

Uppdrag Tjänsteväxel

Etapp 1

Delrapport 1

Utvärdera pågående arbeten,

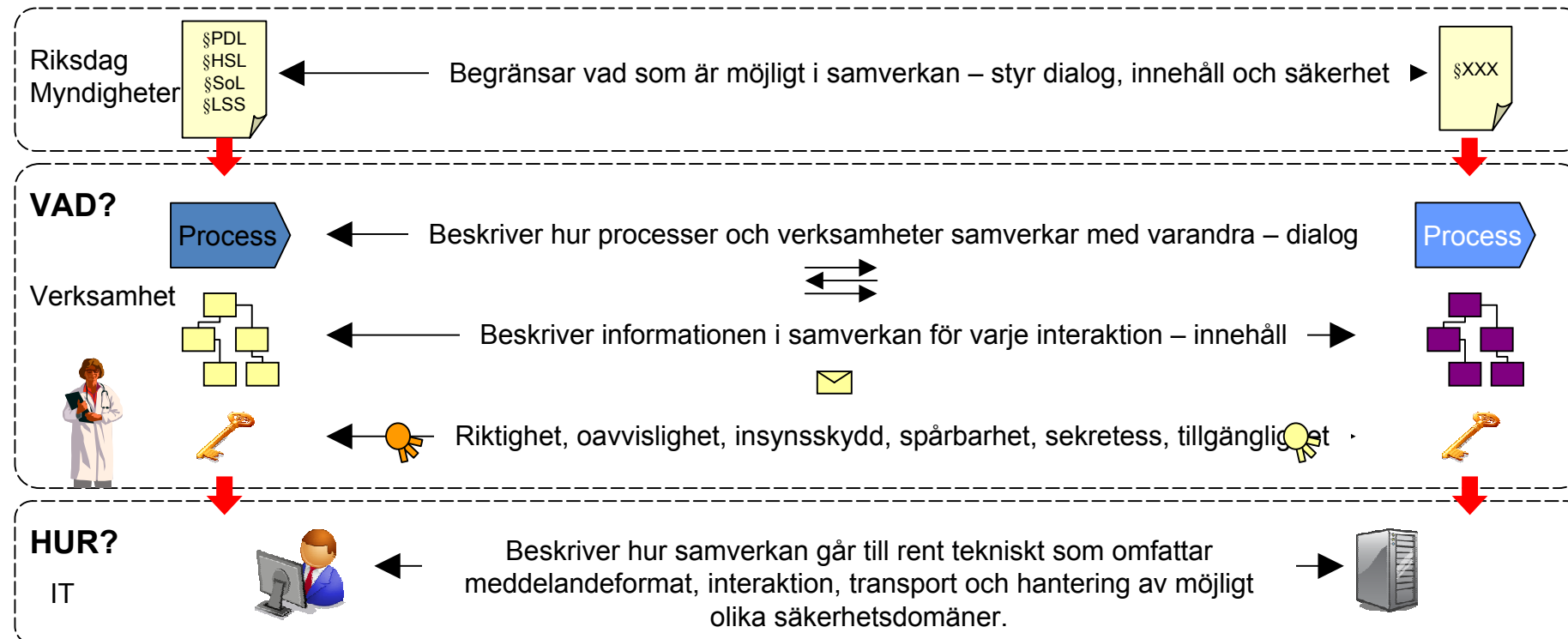
Legala aspekter för extern
kommunikation

Johan Eltes, AL T-Gruppen

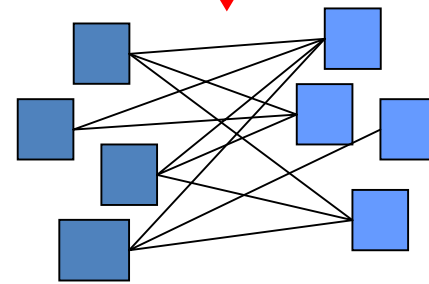
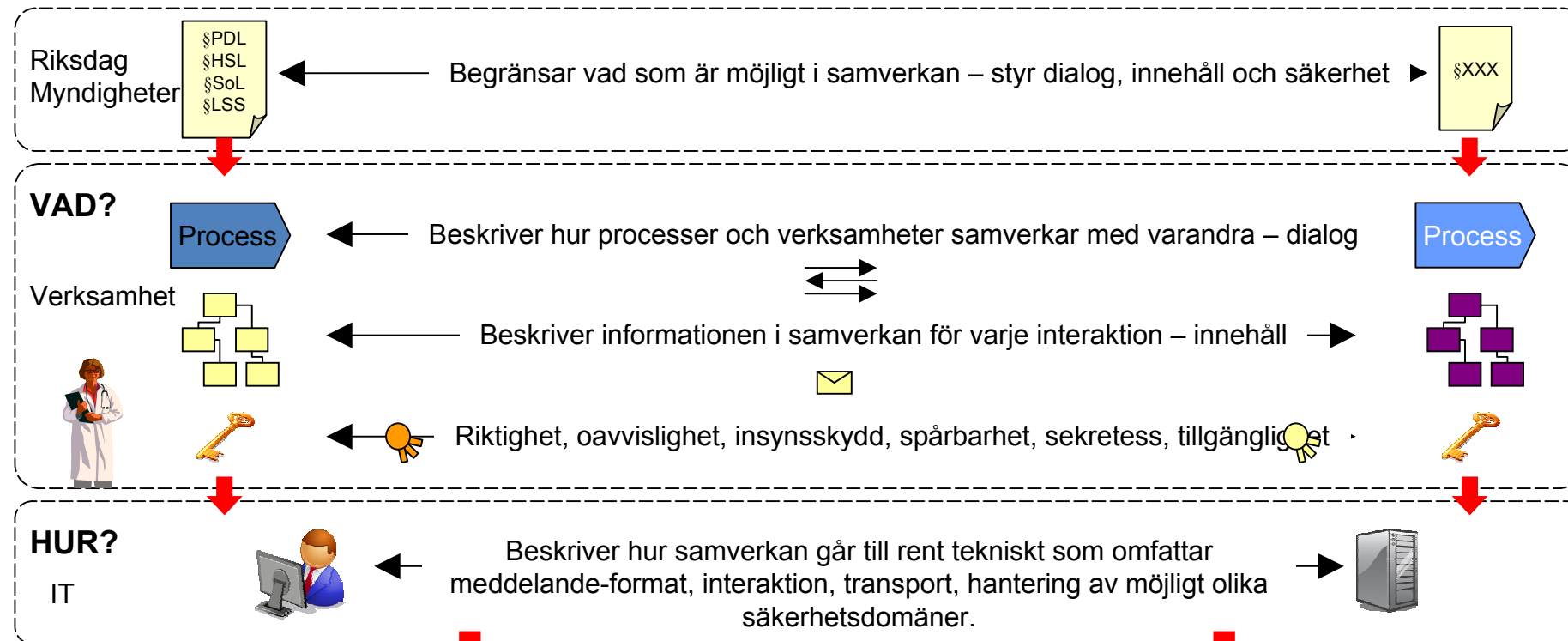
Bakgrund

- Uppdrag från Arkitekturledningen
 - Att få ett gemensamt sätt att förhålla sig till vid kommunikation med externa parter
 - Etapp 1 – Kartläggning och kravspecificering
- Första delrapporten i etapp 1
 - Utvärdera pågående arbeten
 - Legala aspekter för extern kommunikation

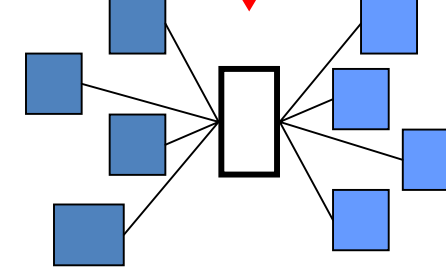
Samverkan med externa parter



Samverkan med externa parter

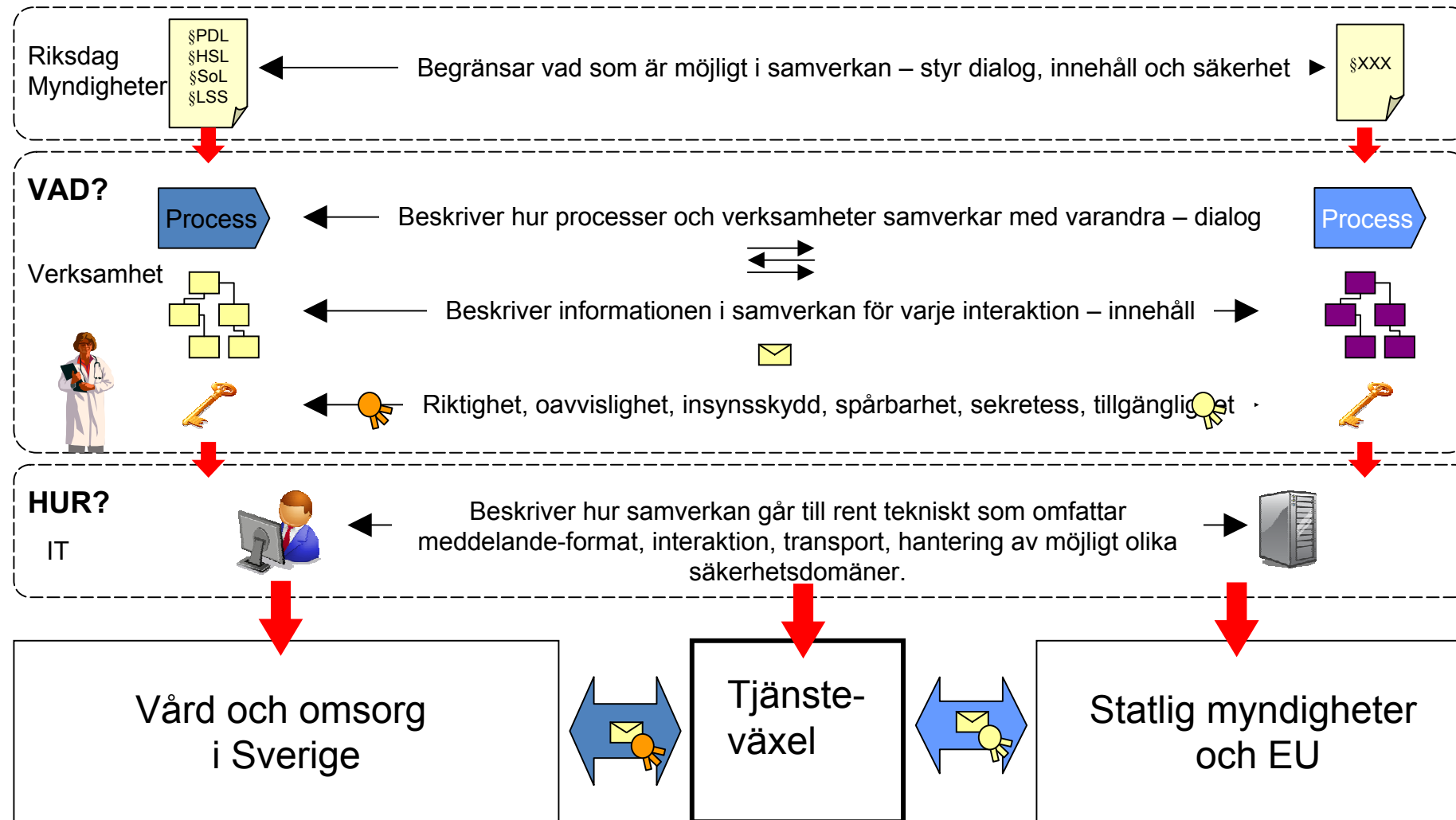


Alla kommunicerar med alla, varje projekt löser det på sitt eget sätt



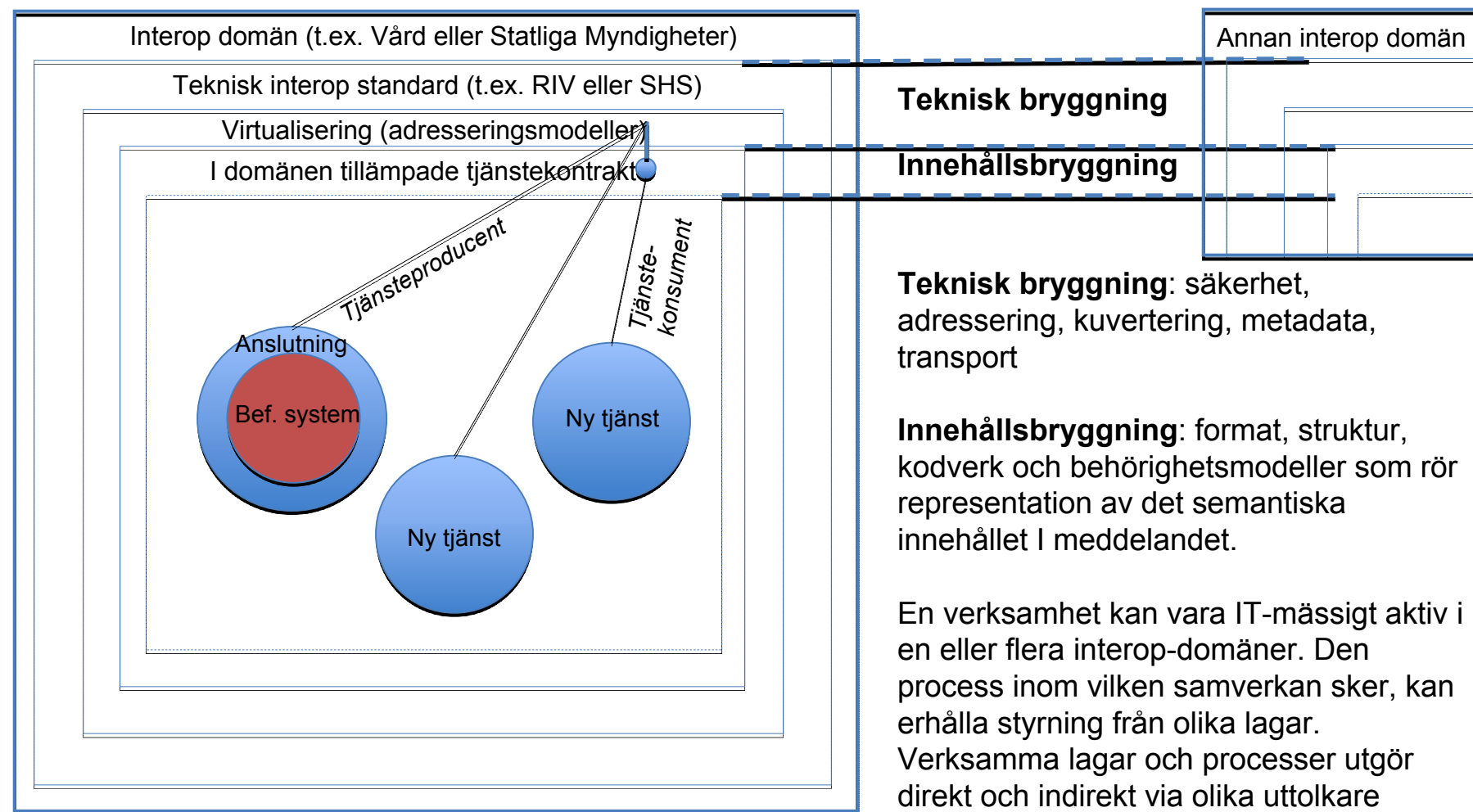
Vård och omsorg kommunicerar med omvärlden via gemensam "tjänsteväxel"

Samverkan med externa parter



Referensmodell

IT-samverkan över interoperabilitetsgränser



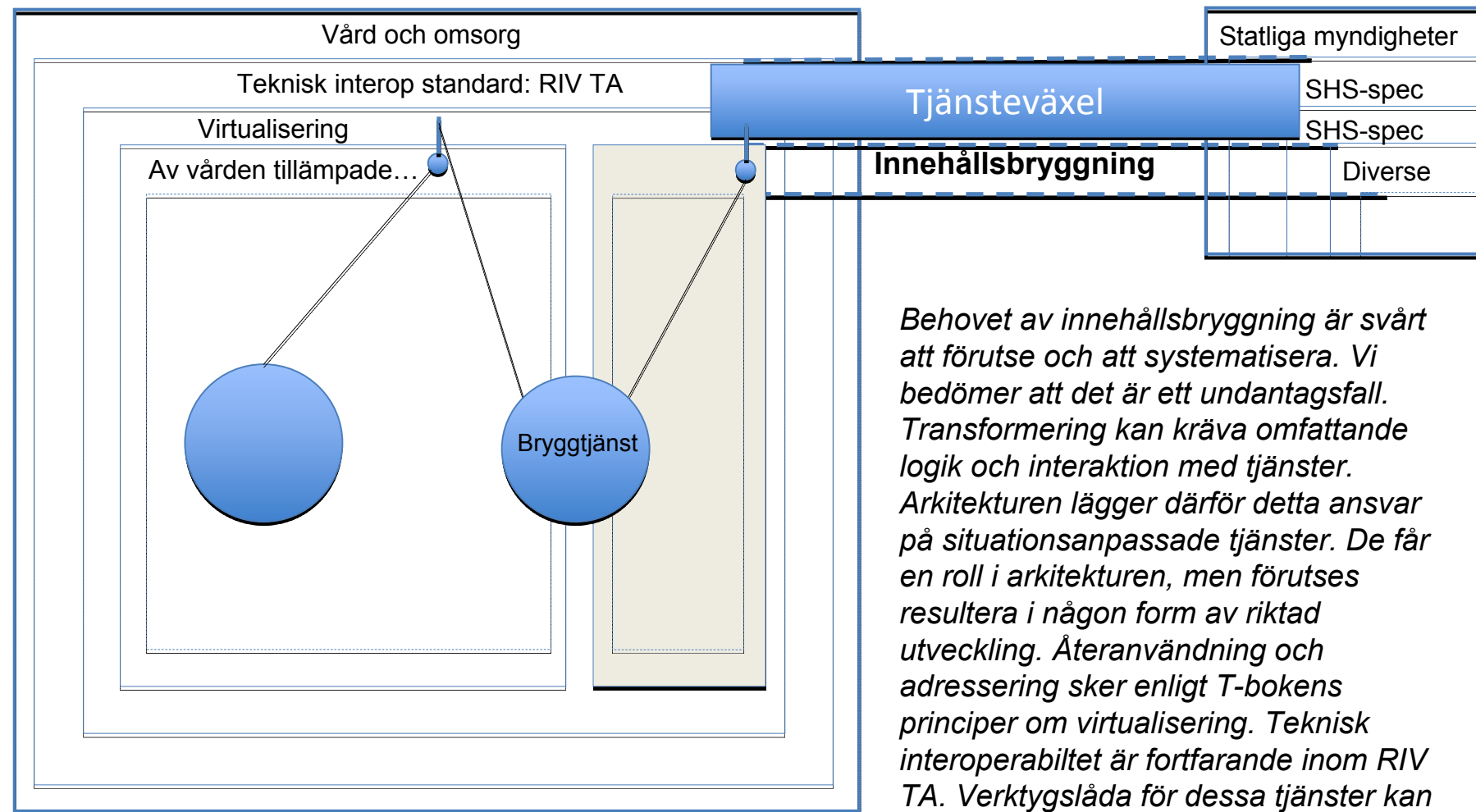
Begreppsdefinitioner finns som anteckningar till denna bild

Teknisk brygning: säkerhet, adressering, kuivering, metadata, transport

Innehållsbrygning: format, struktur, kodverk och behörighetsmodeller som rör representation av det semantiska innehållet i meddelandet.

En verksamhet kan vara IT-mässigt aktiv i en eller flera interop-domäner. Den process inom vilken samverkan sker, kan erhålla styrning från olika lagar. Verksamma lagar och processer utgör direkt och indirekt via olika uttolkare kravställare på den IT-samverkan som sker inom och mellan interoperabilitetsdomäner.

Innehållsbryggning



Behovet av innehållsbryggning är svårt att förutse och att systematisera. Vi bedömer att det är ett undantagsfall. Transformering kan kräva omfattande logik och interaktion med tjänster. Arkitekturen lägger därför detta ansvar på situationsanpassade tjänster. De får en roll i arkitekturen, men förutses resultera i någon form av riktad utveckling. Återanvändning och adressering sker enligt T-bokens principer om virtualisering. Teknisk interoperabilitet är fortfarande inom RIV TA. Verktygslåda för dessa tjänster kan delas med anslutningstjänster, där så är rationellt.

Avgränsning – Tjänsteväxel

- Behov av teknisk brygging föranlett av att motpart ej använder vårdens standarder för kommunikation
 - T.ex. RIV, HSA och SITHS-certifikat
- Ofta, men inte nödvändigtvis – befinner sig parternas tjänster i olika kommunikationsnät (t.ex. SjuNet / Annat nät).
- Den central funktionen är att etablera teknisk samverkan mellan IT-stöd som tillhör olika interoperabilitetsdomäner
- Brygging av skillnader i representation av innehåll i meddelanden är inte en uppgift för tjänsteväxel
- Tjänsteväxling är inte en strategisk komponent i arkturen. Den strategiska inriktningen är standardbaserad samverkan baserad på en för vården och myndigheter gemensam PKI, baserad på WS-Security. Målbilden är en nationell interop-domän som spänner över såväl vårdens som myndigheters verksamheter. I det långsiktiga perspektivet behövs ingen tjänsteväxel för vården.

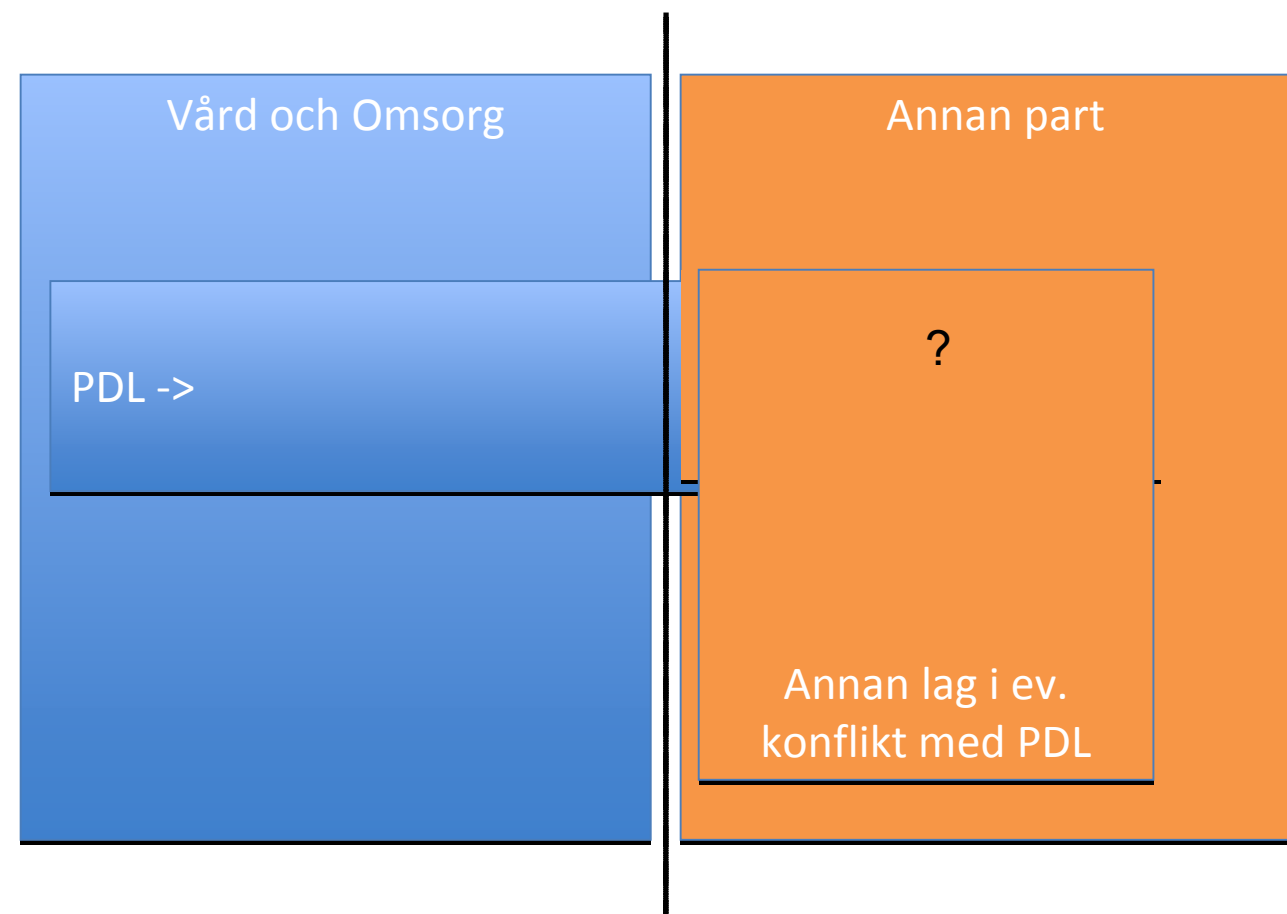
Perspektiv på tjänsteväxling

- Lagar
- Adressering
- Säkerhet
- Tjänsteinteraktioner
- Teknisk kuvertering
- Teknisk arkitektur

Legal interoperabilitet

- Uppstår när parter är underordnade olika / inkompatibla lagkrav
- Lagar och deras uttolkare påverkar kravställning av säkerhetslösningar
 - Insynskydd, spårbarhet, ursprung och äkthet, auktorisation
- Utgångspunkt tills avstämt med Britt
 - Varje part får avgöra vilka lagar som styr fram till tjänsteväxel och meddela eventuella krav till motparten
 - Ansvar för bedömning och tillämpning åligger respektive part
 - Beslut om bryggning av säkerhet blir ett resultat av förhandlingar mellan parterna (t.ex. WS-Security hos vården och enbart kanalkryptering hos myndighet)
 - Britt har dokumenterat vårdens policier för följsamhet mot PDL. T-boken redovisar vårdens säkerhetslösning för att tillmötesgå dessa krav.

Legal interoperabilitet



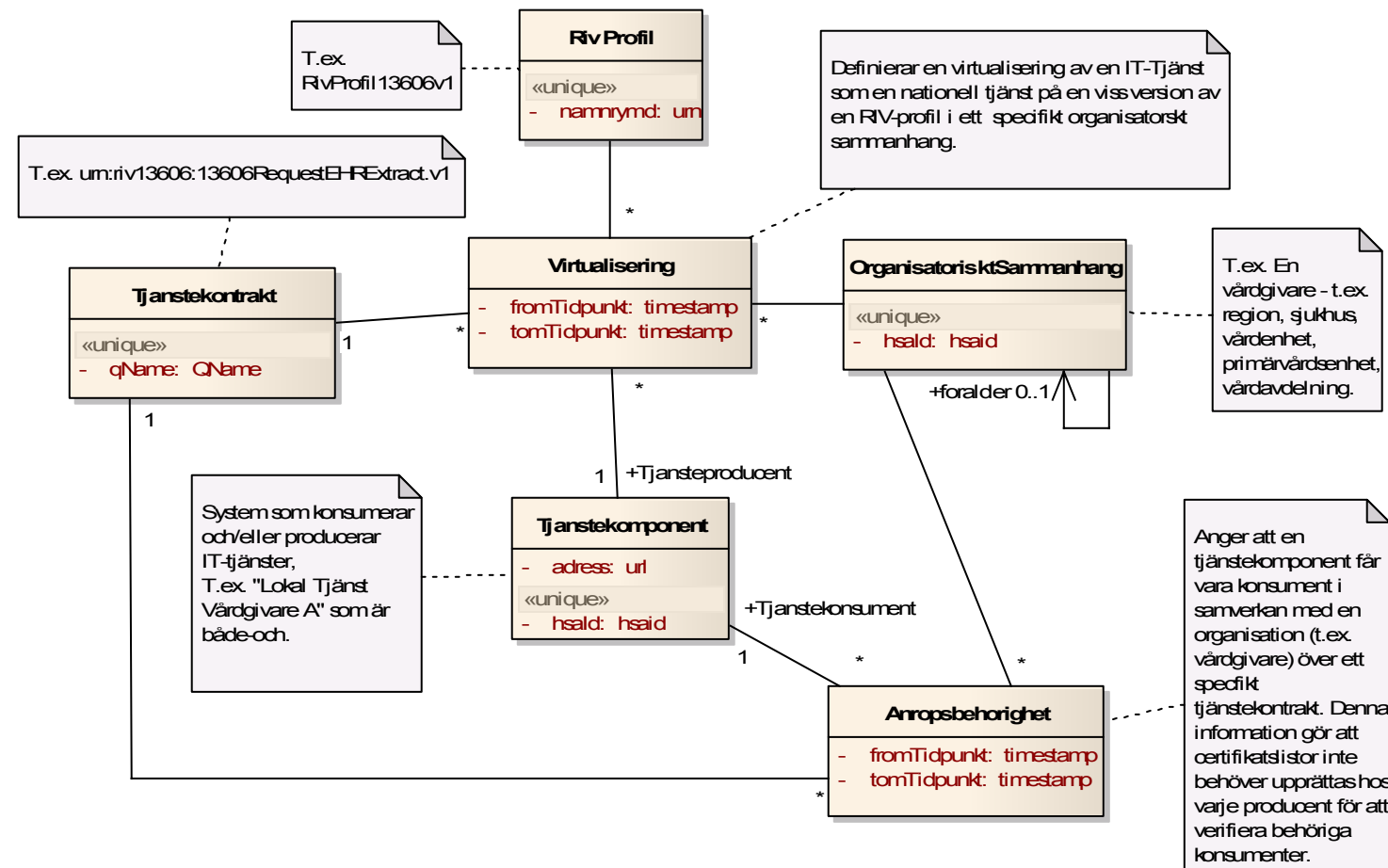
Antagande: Beslut om vilka lagar som tillämpas och deras inverkan på val av säkerhetslösning hos respektive sida tas av respektive part. Bryggan ska ge sken av att motstående part "sköter sig" ur respektive parts perspektiv.

Addressering

- T-bokens adresseringsmodell
 - Strategi
 - Genom att ge sken av att vårdens IT-stöd är nationellt, kan effekter av IT-mässiga och organisatoriska konsolideringar ske utan risk för domino-effekter
 - Krav
 - Möjliggöra inkrementell utveckling av RIV TA
 - Nationell virtualisering av nationella tjänstekontrakt
 - Stabila tjänsteadresser (HSA-id eller teknisk adress)
 - Verksamhetsmässig adressering av logisk samverkanspart
 - Samverkanspart (HSA-id för organisation) hittas via indextjänst eller sortimentskatalog, om ej “direkt indata”

T-bokens adresseringsmodell

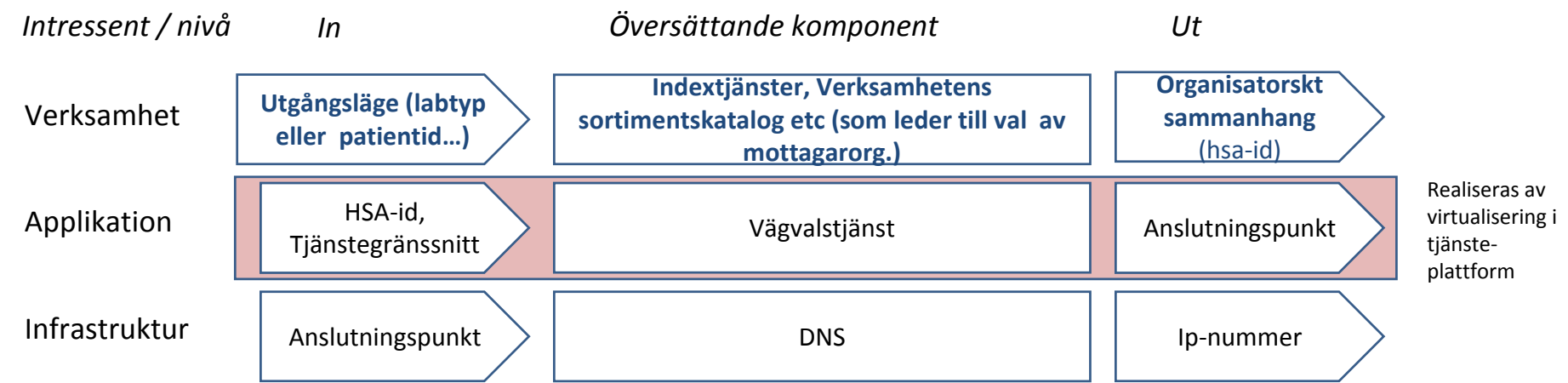
- T-bokens modell över adressering
 - Uppdaterad/kvalitetssäkrad av PoC



Addressering i praktiken

Schematisk bild av ansvarsfödelningen för adressering i olika nivåer.

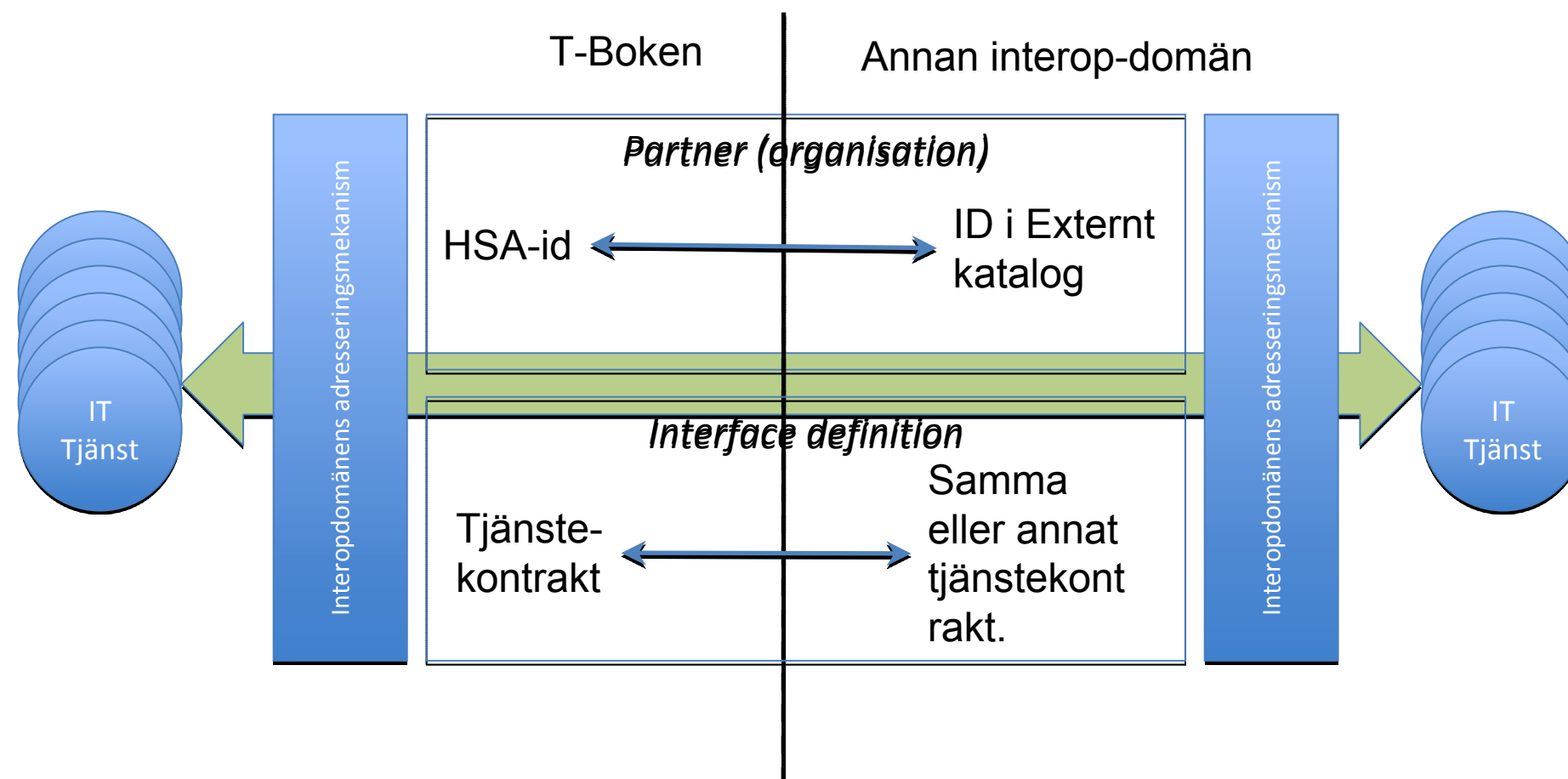
T-boken



Tjänsteväxel behöver brygga de begrepp som ligger till grund för adressering i runtime:

- HSA-id för adresserad verksamhet
- Tjänstekontrakt (ev. också ett HSA-id). Beskriver ett gränssnitt som en eller flera IT-tjänster realiserar. Det kan t.ex. realiseras av integrationstjänster och anslutningstjänster.

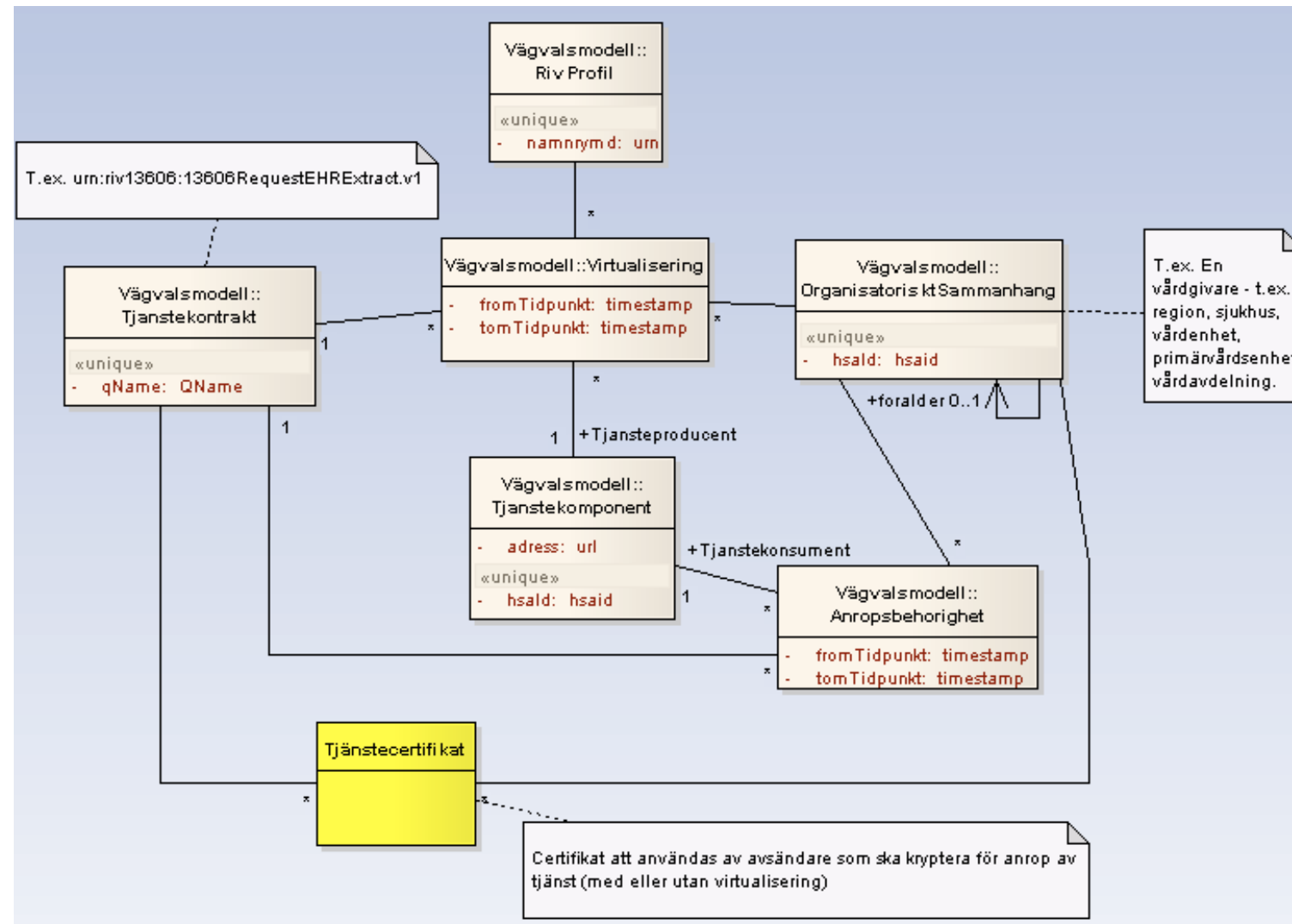
Bryggning av Adresseringsmodeller



Säkerhet

- Långsiktigt
 - Krav på end-to-end-säkerhet
 - WS-Security (T-boken) utan behov av tjänsteväxel
 - Säkerhetsmodell integrerad med adresseringsmodell och WS-Trust
- Kortsiktigt
 - Nuvarande säkerhetsstandards inom myndigheter behöver bryggas
 - Meddelande-säkerhet enligt WS-* troligen ovanlig
 - Medför “degradering” av säkerhetsnivå vid tjänsteväxel
 - Brandväggars inverkan vid kanalkryptering?
 - Vilka brandväggspolicies finns inom myndigheter och inom sjunet?

Integration av säkerhetsmodell



Tjänsteinteraktioner

- Innehållsbrygning är en separat tjänst - ej del av tjänsteväxel
- När finns behov?
 - Om Vård och myndighet båda har nationell standard för samma logiska tjänst
 - Den som “förlorar” förhandlingen gömmer konvertering bakom situationsanpassad brygg-tjänst
 - Vi tror detta är ett undantagsfall!
- Om enighet kring ett tjänstekontrakt som gemensam nationell tjänst (och produkttyp)
 - Två namn, två kataloger – fortsatt översättningsbehov för adressering
- Tjänsteinteraktionstyper
 - Kan vi begränsa kraven till T-bokens enkla modell?
 - RIV ställer mycket komplexa krav, som kanske kan bantas tills vi sett konkret behov?

Teknisk kuvertering

- Krav
 - Konvertera mellan olika RIV-versioner och olika versioner av standards från andra domäner

Teknisk arkitektur

- Hur ser en deploymentarkitektur ut?
- Tjänsteväxels federering?
- Todo....

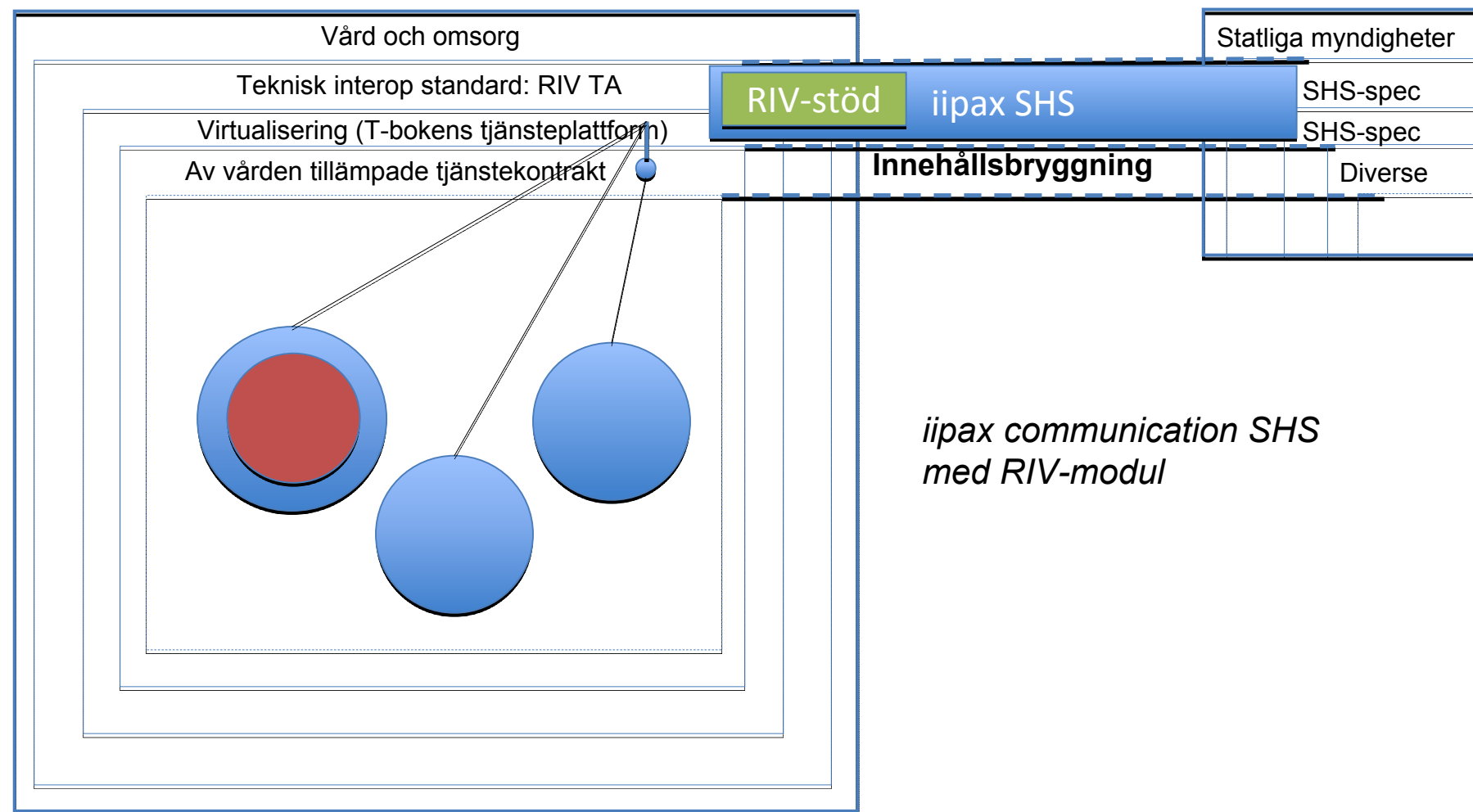
Utvärderade kandidater

- Försäkringskassan / SHS
 - Utvärdering fokuserad på SHS och RIV-brygga
 - EJ I DRIFT IDAG FÖR VÅRDEN
- VIF-lösning mot Skatteverket
 - Specifik lösning som vi kan lära ifrån
- Utvärderingarna är uppställda efter beskrivna perspektiv (från adressering och vidare)

Bakgrund SHS

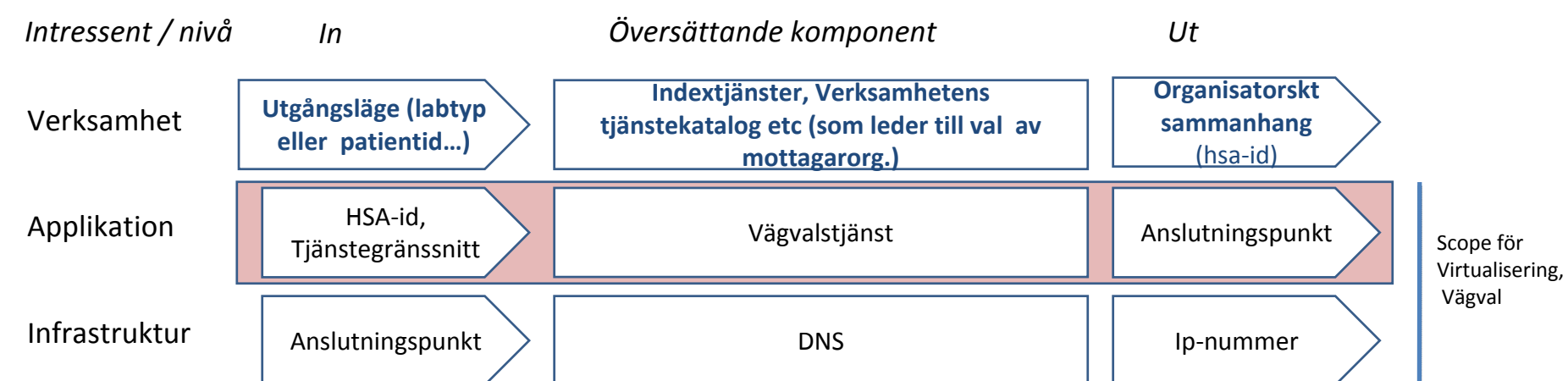
- En specifikation – ägs av kammarkollegiet
 - Specificerar ett protokoll och en arkitektur i vilken protokollet verkar, inklusive en katalog för bilaterala avtal, tjänstekontrakt och partner-register
 - Implementationer valideras av Ladoc (Umeå)
 - Ladoc (Umeå) driftar nationella SHS-katalogen
- Tillgängliga implmentationer (avropas mot Verva-avtal)
 - Ida InFront (iipax communication SHS)
 - Ledande implementation (utbredning, antal meddelanden)
 - Bygger på generellt bryggningsramverk där SHS-protokollet är ett exempel på tillämpning
 - Byggt på modern plattform (Java EE), kan driftas i stort antal kombinationer avseende fabrikat på JavaEE-servrar och databaser
 - Erbjuder som enda implementatör teknisk brygging mellan RIV TA och SHS-protokollet (avropsbar via Verva)
 - Curalia
 - Ej full implementation (ej validerad mot spec)
 - Bygger på Öppen-Källkod-ESB Service Mix
 - Sirius IT
 - En produkt som bara används som SaaS (“tjänsteväxel som molntjänst”)
 - Små kunder med låga säkerhetskrav

iipax communication SHS

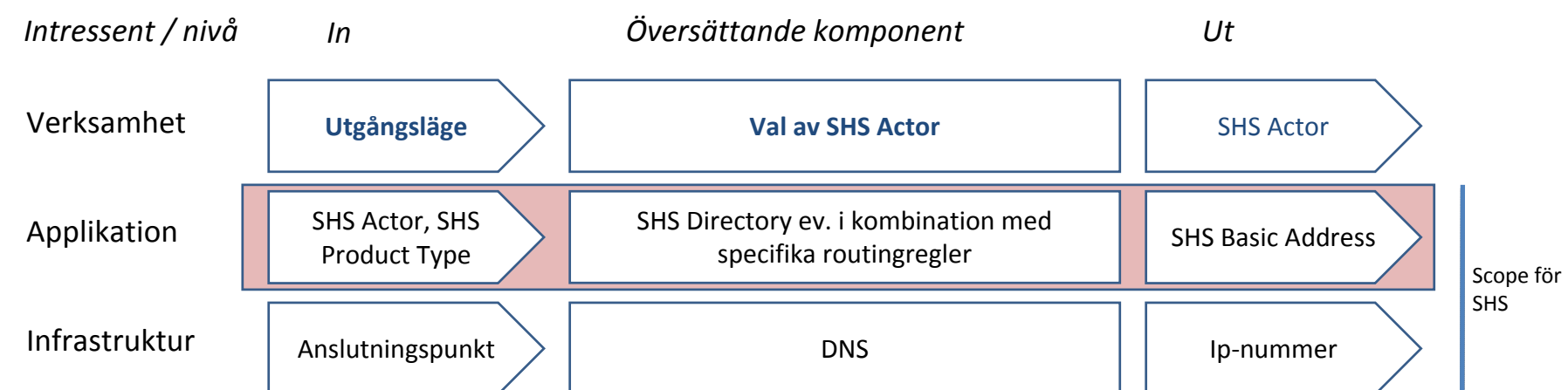


Addressering

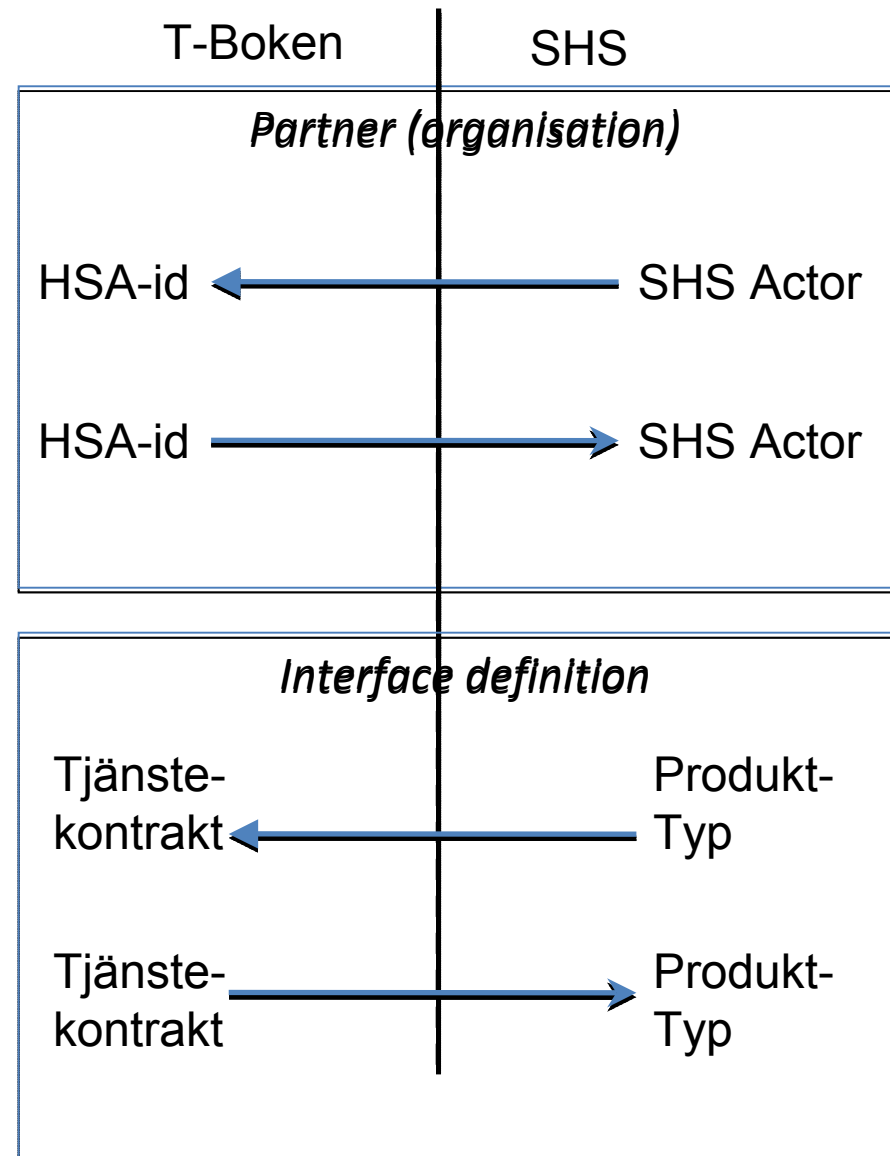
T-boken



SHS



Bryggning Adressering SHS



Adressering: Bryggning Partner

- T-bok -> SHS
 - Mottagande myndighet behöver finnas med HSA-id i HSA
 - Detta HSA-id anges av konsumenten som RivHeaders ReceiverId
 - SHS-RIV-nodens adress pekas ut av vägvalstjänst baserat på organisationens HSA-id (som vanligt)
 - SHS-RIV-modulen läser av HSA-Id och använder HSA för att hämta organisationsnummer (SHS Actor)
- SHS -> T-Bok
 - Tjänstekonsument hos myndighet bygger upp SHS Actor med organisationsnumret för organisationen i vården som ska adresseras. Om enhet inom vårdorganisation är mottagare, adderas vårdenhetens HSA-id till SHS Actor av tjänstekonsument.
 - SHS-RIV-modulen använder vårdenhetens HSA-id som ReceiverId om sådan finns, annars anropas HSA för att översätta orgnummer till HSA-id.
 - senderId sätts till organisationsnumret för avsändande organisation, med prefix SHS, vilket ger virtualiserade tjänsten möjlighet att verifiera anropsbehörighet.

Adressering

Bryggning Tjänstekontrakt

SHS --> T-boken

- Ingen bryggning behövs
 - Tjänstekontrakt är automatiskt angivet av avsändaren eftersom det identifieras av rotelementets namnrymd.

Adressering

Bryggning Tjänstekontrakt

T-boken -> SHS

- RIV-SHS-modulen mappar rotelementets kvalificerade namn (som identifierar tjänstekontrakt) till produkttyp via intern mappningstabell eller info i SHS-katalogen

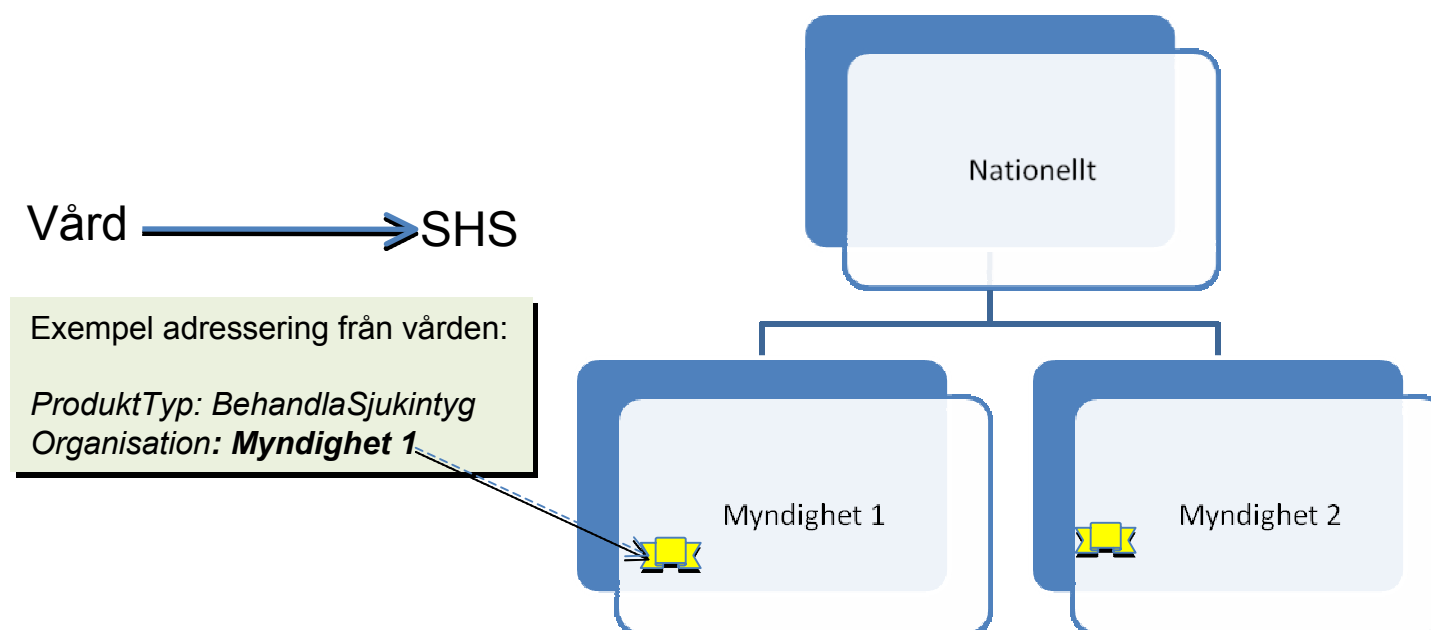
Adressering - Sammanfattning

- Samma adresseringmodell i T-boken och SHS
 - De är systematiskt bryggbara
 - Ingen situationsspecifik routing behöver konfigureras
- SHS-organisationer behöver finnas i HSA-katalogen

Säkerhet

- WS-Security
 - SHS har internt kanoniskt kuvert och stödjer därför I dagsläget inte standards där kryptering av payload smittar header
 - Ej stöd för brygning av WS-Security
- SHS-tjänsteväxel (RIV-modulen) får agera “ändpunkt” på samma sätt som t.ex. i VIF
 - Vården -> SHS: Dekryptera fråga, kryptera svar, lämna över till SHS-bussen.
 - SHS -> Vården: Omvända

Säkerhetsmodell SHS



Avsändaren krypterar med certifikat för mottagande organisation.
Motsvarar i praktiken ett certifikat per SHS-instans (en per myndighet). Betyder att myndighetens SHS-nod måste dekryptera.

Uppfyller ej kravet på end-to-end-säkerhet lioch med omkryptering i tjänsteväxel.

Säkerhet – Sammanfattning

- SHS-myndigheter använder idag ej WS-Security
- SHS saknar stöd för WS-Security
- Generellt: SHS kan inte hantera säkerhetskoncept som “smittar” transporten utanför payload
- Kryptering behöver ske på applikationsnivå för att kunna hanteras utan omkryptering i tjänsteväxel
 - Vid kanalkryptering och vid brygging mellan RIV- och kanalkryptering sker omkryptering
 - Om meddelandet krypteras på applikationsnivå med personlig krypteringsnyckel (jämte e-signering) skapas insynsskydd end-to-end

Tjänsteinteraktioner

- Tjänsteinteraktionstyper
 - Kan vi enas om T-bokens enkla modell?
 - RIV ställer mycket komplexa krav, som kanske kan bantas tills vi sett konkret behov
- Interaktionsmönster
 - RIV-bryggan är ett försök att implementera RIV-specifikationens interaktionsmönster, men inte funnit tillräcklig information kring ackningsmönster på olika nivåer för att kunna verifiera realiseringen.
 - Täcker förmodligen T-bokens krav på interaktionsmönster
- SHS saknar koncept för Tjänstekontrakt
 - Hanterar enskilda operationer inom tjänstekontrakt som tjänstekontrakt
 - Kallas ProduktTyp i SHS
 - Skillnaden i granularitet har ingen praktisk betydelse vid bryggning av adressering

Teknisk kuvertering

- Bryggfunktion översätter mellan RIV och SHS-kuvertering
 - Översättning mellan kuverteringsformat (headers)
 - Översättning av adresseringsidentiteter
 - Tjänstekontrakt (operation i tjänstekontrakt) <-> ProduktTyp
 - HSA-id (organisation) <-> SHS-Actor

RIV-modul för SHS

- Kvittenshantering
 - Leverantören anser inte kvittenshanteringen vara implementerbar (någon variant pilotmässigt implementerad)
- Generella kommentarer från implementatör
 - RIV Brygga ej använd i praktiken
 - RIV oprecis och komplex spec.
 - Valda delar implementerade efter bästa förmåga
 - Adresseringsarkitektur saknas för RIV
- RIV-SHS-modulen behöver vidareutvecklas och testas i POC
 - Bör slutföras mot en uppdaterad RIV med T-bokens adresseringsmodell införd hos vården
 - Leverantören rekommenderar vidareutveckling tillsammans med verkligt pilotprojekt

Teknisk arkitektur

- Vården kan starta med en SHS-nod
- Utskalning kan vid behov ske genom att partitionera trafik n
 - T.ex. 5 tjänstekontrakt per SHS-Nod
 - T.ex. Fördela trafik över ett antal noder med vårdgivare som bas
- Försäkringskassans SHS-nod kan tekniskt sett användas
 - Kan övervägas under pilotfas om IVF2 är pilot för tjänsteväxel

Sammanfattning SHS

- En teknisk ingång till SHS-myndigheternas samtliga tjänster
 - Regleras genom konfiguration av anropsbehörigheter
- Adressering är fullt interoperabel med T-bokens referensarkitektur
 - Kan verifieras med befintlig POC
- SHS-RIV-modulen behöver vidareutvecklas och kvalitetssäkras
 - Förutsätter kvalitetssäkring av RIV tekniska anvisningar
- iipax tjänsteväxel för SHS är byggd på en modern plattform
- Välutvecklade funktioner för övervakning, loggning och spårning
- I viss mån en konkurrensutsatt marknad, då den är baserad på en specifikation med flera implementatörer
- Kan ej brygga WS-Security med WS-Trust vilket framtvingar omkryptering

Informationskällor

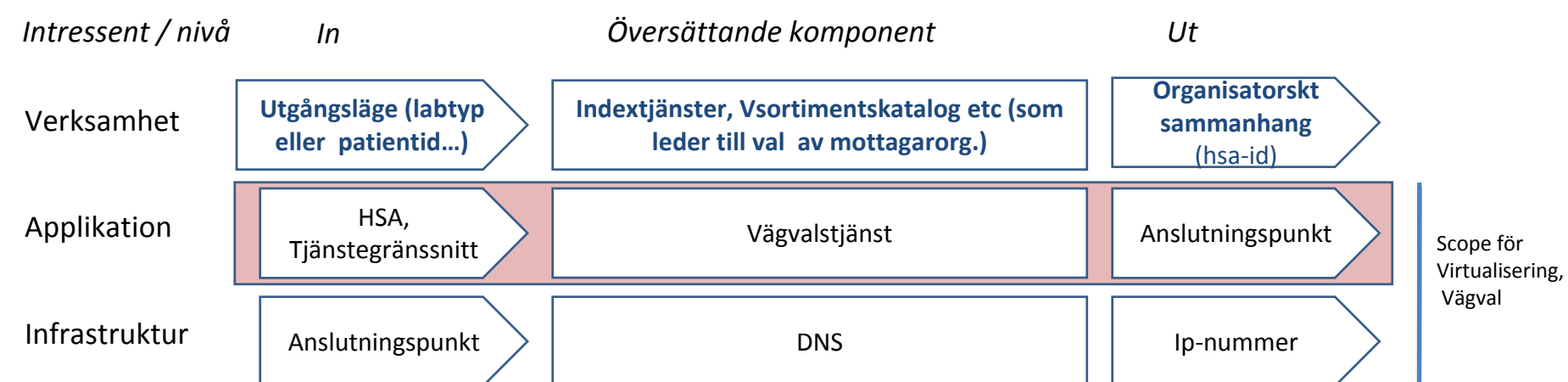
- Intervju med Keijo Ojala, Försäkringskassan
- Intervju med Håkan Svenson, Ida Infront AB, leverantör av försäkringskassans SHS-växel.
- Kammarkollegiets hemsida
 - http://avropa.se/templates/ramavtalsomrade___1180.aspx

Bakgrund VIF

- Integrationstjänst för vårdens registrering av nyfödda hos skatteverket
- Ej generell tjänsteväxel, men belyser väl frågeställningar som behöver systematiseras

Kompatibla adresseringmodeller

T-boken



VIF

Adresseringsmodell ej systematiserad då behov ej föreligger för den specifika tillämpningen. T-bokens adresseringsmodell ej tillämpad,

Säkerhet

- VIF-tjänsten agerar orkestrerande tjänst. Dess arkitektur saknar därmed mekanismer för end-end-säkerhet (trust) mellan parterna vars kommunikation ska bryggas.
 - Detta ligger helt i linje med de specifika krav som drivit utveckling av tjänsten. Den är resultatet av ett utvecklingsuppdrag för en koppling mellan två specifika aktörer.
- Tjänsten är därmed tillämpningsspecifik med avseende på...
 - Vilka säkerhetsmodeller som tillämpas av integrerade parter
 - Vilket adresseringsbehov som finns för den specifika lösningen
 - Vilken riv-version som används
 - För applikationen specifika behörighetsbehov (specade men ej realiserade)
- Säkerhetsnivåer
 - På vårdsidan tillämpas i detta fall en säkerhetsnivå som saknas hos Skatteverket (“utsidan”)
 - RIV följs därmed säkerhetsmässigt väl mellan journalsystem-användaren och VIF-tjänsten, men nyttan av denna ambition kan ifrågasättas ur ett kortsiktigt praktiskt perspektiv. Fram tills T-boken och RIV utökats med en trustmodell för mediering som också statliga myndigheter tillämpar har meddelandesäkerhet (kryptering) ingen praktisk säkerhetshöjande effekt utöver den kanalsäkerhet som ändå föreskrivs.

Tjänsteinteraktioner

- VIF
 - VIF hanterar specifikt tjänsteinteraktionen Födelseanmälan (dock utan semantisk bindning till det verksamhetsmässiga meddelandet)
 - VIF genomför applikationsspecifik auktorisationskontroll
- Ägare
 - Skatteverket är ägare av det nationella formatet
- Metod och beskrivning
 - Formatet är framtaget med RIV-metoden
 - Abstrakt tjänstebeskrivning saknas (enskilda meddelanden är beskrivna på V-nivå, men inte roller och deras interaktioner)
 - Abstrakt beskrivning ej åtskild från teknisk lösning

Tjänsteinteraktioner...

- Några avvikelser från RIV TA et al.
 - WSDL refererar ej schema
 - Bristen finns inte i tjänstebeskrivningen, utan i den faktiska artefakten, som därmed avviker från tjänstebeskrivningen
 - WSDL kan ej användas för att validera (hos producenter och konsumenter)
 - Försvårar realisering för anslutningar och konsumenter
 - WS-Policy används ej
- Några avvikelser från T-boken
 - Versioneringsstrategi saknas (utökningsbarhet utan att bryta bakåt/framåt-kompatibilitet)

Deployment/Drift

- Deployment-topologi ej definierad
 - Relation till HSA-katalog viktig att förtydliga
 - Regional eller nationell katalog ? Krav på SLA för HSA?
- Tillgänglighetskrav ej redovisade
- SAD i behov av uppdatering
 - Skrivfel kring Javaversioner och ansvar för behörighetskontroller

Slutsatser, VIF

- VIF som lösning för komponenten Tjänstväxel i den nationella arkitekturen?
 - Ej tillämbart, då det är en applikation för en specifik integration
 - Uppskalning innebär ny mjukvara att utveckla, drifta och förvalta för varje brygningsbehov. Det är alltså inte en tjänstväxel utan ett sätt att utveckla enskilda integrationstjänster .
- Som förebild/förlaga för kortsiktig utveckling av liknande tjänster
 - För nästa projekt med motsvarande behov är det bäst om nationella komponenten Tjänstväxel kan utvecklas och användas
 - Om ett projekt behöver en lösning för extern kommunikation innan Tjänstväxeln finns på plats kan VIF användas som mall (efter att påpekade brister åtgärdats). Skulle då med fördel ges en tydligare uppdelning i integrationstjänst och brygg-tjänst
- T-boksgranskning av den specifika lösningen (ej ur brygg-perspektiv)
 - Anmärkningar finns vad gäller tjänstekontraktets tekniska utformning
 - Intern arkitektur bedöms vara god (dock utanför T-bokens ansvar)
 - Tillgänglighetskrav ej redovisade
 - Driftsarkitektur (deploymentarkitektur) behöver fastställas, speciellt m.a.p. HSA-integration och överensstämmelser mellan SLA för VIF och HSA
 - HSA ej integrerad
- Att återföra till AL
 - Projekten behöver en generell policy för hotbilden inom Sjunet att förhålla sig till
 - Policy för användning av enklare säkerhetsmodell än WS-Security behöver finnas på kort sikt för brygning. WS-Security i VIF har drivit mycket kostnad utan tydligt identifierbara värden.
 - TIS-dokumentet är en sammanblandning av V, I, T och specifik tjänst
 - Bra struktur på SAD. Avsnittet "Arkitekturmål" skulle med fördel föras in i SAD-mallen för granskningsprocessen.

Informationkällor

- VIF
 - VIF-SAD-v0.2.pdf
 - VIF_Födelseanmälan_baskrav_v0.1.pdf
 - VIF_Födelseanmälan_tjänstebeskrivning_v0.2.1.pdf
 - Beskrivning_Testbank1_v1.0.1a.pdf
 - Installation_VIF_Testbank1_v1.0.1.pdf
 - Releasetext_Testbank1_v1.0.1.pdf
 - RIV_TIS_VIF_v0.8.doc
 - Intervju med Sari Sahlsten, Omegapoint, 2009-02-04

Information från intervju

- WSDL i tjänstespecifikation avviker från verklig WSDL
- HSA-kopplingar har inte införts (varken behörighet eller tjänsteadressering)
- Krav på tillgänglighet ej kända
- Skrivfel i SAD m.a.p. Javaversioner och JavaEE-beroende. Ska vara Servlet 2.5 och Java SE 6

AL-restpunkter

- Nya principer till T-boken
 - Förtydliga ansvarsförhållanden kring innehållstransformering (representation)
 - Förslag finns som anteckning till denna bild
 - Princip om att söka beprövade lösningar (best-practice)
- Policy för säkerhetsmässiga hot i Sjunet
 - Så att projekten ej behöver utreda frågan inom ramen för internt arkitekturarbete