Mawell | more time to care

Nationell Listningstjänst

Software Architecture Document

skapad av:

Robert Georén

Version: 1.2

Datum: 2009-06-08

adress	telefon	e-post	organisationsnr
Mawell	+46 (0)8 527 400 00	contact@mawell.com	556582-5634
Solna Torg 3, 3 tr	**fax**	**hemsida**	
171 45 Solna	+46 (0)8 527 400 40	www.mawell.com	

Förändringar		
Vem	**När**	**Vad**
Robert Georén	2009-05-18	Version 1.0.
Robert Georén	2009-06-08	Lagt in synpunkter som inkommit ifrån Skåne, AL. Nytt användingsfall tillagt, ’Visa verksamhetsregler’. Version 1.1.
Robert Georén	2009-08-26	Bytte namn på vårdenhet till tjänsteutövare.
Robert Georén	2009-09-15	Ändrade psuedo-kod för ’byta tjänsteval’.v 1.2

Innehåll

1 Introduktion

Detta dokument är tänkt att beskriva hela arkitekturen för den nationella listningstjänsten. Dokumentet ska ge en god överblick på vad den nationella listningstjänsten är.

1.1 Definitioner och förkortningar

UP /RUP: Rational Unified Process.

UML: Unified Modeling Language.

SAD: Software Architecture Document.

HVAL: Husläkarval.

Micro SAD: En arkitekturbeskrivning som används som input för en SAD och för att kunna göra initiala beslut.

Källsystem: Regionala vårdvalssystem, kan t.ex. vara ListOn, Lissy eller Journalsystem.

AL: Arkitektur Ledningen

BIF: Bastjänster för Informations Försörjning, ingår i VIT-Boken

VIT-Boken: Verksamhet Informatik och Teknik boken, regelverk för hur bl.a. system arkitekturen ska se ut inom Vård och omsorgs.

SJUNET: VLAN För hög tillgänglighet och tillit.

13606: Standard för att kommunicera delar av/hela EHR(Electronic Health Record) för en patient

Commercial Application: Mått enligt MSDN (Microsoft) för när ett system har tillgänglighet på 99.5%.

Non-Commercial application: Mått enligt MSDN (Microsoft) för när ett system har tillgänglighet på 99%.

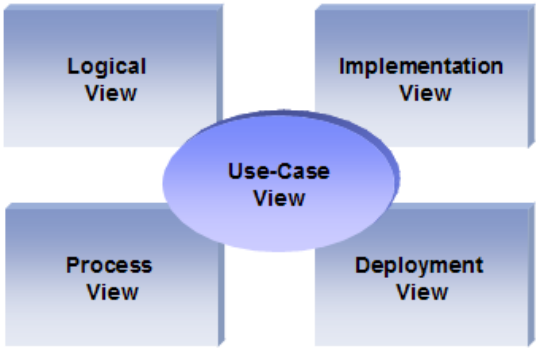
JupiterResearch: Undersökning som resulterade i att 4 sekunder är acceptabel svarstid för en websajt.

HTTP basic authentication: Användaren identifierar sig med namn och lösenord som skickas i HTTP headern till WebServices.
HTTPS mutual authentication: Både klient och server identifierar sig för varandra innan kommunikation etabiliseras (det handlar främst om ”trust”).
SSL: Secure Socket Layer används för att kryptera kommunikationen mellan två värdar.

SLA: Service Level Agreement. Används för att definiera krav på Anslutningspunkter.

2 Arkitektur representation

Detta dokument detaljerar arkitekturen med hjälp av vyer som definieras i “4+1” [KRU41] modellen, men använder sig av RUP namn.



3 Arkitekturella mål och begränsningar

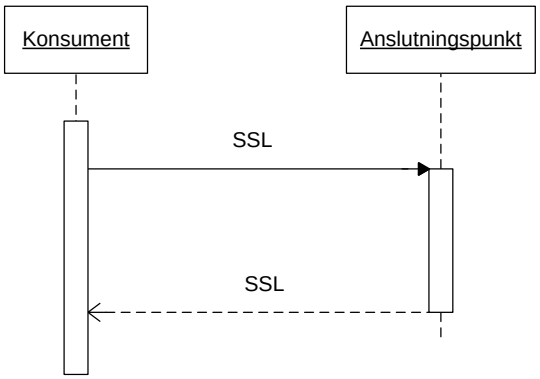
Detta avsnitt beskriver de icke-funktionella kraven som påverkar arkitekturen. Arkitekturen har för avsikt att följa VIT-boken.

3.1 Teknisk Plattform

Den principiella inriktningen är att använda open-source och Java plattformen på serversidan (detta i enlighet med 24-timmarsmyndigheten). Lokala avvikelser kommer att förekomma.

3.2 Säkerhet

Det finns två tjänster som hanterar säkerhet beskrivna i VIT boken, Authentiseringstjänsten och Åtkomstkontrolltjänsten. Dessa två säkerhetstjänster använder sig av en SAML biljett. Eftersom Åtkomstkontrolltjänsten ej är driftsatt ännu (beräknas till Maj 2010) så görs en tillfällig lösning tills att allt är klart. Den tillfälliga lösningen syftar till att hitta en så enkel lösning som möjligt men ändå uppfylla vissa grundläggande krav. Grundläggande krav är ”tillit” och säker kommunikation enligt VIT-boken.



** Beskriver hur grundläggande krav uppfylls med SSL.*

- Authentication (verifiera användarens identitet): Mellan konsument (ex. MVK) och Ansluntningspunktså används ett SSL server certifikat och ett klient certifikat (även kallat "HTTPS mutual authentication"). Detta eftersom det ger 1. en enkel tillfällig lösning och 2. passar bra med confidentiality antagandet. SITHS funktionscertifikat kommer att användas.
- Confidentiality: SSL (kryptrering) används mellan Konsument och Anslutningspunkt. Detta för att informationen som applikationen tillhandahåller kan vara känslig och ingen annan ska kunna se den på väg till Konsumenten. Att använda SSL i SJUNET medför att huvudmännen får det svårare att kontrollera om konfidentiell information är på väg att lämna huvudmannen. Detta är avstämt med ansvarig på SVR huruvida huvudmännen upplevt detta (sk. HTTPS/SSL Inspection) som ett bekymmer, vilket de inte har upplevt.
- Integrity (att datat inte ska fövanskas): Mellan Konsument och Anslutningspunkt används SSL som integritetsskydd. Ett scenario där det är mycket viktigt att informationen inte förvanskats är om man inte kan kontakta ansvarig primärvårdsenhet för en patient.

3.3 Pålitlighet/Tillgänglighet (Reliability/Availability) (failover)

Det är Konsument applikationerna som användare interagerar med vilket medför att det är utifrån Konsumenten som den totala tillgängligheten beräknas.

Estimerad nertid på ca. 50 minuter/vecka ger att systemet är tillgängligt 99.5% av tiden, dvs ”Commercial” applikation enligt MSDN.

En rimlig beräkning för de ingående komponenterna i systemet är:

$A = A_{GUI} * A_{ANSLUTNINGSPUNKT} * A_{KÄLLSYSTEM}$.
99.5 % = 99.8 % * 99.8 % * 99.8 %.

Fördjupad bakgrund

Eftersom tjänsten kommer att användas av andra tjänster kommer den att betraktas som att den ”opererar i serie”. Detta medför att den totala availabilityn räknas ut som : $A = A_x * A_y$. Availabilityn kommer att variera beoroende på hur lång serien blir, exempel: $A = A_{GUI} * A_{ANSLUTNINGSPUNKT} * A_{KÄLLSYSTEM}$.

Exempel: Bara ett GUI utan kopplingar till andra system.
$A = A_{GUI}$ = 99.5 %.
Exempel: Lite fler system är inblandande och alla system har samma tillgänglighetskrav (99.5%).
A(Total tillgänglighet) = $A_{GUI} * A_{HSA} * A_{ANSLUTNINGSPUNKT} * A_{KÄLLSYSTEM}$.
A = 0.995 * 0.995 * 0.995 * 0.995 = 98 %. En sänkning med 1.5 % är en rejäl minskning av tillgänglighetskraven. Den total tillgängligheten kategoriseras då som ”Non-Commercial application” (< 99 %) enligt MSDN definitionen (se under rubriken ”Definitioner och förkortiningar”.

3.4 Performance (prestanda)

Utifrån en användares synvinkel så definieras svarstiden som prestanda. Ett vanligt mått på maximal svarstid är 3 sekunder (det finns många studier, t.ex**.** JupiterResearch) . Med den svarstiden så är det rimligt att en anslutningspunkt tar max 30 % av den tiden i anspråk, alltså ca. en sekund. Svarstiderna är uppdelade på användningsfall:

Fördjupad bakgrund

Tjänsten används i serie vilket gör att beräkning av svarstiden är: $T = T_x + T_y$.

Scenario: Kort anropskedja.
$T = T_{MVK} + T_{HSA} =$ 1.5 + 1.5 = 3 sekunder, dvs 50 % av totaltiden.
Scenario: Längre anropskedja

$T = A_{MVK} + A_{HSA} + A_{ANSLUTNINGSPUNKT} + A_{KÄLLSYSTEM}$ = 0.75 + 0.75 + 0.75 + 0.75 = 3 sekunder. Svarstiden påverkas mycket ju längre anropskedjan är.

3.5 Kapacitet

Definition: # transaktioner / sekund.

Kapaciteten är viktig för att kunna beräkna hårdvaru/skalnings- behov.

3.6 Skalbarhet

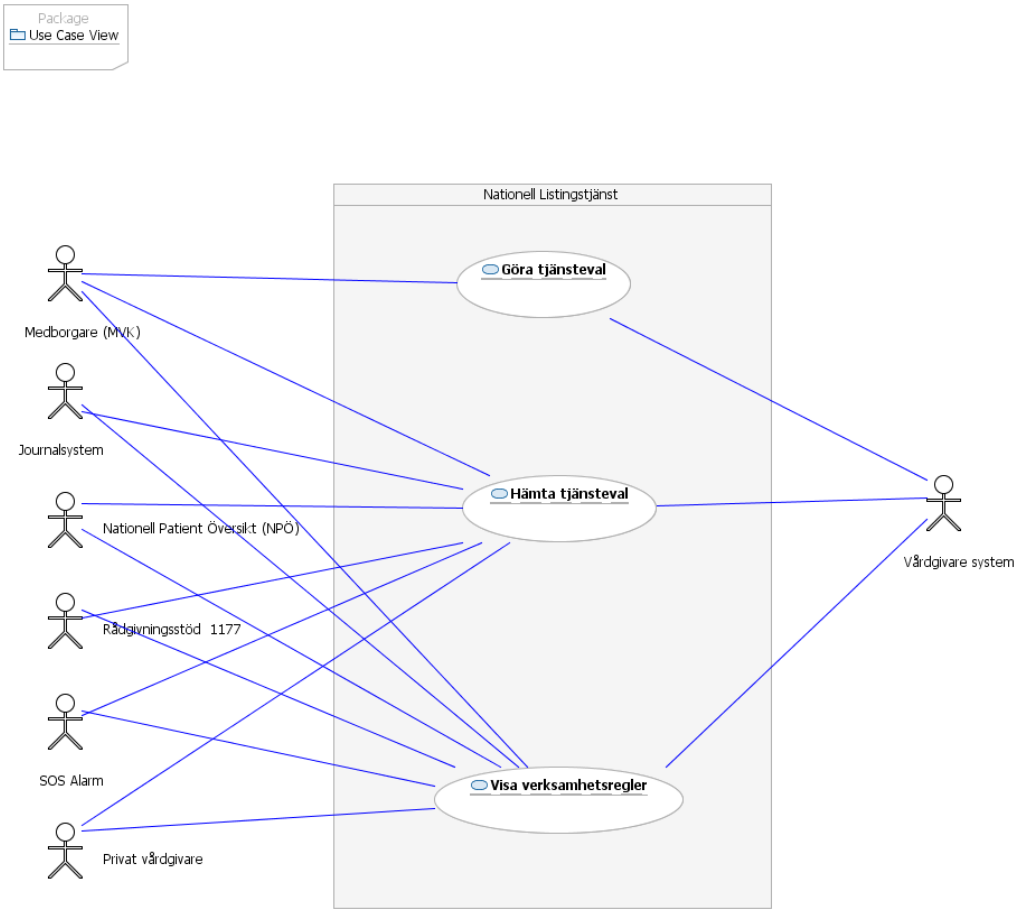
Systemet ska vara både vertikalt (mer RAM och CPU) och horisontellt (mer servrar) skalbart.

Krav: Givet är att registrerade personer inte kan bli fler än invånare i respektive region/Län, alltså en volym på ca. 2 miljoner personer för största länet Stockholm.

3.7 Testability

Systemet ska vara enkelt att testa. Automatiska tester och testprocesser behövs eftersom systemet ska drivas på nationell nivå och kvalitet är viktigt. Test Driven Development (TDD) rekommenderas.

4 Use Case View



** Use Case Modell*

4.1 Hämta Tjänsteval (vårdval)

Som en konsument av tjänsten skulle jag vilja få fram vilken tjänsteutövare (t.ex vårdenhet) som en person är registrerad på eftersom jag behöver veta vart personen ska vända sig för sina vårdrelaterade frågor.

4.2 Göra Tjänsteval (vårdval)

Som medborgare skulle jag vilja byta tjänsteutförare eftersom jag vill använda en annan tjänsteutövare.

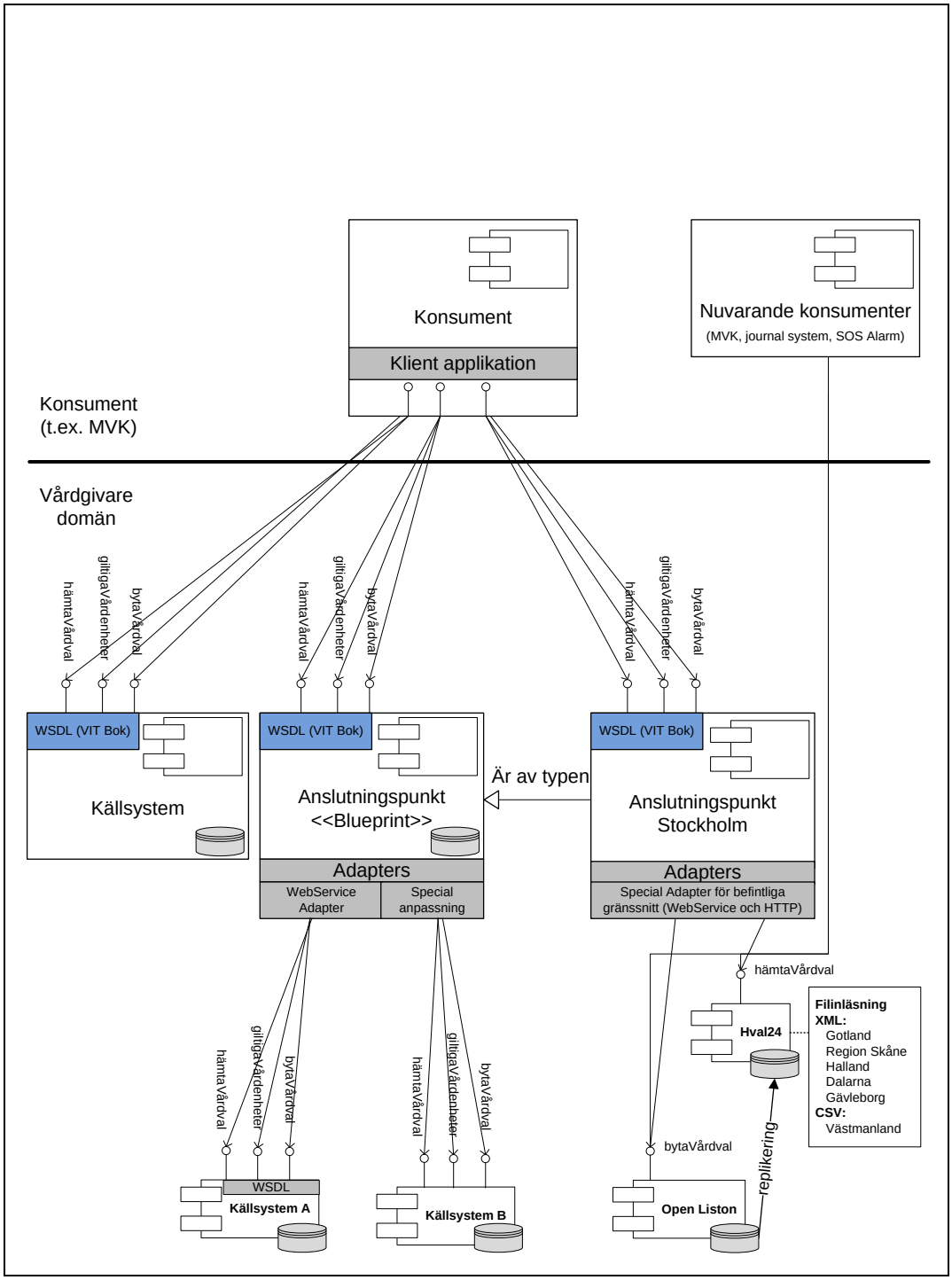
För att byta tjänsteutövare väljer medborgaren vilken typ av tjänsteval som han/hon vill ändra och därefter väljer medborgaren en tjänsteutövare i listan av tillgängliga tjänsteutövare.

4.3 Visa verksamhetsregler

Som en konsument av tjänsten skulle jag vilja få reda på verksamhetsregler som gäller för tjänsteval hos respektive huvudman eftersom jag behöver information om eventuella begränsningar som huvudmannen har.

5 Logical View

5.1 Översikt



** Översikt av systemets komponenter.*

Enligt den nationella IT strategin så ska det in en till komponent mellan Konsument och Anslutningspunkt, en sk. Virtualiseringstjänst (Vägvalstjänst). Virtualiseringstjänstens uppgift är att dirigera meddelanden till rätt Anslutningspunkt. Virtualiseringstjänsten finns dock endast på ritbordet vilket gör att den inte kan användas än (2009-05-08).

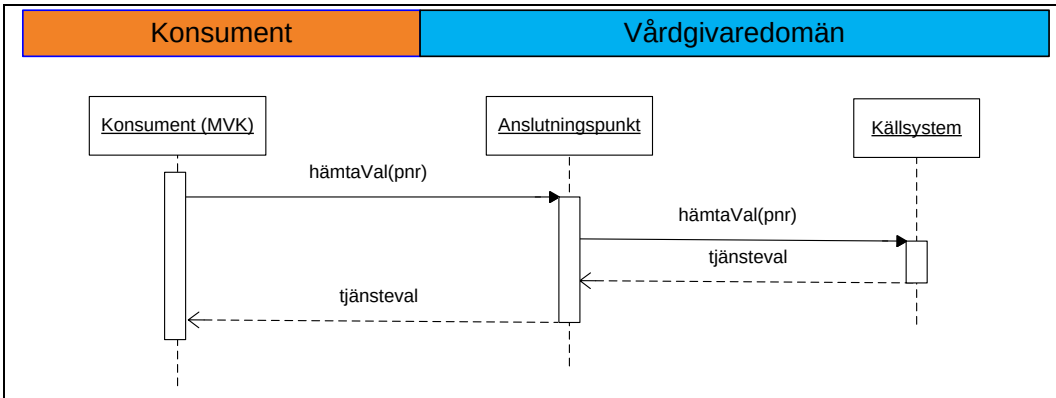
5.2 Arkitekturellt signifikanta design paket

Beskriver hur kraven realiseras i arkitekturen. Kontrakt mellan komponenter ska vara semantiska i enlighet med VIT boken.

Anslutningspunkterna kan implementeras på två olika sätt:

1. Synkron hantering av källsystemet.
2. Asynkrona hantering av källsystemet. Alltså en lokal cache används i anslutningspunkten för att avlasta källsystemet. Detta alternativ görs när Källsystemet inte kan uppfylla SLA för Anslutningspunkter.

Mållösningen är synkronhantering i Anslutningspunkter.



** Beskriver en asynkron hantering av källsystemet, se punkt (2) ovan.*

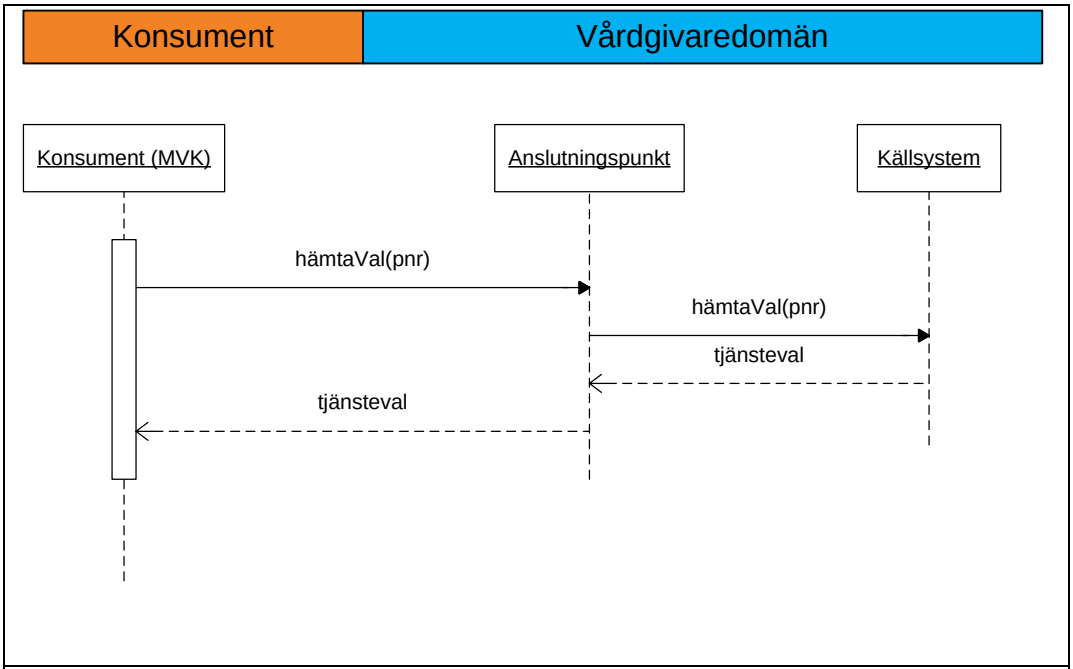
Beskrivning av logiska namn i sekvensdiagrammen:

Konsument(MVK): Konsument av den Nationella Listningstjänsten, för närvarande MVK.

Anslutningspunkt: Vårdgivarens anslutningspunkt till den Nationella Listningstjänsten.

Källsystem: Vårdgivarens listningssystem.

5.2.1 Hämta tjänsteval/vårdval



** Sekvensdiagram för att hämta ett tjänsteval.*

Kontrakt - Konsument till Vårdgivaredomän

Beskrivning: Hämtar en listning för angivet personnummer. Hämtar endast personens aktuella val, ej historisk data.

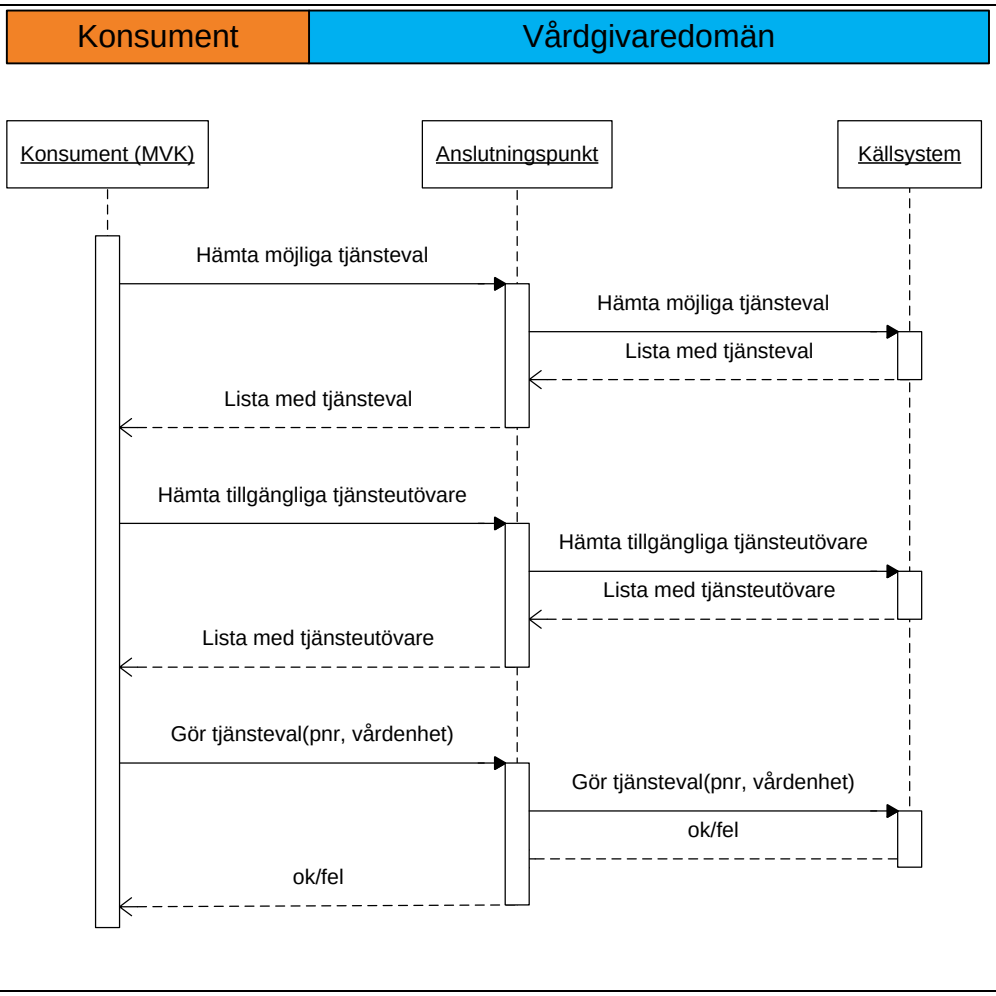
Operation (pseudokod):

getListing(socialSecurityNumber: String) : ehr_extract

* *Med* ehr_extract *avses en datarepresentation av listningsinformation i dataformatet EN13606.*

.

5.2.2 Göra tjänsteval



** Sekvensdiagram som beskriver att göra ett tjänsteval.*

Att göra ett tjänsteval måste gå mot källsystemen eftersom det kan finnas lokala regler för när en person kan välja en tjänsteutövare (t.ex vårdenhet). Vårdgivarens system meddelar Konsumenten eventuella lokala regler (t.ex. när listningen börjar gälla) via retur meddelande i anropet. Nedan tjänstekontrakt är mellan Konsumenten och Vårdgivaredomänen. Kontrakten till Källsystemet har inget med den nationella tjänsten att göra.

Hämta möjliga tjänsteval

Beskrivning: Hämtar en lista med möjliga tjänsteval som vårdgivaren tillhandahåller. Det kan t.ex. vara ’Husläkare’, ’Husläkarmottagning’, ’BVC’ och ’Familjeläkare’ etc.

Operation (pseudokod):

getAvailableHealtcareChoices() : List<tjänsteval>

Hämta möjliga tjänsteutövare

Beskrivning: Hämtar en lista med möjliga tjänsteutövare (t.ex vårdenheter eller läkare) som medborgaren kan välja som tjänsteutförare.

Operation (pseudokod):

getAvailableOrganizationUnits() : List<HSAID>

Göra tjänsteval (vårdval)

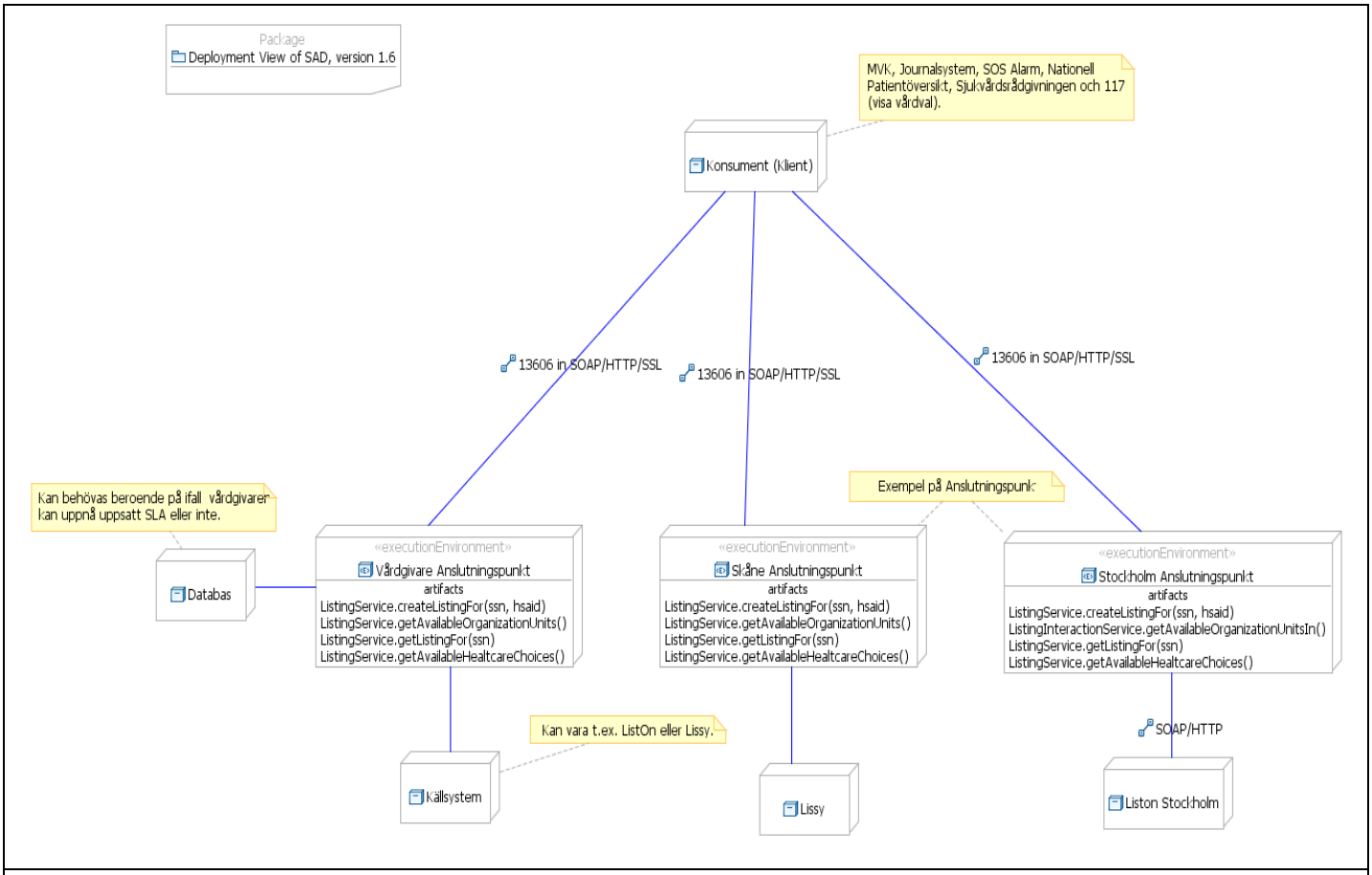
Beskrivning: Utför ett tjänsteval och returnerar en retursträng med beskrivning av eventuella verksamhetsregler. En regler kan vara när valet/listningen börjar att gälla. Att *lista sig* betyder att en person registrerar sig hos en specificerad tjänsteutövare.

Operation (pseudokod):

createListingFor(ehr_extract: EHR_EXTRACT) : String

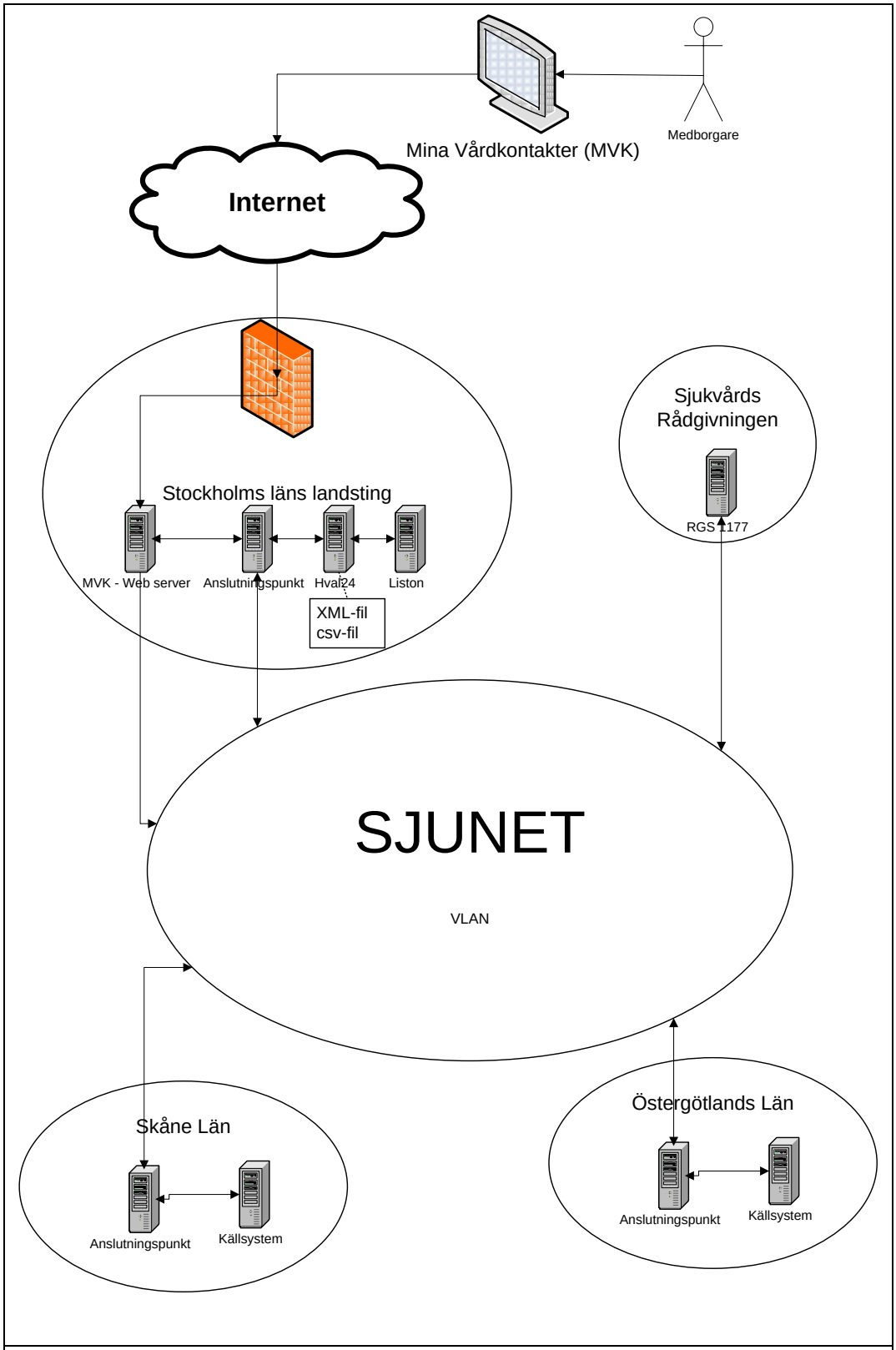
* *Med* ehr_extract *avses en datarepresentation av listningsinformation i dataformatet EN13606.*

6 Deployment view



** Översikt på hur systemet kan deployas.*

6.1 Fysisk Topologi



** Beskriver hur datorerna kopplas ihop.*

7 Data View

** Beskriver viktiga begrepp i systemet.*

En person kan vara listad på flera ställen samtidigt.

Scenario - Sommarställe: En person bor i Skåne men har landställe på Gotland, detta innebär att han/hon är listad i två Län. Dock ska detta betraktas som ett undantag. För att visa/göra listningar i detta scenariot så behövs Virtualiseringstjänsten (se tidigare beskrivning).

8 SLA

Nedan är en sammanfattning av SLA för en Anslutningspunkt.

Volym:

- *Mätning behövs för att bestämma Transaktioner/sek.*

Performance:

- Maximal svarstid är 3 sekunder sett utifrån de som använder Konsument applikationerna.
- Use Case - Hämta tjänsteval: Svarstiden ska vara mindre än 1 sekund vid 95% av anropen.
- Use Case - Byta tjänsteval: Svarstiden ska vara mindre än 2 sekunder vid 95 % av anropen.
- Vid belastningstoppar (4 gånger vanlig belastning) ska systemet ha svarstider på mindre än 6 sekunder (Dubbel så lång maximal svarstid som vid normalfall). Detta mått är sett utifrån Konsument perspektivet.

Testning

- Varje huvudman ska tillhandahålla en testmiljö för Konsumenterna.

- Det ska alltid finnas en person i produktionsystemet med personnummer: 121212-1212.

Tillgänglighet:

- 99.5 %. Estimerad nertid på ca. 50 minuter/vecka ger att systemet är tillgängligt 99.5% av tiden.
- Servicefönster är kvällstid, Torsdag kl. 23.00 till Fredag kl. 01.00.

9 Kvalitet

Följande kvalitetsmål har identifierats:

Testability:

- **Beskrivning:** Systemet ska ha automatiska tester.
- **Lösning** : Använd Continous Integration verktyg (CI) där automatiska enhetstester och integrationstester körs regelbundet.