

Software Architecture Document

skapad av:

Robert Georén

Version: 1.3

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 användningsfall tillagt, 'Visa verksamhetsregler'. Version 1.1.
Robert Georén	2009-08-26	Bytte namn på vårdenheter till tjänsteutövare.
Robert Georén	2009-09-15	Ändrade pseudo-kod för 'byta tjänsteval'.v 1.2
Robert Georén	2010-06-04	Uppdaterat till hur lösningen blev för Release 1.0 av NLT. Version 1.3.

Innehåll

1	Introduktion	4
1.1	Definitioner och förkortningar	4
2	Arkitektur representation	5
3	Arkitekturella mål och begränsningar.....	5
3.1	Teknisk Plattform	5
3.2	Säkerhet	5
3.3	Pålitlighet/Tillgänglighet (Reliability/Availability) (failover)	6
3.4	Performance (prestanda)	7
3.5	Kapacitet	8
3.6	Skalbarhet	8
3.7	Testability	8
4	Use Case View	9
4.1	Hämta vårdval (listning)	9
4.2	Göra vårdval	9
5	Logical View	10
5.1	Översikt	10
5.2	Arkitekturellt signifikanta design paket	11
5.2.1	Hämta vårdval.....	12
5.2.2	Göra vårdval.....	13
	Punkt 1 - Hämta köinformation för en person	14
6	Deployment view	15
6.1	Fysisk Topologi	16
7	Data View	17
8	SLA.....	17
9	Kvalitet	18

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 etableras (det handlar främst om "trust").

SSL: Secure Socket Layer används för att kryptera kommunikationen mellan två värdar.

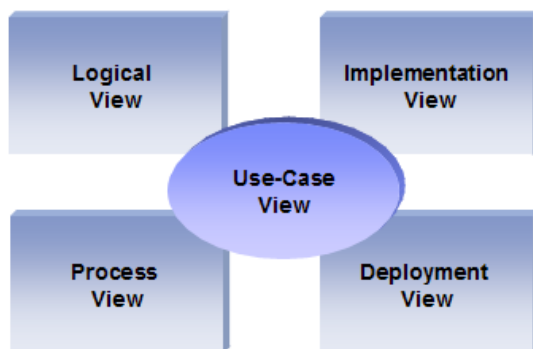
SLA: Service Level Agreement. Används för att definiera krav på Anslutningspunkter.

Listning: En person kan vara registrerad på en vårdcentral och det kallas en listning.

Nationell Tjänsteplattform: <http://skltp.forge.osor.eu/>

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

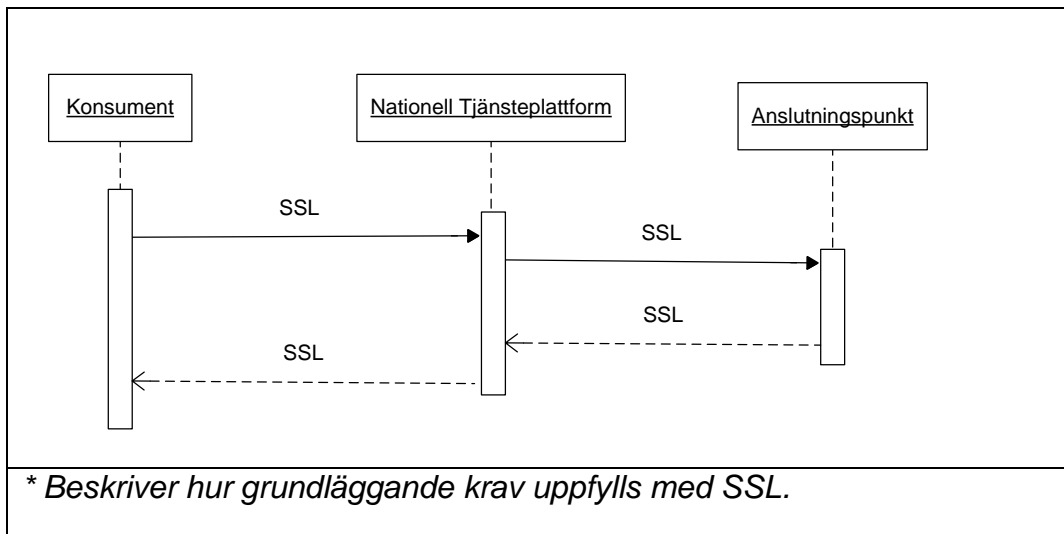
Detta avsnitt beskriver de icke-funktionella kraven som påverkar arkitekturen. Arkitekturen har för avsikt att följa VIT-boken.

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.



- Authentication (verifiera användarens identitet): Mellan konsument (ex. MVK) och Nationell Tjänsteplattform används ett SSL server certifikat och ett SSL 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. Likadant sker för identifiering mellan Nationell Tjänsteplattform och Anslutningspunkter.
- Confidentiality: SSL (kryptering) används vid kommunikation. 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 förvanskas): SSL används 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 beroende 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%).

$$A(\text{Total tillgänglighet}) = A_{GUI} * A_{HSA} * A_{ANSLUTNINGSPUNKT} * A_{KÄLLSYSTEM}.$$

$A = 0.995 * 0.995 * 0.995 * 0.995 = 98 \%$. 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 förkortningar").

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.

$$T = T_{MVK} + T_{HSA} = 1.5 + 1.5 = 3 \text{ sekunder, dvs } 50 \% \text{ av totaltiden.}$$

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

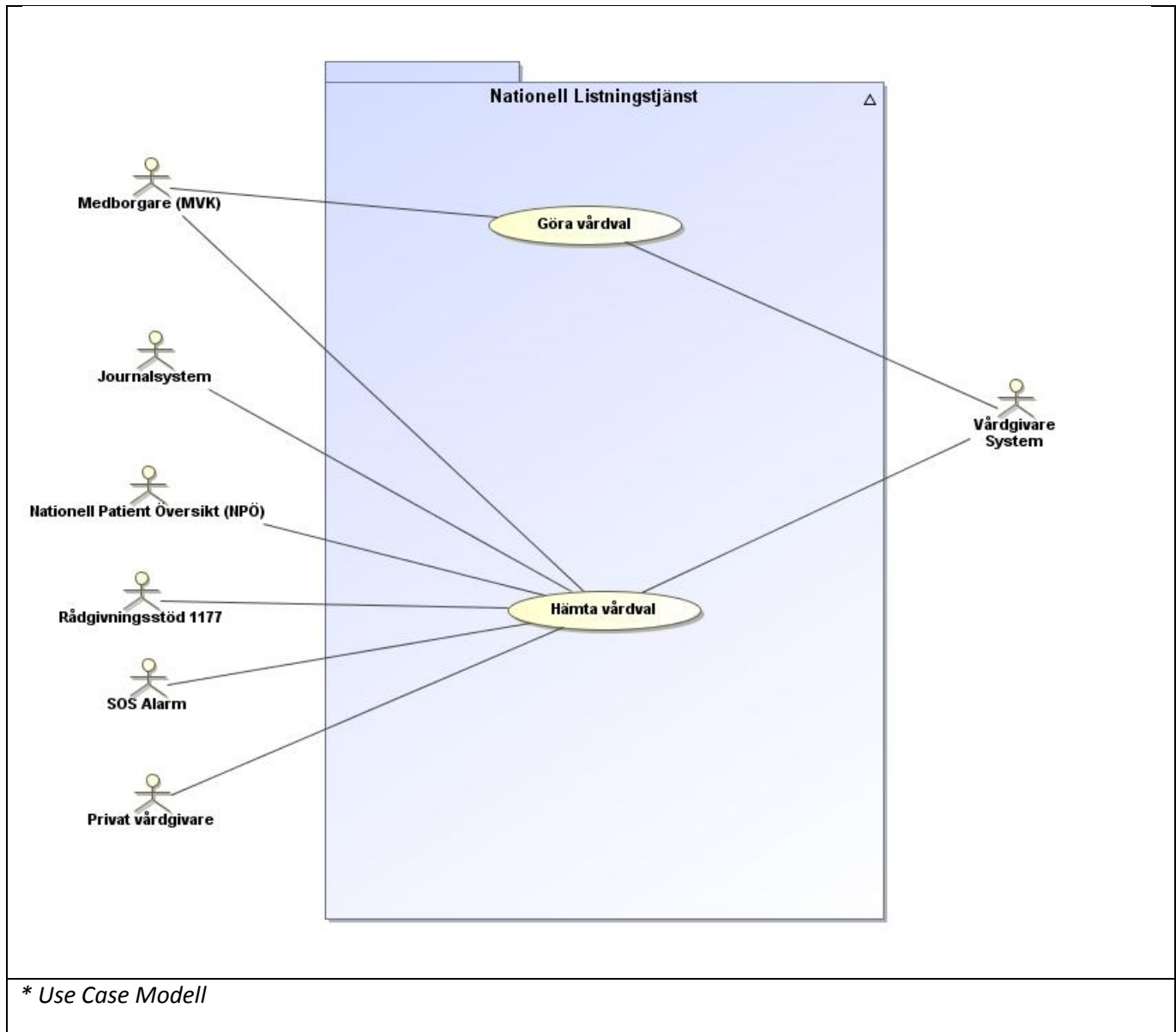
Systemet ska vara både vertikalt (mer RAM och CPU) och horisontellt (mer servrar) skalbart.

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



4.1 Hämta vårdval (listning)

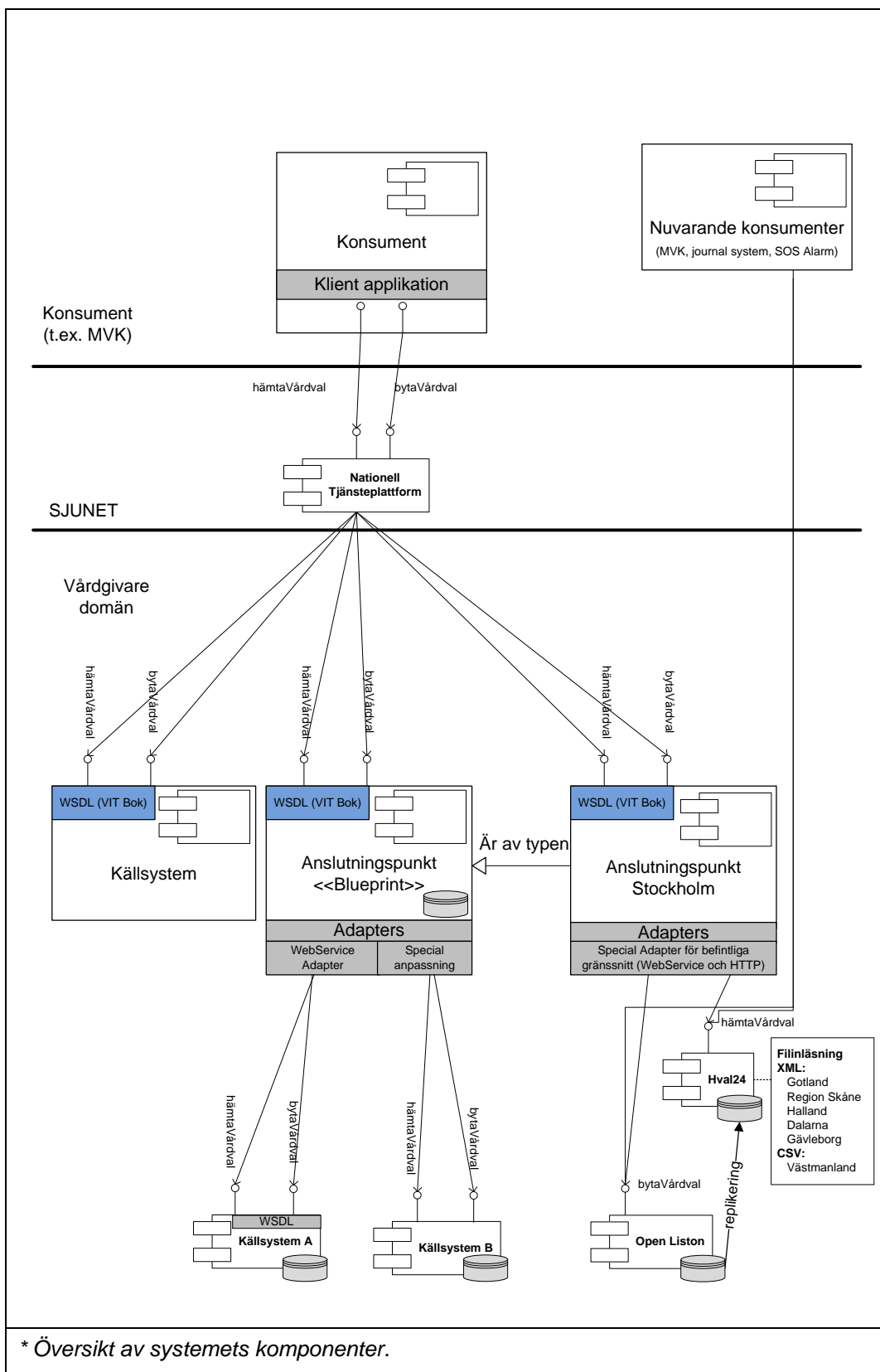
Som en konsument av tjänsten skulle jag vilja få fram vilken tjänsteutövare (t.ex vårdenheter) som en person är registrerad på eftersom jag behöver veta vart personen ska vända sig för sina vårdrelaterade frågor.

4.2 Göra vårdval

Som medborgare skulle jag vilja byta vårdval eftersom jag vill använda en annan vårdgivare.

5 Logical View

5.1 Översikt



Enligt den nationella IT strategin så ska det in en till komponent mellan Konsument och Anslutningspunkt, den sk. Nationella Tjänsteplattformen. Tjänsteplattformens uppgift är att dirigera meddelanden till rätt Anslutningspunkt.

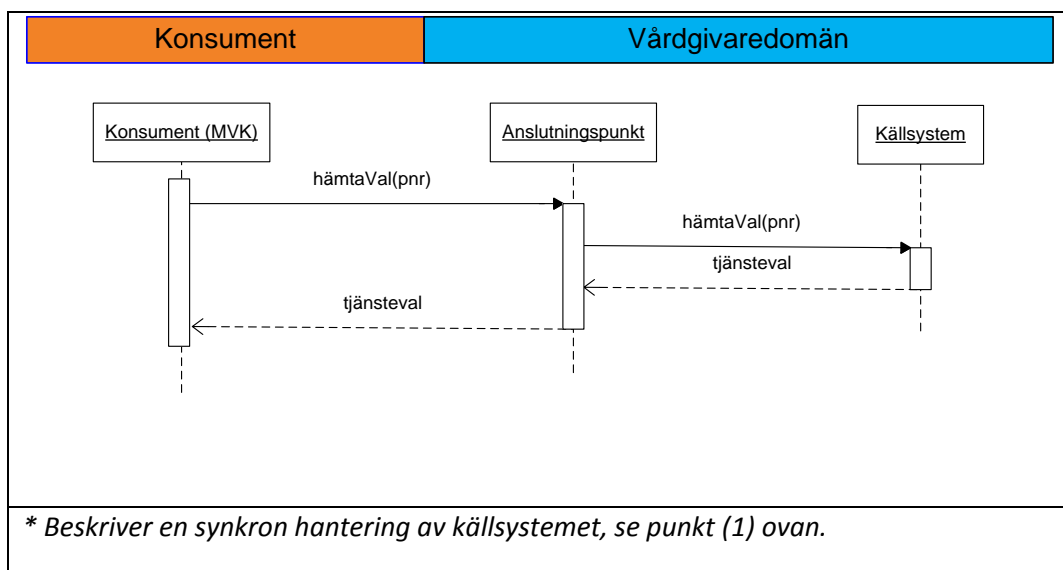
5.2 Arkitekturellt signifikanta design paket

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.



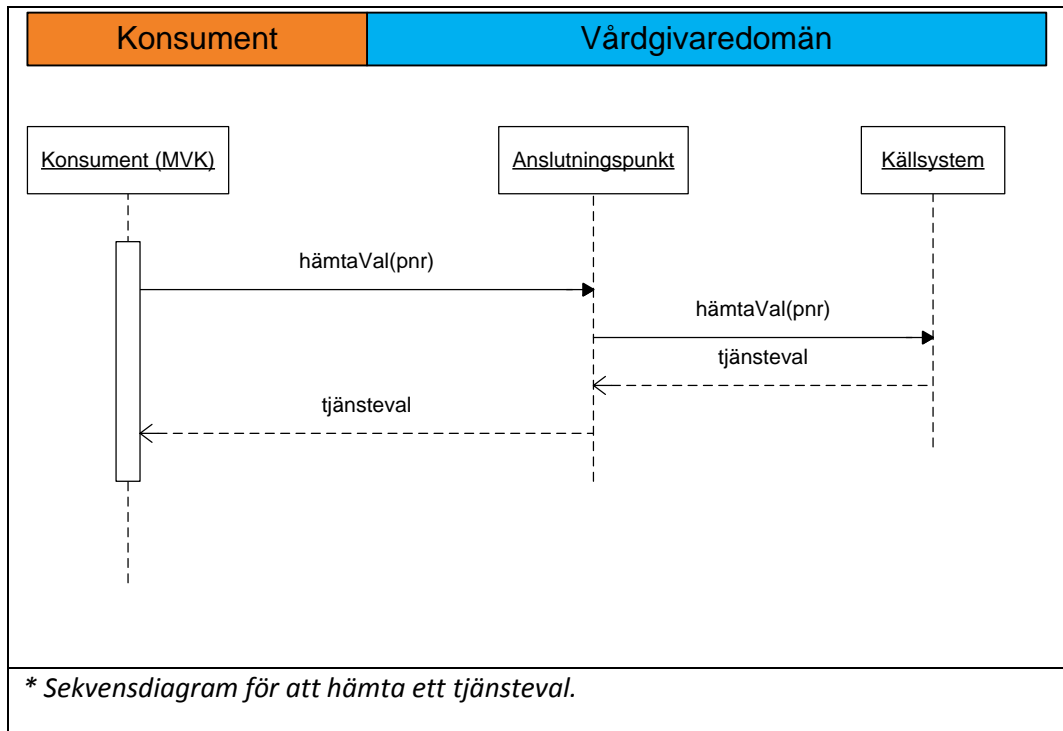
Beskrivning av logiska namn i sekvensdiagrammen:

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

Anslutningspunkt: Vårdgivarens anslutningspunkt till den Nationella Listningstjänsten.

Källsystem: Vårdgivarens listningssystem.

5.2.1 Hämta vårdval



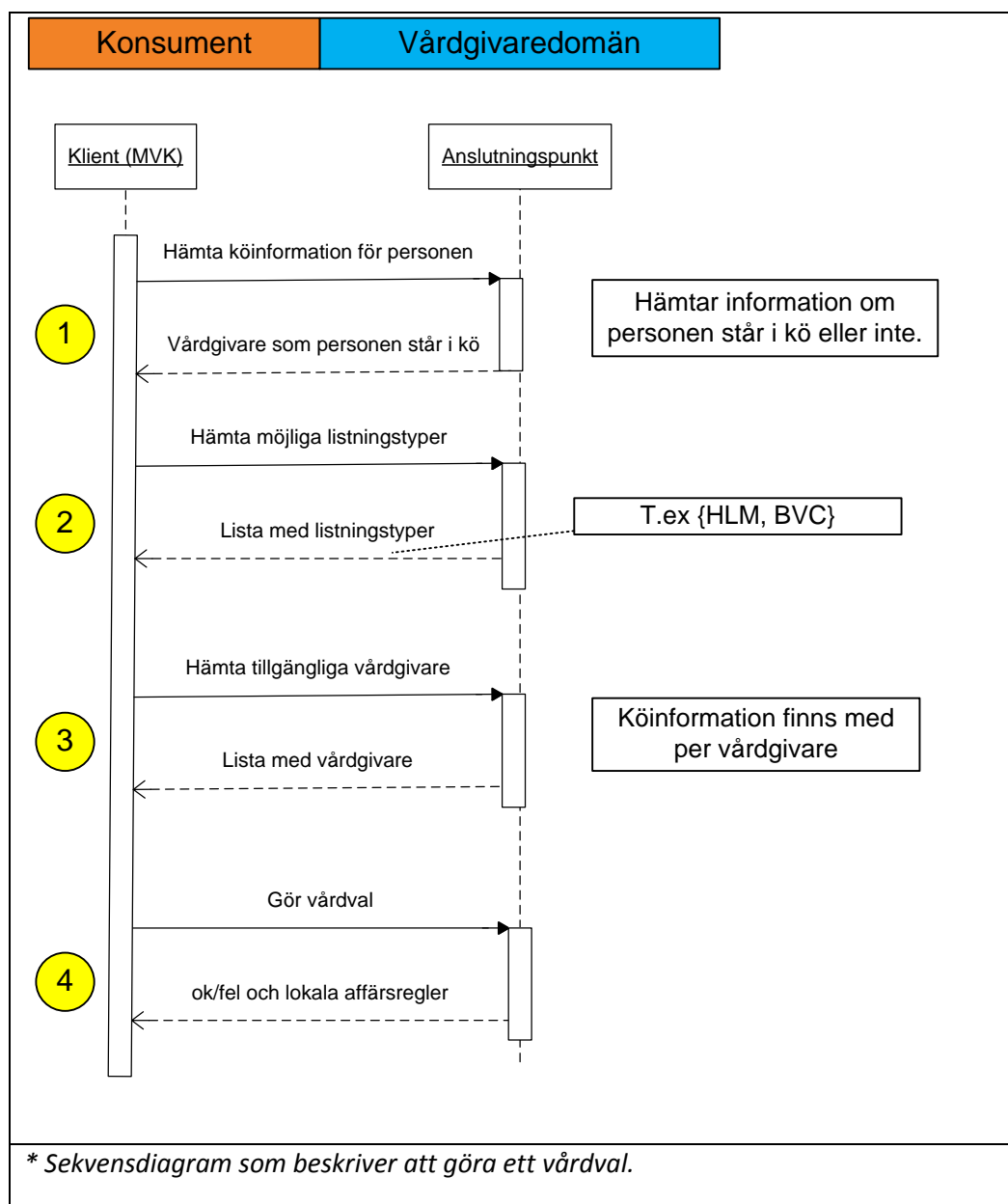
Beskrivning: Hämtar en listning för angivet personnummer. Hämtar endast personens aktuella val, ej historiska listningar.

Operation (pseudokod):

GetListing(personId: String) : SubjectOfCare

5.2.2 Göra vårdval

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



Punkt 1 - Hämta köinformation för en person

Beskrivning: Om angiven person står i kö så returneras den vårdgivaren.

Operation (pseudokod):

GetPersonQueueStatus(person ID): Vårdgivare

Punkt 2 - Hämta möjliga listningstyper

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

Operation (pseudokod):

GetListingTypes(person ID) : Lista med listingstyper

Punkt 3 - Hämta tillgängliga vårgivare

Beskrivning: Hämtar en lista med tillgängliga vårdgivare (t.ex vårdenheter eller läkare) som medborgaren kan välja som vårdgivare. Användaren kan ange vilka vårdgivare som information önskas för och vilka listningstyper som vårdgivare måste stödja.

Operation (pseudokod):

GetAvailableFacilities(vårdgivare, listningstyper) : Lista med Vårdgivare

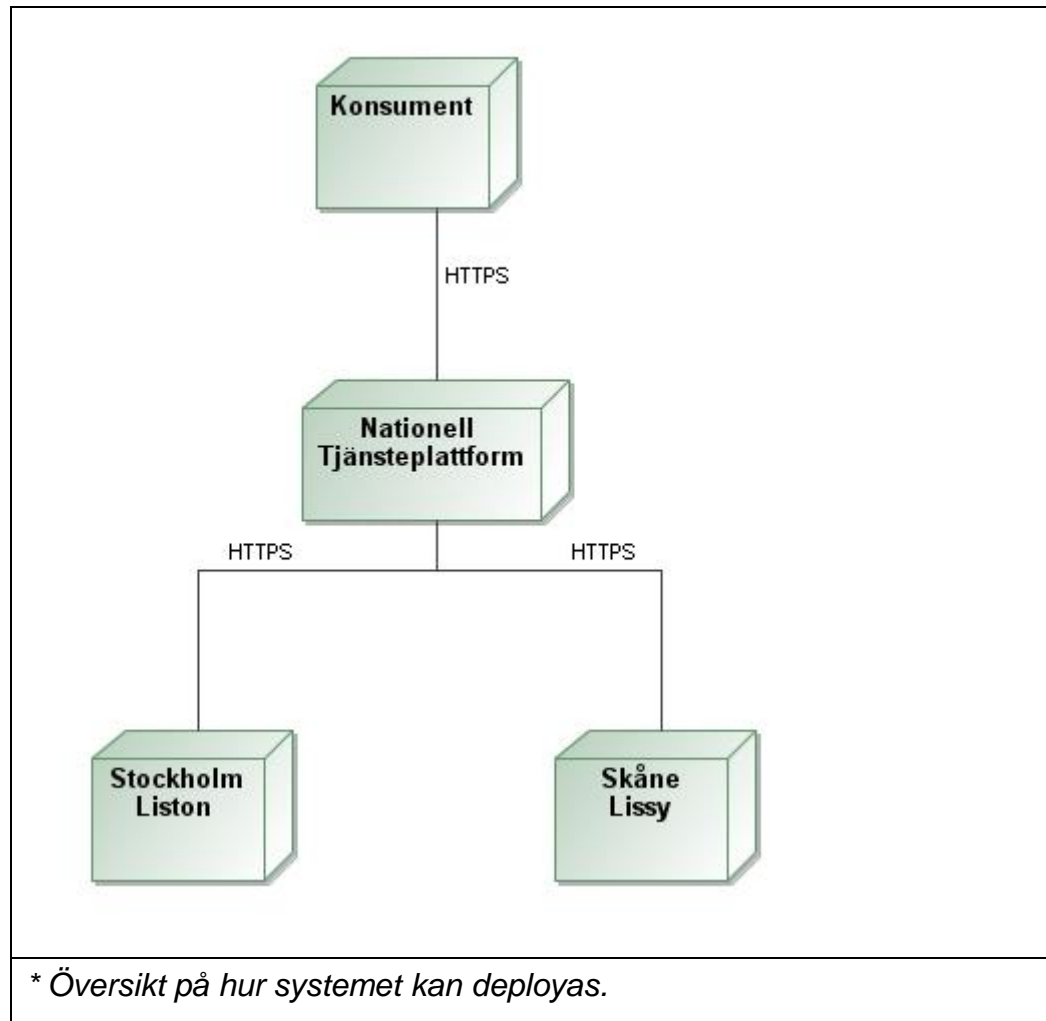
Punkt 4 - Göra vårdval

Beskrivning: Utför ett vårdval 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 vårdgivare.

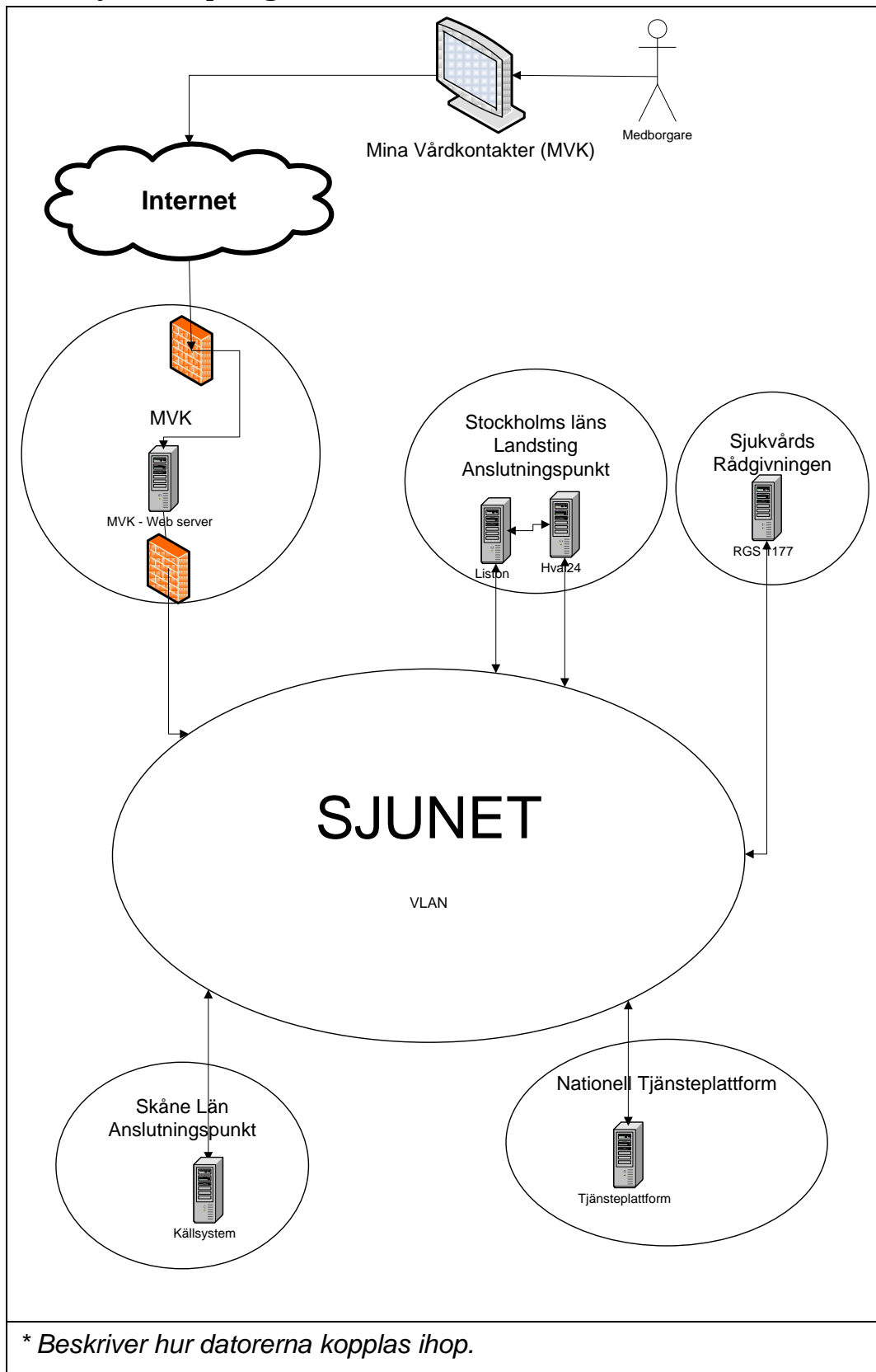
Operation (pseudokod):

CreateListing (person ID, listningstyp, vårdgivare, resurs, att ställa sig i kö) : listningsstatus

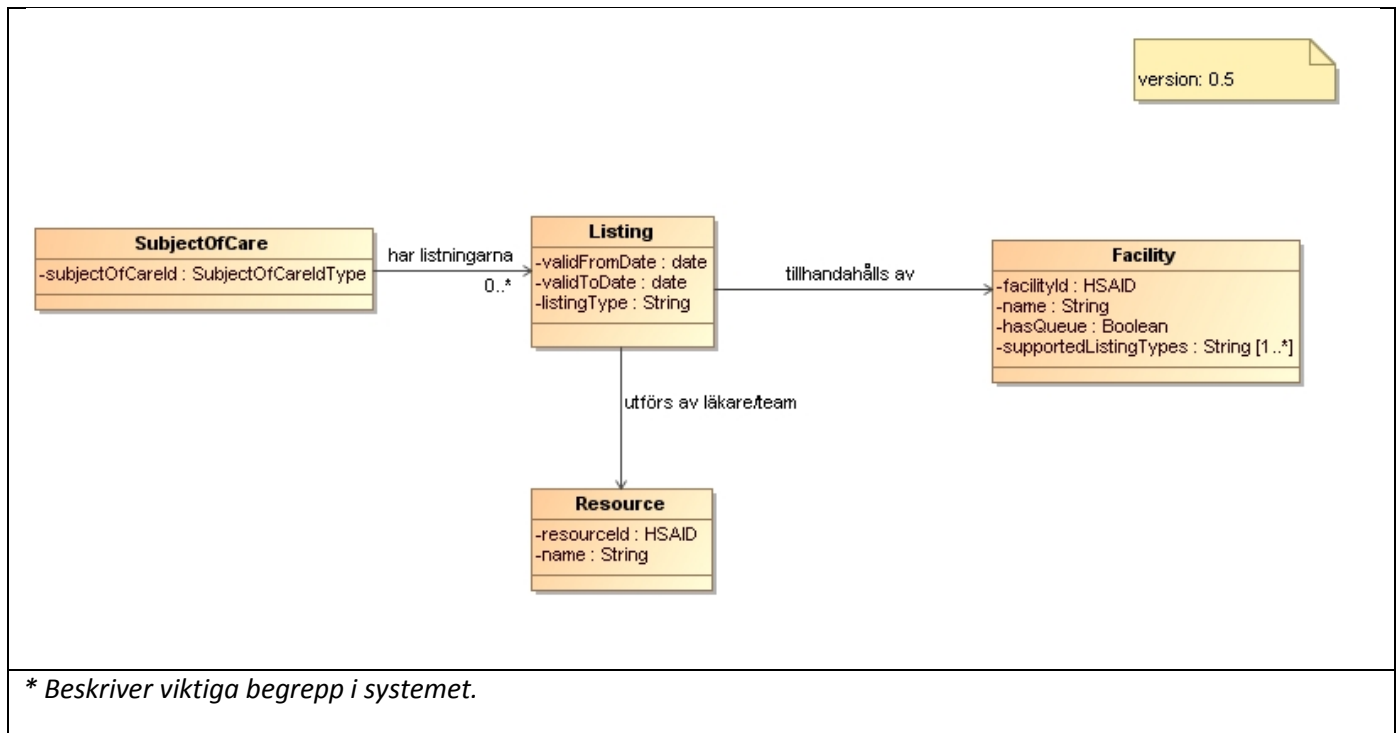
6 Deployment view



6.1 Fysisk Topologi



7 Data View



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 den Nationella Tjänsteplattformen.

8 SLA

Nedan är en sammanfattning av SLA för en Anslutningspunkt.

Performance:

- Maximal svarstid är 3 sekunder sett utifrån de som använder Konsument applikationerna.
- Use Case - Hämta vårdval: Svarstiden ska vara mindre än 1 sekund vid 95% av anropen.
- Use Case - Byta vårdval: 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 produktionssystemet 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.