahåller `Window`-objektet ett attribut kallat `document` som innehåller ett s.k. DOM Document Object som representerar det dokument som är laddat i webbläsarfönstret, [3]. I den minimala prototyp som presenterades i förra kapitlet så representerar `document`-objektet den HTML-kod som bl.a. innehåller länken till 1177 Vårdguiden.

I en webbläsare med flikar, vilket de flesta moderna webbläsare har idag, så representeras varje flik av sitt eget `Window`-objekt. Ett JavaScript som körs i en flik har alltid tillgång till det `Window`-objekt som representerar den flik som JavaScriptet körs i. Även en iFrame i ett HTML-dokument representeras av ett eget `Window`-objekt. Det innebär att en ny webbläsarflik och en iFrame behandlas på samma sätt av webbläsaren, d.v.s. som ett eget `Window`-objekt.

Ett JavaScript som exekveras i en HTML-sida som innehåller en iFrame eller där JavaScriptet skapar en ny webbläsarflik kan skapa en referens till det `Window`-objektet som representerar iFramen respektive den nya fliken. Vilka möjligheter har JavaScriptet att läsa eller ändra i dessa `Window`-objekt och deras tillhörande `Document`-objekt?

Dessa användningsfall hanteras av en regel som kallas *Same-origin policy*, [4]. Webbläsare som följer detta regelverk, vilket alla moderna webbläsare gör, ger endast JavaScript från ett webbläsarfönster (t.ex en flik) full åtkomst till ett `Window`-objekt i ett annat webbläsarfönster (t.ex. en iFrame eller en annan flik) om dokumentet i respektive fönster har laddats från samma plats.

I exemplet med den minimala prototypen så innebär det att HTML-koden som visas i bild 5 och 6 måste laddas från samma webbserver som 1177 vårdguiden, för att eventuella JavaScript i dessa HTML-dokument ska få tillgång till data från 1177, oavsett om patientöversikten från 1177 visas i en iFrame eller en ny flik.

Eventuella JavaScript i dessa HTML-dokument har dock en begränsad tillgång till `Window`-objekten i den iFrame eller den flik som har laddats från https://e-tjanster.1177.se, men det handlar om funktioner och attribut som inte anses vara direkt relaterat till informationsinnehållet, [5].

7.2.4 Slutsats

Frågan som skulle besvaras var om samma juridiska tolkning kan göras oavsett om den nationella e-tjänsten visas i en ny webbläsarflik eller i en iFrame. Detta kapitel har därför gjort en detaljerad teknisk genomgång för att påvisa att även om dessa lösningar ser grafiskt olika ut så behandlas de tekniskt på samma med avseende på patientapplikationens möjligheter att läsa, förändra eller på andra sätt bearbeta informationen som e-tjänsten erbjuder till användaren. Dessa två lösningsvarianter bör därför rimligen även kunna bedömas på samma sätt ur ett juridiskt perspektiv.

7.3 Cookies

Om en användare väljer att logga in på 1177 Vårdguiden i den minimala prototyp av en patientapplikation som presenterades i förra kapitlet så uppstår det problem med iFrame-lösningen.

Nedan visas vad som händer när användaren klickar på länken för att ”logga in” till 1177 Vårdguiden i den prototyp som öppnar en ny flik i webbläsaren för 1177 Vårdguiden:

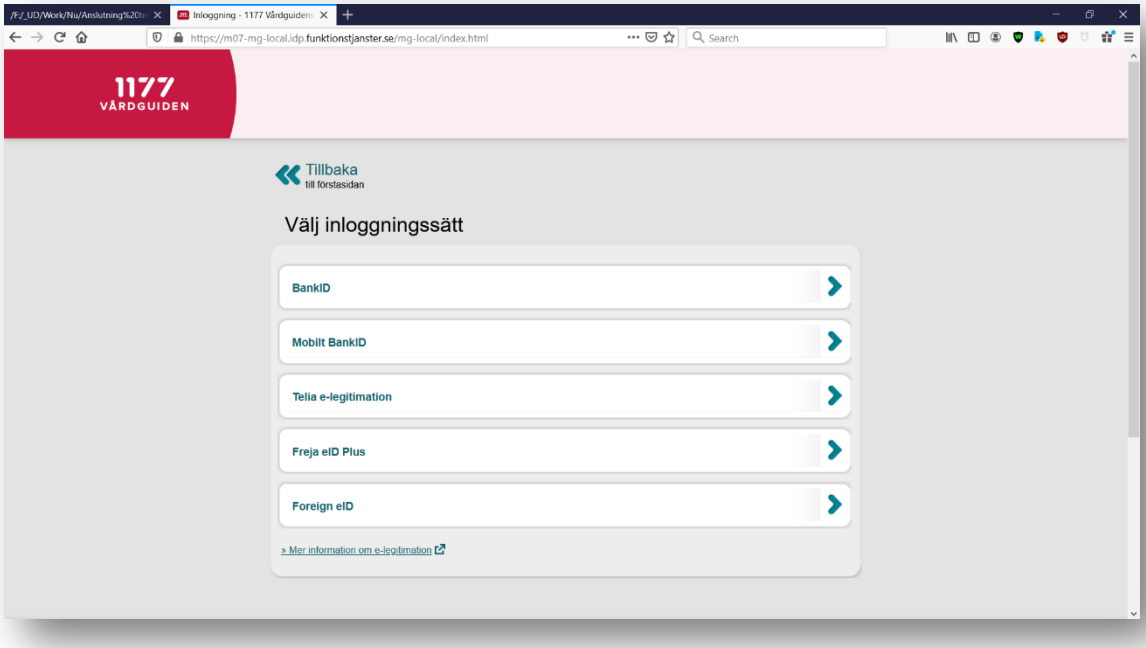


BILD 7

Bilden visar att användaren skickas till 1177 Vårdguidens sida för att välja inloggningsmetod.

I nästa bild visas vad som händer när användaren klickar på länken för att ”logga in” till 1177 Vårdguiden i den prototyp som istället använder en iFrame:

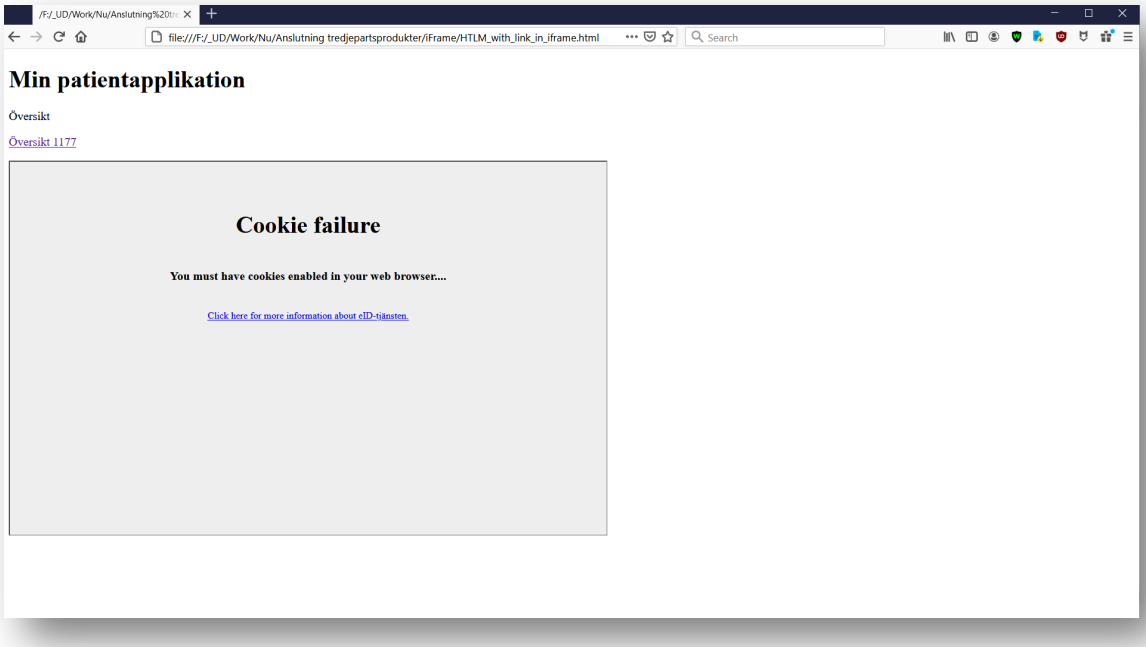


BILD 8

Istället för att skickas till 1177 Vårdguidens sida för att välja inloggningsmetod så visas ett felmeddelande som säger ”Cookie failure” samt ”You must have cookies enabled in your web browser”.

För att förstå orsaken till felmeddelandet och eventuella möjligheter att lösa problemet är det viktigt att ha en grundläggande förståelse för hur cookies fungerar.

7.3.1 Vad är en Cookie?

En cookie är data som kan sparas hos en webbläsare enligt specifikationen ”RFC6265bis-03”, [7]. Syftet är att göra det möjligt för HTTP-servrar att lagra tillstånd hos klienter, eftersom HTTP-protokollet i huvudsak är tillståndslöst.

En server kan instruera en webbläsare att spara en cookie genom att använda HTTP-headern `Set-Cookie`. Om webbläsaren stödjer cookies så kommer den att spara denna cookie och skicka med den till HTTP-servern i varje framtida förfrågan till servern.

Nedan visas hur en webbläsare skickar sin första förfrågan till webbplatsen `www.exempel.se`:

```
GET /index.html HTTP/1.1
Host: www.exampel.se
...
```

Webbplatsens server svarar med att skicka tillbaka det efterfrågade HTML-dokumentet (dokumentet visas ej i nedanstående utskrift) men skickar samtidigt med en instruktion om att spara två cookies i webbläsaren:

```
HTTP/1.0 200 OK
Content-type: text/html
Set-Cookie: nisse=xyz
Set-Cookie: sessionToken=abc123; Expires=Wed, 28 Jul 2021 12:00:00 GMT
...
```

De två cookies som visas ovan har namnen `nisse` respektive `sessionToken`. Varje namn har även ett associerat värde, i ovanstående exempel är det `xyz` respektive `abc123`. En cookie kan även ha ett antal attribut som finns definierade i ”RFC6265bis-03”, [7]. I ovanstående exempel används attributet `Expires` som anger när webbläsaren ska radera denna cookie. `nisse` har inte detta attribut och ska därför rensas bort av webbläsaren när användaren stänger webbläsaren.

Därefter frågar webbläsaren efter en sida som kallas `page1.html`. Webbläsaren skickar då med de två cookies som sattes av HTTP-servern för den aktuella webbplatsen. Attributen för en cookie skickas däremot aldrig med:

```
GET /page1.html HTTP/1.1
Host: www.exampel.org
Cookie: nisse=xyz; sessionToken=abc123
…
```

Cookies kan även läsas, skrivas och raderas med hjälp av JavaScript i webbläsaren. JavaScript använder då attributet `document.cookie`.

Ovanstående två cookies kan skapas av JavaScript i webbläsaren på följande sätt:

```
document.cookie = "nisse=xyz";
document.cookie = "sessionToken=abc123; Expires=Wed, 28 Jul 2021
12:00:00 GMT";
```

De kan läsas av JavaScript på följande sätt:

```
var x = document.cookie;
```

Resultat av ovanstående operation blir en sträng som innehåller alla cookies för den aktuella webbplatsen:

```
"sessionToken=abc123; Expires=Wed, 28 Jul 2021 12:00:00 GMT";
```

Precis som i fallet med HTTP-protokollet så får JavaScript inte tillgång till attributen i en cookie. Det går även att förhindra att JavaScript får tillgång till en cookie genom att sätta attributet `HttpOnly`. Denna flagga signalerar till webbläsaren att denna cookie endast ska skickas med i HTTP-anrop och inte får läsas av JavaScript.

Cookies är alltid är kopplade till en domän, och vissa fall även en sökväg inom denna domän, för att förhindra att webbplatser får tillgång till cookies som de inte borde. En server kan ange vilken domän en cookie hör till genom att använda attributet `Domain`, [8], men webbläsaren kommer bara att acceptera domäner som inkluderar värd-adressen för den server som vill sätta en cookie.

Exempelvis kommer en webbläsare att acceptera en cookie med `Domain=exemple.com` eller `Domain=foo.example.com` från en server med adressen `foo.exemple.com`, men webbläsaren kommer inte att acceptera `Domain=bar.example.com` eller `Domain=baz.foo.example.com`. Om `Domain`-attributet *inte* är angivet så returnerar webbläsaren endast cookies till den ursprungliga servern.

`Domain`-attributet anger vilken värddator som en cookie ska returneras till och regelverket följer här samma princip som `SameSite`-attributet (se nästa kapitel). Exempelvis, om värdet för `Domain`-attributet är `exemple.com`, så kommer webbläsaren att skicka med denna cookie i en HTTP-förfrågan till `example.com`, `www.example.com` och `www.corp.example.com`.

På liknande sätt kan `Path`-attributet användas för att begränsa en cookies användning till att endast gälla vissa kataloger på en server, [9].

När JavaScript skapar, läser eller raderar cookies gäller samma regelverk. Det är den HTML-sida som laddade JavaScriptet som styr vilken domän en cookie kan tillhöra.

7.3.2 Påverkan på iFrame-lösningen

Tidigare har huvudregeln varit att en cookie alltid ska skickas med av webbläsaren vid en förfrågan till en HTTP-server med en URL som matchar regelverket för `Domain`-attributet och `Path`-attributet. Detta beteende ändrades dock med införandet av ett nytt cookie-attribut kallat `SameSite` (specificerat i *RFC6265bis*, [6]).

Cookie-attributet `SameSite` styr om tredjeparts-cookies ska skickas med vid en förfrågan från webbläsaren till den server som har skapat en tredjeparts-cookie. Lite förenklat kan man säga att förstaparts-cookies är cookies vars `Domain`-attributet är en del av den URL som visas i webbläsarens adressfält. Alla andra cookies är tredjepartscookies.

Något mer formellt så ska den aktuella webbplatsen och cookiens `Domain`-attributet ha samma toppdomän (även kallat nivå 1, exempelvis .com, .se, .nu) och samma domännamn på nivå 2 (namnet som står före toppdomänen) för att cookien ska betraktas som förstaparts-cookie. Exempel:

`www1.web.dev` och `www2.web.dev` tillhör samma webbplats.

`www.web1.dev` och `www.web2.dev` tillhör olika webbplatser.

Med hjälp av cookie-attributet `SameSite` kan en webbplats styra om deras cookies ska skickas med i en förfrågan när de betraktas som tredjepartscookies. Ett exempel är om webbsiten `www.exempel.se` innehåller bilder från `www.bilder.se`. Om webbplatsen `www.bilder.se` har sparat cookies i webbläsaren sedan tidigare så betraktas dessa cookies som tredjeparts-cookies när användaren besöker webbplatsen `www.exempel.se`. Beroende på vilket värde webbplatsen `www.bilder.se` har gett till `SameSite`-attribuet så kommer deras cookie antingen att skickas med i förfrågan eller blockeras av webbläsaren.

Attributet `SameSite` kan ha värdet `Strict`, `Lax` eller `None`. Dessa värden har följande innebörd:

- `SameSite=Strict`: En cookie med detta attribut skickas endast med i en förfrågan till sin HTTP-server när den betraktas som en förstaparts-cookies, d.v.s. när cookiens `Domain`-attributet är en del av en URL som står i webbläsarens adressfält.
- `SameSite=Lax`: Samma som `SameSite=Strict`, men webbläsaren skickar även med cookies när användaren navigerar till en ny webbplats toppnivå (.com, .se, etc.). Exempelvis om användare befinner sig på webbplats `www.exempel.se` och klickar på en länk till `http://www.annatexempel.se/` så skickas cookies med som `http://www.annatexempel.se/` har sparat sedan tidigare besök på deras webbplats. Om cookies från `http://www.annatexempel.se/` är märkta med `SameSite=Strict` så kommer de inte att skickas med.

  Cookies skickas endast med när navigeringen görs med säkra metoder som t.ex. HTTP `GET` (t.ex. med en standard `<a href=...>` länk), men inte om `POST` används. Cookies skickas inte heller med när navigeringen görs till en iFrame som inte tillhör samma webbplats, d.v.s. den URL som visas en iFrame är inte en del av den URL som står i webbläsarens adressfält.
- `SameSite=None`: Cookies med detta attribut skickas alltid med i en förfrågan till sin HTTP-server, d.v.s. de fungerar på samma sätt som cookies har fungerat tidigare. IETF har även föreslaget att cookies som använder `SameSite=None` även måste sätta

attributet `Secure` vilket innebär att dessa cookies endast får skickas över en säker anslutning (HTTPS). Denna regel implementeras numera av de flesta webbläsare.

Attributet kan också utelämnas helt, vilket i de senaste versionerna av Chrome och Firefox leder till att webbläsaren behandlar förfrågan på samma sätt som om `SameSite=Lax`. Standarbeteendet var tidigare att behandla förfrågan som om `SameSite=None`.

Detta är förmodligen förklaringen till varför lösningen med att öppna en ny flik för att logga in på 1177 Vårdguiden fungerar, men inte lösningen med iFrame. 1177 Vårdguiden har troligen inte satt något värde på `SameSite`-attributet, vilket innebär att webbläsaren sätter standardvärdet `SameSite=Lax`. Enligt beskrivningen ovan så medför det att webbläsaren *inte* skickar tillbaka en cookie till 1177 Vårdguiden när den webbplatsen visas i en iFrame som tillhör en annan webbplats. 1177 Vårdguiden tolkar detta som att användaren har stängt av användning av Cookies i webbläsaren, därav felmeddelandet.

Lösningen för att få iFrame-lösningen att fungera i moderna webbläsare är att 1177 Vårdguiden sätter cookie-attributen `SameSite=None` och `Secure` på sina cookies. Det innebär att cookies fortsätter att hanteras på samma sätt som idag, men ger samtidigt inte det extra skydd som man kan få genom att använda `SameSite=Lax`. Nästa kapitel ska därför titta närmare på vad detta innebär ur ett IT-säkerhetsperspektiv.

Värt att nämnas är att även mobilapplikationer som använder en WebView-komponent, eller en så kallad Integrated In-App Browser (IIAB), kommer att fungera på ungefär samma sätt som en iFrame och kräver därför också att cookie-attributen `SameSite=None` och `Secure` används av 1177 Vårdguiden.

7.3.3 Säkerhetsaspekter

Det hot som införandet av cookie-attributet `SameSite` främst försöker att skydda mot är Cross-Site Request Forgery (CSRF). EN CSRF-attack går ut på att lura en användare att skicka en förfalskad HTTP-förfrågan till en webbplats, tillsammans med en cookie som identifierar användaren.

Ett exempel är om användaren är inloggad hos sin bank och sedan surfar till en annan webbplats som attackeraren kontrollerar. Attackerarens webbplats innehåller en falsk bild-tag med storleken 0x0 som skickar en förfrågan till användarens bank istället för att ladda en bild:

```
<img src =
"http://bank.se/app?action=transferFunds&amount=1000&destinationAccoun
t=attackersAccountNNNN" width = "0" height = "0" />
```

Eftersom användaren redan är inloggad hos sin bank så skickas en cookie med som identifierar användaren, varvid transaktionen som definieras i URL-förfrågan genomförs.

Cookie-attributet `SameSite` är ett instrument för att förhindra CSRF-attacker. I ovanstående exempel skulle attacken inte lyckas om banken hade markerat sin cookie med `SameSite=Strict` eller `SameSite=Lax`. Däremot skulle attacken lyckas om bankens cookie markerades med `SameSite=None` och `Secure`, vilket motsvarar hur cookies fungerar idag.

Enligt förra kapitlet behöver 1177 Vårdguiden sätta cookie-attributen `SameSite=None` och `Secure` på sina cookies för att iFrame-lösningen ska fungera. Det innebär att 1177 Vårdguiden

behöver använda andra metoder för att skydda sig mot CSRF-attacker. Ett antal olika metoder finns beskrivna på webbplatsen för Open Web Application Security Project, OWASP, och deras sida om CSRF [10].

Man bör dock komma ihåg att CSRF-attacker syftar till att åstadkomma en tillståndsförändring hos webbplatsens server, t.ex. ändra användarens mejl-adress eller lösenord. Attacken syftar *inte* till att hämta eller läsa data eftersom den som utför attacken inte är mottagare för svaret på HTTP-förfrågan. Det är användarens webbläsare som tar emot svaret.

En möjlig lösning, utöver de som beskrivs av OWASP, är därför att tillhandahålla anpassade vyer av 1177 Vårdguiden som kan användas av en iFrame-lösning. Tanken är att dessa vyer endast ska tillhandahålla information för läsning och inte erbjuda några möjligheter att ändra på användaruppgifter eller annan data. En sådan vy kan tillåta tredjeparts-cookies utan risk för att drabbas av skadliga CSRF-attacker, även utan några andra åtgärder.

7.4 Mobilapplikationer

Alla presenterade lösningar är tänkta att nyttjas även av mobilapplikationer. Detta kapitel innehåller en kortfattad beskrivning av de huvudsakliga implementationsvarianterna. Kapitlets huvudsyfte är dock att göra en djupare analys av lösningsmönstret i kapitel 2.6 ”Hämta samlad patientinformation 1d” ur ett juridiskt perspektiv när mönstret realiseras av en mobilapplikation.

En analys av lösningsmönstret i kapitel 2.6 ”Hämta samlad patientinformation 1d” när det realiseras som en webbapplikation och med fokus på iFrame-varianten har redan gjorts i ett tidigare kapitel. Detta kapitel undersöker om samma slutsatser även gäller för en mobilapplikation.

Utgångspunkten är att patientens åtkomst till sin journalinformation från andra vårdgivare än den vårdgivare som tillhandahåller patientapplikationen kan betraktas som enskilds direktåtkomst om vårdgivarens applikation inte behandlar personuppgifterna som kommer från andra vårdgivare. Om lösningen uppfyller detta villkor så är den godkänd ur ett juridiskt perspektiv.

7.4.1 Huvudsakliga implementationsvarianter

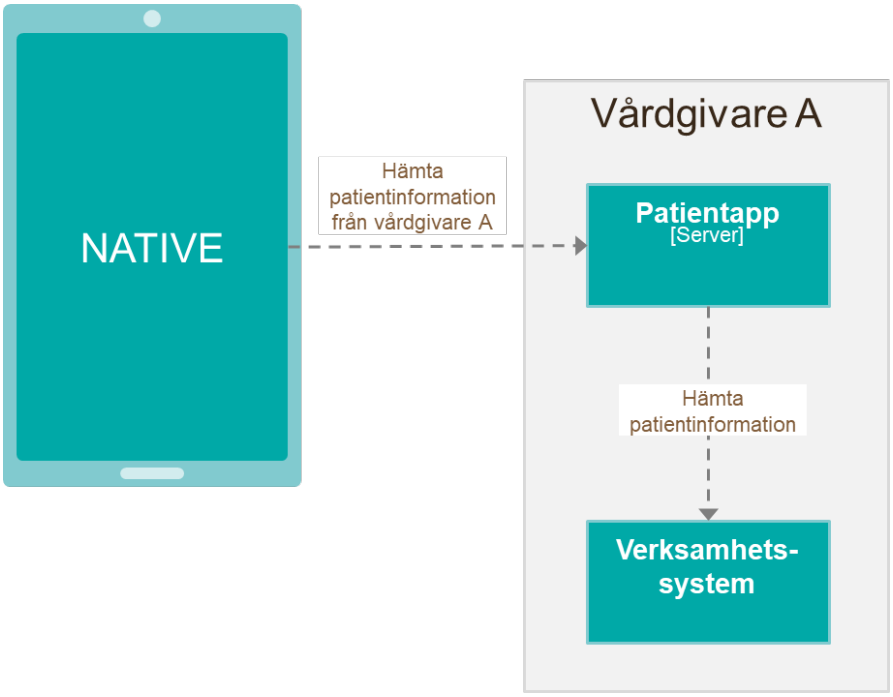
En mobilapplikation kan realiseras på flera olika sätt. Följande tabell presenterar huvudkategorierna:

Typ	Beskrivning	Tillgång till mobilens API	Distribueras via App Stores	Plattforms-oberoende
Native app	En app som är skriven i ett programspråk som är kompatibelt med mobilens operativsystem (t.ex. Objective	Ja	Ja	Nej

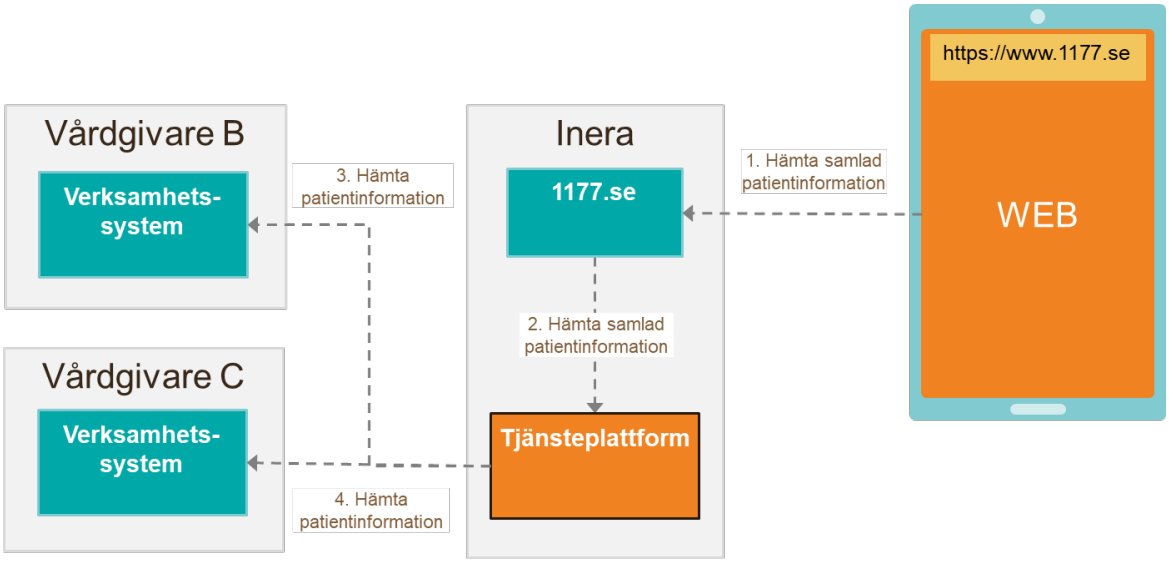
	C för iOS och Java för Android)			
Hybrid-app	En native-app som även nyttjar en webbläsar-komponent som är inbäddad i applikationen	Ja	Ja	Beror på hur mycket native-kod som används
Webb-app	Egentligen inte en mobil-applikation utan snarare en webbplats som är implementerad så att den kan ge en liknande användar-upplevelse som en nativ- eller hybrid-app.	Delvis. Samma begränsningar som för en webbläsare	Eventuellt. Kräver att bl.a. kriterier för användbarhet är uppfyllda, vilket är fullt möjligt att åstadkomma med HTML 5. Applikationen ska fungera som de flesta appar (gester m.m.) och kunna hantera att mobilen tidvis kan vara bortkopplad från internet.	Ja

7.4.2 Native app

En native-app är troligen inte aktuell för lösningsmönstret i kapitel 2.6 ”Hämta samlad patientinformation 1d” eftersom det mönstret bygger på att en nationell e-tjänst nyttjas, vilket i sin tur kräver en webbläsare. Däremot så går det att utmärkt att bygga en native-app för att visa patientinformation från den vårdgivare som har upphandlat applikationen och troligen även integrerat den med sitt verksamhetssystem:



En native-app kan dock välja att öppna en URL till 1177 Vårdguiden i mobilens standardwebbläsare, men det är inte troligt att appleverantören är intresserad av att användaren lämnar deras vårdapp för att kunna se sin översikt. Ur ett IT-säkerhets och juridiskt perspektiv så är dock en sådan lösning önskvärd eftersom det helt och fullt motsvarar att användaren klickar på en länk till 1177 Vårdguiden som leder till att en ny webbläsarflik öppnas.

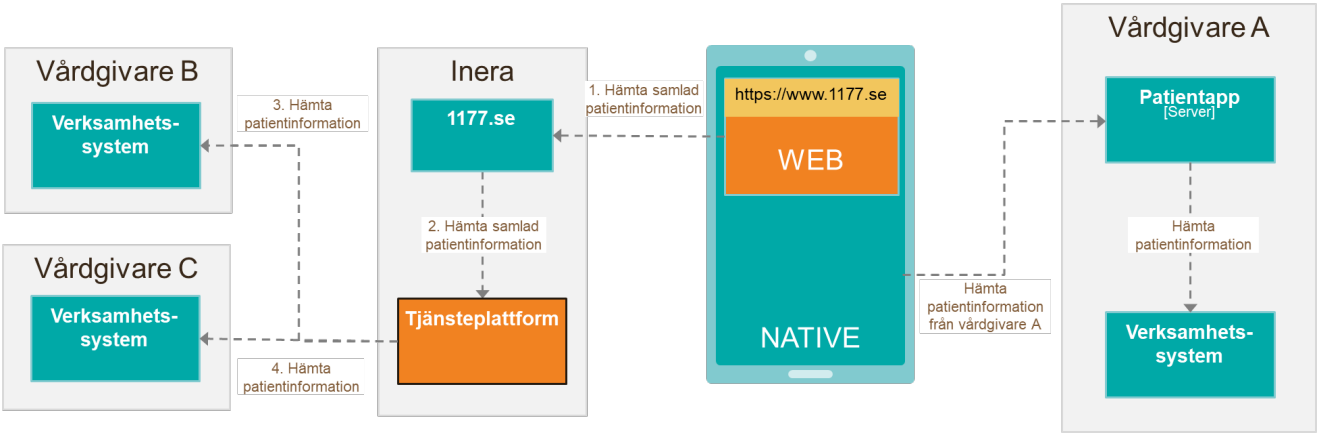


En native-app kan således inte implementera en iFrame-lösning, däremot så kan den öppna en URL till 1177 Vårdguiden i mobilens standardwebbläsare. I det fallet sker all kommunikation från 1177 Vårdguiden direkt till mobilens webbläsare och vårdgivarens applikation behandlar

därför inga personuppgifter från andra vårdgivare. Användningen kan därför betraktas som enskilds direktåtkomst och bör därmed vara godkänd ur ett juridiskt perspektiv.

7.4.3 Hybrid app

En hybrid-app kan relativt enkelt implementera lösningsmönstret i kapitel 2.6 ”Hämta samlad patientinformation 1d” genom att använda en så kallad WebView för att visa webbrelaterat innehåll. WebView finns både för iOS (Apple) och Android (övriga mobiltillverkare) och är en komponent som fungerar som en inbäddad webbläsare i appen, dock utan alla de menyer och knappar som en normal webbläsare erbjuder.



En WebView-komponent förhåller sig till en native-app på ungefär samma sätt som en iFrame förhåller sig till en webbsida. De är därför troligt att hanteringen av cookies kräver samma åtgärder som för en iFrame, d.v.s. 1177 Vårdguiden måste sätta cookie-attributen `SameSite=None` och `Secure` för att kunna nyttja cookies i en WebView i en hybrid-app som inte har publicerats av 1177 Vårdguiden själv.

Skillnaden mot iFrame-lösningen ligger bl.a. i att JavaScript som exekveras i en WebView har större möjligheter att göra anrop direkt till operativsystemets underliggande API jämfört med en webbläsare samt att det är appleverantörens ansvar att bygga eventuella användarmenyer och navigeringsmöjligheter till en WebView, vilket normalt sett tillhandahålls av en webbläsare.

Inget av detta är ett problem ur ett juridiskt eller IT-säkerhetsperspektiv i detta specifika fall, däremot så kan det vara ett problem att säkerhet runt en WebView generellt sett är sämre än motsvarande säkerhetsramverk i en Webbläsare. I en WebView har exempelvis native-appen tillgång till de JavaScript som körs i en WebView. Detta går delvis att åtgärda med hjälp av olika konfigureringar, men det är helt upp till appleverantören att införa dessa begränsningar.

En bättre lösning är att använda en så kallad Integrated In-App Browser (IIAB) där Chrome erbjuder Chrome Custom Tabs (CCT) för Android och Safari erbjuder Safari ViewController (SFSVC) på iOS. Denna teknik gör det möjligt för en native-app att öppna en URL i en webbläsare inuti appen, men där den integrerade webbläsaren fungerar i stort sett som standardwebbläsaren på mobilen. Denna lösning erbjuder betydligt bättre säkerhet där native-appen tillgång till information samt de JavaScript som exekveras i en IIAB styrs av samma regelverk som ett HTML-dokuments tillgång till en iFrame. Denna lösningen är därför betydligt

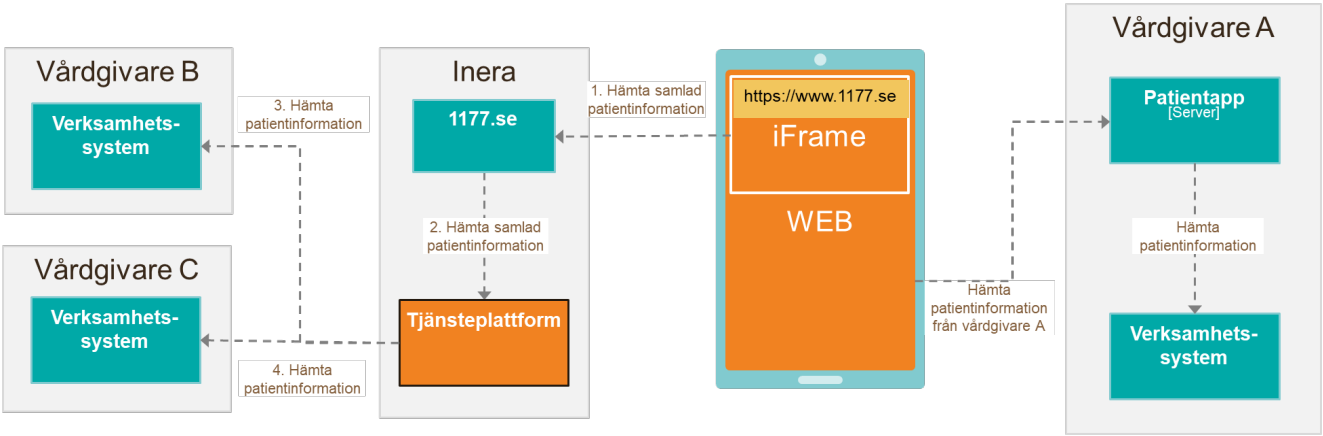
bättre och också mer lik en normal iFrame-lösning, både ur ett IT-säkerhetsperspektiv och ur ett juridiskt perspektiv.

Lösningen med WebView är svårbedömd både ur ett IT-säkerhetsperspektiv och ur ett juridiskt perspektiv eftersom säkerheten och skyddet runt en WebView är sämre än i en webbläsare. Möjligen skulle man kunna tillåta denna typ av implementering om det finns en fungerande certifieringsprocess med kodgranskning, men en effektivare lösning är att ställa krav på att en IIAB används.

Om en IIAB används så kan man betrakta skyddet för att otillåtet läsa eller ändra informationen som likvärdigt det som tidigare beskrevs för en iFrame-lösning. Man kan välja att betrakta den integrerade webbläsaren (IIAB) som en del av vårdgivarens applikation eller som en extern komponent, men oavsett vilket så gäller att all kommunikation från 1177 Vårdguiden går direkt till den integrerade webbläsaren med alla de begränsningar som tidigare har beskrivits när det gäller native-appens möjligheter att läsa eller ändra innehållet. Vårdgivarens applikation behandlar därför inga personuppgifter från andra vårdgivare. Användningen kan därför betraktas som enskilds direktåtkomst och bör därmed vara godkänd ur ett juridiskt perspektiv.

7.4.4 Webbapp

Den tredje huvudvarianten, som kallas för webbapp i ovanstående tabell, är helt identisk med lösningsmönstret i kapitel 2.6 ”Hämta samlad patientinformation 1d” eftersom detta egentligen inte är en mobilapp utan en webbplats som har byggs med hjälp av webbteknik som även erbjuder en upplevelse på en mobiltelefon som motsvarar den upplevelse som en native- eller hybrid-app kan erbjuda.



En webbapp kan dock implementeras på flera olika sätt, allt från en gammaldags, servertung webbplats, till en modern, klienttung Single-Page App (SPA) eller en Progressiv Web Application (PWA). En PWA är, mycket förenklat, en modern webbapplikation (SPA) som även har inbyggda möjligheter att hantera avbrott från Internet och gester på en mobil.

För att kunna publiceras via en App Store, t.ex. Apple App Store eller Google Play Store, så krävs många av de egenskaper som förknippas med en PWA. En gammaldags, servertung webbplats får t.ex. svårt att hantera kravet på att även kunna användas vid avbrott mot internet.

Man bör dock komma ihåg att regelverket för en App Store mer kan ses som riktlinjer än hårda regler.

Oavsett val av teknik för en webbapp så gäller dock resonemanget runt IT-säkerhet och juridik från tidigare kapitel, d.v.s. detta är en webbapplikation som exekveras på en mobiltelefon och all kommunikation från 1177 Vårdguiden går direkt till en iFrame eller en flik i mobilens webbläsare med alla de begränsningar som tidigare har beskrivits när de gäller webbapplikationens möjligheter att läsa eller ändra innehållet. Vårdgivarens applikation behandlar därför inga personuppgifter från andra vårdgivare. Användningen kan därför betraktas som enskilds direktåtkomst och bör därmed vara godkänd ur ett juridiskt perspektiv.

8. Referenser

Referens	Dokument
1	AOR-1915 – Konsumentåtkomst till engagemangsindex https://inera.atlassian.net/wiki/spaces/AOR/pages/231541075/AOR-1915+-+Konsument+tkomst+till+engagemangsindex+EI
2	The Window Object https://www.w3schools.com/jsref/obj_window.asp
3	The HTML DOM Document Object https://www.w3schools.com/jsref/dom_obj_document.asp
4	Same-origin policy https://en.wikipedia.org/wiki/Same-origin_policy
5	Same-origin policy https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy
6	Same-Site Cookies, draft-ietf-httpbis-cookie-same-site-00 https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site-00
7	Cookies: HTTP State Management Mechanism, draft-ietf-httpbis-rfc6265bis-03 https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-03
8	Cookies: HTTP State Management Mechanism: 4.1.2.3. The Domain Attribute https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-03#section-4.1.2.3
9	Cookies: HTTP State Management Mechanism: 4.1.2.4. The Path Attribute https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-03#section-4.1.2.4
10	OWASP, Cross Site Request Forgery (CSRF) https://owasp.org/www-community/attacks/csrf
11	Device fingerprint

	https://en.wikipedia.org/wiki/Device_fingerprint

9. Termer och förkortningar

Term	Beskrivning
NTjP	Nationella Tjänsteplattformen
TAK	Tjänsteadresseringskatalogen