VINNOVA
Sveriges innovationsmyndighet

Peder Blomqvist, +46 8 473 3205
peder.blomqvist@vinnova.se

2021-03-21
Dnr: 2021-01543_13

Vinter

REFERENSARKITEKTUR FÖR INFRASTRUKTUR

Vinnova – Sveriges innovationsmyndighet
Mäster Samuelsgatan 56, 101 58 Stockholm // Tel: 08 473 30 00 // vinnova.se

Fakturaadress: Vinnova, FE 34, 838 73 Frösön
Leveransadress: Klara Norra Kyrkogata 14
Organisationsnummer: 202100-5216

Dokumentnamn: Vinnova_Vinter_Ramverksvolym_4.2_v6_Referensarkitektur för Infrastruktur

Peder Blomqvist, +46 8 473 3205
peder.blomqvist@vinnova.se

2021-03-21
Dnr: 2021-01543_13

Introduktion till dokumentet

Syfte

Detta dokument beskriver den referensarkitektur och de byggblock som gäller för tävlingskategorin Infrastruktur i Vinter. Syftet är att ge tävlingsdeltagare förståelse för de byggblock som bygger upp en önskvärd infrastrukturlösning för hälso- och sjukvården.

Målgrupp

Målgruppen för dokumentet är projektledare, arkitekter och utvecklare som behöver förstå hur referensarkitekturen är uppbyggd. Även jurister, tävlingens jury och andra intressenter kan ha nytta av dokumentet för att förstå hur den tekniska miljön kan byggas upp samt hur säkerhetsfunktionerna behöver samverka med tekniken för att klara de legala kraven på hantering och lagring av sekretessbelagda hälsodata i en framtida nationell infrastruktur för hälso- och sjukvårdsdata

Omfattning

Arkitekturen beskriver ett antal byggblock som möjliggör säkert informationsutbyte.

Begrepp och akronymer

Begrepp/Akronym	Betydelse	Källa
Arkitekturbyggblock (ABB)	En samling funktionalitet som syftar till att uppfylla verksamhetskrav. Varje byggblock är löst kopplat mot realiseringen av det, dvs varje byggblock kan realiseras på flera olika sätt.	TOGAF 9.2

Peder Blomqvist, +46 8 473 3205
peder.blomqvist@vinnova.se

2021-03-21
Dnr: 2021-01543_13

Innehåll

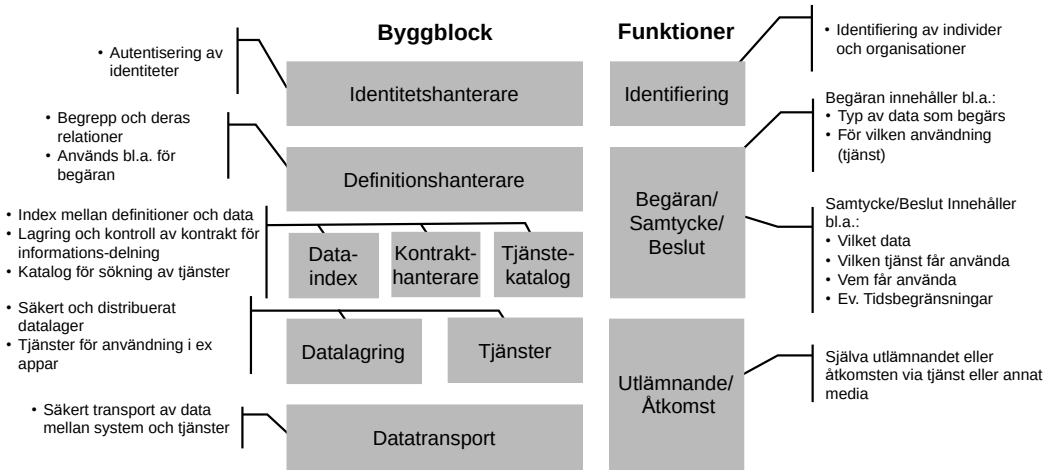
Peder Blomqvist, +46 8 473 3205
peder.blomqvist@vinnova.se

2021-03-21
Dnr: 2021-01543_13

Översikt

Referensarkitekturen är utformad för att stödja ett antal grundläggande funktioner som är nödvändiga för att åstadkomma ett säkert informationsutbyte som uppfyller de legala krav som ställs då hälso- och sjukvårdsdata ska delas.

Funktionerna och byggblocken som visas i bilden nedan beskrivs i mer detalj i kommande kapitel.



Tävlingsdeltagare kan tävla med att utveckla en eller flera delar av de olika byggblocken i referensarkitekturen.

Peder Blomqvist, +46 8 473 3205
peder.blomqvist@vinnova.se

2021-03-21
Dnr: 2021-01543_13

Verksamhetsbehov och lagrum

För att hälsodata ska kunna användas och därmed nyttiggöras, krävs att relevanta data finns tillgängliga och att dokumentationen gjorts på ett sådant sätt att data går att konsumeras både i ett primärt, men också sekundärt syfte.

Dokumentation i journal respektive till hälsodata- och kvalitetsregister som sker i samband med en vårdsituation görs vanligtvis inte med en tanke kring sekundäranvändning.

Den primära dokumentationen sker alltför sällan i strukturerad och standardiserad form. Däremot i form av fritext och/eller lokala/regionala eller diagnosspecifika standarder vilket försvårar/omöjliggör sammanställning och analys av data på ett effektivt och tillförlitligt sätt.

Det, i kombination med otydliga lagrum, är sannolikt bidragande orsaker till att hälsodata, i synnerhet från de nationella kvalitetsregistren, inte används i större utsträckning, varken i kvalitetsutveckling i hälso- och sjukvården eller för forskning.

Hälsodata som samlas in och dokumenteras i hälso- och sjukvården, regleras idag av Patientdatalagen respektive EU:s dataskyddsförordning som trädde i kraft i maj 2018. Hälsodata som samlas in av enskild medborgare och för eget bruk exempelvis via en app regleras via Dataskyddsförordningen i det läge som medborgaren väljer att dela sina data med exempelvis en vårdgivare.

Ett antal utredningar har inletts med anledning av de förändringar i lagstiftningen och som dataskyddsförordningen påverkar, exempelvis Rätt att forska – långsiktig reglering av forskningsdatabaser (SOU 2018:36) och Personuppgiftsbehandling för forskningsändamål (SOU 2017:50) respektive Framtidens biobanker (SOU 2018:4) däremot har det inte gjorts någon översyn gällande den existerande lagstiftningen i Patientdatalagen (2008:355) och den kompletterande patientdataförordningen (2008:360). Det är vidare ännu inte klart vilka förslag från utredningarna som kommer att resultera i förändrad lagstiftning.

Dataskyddsförordningen begränsar möjligheterna till en bred, prospektiv datainsamling. Det innebär att det inte finns stöd i förordningen att dokumentera och samla in uppgifter om det vid insamlingstillfället inte går att precisera hur, när och av vem uppgifterna ska användas i ett senare skede. Det gäller även om datainsamlingen sker med stöd av ett samtycke eftersom samtycket måste precisera just dessa frågor. I det fall som dokumentation och datainsamling sker med stöd av Patientdatalagen reglerar lagen för vilka ändamål som insamlade data kan användas samt vilken information som har stöd för att dokumenteras. Däremot, anges inte *hur* informationen ska dokumenteras (format/standard) och här finns det utrymme för förbättring utan krav på förändrad lagstiftning.

Peder Blomqvist, +46 8 473 3205
peder.blomqvist@vinnova.se

2021-03-21
Dnr: 2021-01543_13

Former av data

Ref: Mikael Hoffmann, stiftelsen NEPI – nätverk för läkemedelsepidemiologi har definierat ett antal typer av data som är tillämpliga inom hälsa, vård och omsorg.

I **identifierade data**, exempelvis journaldata, finns tydliga identifierare. Kan vara personnummer, namn & adress eller t ex löpnummer som av forskargruppen eller annan kan kopplas till en viss individ. Viktigt: sammanställning utan id men där det är enkelt att koppla till id är identifierade data.

Avidentifierade data är individdata där varje individ identifieras med pseudonym t ex löpnummer men där forskargruppen saknar nyckel som kopplar pseudonymen till en viss identifierad individ. Ett annat namn för avidentifierade data är pseudonymiserade data. Detta är inte anonyma data (!) eftersom bakvägsidentifiering ofta är möjlig.

Aggregerat data är när man har beräknat tex ett medelvärde eller ett totalvärde över en hel grupp och ur vilka man inte kan utläsa enskilda händelser eller individer. Det kan tex vara totalt försäljningsvärde eller ett medelvärde för ett blodprov.

Bakvägsidentifiering innebär möjlighet att genom detaljerade uppgifter på individnivå identifiera en, flera eller alla individer. Kan röra sig om datum för viss åtgärd vid viss enhet, flytt mellan 2 kommuner ett visst månadsskifte, ovanlig diagnos eller mycket hög ålder. *Pseudonymiserade data är därför INTE anonymiserade.*

Anonyma individdata är pseudonymiserade individdata där datamängden (fr a variabler) reducerats så kraftigt att bakvägsidentifiering inte är möjlig. Utlämnande enhet måste ha genomfört en menprövning av detta. Idag är det en begränsad efterfrågan av sådana datafiler men i framtiden kan sådana uttag komma att efterfrågas i högre grad för att bilda underlag för artificiell intelligens, AI.

Den typ av data som forskare samt Life science företag idag oftast efterfrågar är pseudonymiserade data. Detta får INTE kallas anonyma data för det är inte anonyma data. Datat får bara lämnas ut efter etisk prövning, bara användas för visst angivet ändamål och måste hanteras som det känsliga personregister det är där enskilda individer kan bakvägs identifieras.

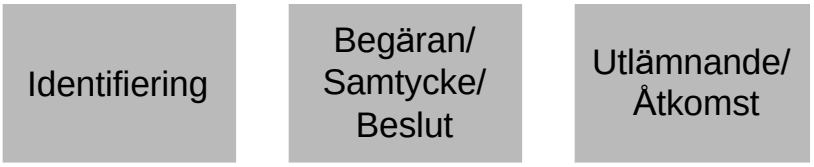
Applikationsfunktioner

Här beskrivs de applikationsfunktioner som måste finnas i en hälsodata infrastruktur. Dessa är utformade för att möjliggöra verksamhetsprocesser och förmågor inom alla verksamhetsområden. De funktioner som beskrivs här är alltså

Peder Blomqvist, +46 8 473 3205
peder.blomqvist@vinnova.se

2021-03-21
Dnr: 2021-01543_13

inte riktade mot någon speciell process eller förmåga utan är utformade för att uppfylla de lagkrav som finns för utlämnande och hantering av persondata.



Identifiering

Denna funktion säkerställer att individer och organisationer kan identifieras på ett korrekt sätt. En korrekt identifiering är en förutsättning för att kunna begära och lämna ut data så länge det inte är fråga om öppna data. Identifiering kommer alltså ske i alla tjänsteinteraktioner.

Begäran / Samtycke / Beslut

Här grupperas ett antal närbesläktade funktioner som syftar till att säkerställa att eventuellt utlämnande eller åtkomst till data är överenskommet på ett spårbart sätt. Man kan jämföra dessa funktioner med en avancerad behörighetsfunktion.
En begäran görs av den aktör som önskar få tillgång till data för ett visst syfte. Därmed måste en begäran alltså beskriva vem som begär data, vilket data som begärs och vilken tjänst som begäran avser.
En begäran hanteras av samtyckesfunktionen och resulterar i ett dokumenterat beslut i form av ett kontrakt (avtal) som beskriver vem som får åtkomst till vilket data och under vilka omständigheter, exempelvis under vilken tidsperiod åtkomst ska vara möjlig.
En annan form av kontrakt är ett samtycke där en individ frivilligt kan ge en organisation lov att behandla personuppgifter.
Observera att det också kan finnas andra skäl för en personuppgiftsansvarig att behandla personuppgifter vilket inte kräver ett samtycke eller avtal. Detta inkluderar bl.a. om det finns lagar eller regler som gör att uppgifterna måste behandlas eller om det ingår i en myndighetsuppgift.

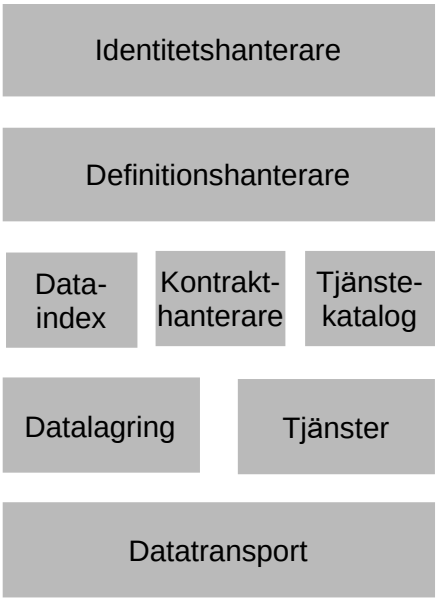
Utlämnande / Åtkomst

Denna funktion möjliggör överföring eller åtkomst till data i enlighet med de kontrakt som skapats genom ovanstående funktioner. Här skiljer man på utlämnande och åtkomst på det sätt att utlämnandet sker en gång och med en fördefinierad mängd data. Med åtkomst menas att data kan hämtas vid valfritt tillfälle och datamängden kan ändras. Exempelvis kan journalinformation ändras då nya inlägg i en patients journal skapas.

Peder Blomqvist, +46 8 473 3205
peder.blomqvist@vinnova.se

2021-03-21
Dnr: 2021-01543_13

Arkitekturbyggblock



Identitetshanterare

Detta byggblock hanterar identiteter för individer och organisationer. Här ingår livscykelhantering (skapande, uppdatering, borttagning) av identiteter och autentisering av identiteter då tjänster ska användas.

Autentisering (fastställande) av identiteter kan ske på flera olika sätt, exempelvis med tvåfaktorsautentisering (användarnamn/lösenord) eller multifaktorsautentisering.

Identitetshanteraren håller en unik identifierare på alla identiteter och kan också omfatta personinformation såsom namn, adress, telefonnummer etc. Detta gör det möjligt att använda identitetshanteraren i anonymiseringsscenarios.

Definitionshanterare

Detta byggblock hanterar begreppsdefinitioner och beskriver hur begrepp relaterar till varandra. Detta är viktigt för att säkerställa att olika aktörer har samma uppfattning om vad begrepp betyder.

Begreppsbetydelser är av vikt både när människor kommunicerar med varandra, men också för att säkerställa att exempelvis en begäran av dataåtkomst gäller rätt saker. Därmed är begreppshanteraren användbar både i ett utvecklingsstadium, när tjänster identifieras och designas, men kan också användas av tjänster i ett operativt skede.

Peder Blomqvist, +46 8 473 3205
peder.blomqvist@vinnova.se

2021-03-21
Dnr: 2021-01543_13

Dataindex

Syftet med detta byggblock är att skapa en länk mellan definitioner och faktiska instanser av data. Genom detta ges möjligheten att hitta data utifrån definitioner och tvärtom.

Möjligheten att hitta data genom att söka i definitioner är viktig i exempelvis en begäran. Frågaren kan genom definitioner beskriva vilket data som efterfrågas utan att i förväg ha tillgång till det. Därefter kan dataindexet svara på var data finns och en begäran kan skickas till en samtyckesfunktion för respektive tjänst som kan tillgängliggöra data.

Spårbarheten mellan definition och data kan vara känslig beroende på innehållet. Indexet är därför utformat att fungera antingen som ett fullt index med data eller som ett skikt mellan data och definition.

I det första fallet fungerar indexet som vilken sökmotor som helst. Data indexeras och görs sökbart. Denna metod är lämplig för öppen eller eventuellt avidentifierade data.

I det andra fallet innehåller indexet endast en referens till var data finns, men känner inte till själva datavärdena. Genom indexet kan man därmed förstå att det finns data för ett visst begrepp, men inte hämta själva datamängden. Det är alltså bara den som har access till datamängden som kan läsa den.

Det finns också ett tredje och ännu mer känsligt fall där det inte är lämpligt att meddela att det finns data över huvud taget. I denna situation används inte indexet.

Kontraktshanterare

Genom detta byggblock kan aktörer skapa och kontrollera kontrakt för informations- och datautbyte eller delning. Det kan finnas olika typer av kontrakt ur ett juridiskt perspektiv, exempelvis samtycke eller informationsutbytesavtal. Beroende på typen av kontrakt kan de se olika ut och hanteras på olika sätt, men i grunden består kontrakten av:

- Identiteter mellan vilka kontraktet upprättats (Avtalsparter)
- Definition av det data som kontraktet gäller
- Vilken eller vika tjänster kontraktet avser
- Vem som får använda tjänsterna
- Eventuella begränsningar, exempelvis tidsbegränsningar eller vad användaren får göra med datamängden som utlämnats.

Peder Blomqvist, +46 8 473 3205
peder.blomqvist@vinnova.se

Kontraktshanteraren är ett centralt byggblock för att implementera funktionerna Begäran, Samtycke och Beslut. Den stöttar även Utlämnande och Åtkomst genom att tjänsteproducenter kan kontrollera konsumenters rättighet att använda tjänsten.

Kontraktshanteraren använder sig också av identitetshanteraren för att verifiera identiteter på kontraktsparter och för att svara på om utlämnande/åtkomst får ske.

Tjänstekatalog

Detta byggblock innehåller en katalog av de tjänster som tävlingsdeltagare tillhandahåller. Respektive leverantör registrerar de tjänster som de vill tillgängliggöra vilket gör de sökbara för potentiella konsumenter.

Katalogen innehåller därmed tjänstebeskrivningar som utformats enligt Vinter Tjänstebeskrivningsramverk (Volym 4.1).

Tjänster

Detta arkitekturbyggblock är en sammanfattning av alla tekniska tjänster som realiseras i tävlingen. Tjänsterna är inte kända av organisatören från början, men beskrivs av leverantörerna enligt Vinter Tjänstebeskrivningsramverk (Volym 4.1) och lagras i tjänstekatalogen.

Datalagring

Detta byggblock representerar det datalager som respektive tjänst använder. Datalagret kan utformas som en enskild fysisk databas eller i distribuerad form beroende på tillgänglighetskrav mm.

Tävlingsvärdens datalagringstjänst

Tävlingsplattformen innehåller även ett generiskt datalager som kan användas för säker lagring och distribution av filer. Detta datalager är inte kopplat till någon specifik tjänst utan används då tjänster inte finns färdiga och för att utbyta tävlingsadministrativ information.

Enligt svensk lag måste en nationell lösning för datalagring av sekretessbelagd hälso- och sjukvårdsdata måste förutom de säkerhetskrav som ställs också innebära att den som levererar en säker lagringstjänst måste lyda under svensk lag, dvs vara ett helsvenskt företag, (ej internationellt ägda företag). Detta svenska företag får inte ha några som helst kopplingar till utländska underleverantörer eller ha dotterbolag etc som kan innebära att utländska myndigheter eller regeringar kan begära ut svensk hälsodata.

Företagets servrar måste också stå i Sverige, samt ju högre säkerhet man har i en lösning ex genom kryptering och hantering av kryptonycklar desto bättre är det, hanteringen av detta måste också med i regelverket för hanteringen av hälsodata.

Peder Blomqvist, +46 8 473 3205
peder.blomqvist@vinnova.se

2021-03-21
Dnr: 2021-01543_13

Datatransport

Detta byggblock består av standardiserade protokoll och mekanismer för IP-baserad kommunikation med transportskydd.

Kommunikation sker med förbindelser över internet mellan aktörer som deltar i tävlingen.