STIL-ramverk

En ansats för samverkan i samhället

STIL-ramverk

Samordnade Tjänster för Information och Ledning

Utgåva 1. En ansats för samverkan i samhället.

Boken finns att tillgå i PDF-format.

107 85 STOCKHOLM

Bokens version 9-6.

För mer information se

www.opensis.org

Framtagen i samverkan mellan:

FÖRSVARSMAKTEN

KRISBEREDSKAPS MYNDIGHETEN

Krisberedskapsmyndigheten

Krisberedskapsmyndigheten (KBM) samordnar arbetet med att utveckla krisberedskapen i det svenska samhället. Tillsammans med kommuner, landsting, myndigheter, näringsliv och organisationer minskar vi samhällets sårbarhet och förbättrar förmågan att hantera kriser.

Ett led i detta arbete är att stödja aktörerna i krishanteringssystemet så att robusta lokala, regionala och nationella kommunikations- och informationssystem vid behov kan samverka för att stärka samhällets säkerhet och beredskap.

KBM har ingen föreskriftsrätt i frågan om hur myndigheters system byggs eller hur information delas mellan aktörer i krishanteringssystemet. Vi tror dock att den arkitektur och det regelverk som beskrivs i denna skrift kan utgöra en gemensam plattform och grund för utveckling av system. Härigenom skapas grunden för en gemensam lägesbild och ett koordinerat beslutsfattande hos de olika aktörerna.

KBM kommer att verka för att sprida STIL-ramverket så att det kan utgöra ett underlag för anskaffning av nya verksamhetssystem inom sektorerna. Vi är övertygade om att utveckling enligt ramverket kommer att bidra till verksamhetsnytta både vid kris och i vardagen.

Lars Löfqvist

KBM, Tekniska enheten

Försvarsmakten

Försvarsmaktens ledningssystemutveckling fas 2 mot det nätverksbaserade försvaret (NBF) avslutades 2006-12-31. Resultaten från denna fas visar att den valda inriktningen mot ett nätverksbaserat försvarskoncept är lämplig och möjlig att uppnå. Införandetakten och ambitionsnivån kommer att styras av resurstillgång och operativa prioriteringar. Men också sett mot behovet av att ha en koordinerad förmågetillväxt med viktiga samarbetspartners - nationella och internationella, civila och militära.

Resultaten och erfarenheterna från genomförd verksamhet lägger nu grunden för ett införande av konceptet nätverksbaserat försvar inom Försvarsmakten. Bland annat finns nu underlag för att inrikta anskaffningen i närtid av ledningssystem mot effektivare lösningar.

På det internationella planet har arbetet gett möjlighet till att tidigt få ta del av utvecklingen av operativa ledningsmetoder och tekniska vägval. Detta med grunden i ett helhetsbaserat civil-militärt effekttänkande. En utveckling motsvarande vår egen och med motsvarande tidsförhållanden pågår även hos våra viktigaste internationella samarbetspartners. Genom det ökade internationella samarbetet som möjliggjorts genom NBF-utvecklingen skapas interoperabilitet. Det ges även möjligheter till vinster i form av förbättrad kvalitet och lägre anskaffningskostnader, t ex genom gemensam kravställning och/eller anskaffning.

På det nationella planet vill Försvarsmakten bidra till en utveckling som möjliggör att samverkan mellan myndigheter förbättras vid katastrofer, kriser och konflikter. Om myndigheter och organisationer tillämpar bokens regelverk och arkitektur vid utvecklingen av olika ledningssystem förbättras förutsättningarna för att åstadkomma en gemensam lägesbild som underlag för koordinerat beslutsfattande. Med gemensam lägesbild och ensade kommunikationsgränssnitt skapas förutsättningar även nationellt för ett mer helhetsbaserat civil-militärt effekttänkande.

Denna boks regelverk och arkitektur bygger således på resultaten från genomförd NBF utveckling. Den är ett led i utlovad resultatöverföring från Försvarsmakten till andra myndigheter.

Michael Moore

Försvarsmaktens utvecklingschef

Introduktion till STIL-ramverk

Information, samverkan och ledning är nyckelbegrepp i dagens och morgondagens samhälle. Med rätt information och med insiktsfull ledning kan organisationer mer målmedvetet och välgrundat svara upp mot samhällets krav. Ett ramverk för Samordnade Tjänster för Information och Ledning (STIL) skapar förutsättningar för optimalt anpassad information och därmed effektivare samverkan mellan organisationer.

STIL-ramverk, som beskrivs i denna skrift, redovisar en helhetssyn, som visar hur man kan utveckla förutsättningar för samverkan, med fokus på information. Ramverket beskriver ett flexibelt och robust koncept för hur befintliga informationssystem kan nyttjas effektivt och ekonomiskt. I konceptet läggs extra vikt vid integritet, sekretess och anpassad säkerhet för samverkan.

Ett komplext samhälle i snabb utveckling innebär ständigt nya utmaningar, som ofta överskrider en enskild organisations egna resurser för utveckling och nya investeringar. Genom att skapa samverkan före, under och efter insats, kan organisationer med olika förmågor skapa ett effektivt nyttjande av samhällets resurser. Detta gäller såväl vid hantering av vardagsolyckor som extraordinära händelser.

Organisationer och myndigheter blir alltmer beroende av att kunna utnyttja och utbyta information med hög tillgänglighet, säkerhet och effektivitet. I samhället finns mycket att vinna på att stödja utbyte av informationsresurser från flera aktörer anpassat efter kända, men också helt nya icke förutsägbara behov.

En informationsinfrastruktur stödjer samverkan genom regelverk, metoder och teknik som ger tillgång till information på ett flexibelt och behovsdrivet sätt. Grunden för detta är en tjänstebaserad arkitektur. Tjänstebaserad samverkan ger möjlighet till informationsutbyte med situationsanpassad integritet och informationssäkerhet.

En gemensam samverkansarena, inom informationsinfrastrukturen, ger ett bättre stöd för att identifiera utmaningar och hot, formera

insatsresurser så att de svarar mot uttalade behov, och genomföra uppdrag och insatser med samsyn på ett flexibelt och effektivt sätt.

Genom att samverkande organisationer har tillgång till varandras information, läggs grunden för att de kan agera samordnat. Information från flera källor kan sättas samman till ”gemensam lägesinformation”, att användas vid ledning och styrning av insatser.

STIL-ramverk baseras bl a på resultat från Försvarsmaktens arbete med att ta fram en flexibel och kvalitetssäkrad arkitektur för ledning och information. Arkitekturen har till stor del prövats och verifierats inom ledningssystemarbete i projekt för det nya svenska Nätverksbaserade Försvaret. Den utvecklingsmiljö som levereras som del av STIL-ramverket, är sedan tre år i drift vid försvarsmaktens ledningssystemutveckling. Konceptet har också prövats vid projekt för civil ledning och informationssamverkan vid Security Arena, Lindholmen Science Park.

STIL-ramverket ger en grund för Samordnade Tjänster för Information och Ledning i samhället. Denna skrift är indelat i tre delar.

Del 1 ger en introduktion till ramverkets grundprinciper och teori. Här beskrivs olika förutsättningar och begrepp för information och informationsinfrastruktur. Den struktur som samverkan kan byggas på, viktiga ställningstaganden såsom säkerhetsaspekter m m redovisas.

Del 1 består av fyra huvudkapitel, som ringar in grundprinciper och grundbegrepp inom STIL-ramverk. Denna del av ramverket bör läsas som en helhet och ger också förutsättningar för djupare läsning i Del 2 av ramverket.

I Del 2 återfinns ett antal beskrivningar, så kallade ”White papers” med grunder, regler, metoder och synsätt som bör gälla för samverkan utifrån den gemensamma informationsinfrastrukturen. Häri redovisas fördjupningar för ett antal olika frågeställningar inom området.

Del 2 gör inte anspråk på att vara heltäckande, utan dessa avsnitt kan läsas fristående av varandra. Dock återfinns en hel del introduktion till fördjupningarna inom Del 1.

Del 3 introducerar en integrationsmiljö för utveckling och användning av tjänster. Denna miljö är fri att använda för prov och försökstillämpningar.

Genom att använda ramverkets idéer för prov och försök, projekt och prototyper i operativ miljö hos civila organisationer, myndigheter och andra intressenter kan denna grund utvecklas vidare. Kombinerat med det bör STIL-ramverk vidareutvecklas genom att ta tillvara ytterligare resultat från ledningssystemutveckling vid Försvarsmakten.

Del 1

Del 2 (*detaljer på följande sidor*)

Del 3

Referenser

Del 1

Grunder

Inledning till Del 1 – STIL-ramverk

STIL-ramverk erbjuder en grund för samverkan i samhället. Grunden bygger på en gemensam informationsinfrastruktur, med koncept för regler, metodik och teknik.

Del 1 i denna skrift ger en introduktion till ramverkets grundprinciper och teori. Här beskrivs olika företeelser och begrepp för information, arkitektur och informationsinfrastruktur. Genom att utnyttja den fulla potentialen i informationsinfrastrukturen, skapas en startpunkt för att växa in i framtiden, med ökande grad av enkla och flexibla samverkansformer**.**

Läsanvisning

Del 1 består av fyra huvudkapitel, som ringar in grundprinciper och grundbegrepp inom STIL-ramverk. Denna del av ramverket bör läsas som en helhet och ger också förutsättningar för djupare läsning i Del 2 av ramverket.

I kapitel 1 presenteras grundbultar för att åstadkomma flexibla och kostnadseffektiva system för ledning och ledningsstöd. Grundbultarna består av några **arkitekturprinciper**, som genomsyrar systemens uppbyggnad och dess förmåga att stödja en effektiv verksamhet.

Kapitel 2 presenterar begrepp och förutsättningar väsentliga för att förstå och grunda en gemensam **Informationsinfrastruktur.** Informationsinfrastrukturen utgör en viktig framgångsfaktor för flexibel och behovsdriven samverkan med stöd av informationssystem.

Kapitel 3 **Informationsinfrastrukturen ur flera perspektiv** ger en helhetsbild av systemtänkandet (i vid bemärkelse). Där behandlas infrastrukturens viktiga byggstenar med förutsättningsskapande och tekniska system för samverkan.

I kapitel 4 om **Säkerhet**, redogörs för en säkerhetsarkitekturmodell omfattande säkerhetsadministration jämte säkerhetsmål, säkerhetsmekanismer och säkerhetsobjekt. I kapitlet diskuteras också avvägningen mellan flexibilitet och säkerhet.

1. Arkitekturens grundprinciper

1.1. Inledning

I detta kapitel beskrivs några fundamentala tendenser i samhället tillsammans med de konsekvenser dessa tendenser har för systemkonstruktion och systemimplementering på en arkitekturnivå.

För att hantera konsekvenserna introduceras ett antal arkitekturprinciper och arkitekturbegrepp som kan användas för att åstadkomma flexibilitet och kostnadseffektivitet. Principerna handlar bland annat om att separera olika systemdelar och göra dem mer självständiga.

1.2. Tendenser i samhället

Samhället förändras. Detta medför att det, förr eller senare, blir nödvändigt att förändra sättet att konstruera och implementera de system som används i samhället. Förändringen behöver, i praktiken, inte innebära ett stort revolutionerande paradigmskifte, i betydelsen att nuvarande principer blir passé, utan snarare att relationen och vikten för olika idéer och principer kommer att förändras.

Här följer några utvecklingstendenser i samhället som gör att det behövs nya sätt att konstruera system.

Mer information

Mer information kommer att behöva sammanställas för att kunna fatta bättre beslut i fler situationer. Detta gör att de system som behövs blir mer komplexa.

Sammanställning av större mängder information medför också att information behövs från många olika källor som till och med kan tillhöra olika organisationer. Detta ger komplikationer genom att "informationsägandet" blir distribuerat och att "revirtänkande" blir vanligt.

För att kunna använda information från många olika källor på ett kostnadseffektivt sätt kan inte varje enskilt system "äga" sina egna informationskällor utan dessa måste samutnyttjas av flera olika system.

Större system

Genom att nya system blir alltmer omfattande kommer nyutveckling framförallt ske genom integrering av befintliga system. System kommer därför i första hand att kommunicera med andra system och bara i andra hand med mänskliga användare. Den mänsklige systemanvändaren kommer inte att vara den som kommunicerar information mellan olika system genom att läsa från ett system och mata in i ett annat system. Människan blir mer av en övervakare som ser till att informationen flyter rätt och som bara ingriper om något går snett.

Snabbare förändringar

När samhället förändras i en allt snabbare takt behövs en allt snabbare reaktion på nya tendenser i samhället. Detta kan gälla nya hot såväl som nya strömningar. För att kunna möta nya hot samt utnyttja alla nyheter behövs en kort "time to market". Detta blir enbart möjligt om utvecklingstiden för nya system blir allt kortare.

Automatisering av fler uppgifter

Kostnadsjakten medför att allt fler uppgifter behöver automatiseras. Kostnadsjakten medför också att olika uppgifter blir alltmer standardiserade och anpassade till sitt sammanhang. När sammanhanget ändras är realiseringarna ofta inte så flexibla att de kan användas i det nya sammanhanget.

Så, om inget radikalt händer, kommer utvecklingstiden att ökas eftersom vi bygger större system men också att behöva minskas eftersom systemen behöver anpassas till förändringar i omgivningen som sker fortare och fortare. Detta är naturligtvis en ohållbar situation och principerna för design och implementering av system måste förnyas.

1.3. Arkitekturprinciper och arkitekturbegrepp

För att möta de tendenser som beskrivs ovan är flexibilitet och kostnadseffektivitet viktiga egenskaper som blir drivkrafter i utvecklingen. Användbarhet, skalbarhet etc. är andra viktiga egenskaper som måste hanteras men dessa är inte lika drivande. Säkerhet är ytterligare en annan mycket viktig egenskap som måste bibehållas på en hög och acceptabel nivå vilket ställer nya krav, speciellt genom den ökade flexibiliteten.

Arkitektur handlar om att formulera regler för hur man strukturerar system samt hur delarna i strukturen samverkar. Genom att välja en viss arkitektur för ett system gör man det möjligt för systemet att få vissa egenskaper. Arkitektur handlar därför om hur man strukturerar system på en hög abstraktionsnivå för att lättare uppnå vissa önskade egenskaper hos systemen.

Två principer som är viktiga för att åstadkomma flexibilitet och kostnadseffektivitet är:

- *Separering av skapande och användande av information.*

  Den som skapar information vet inte hur informationen behöver användas i framtiden. En överdriven anpassning av representation och format till en viss användning kan försvåra ett alternativt användande i framtiden.

- *Separering av olika delars livscykel.*

  Genom att från början separera olika delar och göra dessa alltmer självständiga och oberoende kan dessa delar användas på flera ställen och i flera sammanhang.

Lös koppling mellan olika delar i ett system ger möjlighet till nya konfigurationer av olika delar samt möjlighet att separera livscykeln i de olika delarna. Lös koppling eftersträvas i flera olika avseenden:

- mellan mjukvara och hårdvara (funktionalitet och plattform)
- mellan tjänstebeskrivningar och tjänsteimplementeringar
- mellan tjänsteimplementationer
- mellan lokalitet (deployment) och funktion
- mellan affärslogik och infrastruktur

Den lösa kopplingen ger oberoende delar som kan kombineras i nya konfigurationer vilket ger flexibilitet.

Olika arkitekturbegrepp har introducerats för att, på olika sätt, hantera dessa principer. Begreppen *System-av-system, Tjänsteorienterade arkitekturer, Separering av affärslogik och infrastruktur, Nätverksorienterade system, Dynamisk konfigurering för att skapa situations-*

anpassade system och *Gemensam informationsutbytesmodell* beskrivs närmare nedan.

System-av-system

System-av-system är ett nytt systembegrepp som används för att beskriva att man kan bygga storskaliga system genom att integrera många oberoende, självständiga system. Motsatsen till system-av-system är system-av-delsystem där delsystemen har definierats, designats och implementerats för att passa i ett bestämt och väldefinierat sammanhang som utgörs av det omgivande systemet. I ett system-av-system kan delarna, i termer av de oberoende systemen, användas i många olika sammanhang och till flera olika saker medan ett delsystem i ett system-av-delsystem endast fungerar i ett sammanhang. Man kan säga att ett delsystem alltid har samma livscykel som det omgivande systemet medan systemen i ett system-av-system kan ha oberoende livscykler.

Ett speciellt sammanhang där system-av-system begreppet naturligt uppkommer är när man integrerar olika verksamheter med olika redan utvecklade system. Dessa system är definitionsmässigt oberoende och självständiga och integreringen ger naturligt ett system-av-system.

Ett problemområde inom system-av-system är hur man skall balansera utveckling av oberoende system samtidigt som dessa också ska kunna användas som komponenter i tätt integrerade system.

Tjänsteorienterade arkitekturer

I en tjänsteorienterad arkititektur betraktas ett system som en uppsättning tjänster. Detta ger en modularisering och lös koppling mellan olika implementeringar av funktionalitet (affärslogik). Den lösa kopplingen ger möjlighet att kombinera tjänsteimplementeringar på olika sätt och därmed uppnå stor flexibilitet för olika användningsområden och användare.

Separering av affärslogik och infrastruktur för säker samverkan

En anledning till att separera affärslogik och infrastruktur är att infrastrukturen är en gemensam resurs för alla delar, som implementerar olika former av affärslogik. Genom att den är gemensam kan kostna-

den för utveckling och underhåll delas och man kan därmed skapa bättre kostnadseffektivitet.

Genom separeringen kan man också ha olika livscykler på affärslogik och infrastruktur. Därmed kan teknikförändringar inom ett område göras möjliga att utnyttja utan att det påverkar det andra området.

Nätverksorienterade system

I ett nätverksorienterat system finns en gemensam del, nätverket, som hanterar kommunikationen mellan alla delar i systemet. Kommunikationen hanteras på ett gemensamt sätt och nätet förmår att dynamiskt skapa kommunikation mellan godtyckliga accesspunkter. Flexibiliteten blir därmed mycket stor genom att man inte på förhand behöver bestämma olika kommunikationsvägar. Det finns då en potential för olika tjänsteimplementationer att kunna flyttas mellan olika accesspunkter och för att introducera helt nya tjänster vid godtycklig tidpunkt i systemets livscykel.

En komponent, nätverket, kan därmed, kommunikationsmässigt, användas i flera olika sammanhang. En annan del, tjänsteimplementationen, kan erbjuda sin funktionalitet till varje annan del som finns ansluten till nätverket.

Dynamisk konfigurering för att skapa situationsanpassade system

I en värld som förändras allt snabbare är flexibilitet en egenskap som måste eftersträvas. Genom att använda en tjänsteorienterad arkitektur med löst kopplade tjänster är det möjligt att dynamiskt kunna kombinera tjänsteimplementationer till situationsanpassade system. Flexibiliteten erhålles genom att befintliga tjänsteimplementationer konfigureras i nya konstellationer på mycket kort tid, genom att nya tjänsteimplementationer kan installeras, samt genom att nya tjänster kan definieras utan att systemet i stort behöver förändras.

En gemensam informationsutbytesmodell

Strävan efter lös koppling mellan olika delar i ett system gäller också informationsrepresentationen. I många sammanhang var det tidigare nödvändigt att ha en gemensam representation av all information i systemet, dvs. en gemensam informationsmodell. Detta ger en begränsad flexibilitet eftersom en förändring av någon representation

eller introduktion av någon ny slags information gör att alla delar i systemet påverkas.

I en tjänsteorienterad arkitektur utbyts information mellan olika delar enbart med hjälp av tjänster. Detta medför att man kan ha olika representation i olika delar av systemet och att man ”bara” behöver en gemensam informationsutbytesmodell för den information som utbyts mellan olika delar i systemet. Genom tjänstedefinitionerna har man kontroll över vilken information som utbyts och man kan översätta den representation som utbyts till den som används internt. Genom att denna översättning kan vara olika i olika delar så behövs ingen gemensam informationsmodell.

1.4. Användning

Arkitekturbegrepp som introducerats i detta kapitel är **System-av-system, Tjänsteorienterade arkitekturer, Separering av affärslogik och infrastruktur, Nätverksorienterade system, Dynamisk konfigurering för att skapa situationsanpassade system** och **Gemensam informationsutbytesmodell**.

I korthet innebär dessa arkitekturprinciper och arkitekturbegrepp att man skall:

- Definiera den funktionalitet som skall vara gemensam i termer av *tjänster*, samt bestämma hur denna funktionalitet i grova drag skall realiseras. Realiseringen kan ske med befintliga system och/eller genom nyutveckling.
- Göra tjänsterna som definierats och implementerats tillgängliga i en *gemensam infrastruktur* bestående av ett nätverk med gemensamma principer för att hantera säker samverkan.
- Möjliggöra *dynamisk konfigurering* av tillgängliga tjänster för att skapa situationsanpassade system som kan användas i olika uppdrag och situationer.

2. Grunder för informationsinfrastruktur

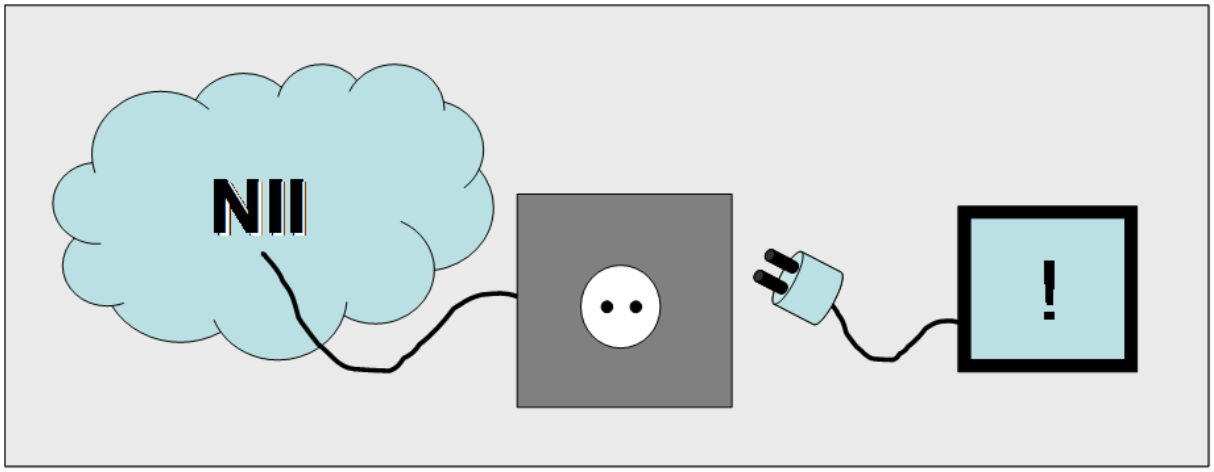
2.1. Syfte

Syftet med detta avsnitt är att bidra till en grundläggande förståelse för nytta och möjligheter förknippade med etablering och användning av en *informationsinfrastruktur*.

Avsnittet omfattar ett föreslag till svensk tolkning av begreppet informationsinfrastruktur och behandlar olika aspekter på och egenskaper hos en sådan. Vidare diskuteras möjliga former för dess struktur och beteende med utgångspunkt från olika modeller och principer för användandet av informationsinfrastruktur. Avslutningsvis diskuteras krav på och användning av en informationsinfrastruktur.

2.1.1. Bakgrund

Informationsinfrastrukturbegreppet gjordes mer allmänt känt under tidiga 1990-talet av Clinton-Gore-administrationen i USA[1]. En idé formulerades om en informationsförvaltande och -förmedlande infrastruktur som är allestädes närvarande, ständigt beredd att tillgodose den informationssökande allmänhetens behov – en National Information Infrastructure (NII). Deras vision avseende tillgängligheten för medborgarna till offentliga informationsresurser påminner lite om svenska Vattenfalls slogan ”två hål i väggen”.



Figur 2.1. En Nationell Infrastruktur (NII) skall finnas lätt tillgänglig för alla som behöver den, liksom elförsörjningen i Sverige.

[1] Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights. Information Infrastructure Task Force. 1995. ISBN: 0-9648716-0-1.

2.1.2. Vad är en Informationsinfrastruktur?

En informationsinfrastruktur (II) är den resursbas som skapas när olika aktörer i ett sammanhang (nation, fackområde, organisation etc.) samverkar genom att ställa individuella informationstillgångar till kollektivets förfogande. En informationsinfrastruktur kan skapas genom att avtal träffas mellan intresserade parter, som ett slags potentiell resurs att tillgå när situationer ställer krav på effektiv samverkan.

Önskvärda egenskaper hos en informationsinfrastruktur är bl.a. att den skall:

- Stödja flexibelt utbyte av information - det skall vara möjligt att modifiera omfattningen av den information som utbytes (kvalitativt såväl som kvantitativt)
- Vara kostnadseffektiv
- På bästa sätt utnyttja existerande och framväxande realiseringsmedel
- Kunna understödja samverkan mellan olika typer av förekommande (affärs)processer
- Ha en flexibel, skalbar och tidsbeständig arkitektur
- Uppfylla krav på tillgänglighet och säkerhet

2.1.3. Är informationsinfrastruktur en fråga för Sverige?

I takt med att Sverige utvecklas från industrisamhälle till kunskaps- och informationssamhälle ökar kraven på det allmänna att verka så att informationsresurserna som förvaltas inom ramen för den offentliga verksamheten kan utnyttjas effektivt och nyskapande.

Det står utom allt tvivel att morgondagens landvinningar väsentligen kommer att baseras på prospektering och exploatering av informationsresurser. För en nation som Sverige finns en stor potential att utveckla metoder för detta samt att omsätta dessa på hemmaplan för att stärka det svenska samhällets konkurrenskraft. *STIL-ramverk för informationsinfrastruktur* kan ses som ett steg att driva på denna utveckling.

2.2. Informationsinfrastruktur - begreppsgrunden

När man ”begåvas” med ett nytt begrepp är det ofta bra att börjar med att utforska begreppets språkliga grund och den idébildning som kan tänkas ligga till grund för begreppet och dess användning.

2.2.1. Information

Inom ramen för det mänskliga medvetandet skapas information, som är betydelsebärande, dvs. den har mening för människan. Ny information läggs till tidigare skapad information i ständigt pågående processer.

Människor externaliserar information i syfte att bevara den för eget senare bruk eller att göra den tillgänglig för andra – att kommunicera. När detta sker skapas fysiska s.k. representationer, exempelvis i form av tal, skrift, bild. Utöver dessa finns olika former av underliggande representationer, t.ex. digitaliserade, maskinellt bearbetningsbara data, burna av olika media.

De ovan beskrivna fysiska representationerna kallas i dagligt tal för information, trots att data sannolikt skulle vara en mer rättvisande term.

I syfte att förenkla och skapa bästa förutsättningar för en såväl nationell som internationell förståelse och acceptans gäller att **begreppet information i återstoden av detta dokument förstås att avse fysiska representationer** - inte mentala företeelser.

Exempel: Sveriges Riksdags nätplats (www.riksdagen.se) tillhandahåller aktuella nyheter och referensmaterial relaterat till verksamheten i Riksdagen. Såväl det som visas i webläsarens fönster som den bakomliggande koden kallas allmänt för information.

2.2.2. Infrastruktur

I vid mening kan en infrastruktur innefatta en uppsättning organisationer, människor, förmågor, teknik, standarder, utbildningsprogram, m.m., som tillsammans skall positivt bidra till att vissa typer av målsättningar kan uppnås.

Inom STIL-ramverk har utvecklats en syn på vad som karaktäriserar en infrastruktur, där vissa nyckelbegrepp har identifierats.

Resurser

En infrastruktur är en samling av samverkande resurser som agerar stödjande för någon verksamhet. Resurserna i fråga förvaltas ofta av någon ansvarig aktör.

Ex Lokala vattenverket

Tjänster

Infrastrukturens prestationer kan beskrivas i termer av de tjänster den erbjuder sina användare eller konsumenter.

Konsumenter

Infrastrukturbegreppet förutsätter att det finns många enskilda konsumenter av infrastrukturens tjänster och att dessa vinner på att nyttja infrastrukturen istället för att försöka tillgodose tjänstebehovet på annat sätt (t ex att var och en löser behovet på egen hand).

Ex Fjärrvärme

Kollektivism

Infrastrukturen och dess tjänster kräver typiskt omfattande investeringar vilka enskilda medborgare, företag eller myndigheter inte ensamt kan eller vill bära. Alltså är infrastruktur ett uttryck för en kollektivistisk syn på hur viss försörjning kan organiseras.

Kapacitet

När en infrastruktur nyttjas av en konsument sker detta normalt genom att konsumenten ges tillgång till någon andel av den tillgängliga kapaciteten hos infrastrukturen.

Ex: När en bilist kör på E4 ockuperar dennes fordon en ”lucka” i trafikflödet, som därmed inte är tillgänglig för någon annan konsument.

Relativitet

Infrastrukturbegreppet är relativt. Detta innebär att det som är infrastruktur för en aktör (konsument) inte nödvändigtvis är det för en annan (t ex en producent).

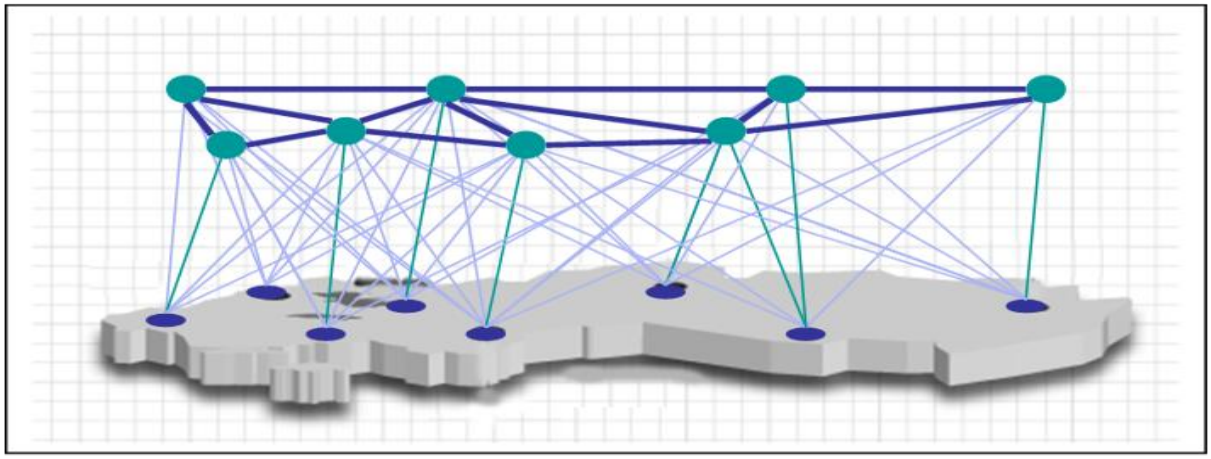
Ex: För SJ är stambanorna infrastruktur. För Banverket är stambanorna själva produkten, medan svenska kraftnätet är infrastruktur för förmedling av elkraft från kraftverk till kontaktledningar.

2.2.3. Begreppet Informationsinfrastruktur

I detta begrepp vävs **information** samman med **infrastruktur**. Information är (här) fysiska representationer. Infrastruktur är samverkande resurser som erbjuder ”nytta” i form av tjänster. Samverkan mellan olika organisationer bygger bl.a. på att information utbyts och utnyttjas som källa för kunskap och som medel för utbyte av kunskap.

En informationsinfrastruktur är ett medel som gör det möjligt för organisationer att effektivt utnyttja och dela med sig av informationen.

I informationsinfrastrukturen innefattas de processer och metoder som ger tillgång till existerande information, ger medel att utöka med ny information, samt tillhandahåller möjligheter att sammanställa och förädla existerande information. Uppsättningen processer och metoder innehåller dessutom stöd för förvaltning av informationen, liksom förvaltning av informationsinfrastrukturen som sådan.



Figur 2.2. En informationsinfrastruktur är ett medel som gör det möjligt för organisa-tioner att effektivt utnyttja och dela med sig av information. Visionen är att använda en Informationsinfrastruktur som nätverksbaserat stödjer samverkan över geografiska gränser, t ex nationellt.

2.3. Informationsinfrastruktur – användning enligt STIL-ramverk

En informationsinfrastruktur kan beskrivas som ett för olika verksamheter stödjande system, vars uppgift är att hantera och tillgängliggöra informationsresurser.

För att en informationsinfrastruktur skall ha något att erbjuda konsumenterna måste det även finnas producenter av information, vilka erbjuder konsumenterna tillgång till denna genom kommunikation (”att göra gemensam”).

Till skillnad från många andra resursslag som kan tillhandahållas av olika typer av infrastrukturer så förbrukas inte resursen information vid användning i betydelsen att den överförs från producenten till konsumenten (jfr bensin). Däremot finns naturligtvis vissa andra faktorer, t ex tillgänglighet eller kommunikationskapacitet, som begränsar exploaterbarheten hos informationsresurserna.

2.3.1. Informationssamverkan

En användbar utgångspunkt för analysen är konceptet informationssamverkan. Det är rimligt att anta att en nationell informationsinfrastruktur skall kunna understödja flera olika typer av samverkan mellan aktörer av olika slag.

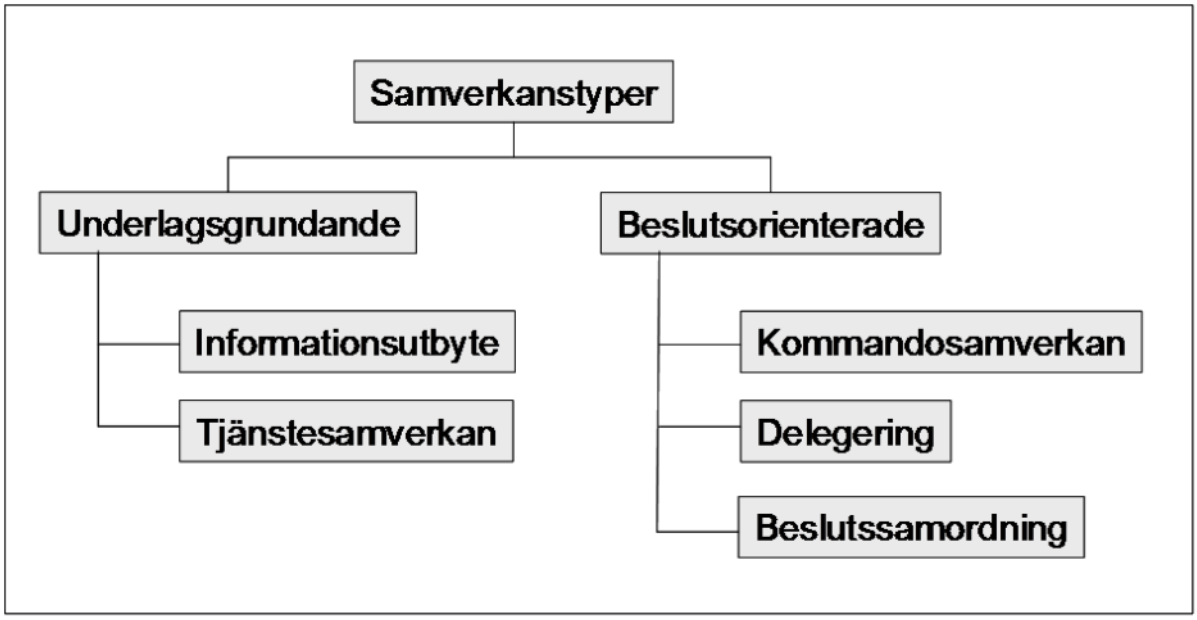
För att utveckla en första uppfattning om vilka tjänster en informationsinfrastruktur skall erbjuda kan samverkanstyperna utgöra ett slags scenarier (eller use-cases).

2.3.2. Samverkanstyper

I figuren nedan presenteras fem samverkanstyper fördelade på två huvudgrupper. Dessa beskrivs närmare i följande avsnitt.

2.3.3. Underlagsgrundande

Med underlagsgrundande samverkan menas samverkan som förser aktörer med beslutsunderlag. Denna typ av samverkan kan mycket väl bidra till en högre grad av samordning eller interoperabilitet mellan aktörer i en koalition, men den adresserar inte samverkan i själva beslutsfattandet.



Figur 2.3. Underlagsgrundade samverkanstyper fokuserar på information som beslutsunderlag medan Beslutsorienterade samverkanstyper fokuserar på hur samverkan sker i förhållande till beslutsmakten.

Informationsutbyte

Med informationsutbyte avses en modell där två eller flera parter ställer mer eller mindre förädlade informationsresurser till varandras förfogande. Denna relativt ”råa” information kan användas av respektive part som underlag för i övrigt okoordinerad analys.

Informationsutbytet bygger som regel på frivilliga bilaterala överenskommelser mellan parterna. Modellen är i princip symmetrisk m.a.p. ansvar och befogenheter - en jämställd modell. I den militära nomenklaturen klassas denna typ av samverkan som ”samverkan genom samordning”.

Funktionalitetsutbyte

Funktionalitetsutbyte innebär en möjlighet för parter att erbjuda mer kvalificerat stöd till intresserade informationskonsumenter. Till skillnad från informationsutbyte kan funktionalitetsutbyte innebära att mer förädlade informationsprodukter och tjänster ställs till förfogande. Funktionalitetsutbyte kan vara interaktiv och i princip innebära att konsumenten avropar viss hantering, utsökning, bearbetning och/eller analys från leverantören.

2.3.4. Beslutsorienterade

Med beslutsorienterade samverkanstyper avses samverkan som innefattar ett samordnat beslutsfattande. Detta innebär en hårdare koppling mellan aktörerna i en koalition, med ökade möjligheter att optimera den gemensamma verksamheten.

Kommandosamverkan

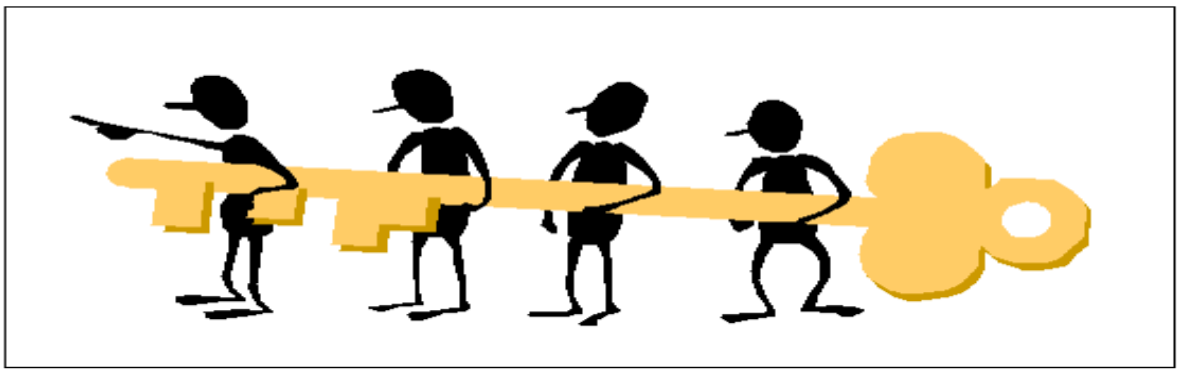
En mer tvingande form av samverkan kan kallas kommandosamverkan. Här sker samverkan genom att den ledande parten förskriver samverkan enligt vissa former som dikteras av denne. Denna samverkansform diskrimineras på basis av makt- och ansvarsförhållanden snarare än i termer av vilken funktionell nivå samverkan avser.

Även i detta fall bygger samverkan på bilaterala överenskommelser mellan parterna, men modellen är asymmetrisk med avseende på ansvar och befogenheter. I den militära nomenklaturen klassas denna typ av samverkan som ”samverkan genom befäl”.

Delegering

Grundprincipen för delegering är att vissa utpekade rättigheter och skyldigheter kan överföras från en part till en annan. Det är viktigt att hålla i minnet att delegering sker i ett visst sammanhang, och att det är med avseende på vissa mål/handlingar osv som delegeringen har mening och effekt.

Eftersom delegering är en princip, så kan principen användas på en mängd olika sätt och därmed kan termen delegering användas för en del ganska skilda användningar.



Figur 2.4. Beslutsorienterad samverkansformer kan t ex utgöras av kommandosamverkan där en ledande part pekar ut vad de andra ska göra.

Ett sätt att förstå delegering är att se dess motsats i termer av mikroledning (”micro management”) där ledning utövas genom detaljstyrning. Detta skapar inga egentliga frihetsgrader för en utförande part. I delegering skapas däremot frihetsgrader, och på så sätt kan man dra fördel av de situationer där vissa parter har bättre förutsättningar att ta på sig olika deluppdrag.

För att göra delegering hanterbar, styrbar och förutsägbar, så bör parter i samverkan komma överens om vilka policies som styr delegeringen. Därmed kan man i förväg fastställa hur delegering skall förstås och relateras till frivillighet respektive tvång.

Beslutssamordning

Med beslutssamverkan förstås en typ av samverkan som innebär ett koordinerat beslutsfattande, där autonoma parter samordnar sina beslut i syfte att åstadkomma viss samordningseffekt, typiskt inom ramen för en gemensam verksamhet (t ex ett projekt eller en incident). Beslutssamverkan kan ses som ett medel inom ramen för funktionen samverkansledning.

2.4. Möjligheter med STIL Informationsinfrastruktur

Potentiella intressenter och blivande aktörer i en informationsinfrastruktur kan ställa sig frågan: ”Vad betyder informationsinfrastruktur för oss och vår egen verksamhet?”

Det första som bör påpekas är att det handlar om relativa bedömningar – hur skall man värdera ansatsen informationsinfrastruktur jämfört med en alternativ ansats, utgående från en specifik behovs- och kravbild, som antas i det följande.

2.4.1. Bred informationsinfrastruktur för lätt och kostnadseffektiv användning

Ett generellt antagande är att *samarbete mellan parter kommer att öka*, och att samarbete i allt högre utsträckning kommer att ske i form av tätare samverkan i informationsområdet såväl som i operativa beslutsområdet. Detta kommer att medföra ökade krav på att hantering av digital information sker smidigt, snabbt, med potentiellt stora informationsvolymer, och att kvalitetskrav kommer att skärpas.

Speciella insatser kommer att behöva genomföras för att uppnå detta. Satsningen på en bred informationsinfrastruktur ser vi som den mest praktiska ansatsen, eftersom den bygger på att automatiserat stöd för generella behov tas fram en gång och sedan används av alla. Detta minskar investeringskostnaderna – men framför allt livscykelkostnaderna - samtidigt som teknisk kvalitet vidmakthålls, eftersom man undviker att skapa en teknisk ”mosaik i anarki”.

Vi kan även skilja mellan de direkta effekter som en informationsinfrastrukturansats får inom en viss organisation, och de konsekvenser som denna ger på effekterna av en samordnad gemensam insats (t.ex. en räddningsinsats). För samordnade insatser uppstår en stor mängd positiva effekter bara genom harmonisk samverkan mellan parterna.

En generell fördel med en gemensam infrastruktur är att den specificeras och struktureras för att på bästa sätt ge nödvändigt stöd åt samverkande parter. Detta ger en generalitet åt plattformen, och därmed möjligheter för en part att anpassa sitt bidrag till en samverkan realiserad ovanpå en informationsinfrastruktur.

En princip för informationsinfrastruktur är att den skall ge gott stöd åt samverkan, samtidigt som den inte förutsätter fullständigt detaljintegrerade verksamheter och plattformar. En informationsinfrastruktur kan snarast karaktäriseras som ett ramverk som stöder *samverkan på armlängds avstånd*. Detta innebär alltså att parter har full kontroll över sina egna interna resurser, men vad gäller den information och de tjänster som en part erbjuder andra, så förutsätts parten leva upp till de krav som parten själv publicerat om sitt utbud.

2.4.2. Framtidssäkring av teknikplattform jämte kvalitetssäkring av verksamheten

På teknisk nivå konfronteras organisationer med ett teknikutbud som är svårt att värdera. Vilka tekniklösningar ger flexibilitet? Vilka är framtidssäkrade? Vilka är interoperabla? I en gemensam satsning kommer teknikbeslut att fattas, och då grundas dels på existerande erfarenhetsbas, dels på fokuserade inventeringar och analyser. Därmed kommer teknikbasen i en gemensam plattformssatsning att vara mer framtidssäkrad än de specifika teknikplattformar som enskilda organisationer typiskt tar fram. Över tiden utnyttjas även en samordning

av underhåll och vidareutveckling, som ytterligare bidrar till att hålla kostnader nere.

Arbetet med att konkret etablera en informationsinfrastruktur kommer att innebära vissa utmaningar för deltagande parter. En sådan utmaning är att parter tvingas tydliggöra sådant som man hitintills lyckats undvika att strikt beskriva. Fullgod samverkan över administrativa gränser förutsätter att deltagande parter kan beskriva ”exporterade vyer” av sin information, sina processer, sin säkerhetspolicies, sina beslutspolicies, etc., så att andra parter kan ha ett välgrundat förhållningssätt till dessa.

Är detta en kostnad för en organisation? Ja, men det är en kostnad som skapar långsiktiga värden. Kvalitetssäkring av den egna verksamheten förutsätter att den egna verksamheten är tydligt beskriven, och detta är i sig en god grund för arbetet med att ansluta till en informationsinfrastruktur. Alltså kan anslutning till en informationsinfrastruktur ge positiva effekter i ett antal andra dimensioner, samtidigt som denna ger ett fullödigt bidrag till informationstillgång och tjänsteutbud jämte goda samverkansmöjligheter.

3. Informationsinfrastrukturen ur flera perspektiv

3.1. Utmaningar för informationsinfrastrukturen

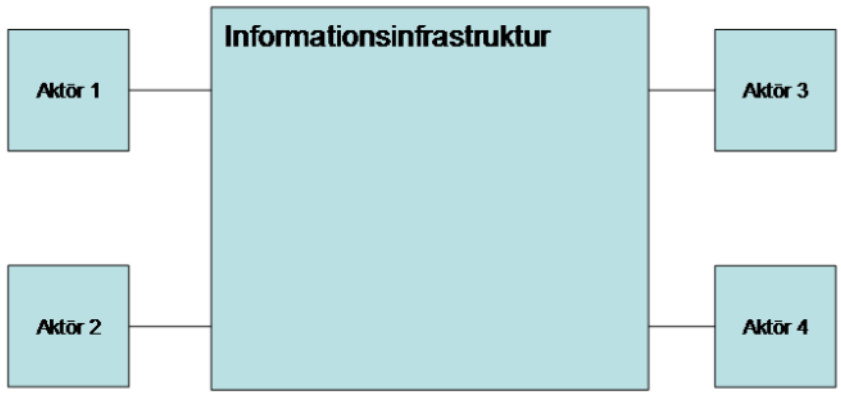
Det finns flera utmaningar som måste hanteras för att kunna etablera effektiv informationssamverkan mellan olika aktörer[1] och framförallt mellan dessa olika aktörers tekniska informationssystem.

Den mest signifikanta utmaningen är att kunna balansera kraven på bibehållen informationssäkerhet, framförallt integritet, samtidigt som delmängder av de olika aktörernas information görs tillgänglig mellan aktörernas informationssystem.

För att nå full effekt av ökad tillgång till information, t ex i ett framtida krisläge, kan kraven på bibehållen integritet och sekretess för en enskild part komma att förändras. Viktigt är att detta görs med medvetet beslutsfattande av de som har befogenhet för dessa beslut.

3.2. Systemsyn över informationsinfrastrukturens perspektiv

Nedan beskrivs informationsinfrastrukturen utifrån ett antal olika perspektiv. Dessa perspektiv följer den systemsyn som finns beskriven i försvarsmaktens arkitektur (FMAR).



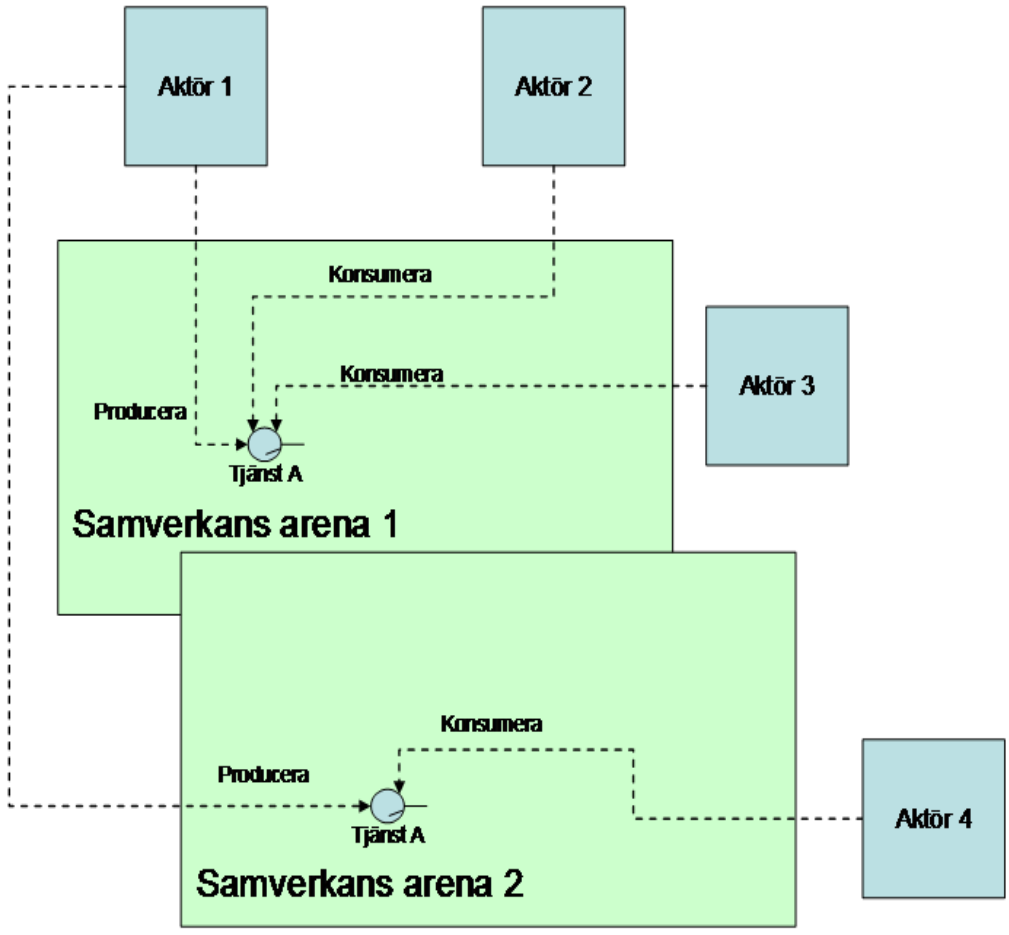
Figur 3.1. Informationsinfrastrukturen och aktörer

[1] Myndigheter, organisationer eller andra intressenter

3.2.1. Systemperspektiv

Syftet med informationsinfrastrukturen är att skapa en miljö där valda delmängder av olika aktörers information kan göras tillgängliga för andra aktörer. De primära användarna av informationsinfrastrukturen är de aktörer som får ett mervärde i form av nya förmågor och ökad effektivitet för befintliga förmågor genom att utbyta information[1] med andra aktörer. Denna effektivitetsökning måste kunna ske samtidigt som aktörerna bibehåller önskad[2] informationssäkerhet, framförallt integritet.

Informationsinfrastrukturen kan användas för att skapa samverkansarenor där olika aktörer kan samverka genom att utbyta information mellan aktörernas tekniska informationssystem. En samverkansarena



Figur 3.2. Samverkansarenor.

[1] Informationsutbytet sker främst genom ett utbyte mellan aktörernas tekniska informationssystem.
[2] Önskad integritet kan vara annorlunda än vad som gäller idag. Integritetskraven kan komma att behöva förändras för att full effekt skall kunna tillvaratas.

är ett situationsanpassat system (SitSyst) där ett antal tekniska informationssystem från olika aktörer har kopplats samman för att samverka med hjälp av tjänster. Vilka tjänster som används är beroende på vilken situation som skall hanteras.

En samverkansarena[1] utgörs av:

- den *information* som utbyts
- den *tekniska miljö* som behövs för informationsutbytet
- den *verksamhet* som bedrivs i form av en överenskommen eller vedertagen samverkansmetod.

Informationsutbytet sker i den tekniska miljön enligt principerna för tjänstesamverkan (se **Systemsamverkan i Del 2**).

För att kunna stödja etableringen (instansieringen) av permanenta eller temporära samverkansarenor innehåller informationsinfrastrukturen ett förutsättningsskapande ramverk, ”Ramverk för informationsinfrastrukturen”.

Ramverk för informationsinfrastrukturen innehåller de komponenter som krävs för att skapa och underhålla de delar av informationsinfrastrukturen som krävs för att göra det möjligt att instansiera samverkansarenor. I ramverket ingår bl.a. metoder, regler, arkitekturbeskrivningar, utbildning och generella tekniska komponenter. STIL ramverk kan ses som en första utgåva av detta förutsättningsskapande ramverk.

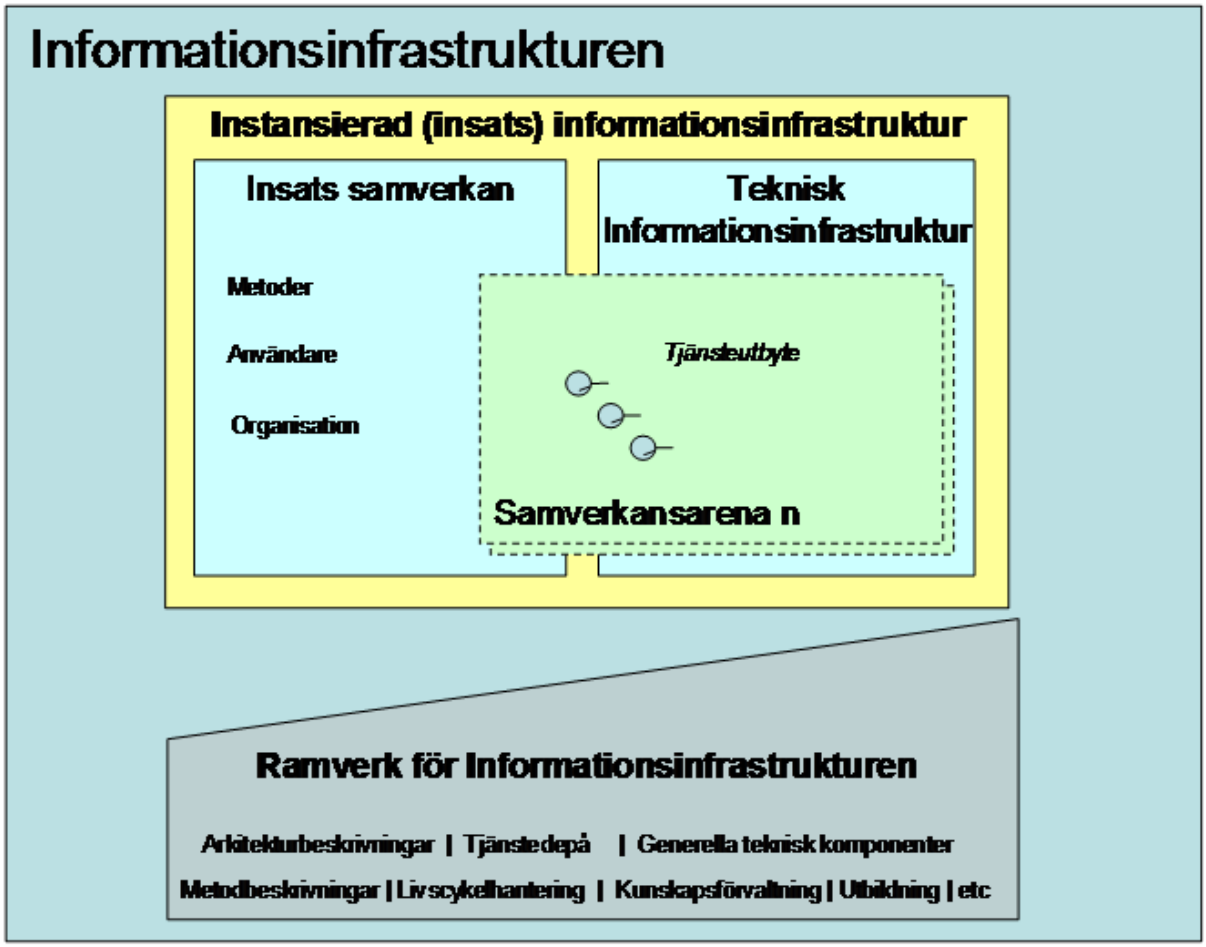
I figuren ovan illustreras de olika delarna som informationsinfrastrukturen består av: *Insatssamverkan* (verksamhet) som stöds av den *tekniska informationsinfrastrukturen*. Dessa delar i förening skapar de *samverkansarenor* som innehåller den nyttoinformation som utbyts. Till stöd för skapandet av de aktiva delarna används *Ramverk för informationsinfrastrukturen*, som också utvecklas kontinuerligt.

3.2.2. Verksamhetsperspektiv

Verksamhet i informationsinfrastrukturen är av två olika typer:

[1] En samverkansarena kan jämställas med ett ”Use Case” för Informationsinfrastrukturen

- dels den *förutsättningsskapande verksamheten* som syftar till att utveckla och förvalta ramverket samt att implementera det hos respektive aktör,
- dels den *insatssamverkan* som bedrivs i samverkansarenor, i samband med aktörernas insatser med sina respektive system.



Figur 3.3. Informationsinfrastrukturens delar

Den förutsättningsskapande verksamheten är förvaltning av ramverket. Detta arbete kan likställas vid förvaltningen av en standard. Den förutsättningsskapande verksamheten bör minst innehålla följande delar:

- utveckling och förvaltning av arkitekturbeskrivningar och beskrivningsramverk
- utveckling och förvaltning av den gemensamma tjänstedepån, (här ingår ex. utveckling och förvaltning av informationsutbytesmodeller)

- utveckling och förvaltning av generella tekniska designkomponenter (ex: tjänsteimplementeringar)
- kunskapsförvaltning och erfarenhetsutbyte
- benchmarking och deltagande i utveckling av liknande verksamheter
- utveckling och förvaltning av metoder för samverkan vid insats- och förvaltningsmetoder. Detta kan inkludera planering och genomförande av gemensamma samverkansövningar.
- implementation av ramverket, inklusive utbildning hos de olika aktörerna.

Insatssamverkan omfattar den verksamhet som bedrivs vid samverkan och nyttjandet av samverkansarenorna under insats. De metoder för samverkan vid insats som de olika aktörerna väljer att använda utvecklas och förvaltas inom ramen för aktörernas normala verksamhetsutveckling. Generella delar, sådana delar som är lika för många olika aktörer, kan dock väljas att förvaltas inom ramverket.

I samband med insatssamverkan så kommer troligen verksamhet för att gemensamt hantera samordningen och optimeringen av informationsinfrastrukturens insatsdelar att behöva ingå. Denna gemensamma systemledning kan med fördel förvaltas inom ramverket och avser den tekniska ledningen av informationsinfrastrukturen.

3.2.3. Organisationsperspektiv

Tillämpning av *Ramverk för informationsinfrastrukturen* kan påverka aktörerna på olika sätt.

För den *förutsättningsskapande verksamheten* så krävs en anpassning hos aktörerna så att de kan ta del i denna verksamhet. Detta ramverk tar inte ställning till hur ingående aktörer ska arbeta effektivt med att förvalta ramverket utan flera olika sätt kan väljas, nedan redovisas kort några.

Ett sätt att samarbeta kring förvaltningen är att välja att hantera förvaltningen av ramverket som förvaltningen av en *standard*. I en sådan förvaltning deltar alla på mer eller mindre lika villkor, man bygger sitt arbetssätt på överenskommelser och konsensus. Arbetet tar tid

men när väl beslut fattas är de väl förankrade och implementering av beslut går ofta relativt fort hos de olika aktörerna.

Ett annat sätt att arbeta på är att samarbeta i en löst kopplad organisation, i ett *nätverk*. Detta arbetssätt bygger mycket på förtroende och det krävs inga gemensamma beslut för att implementera nya idéer. Dessa prövas istället av intresserade aktörer i en öppen miljö och felrättning och förbättringar är tillåten att föreslå av samtliga intressenter.

Ett tredje sätt att arbeta på är att utse en *ansvarig aktör* som tar på sig ledartröjan för förvaltningen av ramverket. Den ansvariga aktören är drivande avseende uppdateringar och planerar in dessa enligt en gemensam överenskommen handlingsplan.

Dessa olika sätt att förvalta ramverket på kan kompletteras med styrning (ex. lagstiftning eller annan typ av reglering) samt även med någon form av stimulering för de som följer angivna rekommendationer.

För samverkan vid insats kan aktörernas organisationer behöva anpassas för att ytterligare tillgodose den *effektökning* som möjliggörs med ett ökat informationsutbyte. Denna anpassning hanteras troligen helt och hållet inom ramen för respektive aktörs ordinarie verksamhetsutveckling. För hantering av de *nya* förmågor som kan komma att uppstå som ett resultat av ett ökat informationsutbyte räcker troligen inte den ordinarie verksamhetsutvecklingen till. Detta beror på att nya förmågor framförallt kommer att uppstå som ett resultat av samverkan och därför berör flera aktörer. Något som berör flera aktörer är dessutom hanteringen av informationsinfrastrukturens insatsdelar, som kan hanteras med en gemensam organisation (kan vara en virtuell sådan).

3.2.4. Kompetensperspektiv

Tillämpning av STIL ramverk kommer att påverka kompetensbehovet hos aktörerna.

För den *förutsättningsskapande verksamheten* så kommer kompetenser kring verksamhetsutveckling (ex. metod- och personalutveckling), förvaltning av standarder samt systemutveckling inom den tekniska domänen att behövas. Dessa kompetenser finns idag i stor utsträckning redan hos de olika aktörerna men ett gemensamt förhåll-

ningssätt till de olika frågorna kommer att behöva utvecklas. En viktig avvägning som måste göras är på vilken nivå, hos de olika aktörerna som denna kompetens skall finnas. Det kan vara så att kompetensen skall finnas centralt och därmed tillgänglig för flera aktörer.

För *insatssamverkan* kommer det fortsatt att hos de olika aktörerna behövas experter på den egna verksamheten. Denna expertkunskap måste dock ytterligare utökas med förståelse och kunskap kring samverkande aktörers villkor och arbetssätt. Dessutom tillkommer behovet av kompetens för gemensam systemledning av tekniken i infrastrukturen.

3.2.5. Informations- och tjänsteperspektiv

I de olika samverkansarenorna som skapas så sker informationsutbytet i form av tjänstesamverkan. Detta innebär att informationen erbjuds som en tjänst och inte som t.ex. en datalänk. Ägaren av informationen (aktören) bestämmer vilken information som kan publiceras till samverkansarenan och systemet erbjuder sedan den informationen i form av tjänster. Tjänsterna registreras i en ”katalog” och är därefter tillgängliga för andra tjänster och system under förutsättning att dessa har behörighet att nyttja den registrerade tjänsten.

Grundidén bakom en tjänsteorienterad arkitektur är att undvika monolitiska system, designade bara för att lösa ett specifikt problem, dyra att uppdatera och kostsamma att anpassa för samverkan till andra system.

En tjänsteorienterad arkitektur gör det istället möjligt att kombinera självständiga system till system av system (se vidare **System av System** i Del 2). De ingående individuella systemen kan vara geografiskt distribuerade och användas som byggblock där funktionaliteten är tillgänglig som tjänster. Dessa olika tjänster tillåter blocken att kombineras på olika sätt, så kallad lös koppling. Lös koppling innebär att systemen kopplas ihop när de behövs och att flera olika kombinationer av ihopkopplingar är möjliga. Möjligheten att skapa olika situationsanpassade system (olika SitSyst) har därmed åstadkommits. Användaren eller en systemadministratör kan nyttja tjänster som blir registrerade i tjänstekatalogen efterhand som behov av en eller flera tjänster uppstår.

En tjänsteorienterad arkitektur gör det dessutom möjligt att tillåta flera olika implementeringar av en tjänst (se **Grund för Tjänstesamverkan** i Del 2). Med flera olika implementeringar av en tjänst menas att den funktionalitet eller det gränssnitt som tjänsten tillhandahåller är implementerad på olika sätt, dvs. samma sak åstadkoms men hur det åstadkoms kan variera. Detta innebär en ökad möjlighet till kostnadseffektivitet då flera olika leverantörer av samma tjänst kan konkurrera. Möjligheten till teknisk utveckling har också åstadkommits då flera olika tekniker kan tillåtas samtidigt.

En tjänsteorienterad arkitektur gör det dessutom möjligt att tillåta flera olika instanser av en tjänst. Att tillåta flera olika instanser av samma tjänst innebär att flera tekniskt exekverbara tjänster som tillhandahåller liknande funktionalitet finns tillgänglig. Detta ökar robustheten och den totala tillgängligheten i systemet.

En tjänsteorienterad arkitektur ökar också möjligheten till att behålla integriteten i de befintliga aktörernas system då tjänsten endast tillhandahåller den information som den designats för att tillhandahålla.

3.2.6. Teknikperspektiv

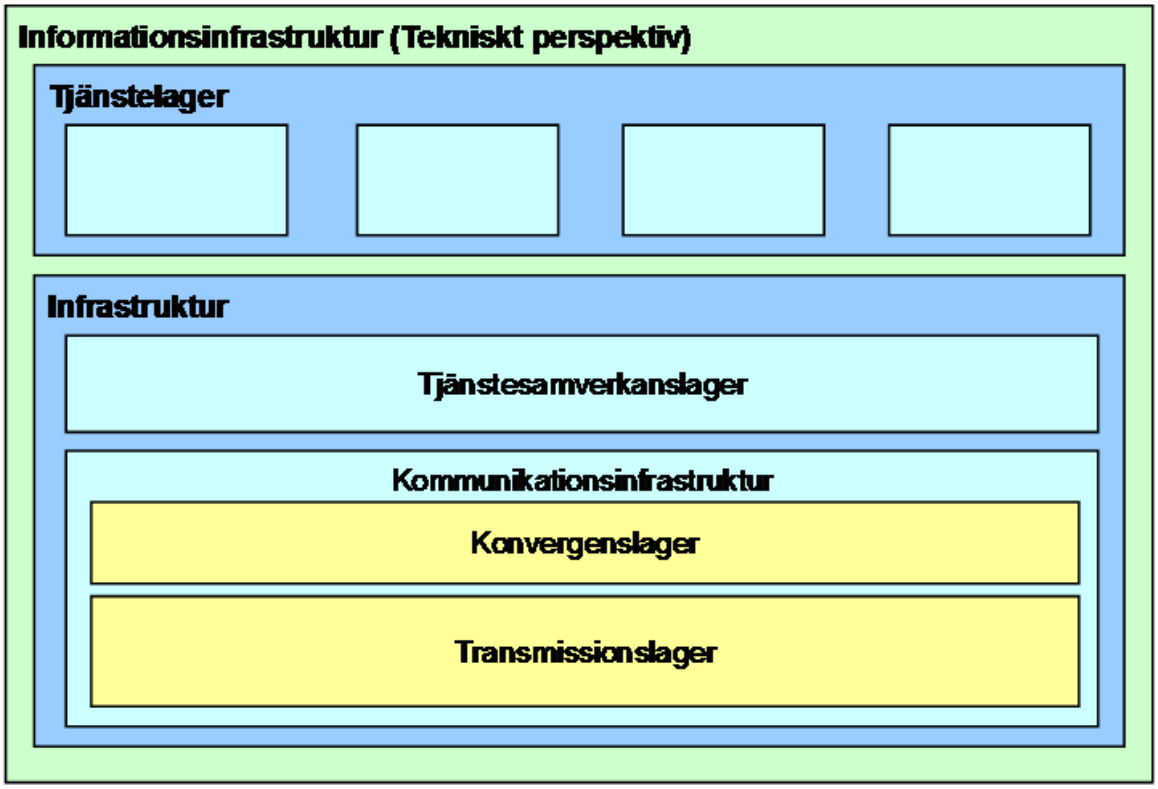
Arkitektur

Den övergripande arkitekturen för den tekniska informationsinfrastrukturen som används för att skapa olika samarbetsarenor innehåller två funktionella lager, *tjänstelagret* och *infrastrukturlagret*.

Det översta lagret, *tjänstelagret* innehåller de informationstjänster som gör det möjligt för aktörerna att samverka genom informationsutbyte samt även den funktionalitet som behövs för ledning och styrning av informationsinfrastrukturen. På sikt kommer tjänstelagret även att innehålla fler typer av tjänster utöver informationstjänster, s k funktionalitetsutbyte, t ex funktionalitet för omvärldsanalys.

Infrastrukturlagret innehåller den funktionalitet som gör det möjligt med tjänstebaserad samverkan över en tjänstebaserad arkitektur. Infrastrukturlagret kan till stor del baseras på kommersiell tillgänglig teknik och kan i sin tur delas in i två ytterligare lager, *tjänstesamverkanslagret* och *kommunikationsinfrastrukturen*.

Tjänstesamverkanslagret innehåller funktionalitet som gör det möjligt att etablera samverkan mellan olika tjänster och applikationer på ett



Figur 3.4. Övergripande arkitektur för informationsinfrastrukturen

säkert sätt. Tjänstesamverkanslagret tillhandahåller t.ex. funktionalitet för registrering av tjänster och behörighetskontroll av användare.

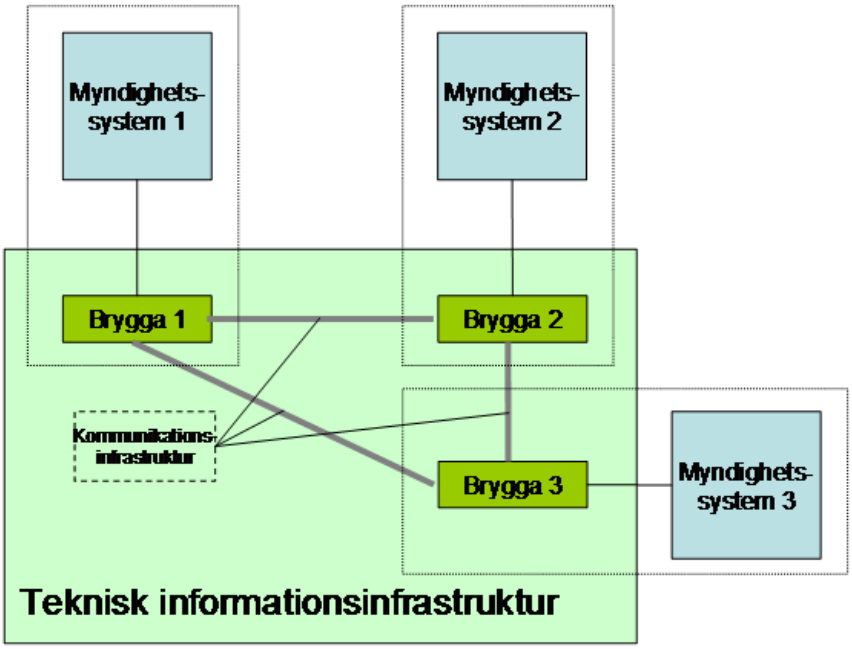
Kommunikationsinfrastrukturen består av ett *konvergenslager* som säkerställer att konnektivitet[1] kan åstadkommas på ett ensat sätt genom nyttjandet av Internet Protocol (IP).

Kommunikationsinfrastrukturen består dessutom av ett *transmissionslager*. Uppdelningen av kommunikationsinfrastrukturen i ett konvergenslager och ett transmissionslager gör det möjligt att nyttja flera olika typer av nätverk för transmission. Kommunikationsnätverken kan ha olika ägare, privata eller publika, och kan exempelvis inkludera taktiska radionätverk, bredbandiga fasta nätverk, fast telefoni och mobila nätverk.

[1] Konnektiviteten- möjlighet att koppla ihop. I detta fall ett kopplingslager mellan tjänstesamverkanslagret och själva transmissionslagret.
[2] Det existerar olika tekniska lösningar för anpassningarna (även kallad tjänstebryggor) till en tjänstebaserad arkitektur, se även FMV LedystT dokumentation, LT1K P06-0051 Design Rule Interoperability och LT1K P06-0008 Design Rule Legacy Integration.

Realisering

Vid en realisering av den tekniska informationsinfrastrukturen vill man åstadkomma minsta möjliga ingrepp i aktörernas olika befintliga system. Detta görs genom att ta fram en specifik *brygga*[1] för varje system som en aktör vill ansluta till den tekniska informationsinfrastrukturen. Respektive brygga är helt distribuerad och skall betraktas som en del av det aktuella systemet. Denna distribuerade komponent skall samtidigt implementera det aktuella systemets del av den tekniska informationsinfrastrukturen. Vid en realisering måste man även upphandla, hyra eller på annat sätt nyttja det kommunikationsnätverk



Figur 3.5. Realisering av teknisk informationsinfrastruktur

som krävs för den tekniska informationsinfrastrukturen. Den gemensamma kommunikationsinfrastrukturen kommer att utgöras av både allmän och enskild (reserverad t ex för myndighet/ organisation) sådan.

En brygga åstadkommer att den information eller funktionalitet som skall göras tillgänglig från de olika systemen anpassas till den tekniska informationsinfrastrukturens arkitektur. Detta innebär att funktio-

[1] Det existerar olika tekniska lösningar för anpassningarna (även kallad tjänstebryggor) till en tjänstebaserad arkitektur, se även FMV LedystT dokumentation, LT1K P06-0051 Design Rule Interoperability och LT1K P06-0008 Design Rule Legacy Integration.

naliteten i en brygga kan vara väldigt enkel (i det ideala fallet ej nödvändig), om informationssystemet från början är konstruerat enligt en tjänstearkitektur och använder överenskomna informationsutbytesmodeller. Samtidigt kan en brygga vara väldigt komplex för andra anslutna aktörers system, där stora skillander i arkitektur skall överbryggas.

En brygga agerar som en adapter (gränssnitt) mellan de olika informationsmodeller och informationsutbytesmekanismer som existerar i de olika systemen (se **Informationssamordning för myndighetssamverkan** Del 2).

Tekniken gör det även möjligt för bryggan att implementera de säkerhetsmekanismer som respektive aktör vill använda för att hantera det aktuella systemets integritet utifrån en gemensam säkerhetsmodell (se kapitlet **Säkerhet** respektive **Tillämpad säkerhet** i Del 2).

3.2.7. Kritiska systemegenskaper

Den tekniska informationsinfrastrukturen kommer att ha ett antal kritiska systemegenskaper. Dessa kritiska systemegenskaper, av vilken informationsutbytet mellan aktörssystemen med bibehållen integritet är den viktigaste, möjliggörs till stor del genom den tjänstebaserade arkitekturansatsen. Bibehållen integritet tillgodoses framförallt genom en gemensam säkerhetslösning som tillåter aktörsspecifika tillämpningar. Detta innebär att olika aktörer tillåts, att inom ramen för den gemensamma säkerhetslösningen, implementera och använda olika säkerhetsmekanismer utifrån aktörens, eller situationens specifika behov (se vidare **Tillämpad säkerhet** i Del 2)).

3.2.8. Fokusområden

För att kunna etablera samverkansarenor för effektiv informationssamverkan mellan olika aktörer, finns det vissa områden som kräver större fokus än andra.

För tjänstelagret i de tekniska delarna av informationsinfrastrukturen så bör fokus vara på det gemensamma informationsbehovet som kan tillgodoses genom att de olika aktörerna utbyter information. Det är även av stort värde att definiera den gemensamma funktionalitet som kommer att krävas för ledning och styrning av den tekniska informationsinfrastrukturen.

För de tekniska systemegenskaperna bör fokus vara på att uppnå en balans mellan behoven av (eller kraven på) informationsutbytet, informationssäkerhet och kostnadseffektivitet. Detta kan bl.a. åstadkommas genom olika typer av säkerhetsmekanismer i anpassningen av informationssystemen.

För ramverket bör initialt fokus vara på att uppnå en samsyn mellan aktörerna avseende etablering av den gemensamma metod som krävs för att utveckla och förvalta ramverket som sådant. Det är dessutom viktigt att tidigt komma igång med etablering av en gemensam tjänstedepå och en gemensam förvaltning av gemensamma tjänster (se **Grund för Tjänstesamverkan** i del 2). Detta kan ske genom att bilda gemensamma tvärsektoriella samarbetsgrupper (se som exempel Security Arena i Göteborg) där arbetet med gemensamma mål för regler, metoder och teknik kan omvandlas till konkreta projektplaner för prov och försök och på sikt skarpa system.

4. Säkerhet

4.1. Utmaning

Säkerhet och flexibilitet är två önskade och övergripande egenskaper som nästan alltid kommer i konflikt med varandra vid både konfigurering och drift av situationsanpassade system. Att hitta rätt balans mellan de önskade kraven på dessa två egenskaper är en stor utmaning som återkommer på många nivåer.

För system i drift visar sig konflikten tydligast i att kravet på flexibilitet ofta medför att information skall vara åtkomlig för så många som möjligt medan kravet på säkerhet medför att åtkomsten till känslig information skall vara begränsad till så få som möjligt.

För konfigurering av system finns det en liknande konflikt då kravet på flexibilitet medför att situationsanpassade system snabbt skall kunna konfigureras för att kunna möta nya och oväntade situationer medan kravet på säkerhet medför önskemål om att alla använda konfigurationer skall vara noga analyserade och verifierade ur säkerhetssynpunkt.

Ett sätt att hantera motsättningarna mellan säkerhet och flexibilitet är framtagen inom FMV:s projekt LedsystT. Detta sätt bygger på en tillämpad riskhantering där balansen mellan informationssäkerhet och operativ nytta kontinuerligt värderas under alla faser av systemets livscykel. För en djupare beskrivning av LedsystT Risk management modell se .[17]

4.2. Arkitektur för informationssäkerhet

4.2.1. Inledning

Säkerhet i informationssammanhang är ett samlingsbegrepp för ett antal egenskaper. Några exempel på sådana egenskaper är sekretess, integritet och tillgänglighet. I den arkitektur som beskrivs i detta kapitel kallas sådana önskvärda säkerhetsegenskaper för säkerhetsmål.

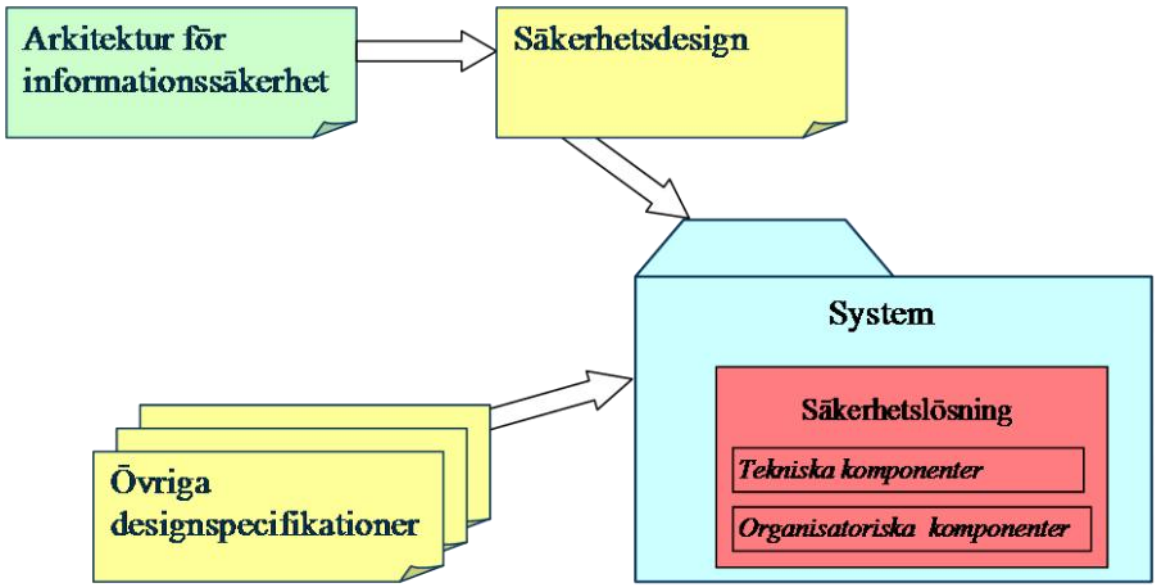
För att kunna uppnå ett kvantifierat säkerhetsmål behövs en eller flera säkerhetsmekanismer. En säkerhetslösning är summan av de säkerhetsmekanismer som behövs för att uppnå alla önskade och kvantifierade säkerhetsmål.

En säkerhetslösning baseras sällan eller aldrig på enbart tekniska komponenter, utan det behövs även organisatoriska komponenter så som metoder och processer. De organisatoriska komponenterna skall bl. a definiera nödvändig administration av lösningarna och regler för hur mänskliga användare skall agera för att önskad säkerhetsnivå skall uppnås.

Ett säkerhetsobjekt är grupperad information eller en tjänst som har ett skyddsvärde ur sekretess, integritet och/eller tillgänglighetssynpunkt. För att kunna förstå när och hur en säkerhetsmekanism skall användas måste dels den/de säkerhetsobjekt som den skall skydda vara identifierade och dels måste säkerhetsobjekten vara klassificerade ur ett informationssäkerhetsperspektiv.

En flexibel säkerhetslösning skall ha möjlighet till säkerhetsadministration, d v s vilka säkerhetsmål som gäller, vilka säkerhetsmekanismer som används och vilka säkerhetsobjekt som skyddas skall kunna styras under drift.

Nedanstående bild visar hur arkitekturen är tänkt att användas.



Figur 4.1. Arkitekturen och dess tänkta påverkan på sin omgivning.

Arkitekturen definierar dels begrepp och övergripande krav och dels regler för hur en säkerhetsdesign skall vara strukturerad.

En säkerhetsdesign definierar hur ett antal säkerhetsmekanismer skall kombineras samman till en säkerhetslösning. Vilka mekanismer som

används och hur de kombineras är beroende av vilken säkerhetsnivå som önskas.

En realisering i form av ett system skall dels uppfylla en säkerhetsdesign och dels uppfylla en eller flera andra designspecifikationer. Dessa övriga specifikationer definierar bland annat systemets egentliga nytta.

Arkitekturen är ensad med den modell för säkerhetsarkitektur som är framtagen inom FMV:s projekt LedsystT. För en djupare beskrivning av LedsystT säkerhetsarkitekturmodell se referens [22].

4.2.2. Övergripande strukturering

Modellen i figur 4.2 används för den huvudsakliga struktureringen av problemområdet.

Figur 4.2. Säkerhetsarkitekturmodell

Modellen har fyra funktionella områden:

- Säkerhetsmål (eng. ”Security objectives”) – specifika mål som en säkerhetsdesign skall uppfylla. Hur och till vilken grad målen uppfylls skall definieras i designen.
- Säkerhetsmekanismer (eng. ”Security mechanisms”) – tekniska lösningar och manuella rutiner som kan användas för att imple-

mentera säkerhetslösningar som uppfyller säkerhetsmålen i varierande grad.

- Säkerhetsobjekt (eng. ”Security objects”) – grupperad information eller tjänster som har ett skyddsvärde ur sekretess, integritet och/eller tillgänglighetssynpunkt. Ett säkerhetsobjekt skall ha metadata för administration av objektet.
- Säkerhetsadministration (eng. ”Security management”) – definition av nödvändig administration av säkerhetslösningen.

Förutom ovanstående så definierar arkitekturen några processområden.

4.2.3. Processområden

Arkitekturen definierar fyra processområden som skall behandlas av en säkerhetsdesign:

Riskanalys

Riskanalys är en process för att utvärdera hot mot värdefull information så att de rätta motåtgärderna kan sättas in för att minimera eller eliminera hoten. Detta område skall dels dokumentera vilken/vilka riskanalyser som har gjorts på säkerhetsdesignen och dels vilken/vilka riskanalyser som skall göras på den färdiga lösningen.

Processer för strategiskt säkerhetsarbete

Detta område skall definiera processer för strategiskt säkerhetsarbete. Exempel på detta är processer för certifiering och ackreditering av nya säkerhetsmekanismer.

Organisation för strategiskt säkerhetsarbete

Detta område skall definiera hur det strategiska säkerhetsarbetet skall fungera i en säkerhetslösning. Det innebär definition av dels hur arbetet skall organiseras och dels nödvändiga kunskaper hos användare. Vidare skall säkerhetsrelaterade regler för användare (eng. ”end users”) vara definierade eftersom mänskliga fel kan göra alla säkerhetslösningar osäkra.

Säkerhetsgranskning och övervakning

Detta område skall definiera processer för granskning och övervakning över vad som sker i system ur en säkerhetssynpunkt. Processerna skall i avskräckande syfte ge en förmåga att kunna upptäcka och bestraffa någon användare som gör saker som de inte har tillåtelse att göra.

4.2.4. Säkerhetsmål

En säkerhetsdesign skall definiera vilka säkerhetsmål som är giltiga och till vilken nivå dessa skall hanteras. Säkerhetsmålen har följande innebörd:

Sekretess

Sekretess innebär att ingen obehörig skall kunna läsa/avlyssna känslig information.

Integritet

Integritet innebär att information skall vara oförändrad från det att den skapades till dess att den konsumeras. Oavsett hur den har transporterats och/eller lagrats under tiden.

Oavvislighet (eng. ”Non-repudiation”)

Oavvislighet innebär att det skall vara möjligt att i efterhand bevisa att:

- En sändare verkligen har sänt ett visst meddelande
- En mottagare verkligen har tagit emot ett visst meddelande

Tillgänglighet

Tillgänglighet innebär att behöriga användare skall kunna ta del av information när de behöver den. Detta inkluderar:

- Skydd mot överbelastningsattacker (Denial of Service)
- Redundans för viktiga resurser
- Automatisk och dynamisk allokering/utnyttjande av kommunikationsresurser

Identifiering/Autentisering

För att kunna försäkra att tjänster, information och andra resurser endast konsumeras av system och användare som är betrodda att göra detta så måste både identifiering och autentisering kunna utföras. Identifiering är påståendet om vem man är och autentisering är förmågan att kunna bevisa detta påstående.

Behörighet/Åtkomstkontroll

Detta mål innebär att all åtkomst till tjänster, system och infrastruktur skall behörighetsprövas. Vid en sådan prövning undersöks om en aktör har behörighet att göra det den önskar, till exempel konsumera en tjänst. Åtkomstkontroll är mekanismen som ser till att beslut om behörighet verkställs.

Säkerhet för personer och övrig omgivning

Detta mål innebär att information och tjänster måste ha korrekta egenskaper när de används i situationer där människors välbefinnande kan påverkas.

Personlig integritet

Detta mål innebär att personlig information endast får användas i auktoriserade sammanhang.

Ackreditering (Assurans)

Assurans är bevisning att ett system verkligen uppfyller sina säkerhetskrav. Common Criteria (CC) kan vara ett lämpligt instrument för att kunna bevisa att ett system uppfyller sina säkerhetskrav.

4.2.5. Säkerhetsmekanismer

Säkerhetsmekanismer är tekniska lösningar och manuella rutiner som kan användas för att implementera säkerhetslösningar som uppfyller de fastlagda säkerhetsmålen till rätt säkerhetsnivå. Exempel på säkerhetsmekanismer är:

- Kryptering
- Digitala signaturer
- VPN (Virtual Private Network)

- Administration av krypteringsnycklar
- Brandväggar
- Informationstrappor
- Virusskydd
- Loggning
- Intrångsdetektering
- Utbildning & träning
- Användarinstruktioner

En säkerhetsdesign skall definiera vilka säkerhetsmekanismer som används för att uppfylla de olika säkerhetsmålen.

4.2.6. Säkerhetsobjekt

Säkerhetsobjekt är grupperad information eller tjänster som har ett skyddsvärde ur sekretess, integritet och/eller tillgänglighetssynpunkt. Säkerhetsobjekt skall värderas och klassificeras ur ett informationssäkerhetsperspektiv. Ett säkerhetsobjekt skall vanligtvis ha metadata för administration av objektet. Exempel på tänkbara säkerhetsobjekt är:

- Nyttoinformation
- Behörigheter
- Lösenord
- Konfigurationer
- Loggar
- Applikationskod
- Virus definitioner
- Tjänstebeskrivningar
- Exekverande applikationer (producenter och konsumenter av tjänster)

- Krypteringsnycklar

En säkerhetsdesign skall definiera dels vilka typer av säkerhetsobjekt det skall finnas och dels vilket eller vilka skyddsvärden som gäller för respektive typ.

4.2.7. Säkerhetsadministration

Säkerhetsadministration är ett område som skall definiera hur nödvändig administration av säkerhetsmål, säkerhetsmekanismer och säkerhetsobjekt skall ske.

Om man vill ha en lösning som kan balansera mellan krav på flexibilitet och interoperabillitet med fastställda säkerhetsmål så rekommenderas det att man skall använda risk och policybaserad säkerhetsadministration.

Risk och policybaserad administration

En policy definierar hur ett antal säkerhetsmekanismer skall konfigureras så att de enskilt eller tillsammans kan uppfylla ett eller flera kvantifierade säkerhetsmål. Man kan t ex definiera en policy som uppfyller säkerhetsmålet sekretess till *hemlig* nivå och en policy som uppfyller säkerhetsmålet sekretess till *konfidentiell* nivå. Risk och policybaserad administration innebär att det skall vara möjligt för en säkerhetsadministratör att momentant kunna välja vilken policy som skall gälla beroende på vilka risker man är beredd att ta i en viss situation.

Policybaserad administration möjliggör också att man, genom policies, kan definiera hur det tekniska systemet skall uppföra sig i olika situationer och få systemet att automatiskt anpassa sig enligt policyn. T ex så kan en policy uttrycka att hemlig sekretessnivå skall gälla för en viss typ av information i det dagliga arbetet men inte i krissituationer. Det tekniska systemet kan då tolka denna policy och automatiskt anpassa sig beroende på om man befinner sig i kris eller inte.

Del 2

Fördjupningar

Inledning till Del 2 – STIL-ramverk Fördjupningar

I denna del återfinns ett antal beskrivningar, så kallade ”White papers” med grunder, regler, metoder och synsätt för STIL-ramverk och den gemensamma informationsinfrastrukturen. Del 2 gör inte anspråk på att vara heltäckande, utan innehåller fördjupningar för ett antal olika frågeställningar i en serie STIL-dokument. Tekniska förutsättningar för samverkande och situationsanpassade system presenteras jämte verksamhetsinriktade förutsättningar för samverkan. Dessa separata ”White papers” behandlar allt ifrån syn på lyckad samverkan till designprinciper vid integration av tekniska system.

Läsanvisning

I **Samverkansnivåer - en utvecklingsväg framåt** kan man läsa om samverkansnivåer och en gradvis utveckling mot högre grad av samverkan. Det kräver stort mått av koordination och kommunikation, när större och extraordinära händelser inträffar, som prövar samhällets förmåga.

Systemsamverkan beskriver hur en enskild samverkansaktör med befintliga datasystem kan agera för att ”kopplas” till en gemensam informationsinfrastruktur. Här beskrivs hur man systemmässigt uppnår både flexibel samverkan och bibehållen integritet.

System av system redogör för potentialen med stora kluster av samverkande system från olika organisationer, där varje system utgör en egen autonom del, men kan sättas samman till något helt.

Mål och medel för Informationsinfrastruktur visar på hur information görs gemensam på genom användning av informationsinfrastruktur och vilka drivkrafter och egenskaper som kännetecknar denna samverkansgrund.

Viktiga förutsättningar för lyckad samverkan återfinns i **Grund för tjänstesamverkan**. En rad modeller, processer och regler skapar en grund som underlättar tvärsektoriell samverkan mellan flera aktörer. Dessutom förstärks denna grund av kvalitetssäkrade, säkerhetskontrollerade och livscykelhanterade tjänster som görs gemensamt tillgängliga i en ”tjänstedepå”.

Vilken information om information (metainformation) som är grundläggande för tekniskt implementerade informationstjänster utreds i **Tjänsternas metainformation**.

I **Informationssamordning för myndighetssamverkan** beskrivs viktiga ställningstaganden för och sätt att mötas i ”samverkansarenor” för delad och gemensam information som stödjer god samverkan.

Hur man utvecklar situationsanpassade system som bäst motsvarar behoven förklaras i **Utvecklingsprocess för utveckling av situationsanpassade system**. Där presenteras en designmetod som använts till att skapa demonstratorer för ledningssystem inom försvarsmakten.

Gemensam lägesinformation beskriver hur man på ett fruktbart sätt i en samverkanssituation utnyttjar konsistent information om läget för flera olika arbetsuppgifter inom insatser och uppdrag. Utifrån ett smörgåsbord av information och tjänster vill man snabbt kunna sammanställa relevant information och göra den tillgänglig på flera sätt.

Tillämpad säkerhet beskriver en generisk säkerhetsdesign som kan baseras på öppna standarder vilket möjliggör realisering med olika typer av tekniska komponenter, t ex Open-Source eller kommersiella produkter

I **Riskhantering**, behandlas grundläggande hantering av risker och hot i samband med situationsanpassade system.

Samverkansnivåer - en utvecklingsväg framåt

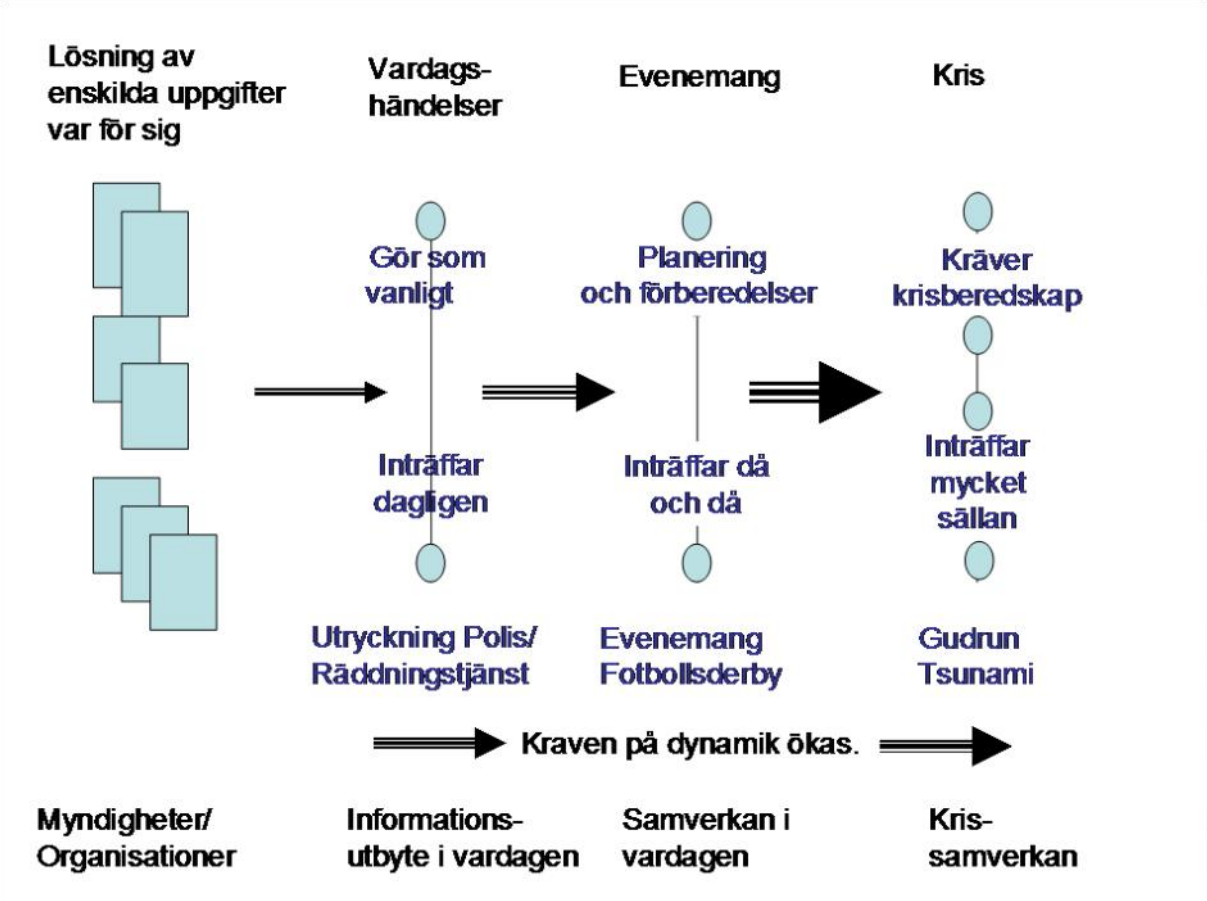
Sammanfattning

För framgångsrika insatser, då olyckan är framme, krävs samverkan. Samverkan mellan myndigheter och organisationer kan bedrivas på olika nivåer och kräva olika typer av stöd. Det finns mycket att vinna på att utveckla samarbete genom ökat informationsutbyte och inte minst ökad informationssamverkan i vardagen. Med informationssamverkan ges också möjlighet till samordnad planering och samordnade uppgifter.

På högsta samverkansnivå kan planering ske gemensamt för att bäst rusta för gemensam problemlösning och fördelning av resurser inom insatser och uppgifter. Användning av gemensam lägesbild, som utnyttjar gemensam informationsinfrastruktur, är en viktig nyckel för flexibel samverkan med stor utväxling. Genom utbildning och övning bör man utveckla samverkansnivåerna gradvis från vardagssamarbete till krissamverkan.

1. Inledning

Detta avsnitt behandlar en modell för hur man kan se på samverkan inom och mellan verksamheter. För att lyckas med samverkan krävs stöd, t ex i form av helhetstänk i infrastruktur och informationshantering. Detta stöd skall bygga på samma principer i vardag som i kris, för bästa effektivitet. Behoven av samverkan varierar med utmaningar och ambition. Vi utgår i beskrivningen här från en utvecklingsväg (i figurerna illustrerat från vänster till höger) mot högre samverkansnivåer. Samverkan fokuseras i denna beskrivning främst på vad som sker *under* en insats. Jämte detta finns väldigt viktiga samverkansfrågor *före* och *efter* insatsen som berörs väldigt lite häri.



Figur 1. Samverkan kan göras på olika samverkansnivåer. Från vänster till höger växer gradvis samverkansnivån. I vardagshändelser sker samverkan mer spontant och ställer inte så stora krav. För lyckad hantering av större samt extraordinära händelser och kris ställs krav på ökad samverkan med bättre grundförberedelse och dynamik.

2. Behovet av samverkan ökar med utmaningen

När händelser går utanför vardagen och eskalerar mot kris[1] finns ett större behov av samverkan. I vardagen löser myndigheter och organisationer, i flertalet fall, enskilda uppgifter var och en för sig. De upplever sällan något mervärde med informationsutbyte, i dessa sammanhang. I vissa vardagshändelser sker reglerat informationsutbyte, t ex skall Räddningstjänsten rapportera till Polisen vid alla utryckningar de åker iväg på. Denna rapport sker enkelriktat och kunde givetvis vara till större stöd om Polisen vid behov replikerade rapporten om de har någon varning att utfärda som påverkar utryckningsväg eller -område. Detta motsvarar ”vardagshändelser”, med informationsutbyte i figur 1.

Vid återkommande, men större, händelser och evenemang ökar kraven på den samlade förmågan, t ex dynamik och därmed även på förberedelser och resursplanering. Utan förberedelse minskar utrymmet för flexibilitet. ”Samverkan i vardagen” (se Figur 1) inbegriper en tvåvägskommunikation mellan flera parter, myndigheter/ organisationer, snarare än envägsrapportering. Exempel på detta är; Förberedande planeringsmöte mellan Polis och diverse kommunala inrättningar, t ex räddningstjänst, samtal med organisationer inför demonstration eller resursallokeringsmöten med andra orters styrkor. Detta utbyte av information underlättar förståelsen och den gemensamma förmågan. Exempelvis kan Räddningstjänsten redan proaktivt vara informerad om vilka områden som är känsliga (p g a polisaktivitet), redan före en inträffad händelse. Det finns mycket att tjäna på att i vardagsarbete tillföra inslag av samarbetsgrund som kan nyttjas vid större händelser eller kris.

Den högsta nivån av samverkan i Figur 1 avspeglas i s k ”Krissamverkan”. Utmaningen ligger här i att något som inträffar väldigt sällan är beroende av att vara väl och smidigt fungerande för de direkt och indirekt berörda. Detta innebär också att rutin och erfarenhet varierar bland de berörda och det finns ett stort behov av utbildning,

[1]Med kris menar vi en händelse som drabbar många människor och stora delar av vårt samhälle. En kris hotar grundläggande funktioner och värden som exempelvis elförsörjningen eller vår hälsa och frihet. (källa KBM)

övning och hjälpmedel för att underlätta uppstart och aktivt ledningsarbete i respektive roller och i stab.

Därför är krisberedskap viktig för att lyckas, inte minst för att proaktivt kunna leda i situationen istället för att bara följa ett skeende. Utöver detta är det viktigt att utnyttja flexibilitet och situationsanpassning såväl för organisation, resurser, information och system för situationer som ej är förutsägbara.

Krisen kan smyga sig på utan större förvarning från en enskild händelse eller en kombination av flera mindre händelser. Den kan komma gradvis eller som en blixt från klar himmel. Oavsett kräver den en hel del av de som ansvarar för att agera i situationen, såväl beslutsmässigt som i förmåga att agera trots människans fysiska och psykiska begränsningar. Framgången blir beroende av hur väl krissamverkan fungerar och hur man lyckas agera flexibelt. Såväl organisation och verktyg, som information behöver kunna anpassas enkelt till situationen.

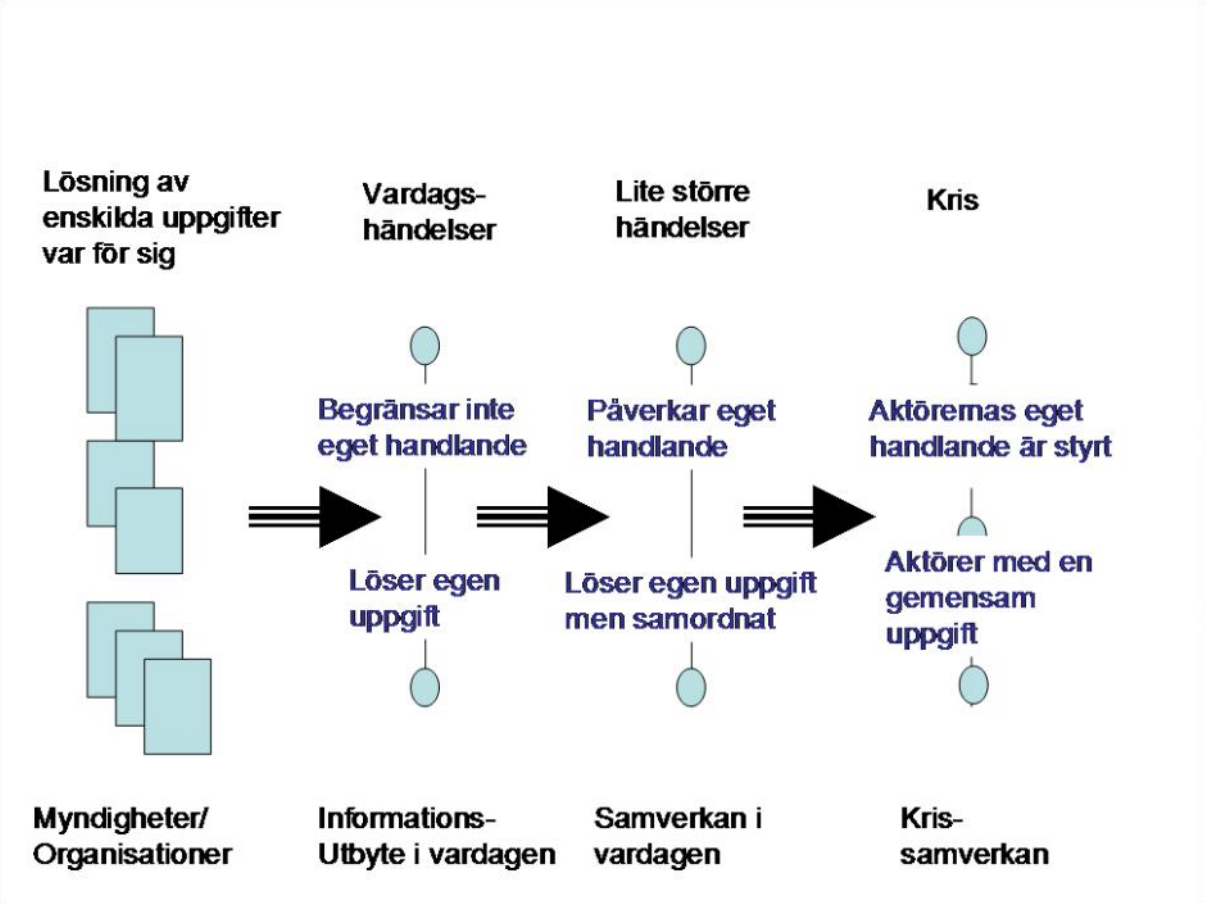
3. Tillväxt till samordnat handlande

Hur en enskild organisation eller aktör agerar skiljer sig vid de olika samverkansnivåerna, beroende på händelsen. Vardagshändelserna ställer låga krav på planerat samarbete och därmed sätter man inte heller några begränsningar på det egna handlandet. Alla löser sin egen uppgift, även om man byter viss information, som inte för den skull behöver leda till någon åtgärd eller beordring av arbete.

Vid större händelser är det däremot viktigt med samordnat agerande. Behovet av informationsspridning växer. Fortfarande löser man den uppgift som man enligt lagar och regler har ansvar för. Det egna handlandet påverkas dock av att samarbete har kommit till stånd.

En hel del finns att vinna på att gradvis förstärka sin samarbetsförmåga, såväl i vardagen som i kris. Liksom i alla större förändringsprojekt är det en viktig framgångsfaktor med stegvis utveckling. Vi utgår från ett synsätt för stegvis utveckling av samverkan och stöd för samverkan till den mest avancerade formen av samverkan där flera aktörer löser en gemensam uppgift.

Större händelser kräver mycket resurser. När krisen drar ut på tiden måste de inblandade, som jobbar för att lösa eller lindra krisen, ersättas av annan personal och bli avlösta på sin post. Resurser kan då be-



Figur 2 Händelser i vardagen kräver mindre samordning än större, mer komplexa händelser och kris. Uppgifter betraktas som egna på lägre samverkansnivåer respektive gemensamma på högre samverkansnivåer. Handlandet påverkas också mot mer styrt och koordinerat handlande.

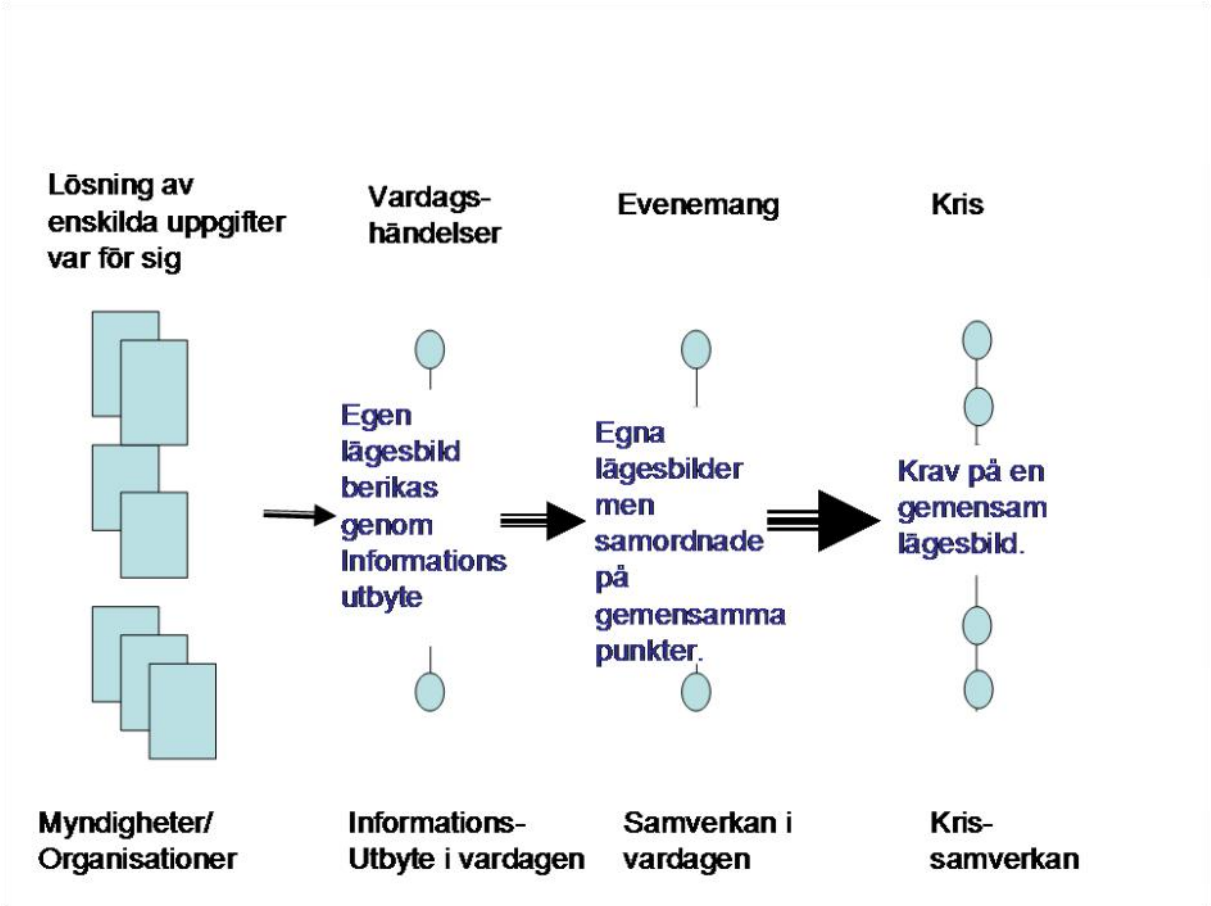
höva göras tillgängliga tvärs flera sektorer. Ett sätt att samverka för att spara resurser och inte dubbelarbeta hos flera aktörer är att erbjuda gemensam information i form av kriskommunikation. Om man t ex för flera parter samlar en informationskapacitet för extern informationsspridning, kan man sprida information av högre kvalitet, än vad som mäktas med som enskild aktör.

4. Från egen till gemensam lägesbild

Vid krissamverkan är behovet av ”rätt information till rätt person i rätt tid” avgörande. Samverkansbehovet ökar vartefter trycket ökar på hjälpande resurser, såväl personellt som vad avser utrustning, maskiner och system. När beslut finns att dela ändamålsenlig information, underlättas arbete för många som kan jobba mot gemensamma planer och förhoppningsvis även med gemensam ledning. Krissamverkan vinner på delad, samlad och gemensam information, i synnerhet i

form av gemensam lägesbild. Det innebär en sammanslagning av information från olika informationskällor för en gemensam presentation, t ex av kartdata, egen resurs, hotbild och beräkningar för prognos etc. Olika behov uppstår för olika roller i olika skeden och optimalt önskas en informationsmodell anpassad till respektive roll och gällande tidsskala.

Informationssamverkan bygger på att de involverade parterna erbjuder godkänd information för delning. Under hela kedjan är det viktigt med avvägd säkerhet och integritet. Genom att proaktivt ha funderat igenom och förberett dessa problemställningar kan information delas på ett ordnat sätt. Det kan vara så att integritet och säkerhet temporärt skall prioriteras ned för att uppnå syftet med insatsen. Idealt vill man

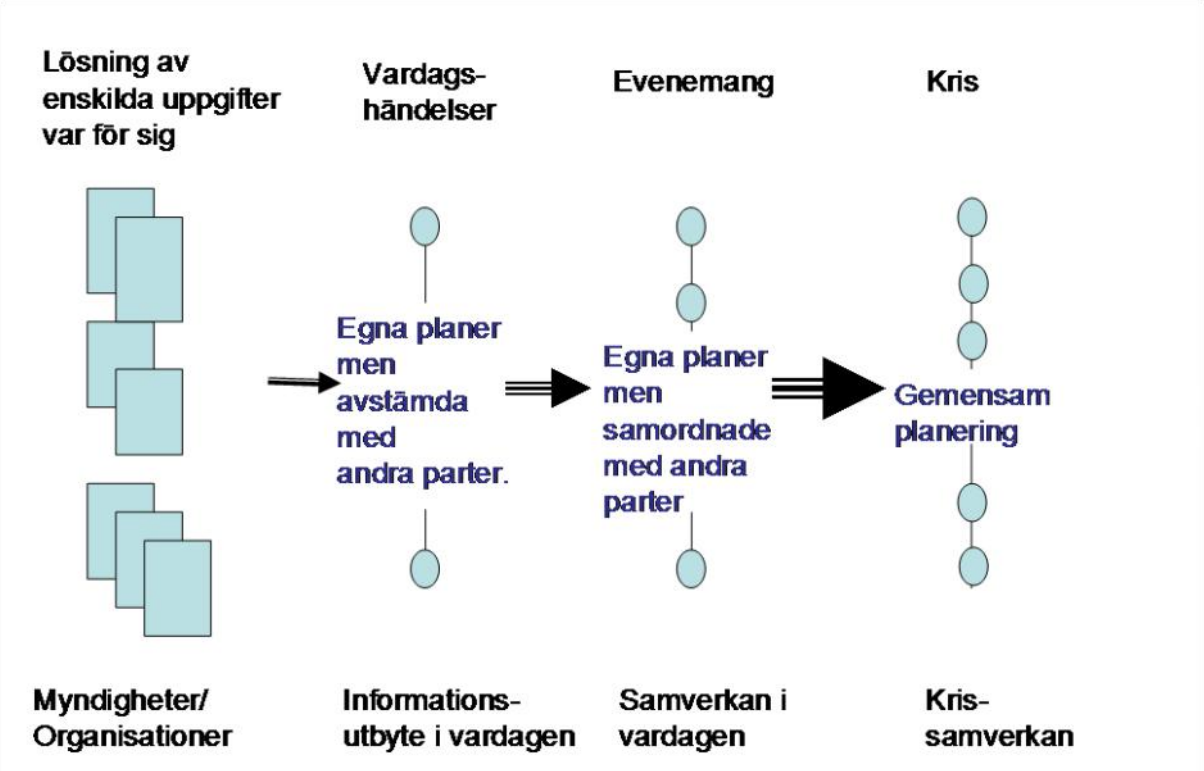


Figur 3. Vid fördjupning av samverkan ställs även krav på möjligheter till gemensam lägesbild och på vägen dit informationsutbyte och informationssamordning

dela all den information som gagnar arbetet för och med den hjälpsökande/samhället. Formerna för detta skall förberedas.

Liksom samövningar genomförs för att åstadkomma effektiv kris-samverkan vid uppfyllande av en gemensam uppgift, bör informationssamarbetet förberedas före kris. Ett framgångsrikt sätt att förbereda sig är att utgå från samma principer och grundverktyg som används vid informationsutbyte i vardagen även till eskalerade och extraordinära händelser. En rekommendation är att förstärka framgångsrika metoder, regler och teknik för vardagsarbete och strukturerat visa på utvecklingsplanen för hur detta kan utnyttjas vidare till högre samverkansnivåer. I ramverket som presenteras i denna skrift finns ett antal viktiga byggstenar för stödjande informationsinfrastruktur till samverkan. En viktig del av informationssamverkan är att underlätta för styrning och ledning (se figur 3) samt för informationsspridning till flera berörda. En gemensam lägesbild underlättar för koordinering av egna styrkor i förhållande till andra, samverkan och kommunikation. Utifrån samma informationsunderlag skapas större effektivitet och man kan göra större tidsvinster.

Efter en större kris finns ett ännu större behov av uppföljning, analys och spårbarhet i information, än i samband med vardagshändelser. Genomgående finns krav på rapportering med information om Vem?



Figur 4. Behov av samplanering ökar ju längre från vardagen som en situation utvecklar sig

När? Hur? Vad? och helst Varför? vissa beslut fattats och vilken påverkan på skeenden som uppstått.

5. Effektivitet genom gemensam planering

Vi kan för de olika samverkansnivåerna se en relation mellan högre ställda krav från situationen som uppkommit och behovet av samplanering. Krissituationer kännetecknas av att ett klart utrett ansvar är nödvändigt för snabbt handlande. Eftersom många aktörer kommer och går under situationens utveckling finns mycket att vinna på en gemensam planering mellan organisationerna. Dock krävs även stor flexibilitet för att möta dynamiken som kännetecknar kriser och extraordinära händelser

Enligt **Figur** 4 utgår vi ifrån egna planer som avstäms med andra parter när samarbetet bara omfattar informationsutbyte i vardagen. Vid den samverkansnivå som följer därpå, t ex vid evenemang och planerade större händelser, samordnar vi våra egna planer med andra parters planer. På så vis åstadkoms en avstämning som stödjer en helhetsbild och alla kan bidra till det gemensamma. Vid krissamverkan är betydelsen av att agera samordnat och utnyttja mer resurser i samverkan så stor att det är svårt att lyckas bra utan en gemensam planering.

6. Första ambitionsnivå för samverkan

Genom detta material vill vi underlätta för att utöka samarbete och höja befintlig samverkansnivå mellan myndigheter och organisationer i det svenska samhället ur flera perspektiv, inte minst förberedande och i efterarbete, förutom rent operativt under kris. Vi vill genom detta ramverk presentera lösningar på problem som åtminstone återfinns vid vardagshändelser, samtidigt som vi bäddar för en lösning som kan expandera till kris och mer komplicerade samverkansnivåer. Dessa lösningar omfattar modeller, system och metodik. De koncept som redogörs för ska hålla för alla samverkansnivåer och erbjuda helhetslösningar, t ex inom problemställningarna information, ledning, resurshantering och säkerhet. Vår rekommendation är att man medvetet jobbar med förändringsarbetet i små steg som efter utvärdering kan byggas på och nyttjas i större skala. På samma sätt bör man utveckla modeller samt informationssystem till stöd för samverkan i mindre steg. Då kan man med lyckat resultat gradvis driftsätta och vidareutveckla till alltmer krävande och lyckad samverkan.

7. Slutsatser

För att lyckas bra med samverkan, krävs stöd i den infrastruktur som samverkansgrunden byggs på. Denna infrastruktur tar ställning till såväl organisation och personal som information, verktyg och arbetssätt. I detta material vill vi visa på att det är viktigt med stöd för samverkansgrunden genom arkitektur, information och säkerhetsaspekter samt system- och verksamhetsutveckling. Ju komplexare samverkanssituation som skall lösas, desto viktigare blir stödet.

Systemsamverkan

Sammanfattning

I framtiden kommer det att krävas ett allt större informationsutbyte. Dessutom kommer samverkan i högre grad ske mellan parter som vill samverka, men på sina egna villkor. Samverkansparter kommer att komma och gå efter vilken uppgift som ska lösas.

Att anpassa alla eventuella samverkande system parvis är slöseri med resurser. Att försöka integrera system när det behövs tar för lång tid.

Lösningen är istället att anpassa systemen till principerna för en distribuerad informationsinfrastruktur som de samverkande parterna kommit överens om tillsammans. Genom att erbjuda information via tjänster kan varje system bibehålla sin integritet och befintliga system kan användas. Lös koppling peer-to-peer ger möjlighet att utnyttja de för tillfället tillgängliga tjänsterna.

1. Inledning

Utgående från att det i framtiden kommer att krävas ett allt större informationsutbyte mellan organisationer och en förmåga att starta samverkan på kort tid, uppkommer ett behov av att ta fram system som stödjer denna typ av samverkan. Att enskilda parter kan gå in i existerande samverkan och gå ur samverkan vid andra tidpunkter än andra parter ställer speciella krav på systemen. Informationsutbytet kommer dessutom i hög grad att ske mellan parter på likvärdiga villkor.

Traditionellt har varje organisation samlat in den information som just den organisationen har varit intresserad av. Informationen har i vissa fall kommit från andra organisationer även tidigare, men då har den kommit på ett specifikt dataformat, beslutat av den organisation som levererar informationen. Detta specifika gränssnitt har sedan integrerats eller snarare byggts in i den mottagande organisationens system.

Om ett större antal organisationer ska utbyta information kommer detta traditionella systemtänkande leda till att alla system skulle behöva anpassas till och integreras med alla andra system. Tekniskt är detta möjligt men kostnadsmässigt och tidsmässigt är detta förfarande helt förkastligt eftersom det är resurskrävande, tar för lång tid och saknar nödvändig flexibilitet. Ett annat alternativ är att välja ett av de samverkande systemen och anpassa alla de andra till just det systemet. Den stora nackdelen med detta alternativ är att all information måste gå via systemet ”i mitten”.

Vad som behövs är ett nytt sätt att tänka och ett nytt sätt att bygga system på. Detta nya sätt skiljer sig från vad vi är vana vid att hantera och från hur vi gjort hittills.

De tre viktigaste skillnaderna gentemot traditionell systemutveckling är:

- Gemensam överenskommelse – systemen anpassas inte till varandra utan enligt en gemensam överenskommelse
- Tjänstebaserat – systemen erbjuder informationen i form av tjänster
- Löst kopplat – systemen kopplas ihop när det behövs

2. Gemensam överenskommelse

Det man vill åstadkomma är att alla samverkande system ska kunna utbyta information med varandra men inte behöva anpassas till varandra i alla möjliga fall. För att lösa det behöver man istället anpassa samtliga system till något gemensamt.

Det gemensamma skulle kunna vara ett av de samverkande systemen. Då kommer emellertid all information bli beroende av det systemet vilket ger en del nackdelar för de andra systemen. T ex kan inte två andra system utbyta information om det gemensamma systemet inte fungerar. Det blir också problem om två system vill utbyta information som dessa två systemen kan hantera men inte det gemensamma systemet. Det är inte säkert att den som äger det gemensamma systemet vill utvidga sitt system med sådan information.

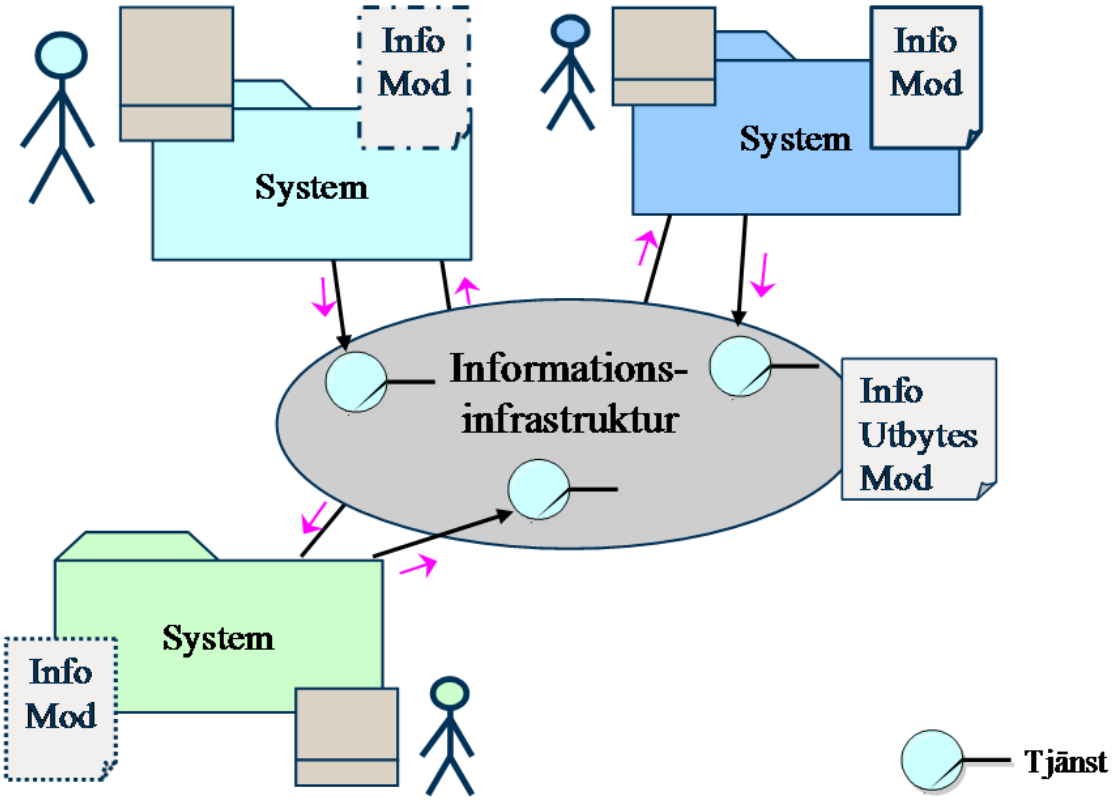
En bättre lösning är att ha ett neutralt system i mitten i form av en informationsinfrastruktur, se Figur 1. De samverkande systemen kan då samverka på lika villkor eftersom alla har samma koppling till informationsinfrastrukturen. Inget av systemen bestämmer heller ensidigt hur informationen som utbyts ska se ut utan det bestäms av de samverkande parterna som tar fram en så kallad informationsutbytesmodell.

För att kunna hantera information har varje system en informationsmodell som bestämmer hur informationen representeras i systemet. Denna informationsmodell skiljer sig mellan olika system vilket betyder att de inte förstår varandras representation. När flera system ska utbyta information behövs en speciell informationsmodell som alla system ”förstår”, en informationsutbytesmodell som beskriver representationen av den information man kommit överens om att utbyta.

Samverkan via informationsinfrastrukturen är tänkt att ske peer-to-peer, d v s system som vill utbyta information kopplar upp sig direkt mot varandra. Det som informationsinfrastrukturen ger är reglerna för utbyte så att systemen kan utbyta information om de är anpassade till informationsinfrastrukturen, oavsett om de samverkat förut eller inte.

Vid koppling av typ peer-to-peer, behöver informationsutbytesmodellen inte finnas som egen informationsmodell utan skulle kunna bestå av ett antal översättningar mellan de ingående systemens informationsmodeller. För eventuella nya system är det emellertid önsk-

värt att den finns som egen informationsmodell eftersom de då kan anpassas direkt till den.



Figur 1. Tre system som samverkar via en gemensam informationsinfrastruktur. Alla tre systemen har var sin informationsmodell och de utbyter information med varandra genom att producera och konsumera tjänster som följer den gemensamma informationsutbytesmodellen (som skiljer sig från informationsmodellerna).

Informationsinfrastrukturen ska inte behöva finnas som separat fysiskt system. Den kan istället vara helt distribuerad över de samverkande parternas system. Det betyder att alla system kommer att ha en liten bit av informationsinfrastrukturen i sig. För varje system som ansluter sig till informationsinfrastrukturen kommer det systemets del att tillsammans med de andra systemens delar (samt kommunikationsinfrastrukturen) att bilda en helhet.

För att denna typ av lösning ska bli framgångsrik krävs *två* saker. Den ena är att den information som utbyts hålls isär från den teknik som används. Detta är ett måste för att tekniken ska kunna bytas ut utan att alltför stora ändringar behöver göras i systemen. Så länge principerna och informationsmodellerna är desamma kommer påver-

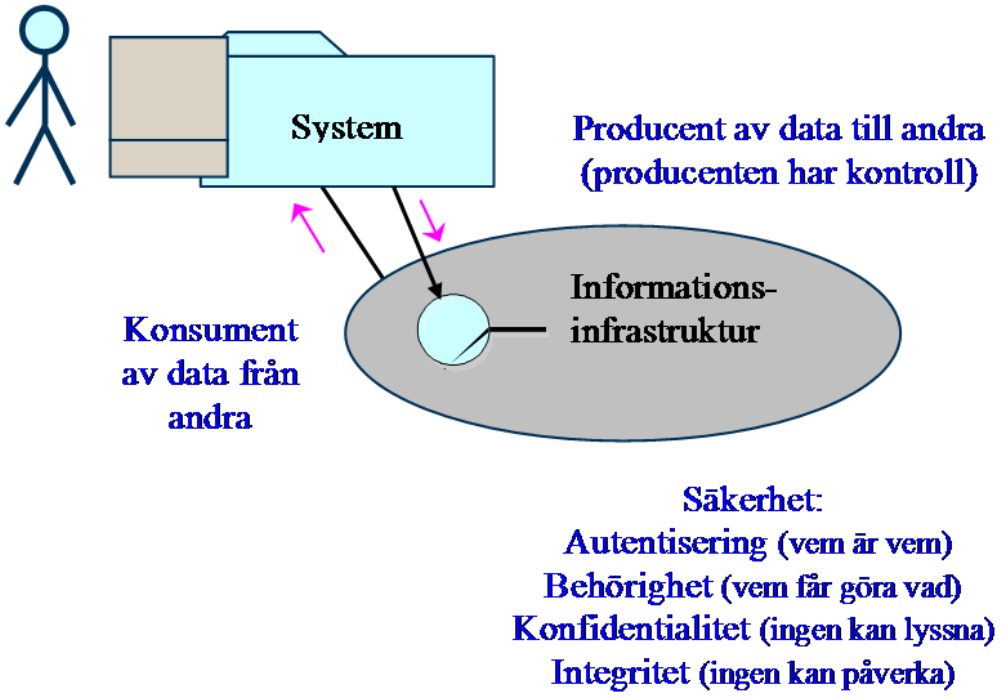
kan på systemen att hållas till ett minimum, trots att tekniken måste bytas med jämna mellanrum.

Den andra är en överenskommelse mellan de samverkande parterna om varifrån vilken information kommer. Vitsen med samverkan är ju i synnerhet att få tillgång till mer information än sin egen.

3. Tjänster

Det hittills vanligaste sättet att kommunicera mellan system har varit att ha en datakoppling där avsändaren skickar data direkt till mottagaren som är bestämd i förväg (ofta genom kodning eller i bästa fall konfigurering).

Figur 2 visar ett systems anslutning till informationsinfrastrukturen. Den största skillnaden gentemot direkt datakoppling är att informationen inte erbjuds som en datalänk utan som en (teknisk) tjänst. Ägaren av informationen bestämmer vilken information som kan exporteras och systemet erbjuder sedan den informationen i form av (tekniska) tjänster. Dessa tjänster anmäls till en ”katalog” i informa-



Figur 2. Anslutning av ett system till informationsinfrastrukturen. Systemet erbjuder informationen i form av tjänster och hämtar information genom att konsumera andra systems tjänster. Kommunikation och säkerhet sköts av informationsinfrastrukturen.

tionsinfrastrukturen. Tekniskt sett tar systemets ansvar slut där och vem som använder tjänsten (om någon gör det över huvud taget) är från systemets sida ointressant.

För ägaren av informationen är det däremot viktigt att informationen inte hamnar i orätta händer. Därför måste informationsinfrastrukturen och dess säkerhetsmekanismer se till att ingen obehörig kan använda tjänsterna. Säkerhetsmekanismerna ska kontrollera vem som försöker göra något (autentisering), om personen är behörig (behörighet) och se till att informationen överförs på ett säkert sätt (konfidentialitet och integritet).

Tjänsterna är inte heller på något sätt en koppling rakt in i systemet. En tjänst är en fasad (realiserad med programvara). Tjänsten måste ha tillgång till informationen som ska exporteras men i övrigt kan kopplingen mellan tjänsten och systemet vara hur begränsad som helst. Huruvida tjänsten körs i systemet eller som en separat komponent är upp till ägaren av systemet. Genom att använda tjänsten kan man hämta den information som exporteras via tjänsten. Övrig information som finns i systemet finns ej tillgänglig från tjänsten och kan därmed inte hämtas via tjänsten[1].

Ägaren av informationen avgör vilken information som kan exporteras. Den aktuella informationen ges till en eller flera tjänster som erbjuder informationen utåt beroende på behörighet. Informationen som exporterats samt all annan information i systemet finns alltid kvar orörd i systemet. Vill man att andra system ska ha möjlighet att uppdatera informationen behöver man erbjuda en tjänst ”ta emot uppdateringar”. När information tas emot kontrollerar man varifrån den kommer och bestämmer sedan om man vill utföra uppdateringen eller inte. Informationen i systemet kontrolleras helt och hållet av systemet självt.

Ny information kan också hämtas från de tjänster som de andra systemen erbjuder. På detta sätt kan man utöka informationen i ett system utan att användarna varken behöver ändra arbetssätt eller verktyg. De arbetar som vanligt i sitt vanliga (egna) system. Skillnaden är att de kan få tillgång till mer information, när systemet klarar av att visa den information som hämtats från de andra systemen.

[1]Om man inte hackar sig in i systemet men då spelar det ingen roll om det är en tjänst eller annan koppling.

4. Lös koppling

Den information, som systemet vill ha från andra system, hämtas från deras respektive tjänster. Det är därmed inte inbyggt i systemet varifrån informationen hämtas, utan den kan hämtas från valfri tjänst av rätt typ. Meningen är att så många som möjligt, som erbjuder samma typ av information, ska erbjuda samma typ av tjänst. Till exempel kan ett flertal leverantörer erbjuda kartdata via tjänster med samma gränssnitt. De erbjuder då samma tjänst (samma gränssnitt, samma funktionalitet) men är olika tjänsteinstanser (olika leverantörer och/eller uppsättningar information). Vitsen med det är att man kan byta leverantör av tjänsten på ett ögonblick. Eftersom leverantörerna inte alltid har den prioriteringen kan det emellertid behövas styrning för att få det dit hän.

Istället för att ha en förutbestämd koppling till ett specifikt system har man förberett en uppkoppling mot en viss typ av tjänst. På så vis får man hög flexibilitet med avseende på vilket system man använder. När behovet av information uppstår, söker man efter en tjänsteinstans av rätt typ i informationsinfrastrukturens ”katalog” och kopplar sedan upp förbindelsen (peer-to-peer). I de fall man vill ha information från ett specifikt system får man se till att söka efter exakt den tjänsteinstansen som hör ihop med rätt system.

Man kan också ”rangordna” tjänsteinstanser efter specifika egenskaper hos instanserna. Det ger möjlighet att vid varje tillfälle välja den mest passande tjänsteinstansen. Till exempel kan man välja en pålitlig (och robust) partner i första hand och ha ett allmänt tillgängligt alternativ i reserv.

Om behovet av information upphör kopplar man ner förbindelsen. Om tjänsten av någon anledning (fel på tjänsten, fel i systemet, fel på kommunikationen) inte är användbar längre kan förbindelsen kopplas ner automatiskt. Då är det lämpligt att automatiskt försöka koppla upp förbindelsen igen eller, om det inte går, koppla upp en förbindelse till en annan tjänsteinstans. Uppkopplingarna mellan system är alltså inte statiska utan anpassas till den rådande situationen. Alla tjänster och system måste kunna hantera att tjänster kommer och går.

Ett fåtal tjänster är så viktiga och kritiska för verksamheten att de alltid måste vara tillgängliga. Leverantören av en sådan tjänst måste då vara medveten om detta och vidta åtgärder beroende på om det krävs

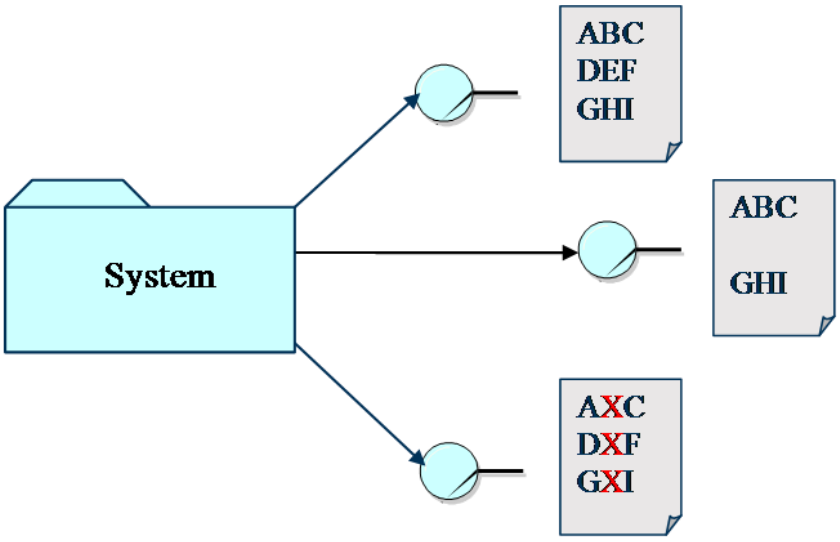
att en och samma tjänsteinstans är tillgänglig eller om det behövs flera tjänsteinstanser med samma information. Högre krav på tillgänglighet leder till större resursanvändning vilket också är en parameter när man väljer tjänsteinstans.

En fördel med detta sätt att samverka och utbyta information är den stora flexibilitet som kan hanteras. I vissa fall vill man, av olika skäl, emellertid inte ha denna flexibilitet. Till exempel kan man vilja ha kontroll på vilka kopplingar som görs mellan systemen. Det är dock en skillnad mellan att flexibiliteten finns att utnyttja och att verkligen utnyttja den. Bara för att infrastrukturen klarar flexibilitet finns det inget som hindrar att man använder den tillsammans med riktlinjer som ger centraliserad styrning när det är lämpligt.

5. Anpassad information

I vissa fall är det inte önskvärt att skicka samma information till alla mottagare. Tänkbara orsaker är till exempel att mottagarna är intresserade av information från olika geografiska områden eller att delar av informationen är känslig och inte får skickas till samtliga mottagare.

Lösningen är att sätta upp ett flertal tjänsteinstanser för samma tjänst där skillnaden är vilken del av information som är åtkomlig, se figur 3. Behörigheter styr sedan vilka tjänsteinstanser som är åtkomliga.



Figur 3. Tre tjänsteinstanser som erbjuder olika utsnitt av informationen.

6. Befintliga system

De allra flesta system som kommer att anslutas till informationsinfrastrukturen kommer inte att ha designats för det från början, utan istället vara de system som finns idag. För att anpassa ett befintligt system behövs ett tillägg i form av programvara som har åtkomst till lämplig information i systemet och som samtidigt erbjuder en eller flera tjänster (egentligen tjänstegränssnitt) utåt.

Eftersom samverkan i detta fall bygger på frivillighet och överenskommelser är det upp till varje part att anpassa sina system till informationsinfrastrukturen (med viss hjälp om det behövs). Hur anpassningen görs kan variera från system till system.

Ett sätt att anpassa ett befintligt system är att göra ett tillägg i systemet som erbjuder tjänsterna så att systemet utifrån ser ut att vara tjänstebaserat från början. Ett annat sätt är att lägga anpassningen som en separat komponent - en brygga. En sådan brygga är anpassad för systemet på ena sidan och tjänsteorienterad på den andra sidan. I de fall kommunikationen med systemet sker på ett standardiserat sätt skulle samma brygga kunna användas för flera system som använder samma standard.

7. Slutsatser

Nya sätt att samverka kräver nya tekniska lösningar. Det sätt att samverka som beskrivits här utgår från:

- Samverkan mellan parter som kan bidra just för tillfället (parter kan komma och gå)
- Samverkan på lika villkor
- Bibehållen integritet för samverkande system
- Användning av de vanliga befintliga systemen

Den tekniska lösning för att underlätta ovanstående som beskrivits här bygger på:

- Användning av en distribuerad informationsinfrastruktur
- Samverkan peer-to-peer

- Löst kopplade system
- Information erbjuds som tjänster

System av system

Sammanfattning

Ett system av system uppstår då distribuerade självständiga system tillfälligt integreras för att tillsammans skapa ny eller förbättrad funktionalitet. Dagens informations- och kommunikationsteknologi gör det teknisk möjligt att koppla samman en stor mängd tekniska system, både mjukvarusystem och hårdvara som t.ex. sensorer, och låta dessa utbyta information, även i realtid. Även människor kan ses som ingående i ett sådant ”system av system”.

1. Inledning

Begreppet system av system definieras och beskrivs här med fokus på tillämpningar inom säkerhet i samhället. Förverkligandet av konceptet befinner sig på ett tidigt stadium och i den form det beskrivs här får konceptet till stora delar ännu betraktas som en vision. Väsentliga frågeställningar för fortsatt realisering av visionen diskuteras, bl.a. frågor om ägande och styrning av system och information, samt principer, verktyg och stödsystem för att skapa och ”situationsanpassa” system av system.

2. Vad är ett system av system?

Ett system av system uppstår då ett antal enskilda system samverkar och under en begränsad tidsrymd tillsammans fungerar som ett större integrerat system. Det finns inte någon helt vedertagen definition av begreppet men ett antal kriterier brukar anges för att man ska tala om ett system av system. Ett system av system är en sammansättning av system där det gäller att de enskilda systemen:

- Fungerar och kan styras ”självständigt”
- Samverkar med olika typer av andra system via ett nätverk
- Kombineras på olika sätt och användas i olika verksamheter
- Är geografisk spridda
- Har olika funktioner
- Kan vara baserade på olika teknologier (heterogena system)

För det sammansatta systemet av system gäller att det:

- Erhåller nya egenskaper som saknas hos de enskilda systemen (emergent properties)
- Kan utvecklas evolutionärt genom att fler och fler enskilda system successivt görs tillgängliga

Som kontrast till ett system av system kan ett ”vanligt” system beskrivas som sammansatt av ”delsystem” på ett mer permanent sätt.

Man ska vara medveten om att det finns olika syn på vad ett system av system är och bör vara även om de flesta är någotsånär överens

om ovanstående kriterier. En omdebatterad fråga är vilken granularitet som är lämplig, dvs. hur stort ett enskilt system bör vara. Systemstorleken kan spänna från, i militär sammanhang, hela hangarfartyg, till en programvarumodul som utför en begränsad uppgift. Det koncept som beskrivs i detta arbete avser typiskt en granularitet någonstans mitt emellan dessa extremer.

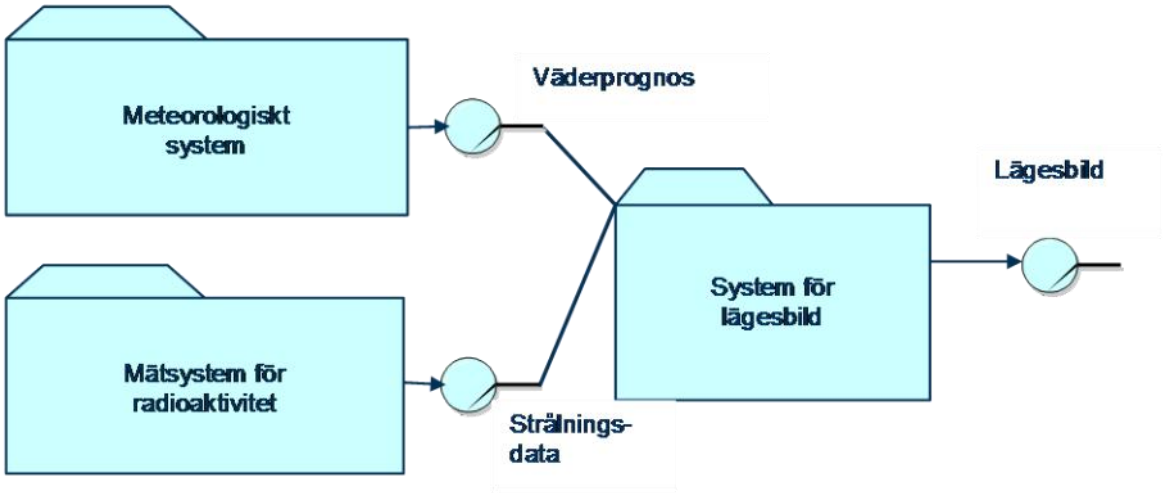
I det koncept för system av system som beskrivs i detta arbete ingår ytterligare en viktig förutsättning: samverkan mellan system baseras på tjänstekonceptet. Det går att definiera ett koncept för system av system utan att basera det på ett tjänstebegrepp men det beaktas inte vidare i detta arbete.

Det koncept som beskrivs här innebär också att system av system aldrig är statiska. Sammansättningar skapas i realtid när de behövs och både sammansättning och de enskilda systemens parametrar varierar över tiden, allteftersom behoven förändras.

Det finns ytterligare termer och begrepp som kan vara identiska med eller ligga nära begreppet system av system som det beskrivs i detta arbete, t.ex. federationer av system eller situationsanpassade system.

Man kan se olika möjliga tillämpningar för system av system inom säkerhet i samhället och naturligtvis finns även olika former av begränsningar. Särskilt inom säkerhet i samhället är det viktigt att kunna styra sammansättningen av system och informationsflödet mellan dessa. Styrningen kan ske dynamiskt vilket leder till att system från olika myndigheter och organisationer samverkar så att den förmåga som krävs i en viss situation erhålls.

Om exempelvis ett radioaktivt utsläpp sker kan ett mätsystem för radioaktiv strålning kombineras med ett väderprognossystem för att ge en bild av strålningsrisker på olika platser. Detta är ett exempel på att ett enkelt tolkningsbart resultat kan uppstå ur en mycket komplex bakomliggande systemsammansättning. Genom att konfigurera det kombinerade systemet först då ett behov uppstår undviks onödig komplexitet och att känsliga sammanställningar av information uppstår i onödan. Istället kan skydd av sekretess och integritet vägas mot nytta i varje enskilt fall.



Figur 1. System- och tjänstediagram för ett exempel på ett system av system. Rutorna symboliserar system och cirklarna symboliserar tjänster.

3. Exempel på system av system

Ett exempel på ett system av system illustreras i nedanstående system och tjänstediagram, se figur 1.

I exemplet kombineras ett meteorologiskt system med ett system för mätning av radioaktivitet och ett system för sammanställning av lägesbilder. I det sistnämnda kan olika typer av information sättas samman med bl.a. geografisk information så att det kan presenteras för en användare. Denna systemkombination är mindre intressant så länge endast normal radioaktiv strålning förekommer. Om ett radioaktivt utsläpp sker kan däremot en sådan sammansättning bli mycket värdefull eftersom den kan bidra till att ge en bild av strålningsrisker på olika platser.

Ett scenario med ett radioaktivt utsläpp kan delas upp i ett antal faser över tiden. I en normal situation har man en kontinuerlig mätfas där strålningsnivåer rutinmässigt registreras. Vid ett utsläpp utlöses en händelsekedja då en förhöjd strålning detekteras av en eller flera mätutrustningar. Detekteringen ger upphov till ett larm och därmed aktiveras nästa fas i händelsekedjan som omfattar analys och beslut om åtgärder. Beslutsfattare kan i denna fas använda lägesbilden i figur 1.

Information från ytterligare system kan också tillfogas, t.ex. information från databaser om särskilt känsliga objekt, som livsmedelsproduktion m.m. Om det bedöms nödvändigt kan man fatta beslut om åtgärder, t.ex. information och varningar till allmänheten eller någon

form av saneringsåtgärder. En ny fas uppstår då en åtgärd ska utföras. Exempelvis kan ett system för varning av allmänheten med hjälp av högtalare användas tillsammans med lägesbilden för att snabbt och effektivt aktivera varningar i relevanta områden. En annan möjlighet är att kombinera lägesbilden med ett ledningssystem för att leda ett saneringsarbete. Information om personalens position, tillgänglig utrustning m.m. kan då presenteras tillsammans med övrig information i lägesbilden.

Scenariot ovan beskriver en händelsekedja bestående av en sekvens av faser där olika sammansättningar av system används i de olika faserna. Ett mönster för samverkan mellan system genom sekvenser av utbyten av tjänster över tiden för att nå ett gemensamt mål kallas tjänstekoreografi (service choreography). Resultatet från en fas utgör grund för aktiviteter i senare faser. I ett givet scenario krävs en viss kvalitet på resultaten från varje fas för att kedjan av aktiviteter ska ”fungera”, t.ex. i detta fall att en varning ska kunna distribueras i tillräckligt god tid så att människor kan hinna ta sig inomhus och stänga fönster och ventilation innan ett radioaktivt moln närmar sig bebyggelse. I de olika faserna är förutom tekniska system även människor aktiva. De mänskliga aktörerna kan ses som system som lämnar ett bidrag till den totala funktionen av ett system av system.

4. Varför system av system?

Vad är nyttan med att arbeta med system av system snarare än ”traditionella” system? Många sammansättningar av system används inte kontinuerligt utan behovet av dem uppstår bara under speciella, och i många fall sällsynta, förutsättningar. I dessa fall är det inte kostnadseffektivt att ”binda upp” systemen som permanenta delsystem i ett fixt sammansatt system. Genom att istället ha möjlighet att använda ett system i olika sammanhang fås så stor nytta som möjligt av varje enskilt system.

När det gäller informationstjänster, som inte ”förbrukas” av att användas, är det heller inte effektivt (och inte lämpligt ur säkerhetssynpunkt) att hela tiden skicka information kors och tvärs och kontinuerligt realisera alla upptänkliga tjänster som kan komma att behövas om t.ex. en krissituation uppstår. Det är långt mer kostnadseffektivt att ha en ”legolåda” med självständiga system som kan kombineras

ihop på olika sätt till situationsanpassade system av system när ett behov uppstår.

Dessutom fås flexibilitet att skapa system av system för att hantera situationer som är svåra att förutse och därmed knappast möjliga att hantera med ett fixt sammansatt system ens till en högre kostnad.

En annan stor fördel är att man inte behöver bygga ett stort system ”färdigt” från början. Att arbeta med system av system stöder och underlättar att man börjar med ett mindre antal system som klarar de viktigaste behoven och sedan successivt tillför system enligt ett evolutionärt arbetssätt. Enskilda system kan också fasas ur och ersättas av nya system på ett enkelt och effektivt sätt.

5. Komplexitet och användbarhet hos system av system

System av system kan tyckas vara komplexa. I jämförelse med permanent sammansatta system av motsvarande storlek innebär dock system av system och tjänstekonceptet en förenkling. Detta uppnås genom den tydliga avgränsningen mellan nivåerna system respektive system av system. Exempelvis kan ett system för framtagning av väderprognoser vara mycket komplext men slutresultatet är samtidigt tydligt och enkelt definierat och kan beskrivas med begrepp som går lätt att förstå. Det är också lätt att förstå vad systemets resultat har för egenskaper och kvaliteter och hur det kan användas. Med hjälp av väldefinierade gränssnitt döljs den inre komplexiteten. Det utgör därmed en stabil grund för fortsatt systembygge på sammansatt nivå. I själva verket är principen för system av system och tillhörande systemsyn snarast en förutsättning för att kunna hantera allt större sammansättningar av system.

Många sammansättningar kommer att användas mycket sällan. För att det ändå ska vara möjligt att hantera dessa när en oförutsedd situation inträffar är det viktigt att i så stor utsträckning som möjligt utnyttja samma system och användninsprinciper i vardaglig och ofta förekommande verksamhet som i krissituationer och andra exceptionella situationer. Sammansättningarna av system kan vara unika men de ingående systemen och användningssättet ska så långt som möjligt kännas igen från situation till situation.

6. Utformning av system av system

I analogi med traditionell systemutformning har en ny disciplin uppstått som behandlar utformning av system av system. De två disciplinerna har vissa delar gemensamt medan andra delar måste hanteras enligt andra principer på nivån system av system. Disciplinen ”System of systems engineering” är i en fas av tidig men accelererande utveckling. En illustration av detta att en ny vetenskaplig tidskrift med titeln ”International Journal of System of Systems Engineering” just nu är planerad att utkomma med sitt första nummer (Inderscience Publishers Ltd.). Konferenser i ämnet hålls regelbundet[1].

Utformning av system av system handlar ytterst om att säkerställa att olika system kan samverka så att förväntat resultat uppstår. Utformning av systemsamverkan via tjänster, vilket brukar kallas tjänsteorkestrering, och samverkansmönster över tiden för att uppnå olika syften, tjänstekoreografi, är delar i detta. En annan del är att analysera tillgängliga realiseringar och säkerställa att tillgänglighet och kvalitet är tillräcklig för att tjänster som behövs i olika situationer fungerar och har tillräckliga prestanda för att som helhet ge önskat resultat. Exempelvis vid utformning av system av system för varning för radioaktivt utsläpp måste alla system som krävs i de olika faserna (mätfas, analysfas, varningsfas) ha tillgänglighet och prestanda som medför att en varning kan utfärdas i tid oavsett var och på vilket sätt utsläppet uppstår. Baserat på ett antal scenarion kan ett system av systems funktioner och förmågor definieras och analyseras, detta kräver i många fall relativt avancerade simuleringsmetoder.

Utformning av system av system omfattar bl.a. modellering och simulering, optimering och visualisering av system av system, analys och utformning av informationsmodeller och informationsflöden samt prestandaanalys. En god utgångspunkt för utformning av system av system är objektorienterad och modellbaserad systemutveckling. Metoderna från systemnivån måste vidareutvecklas i flera avseenden för att passa nivån system av system. Något av det som karakteriserar utformning av system av system är en omfattande användning av realistiska scenarion. Dessutom krävs analys och utformning av samverkan på verksamhetsnivå vilket bl.a. inkluderar analys av beslutsprocesser och utformning av stöd för dessa.

[1]T.ex. IEEE International Conference on System of Systems Engineering som hölls första gången 2006 och planeras att genomföras årligen.

Man måste också kunna ställa krav på enskilda system utgående från det tänkta användandet i system av system. Kravställning på ett enskilt system som ska ingå i system av system skiljer sig från traditionell kravställning. Anledningen är att systemet ju inte bara ska fungera tillsammans med i förväg definierade och välkända system utan kunna fungera tillsammans med ett större antal olika externa system i en stor mängd olika sammanhang. I det traditionella fallet styrs kraven på ett system av ett begränsat antal användningsfall. Nu blir kravet snarare att ge ett så bra bidrag som möjligt till så många relevanta scenarier som möjligt där det förekommer olika andra system att samverka med. Eftersom man vill kunna hantera även scenarier man inte kunnat förutse är de relevanta scenarierna bara delvis kända i förväg och kravbilden är därför med nödvändighet mindre precis än i det traditionella fallet. Det finns ingen möjlighet att deduktivt härleda en kravbild utan kravställning måste ske genom att ansätta systemets egenskaper och värdera dessa i ett antal scenariesituationer. På så vis kan man värdera, och om man utvecklar ett nytt system, även optimera systemet för användning i system av system.

7. Stödsystem och verktyg

Ett antal grundläggande tjänster krävs för att system ska kommunicera och samverka med hjälp av tjänster som ett system av system. Den viktigaste är namntjänsten som anger vilka tjänster som finns tillgängliga och vilka system som tillhandahåller dessa. Ett verktyg krävs också för att i realtid konfigurera den sammansättning av system som önskas, d.v.s. att kontinuerligt skapa och modifiera ett system av system. Verktyget måste kunna användas både för utformning av ”fördefinierade” system av system och konfigurering i realtid.

8. Delning av system och information

I konceptet för system av system ligger att kombinera ihop olika system för att skapa nya nyttiga funktioner. För att kunna genomföra detta ställs man ofta inför problematiken att de system man skulle vilja kombinera, och den information som hanteras, ägs av olika organisationer. Frågan uppstår då i vilken utsträckning de olika organisationer får och vill dela sina system och sin information. När det gäller samverkan mellan myndigheter styrs detta i stor utsträckning av lag-

stiftning. En myndighet har ett stort ansvar för sin information och att denna inte kan missbrukas eller hamnar i orätta händer.

Vägen mot att möjliggöra delning av system och information måste dels gå via ett utvecklande av de ”icke-tekniska” förutsättningarna vad gäller lagstiftning, regler, avtal, samverkansformer m.m. Dessutom måste tekniskt stöd utvecklas för att säkerställa att delning av system och information sker på det sätt man önskar i varje situation. Grunden är att man respekterar varje organisations äganderätt och ansvar för sina system och sin information. Det kan vidare innebära att man vid delning begränsar tillgång till system och information vad avser kvalitet (t.ex. kan man kanske ange ungefär var ambulanser befinner sig men inte exakt), vem som ska få tillgång till information, hur system och information får användas, under vilken tid delning ska ske, under vilka exceptionella förutsättningar (t.ex. större olyckor eller kriser) delning får ske, etc. På detta sätt kan delning ske med bibehållen integritet och kontroll.

9. Styrning av system av system

Med en tjänstemiljö med grundtjänster, verktyg för byggande och modifiering av system av system, stödsystem för integritetsfull delning av system och information har man kommit en lång väg mot att använda system av system men det är fortfarande inte tillräckligt. Hur vet man vilka systemkombinationer som är möjliga och vilken som bäst stöder en given situation? Och om flera aktörer gör anspråk på samma system på ett oförenligt sätt, hur vet man vilken begäran som är viktigast, och hur fattas beslut om hur systemen ska användas?

Vilka systemkombinationer man kan ha nytta av i en given situation kan i enklare fall vara uppenbart för en användare men i mer komplicerade fall krävs ett intelligent stödsystem. En analys i realtid av olika möjliga system av system och dess förmåga att fungerar i aktuella scenarion kan vara nödvändiga för en mer avancerad användning av systemkombinationer. Detta kan ses som en ”realtidsversion” av den simuleringsbaserade värdering av system av system som diskuterades i samband med utformning av system av system.

När ett behov uppstår av en typ av system och dess tjänst kan det naturligtvis inträffa att något system råkar producera tjänsten med godtagbara prestanda men om så inte är fallet kan det uppstå en begäran

om att ”produktion” av tjänsten påbörjas eller förbättras för att uppfylla behovet. Med stor sannolikhet innebär uppfyllan av en sådan begäran en ”kostnad”, t.ex. i form av att ett system om-allokeras på något sätt. I de fall kostnader eller resurskonflikter uppstår krävs en ledningsprincip och ett ledningssystem för att styra systemanvändningen. En ledningsprincip kan bl.a. innebära att ägarskapet av en resurs ska vara helt styrande eller att ”verksamheten som helhet” ska prioriteras. Beslut kan antingen fattas av någon ”överordnad instans” eller alternativt genom ”förhandling” mellan företrädare för de olika systemsammansättningarna. Oavsett ledningsprinciper krävs någon form av beslutsstöd och ledningssystem för att säkerställa att system uppträder och används som avsett. Exempelvis kan det vara nödvändigt att garantera tillgång till en tjänst med vissa prestanda under en viss tid (Service Level Agreement) för att det ska vara rimligt att använda den även i sådana fall då t.ex. människors liv är beroende av att systemet inte plötsligt slutar producera tjänsten.

10.Slutsatser

Det koncept för system av system som beskrivs här är till stora delar ännu så länge en vision. De tekniska förutsättningarna finns dock redan idag för att implementera lösningar enligt principen system av system. Idéer kring denna typ av lösningar får en allt större spridning och system för säkerhet i samhället med inriktning mot konceptet börjar nu också anskaffas av myndigheter på olika håll i världen. Det evolutionära utvecklingssättet gör det möjligt att börja i begränsad skala och successivt skapa förutsättningar för en ökad samverkan mellan olika system.

Mål och medel för informationsinfrastruktur

Sammanfattning

En informationsinfrastruktur utgör en plattform för samverkan mellan parter som är delaktiga i något visst sammanhang, såsom incidenthantering, gemensam övervakning, eller rutinmässig ömsesidigt utbyte av information.

Detta avsnitt lyfter fram några perspektiv på begreppet informationsinfrastruktur, strukturerat i två grupper. Dels de drivkrafter och mål som informationsinfrastrukturen måste bejaka. Dels de fundamentala begrepp som måste stödjas av infrastrukturen, såväl som utgöra styrmedel för anpassning av infrastrukturen.

1. Inledning

I avsnittet ”Grunder för informationsinfrastruktur” gavs en intuitiv och översiktlig beskrivning av vad som menas med en informationsinfrastruktur. Det huvudbudskap som presenterades där är att en informationsinfrastruktur erbjuder en plattform för informationsbaserad samverkan mellan parter inom ett visst sammanhang.

Detta avsnitt beskriver några perspektiv på begreppet informationsinfrastruktur – vilka mål en infrastruktur bör uppfylla eller bidraga till, och hur arkitekturen hos infrastrukturen underbygger dessa egenskaper.

Texten består av två huvuddelar:

- Drivkrafter och mål – lyfter fram några krav som påverkat utformningen av den grundläggande modellen för informationsinfrastruktur
- Modellbaserad infrastruktur – visar hur explicit användning av modeller stöder användning och anpassning av infrastrukturen.

2. Drivkrafter och mål

Nedan redovisas några viktiga pådrivande faktorer och eftersträvade mål som är av central betydelse vid bedömning av de möjligheter en informationsinfrastruktur kan skapa.

2.1. Ökat samverkansbehov

I den offentliga verksamheten finns ett uttalat behov av ökad samverkan mellan olika organisationer, såväl inom det allmänna som med övriga sektorer i samhället.

De organisationer som samverkar (nedan benämnda ”parter”) har egna organisations- och ledningsformer. Samverkan innebär att parter konstruktivt bidrar till den verksamhet som andra parter utför, och att flera parters verksamhet kan ömsesidigt synkroniseras för att uppnå bättre effekter. En grupp av samverkande parter, där samverkandet är ett uttalat mål, kallas en koalition. I begreppet koalition ingår att samverkan sker i enlighet med uttryckta, och accepterade, regler och policies.

En informationsinfrastruktur kan ses som ett slags rum (samverkansrum) där parter "vistas" och interagerar med varandra i termer av in-

formation. En part kan tillhandahålla information till en annan part i samverkansrummet. En part kan ställa frågor till en annan part (eller till flera andra parter) och förvänta sig att få ett (eller flera) svar, eller någon typ av indikation om att frågan inte kan besvaras.

2.2. Smidig samverkan

Det som knyter samman parterna är alltså dels den information som de *kan* utbyta (som det finns kunder för), dels det sätt varpå de deklarerar *att* de vill deltaga i visst informationsutbyte. För att parter i samverkansrummet skall veta hur de kan agera och hur de skall tolka andras beteenden, så krävs en uppsättning gemensamt överenskomna umgängesregler. Genom att följa dessa regler, som berör interaktion part-till-part och mellan en part och den gemensamma infrastrukturen, så uppnås en harmonisering av hur parter beter sig i samverkanssammanhanget, vilket ökar graden av förutsägbarhet i parters agerande. Eftersom reglerna enbart berör beteende som andra parter kan observera, så har enskilda parter stor frihet i hur de väljer att forma sitt interna beteende.

2.3. Delad förståelse

Förutom överenskommelser om umgängesregler, så krävs en samstämmighet i hur parter skall förstå den information som utbytes, så att mottagaren av information kan tolka informationen på ett sätt som är välgrundat. I informationsbaserad samverkan är det viktigt (ofta kritiskt) att parter har likartade uppfattningar om vad information betyder (informationens semantik).

Genom överenskommelser kan informationsinfrastrukturen fungera som ett samverkansrum där även tolkningen av informationen är koordinerad eller överenskommen.

2.4. Optimerad kvalitet

Information används som beslutsunderlag. Information omsätts ytterst till beteende som ger effekter i världen. Information finns som regel ojämnt spridd i en koalition. Olika parter befinner sig olika "nära" till informationskällor, eller har olika möjligheter att skapa information med adekvat kvalitet.

Ur ett kostnadseffektivitetsperspektiv så bör parter som har bättre förutsättningar att skapa högkvalitativ information ta på sig rollen att tillhandahålla sådan information till de andra parter som behöver utnyttja informationen. Detta kan ske genom överenskommelser – i samband med att samverkansformerna etableras – kring vem som tillhandahåller vad, eller genom att informationsleverantörer även tillhandahåller kvalitetsrelaterad metadata om den information de kan leverera.

2.5. Förbättrat mervärde

Informationsutbyte mellan parter i en koalition, är utbyte av sådan information som direkt eller indirekt bidrar till det ändamål som koalitionen definierats för. För en koalition finnas definierade verksamhetsområden, mål och aktiviteter. Information som berör ett sådant insatsområde är del i informationsutbytet. Insatsområdet kan vara strängt avgränsat, eller relativt öppet.

Utgångspunkten är i alla händelser att information som tillhandahålls av någon part ska vara av värde för annan part. Det värde en part kan tillskriva informationen kan vara ett värde delat med andra parter. Tillgång till mer värdefull information ger upphov till bättre beslut, vilket leder till mer värdefulla effekter.

2.6. Stödja sammansatta målbilder

En typ av koalition är den som har ett gemensamt yttersta mål, vilket uppnås genom gemensamma och samordnade ansträngningar av parterna. En annan typ av koalition är den där enskilda parter har egna mål, där varje part strävar mot sitt eget mål, men där andra parter kan ge understöd, t.ex. genom informationsförsörjning. Drivkraften för denna andra typ av koalition är att den på lång sikt optimerar total kvalitet och kostnadseffektivitet.

2.7. Utformning baserad på mål för informationsinfrastruktur

De drivkrafter och mål som kort beskrivits ovan fångar upp – direkt eller indirekt – några av de viktigaste övergripande målen med en informationsinfrastruktur. De har påverkat utformningen av den grundläggande modellen för infrastrukturen, en modell som kort karaktäriseras nedan.

3. Modellbaserad infrastruktur

En informationsinfrastruktur skall vara anpassbar på ett flertal sätt. Ett exempel är när nya deltagare ansluter sig till informationsinfrastrukturen för att samverka med andra; då behöver man typiskt genomföra visst anpassningsarbete. Nya deltagare måste kunna utnyttja sin egen informationsplattform för intern användning, samtidigt som det skall vara möjligt att på ett smidigt sätt samverka med andra deltagare i informationsinfrastrukturen. Detta uppnås genom att bygga in frihetsgrader i informationsinfrastrukturen så att vissa av de anpassningsbehov som nya deltagare konfronteras av, kan stödjas av mer automatiska medel inom infrastrukturen.

En annan anpassning är den som sker över tiden; hur infrastrukturen och deltagande parter förändras över längre tidsperioder. Sådana förändringar kan vara effekter av teknologiutvecklingen i området, av verksamhetsutveckling hos enskilda parter, och liknande. Det är önskvärt att förändringar i någon del av infrastrukturen eller inom domänen för någon av deltagarna görs så lokal som möjligt – de flesta typer av förändringar skall inte drabba *alla* deltagare i informationsinfrastrukturen.

För att underlätta anpassning definieras informationsinfrastrukturen på ett modellbaserat sätt. Hela förändringshanteringen underlättas genom att modellera kritiska delar av av informationshanteringen, verksamhetsprocesser och organisation, liksom av att modellera infrastrukturen själv och de gränssnitt som deltagare har mot infrastrukturen.

I resten av detta avsnitt beskrivs nyckelbegrepp som har en tydlig koppling till verksamhetsnivån, och som dessutom ger en grundval för att bygga stödjande mekanismer i informationsinfrastrukturen.

I avsnittet ges också en bild av vad informationssamverkan är, vilket förtydligar *vilka* samverkansmönster som informationsinfrastrukturen kan stödja, och *hur* de kan stödjas.

3.1. Informationsförsörjning

Informationsförsörjning innebär att information görs tillgänglig på den plats och vid den tid då informationen behöver användas. Typiskt innebär detta att information som registrerats på en plats görs tillgänglig på en annan plats där den senare kommer till användning.

Att få informationen att överbrygga tid och rum innebär ett behov av informationslagring och -överföring.

Det finns två huvudprinciper för informationsförsörjning. Den första kallas *prenumeration* och tillgodoser en allmän önskan om att bli fortlöpande informerad. Här har konsumenten ett stående behov av att förses med viss typ av information. Den andra principen bygger på att behovet av information uttrycks som en *förfrågan* på initiativ av konsumenten, som kan vara riktad till en specifik producent.

Konsumenter av information, har ofta en uppfattning om vilken eller vilka förmedlare av information som kan kontaktas. Konsumenten behöver då inte på förhand veta vem som ytterst är producent av den efterfrågade informationen. Skillnaden mellan en förmedlare (mäklare) och en konkret producent behöver ur mottagarens synpunkt inte vara tydlig.

3.2. Parter

Informationsutbyte sker mellan parter. Dessa parter kan vara del av samma organisation (juridiska person), eller tillhöra olika organisationer.

I det typiska fallet är parter autonoma. Det betyder bl.a. att de former av samarbete som måste stödjas är variationer av jämbördigt samarbete, men även samarbete där någon part definitionsmässigt har en priviligierad roll.

Autonomitet innebär dessutom att verksamhetsformer, processer, organisation och information kan skilja sig drastiskt mellan olika parter. Denna heterogenitet innebär en utmaning för ett ramverk som skall stödja smidig samverkan, eftersom skillnaderna måste överbryggas på trovärdigt och hanterbart sätt.

3.3. Systemsamverkan

I en typisk samverkan (koalition) uppträder parterna i olika roller. Rollen definierar vilken typ av bidrag en part levererar till samverkanskonstellationen.

Inom en koalition kan t.ex. vissa parter vara rena producenter av information. Deras engagemang i koalitionen inskränker sig till att leverera information.

Parterna har sina befogenheter och skyldigheter. En parts agerande inom ramen för samverkan måste överensstämma med de regelverk som reglerar partens verksamhet. Eftersom samverkan innebär att en part gör sig beroende av andra parter (åtminstone i termer av att basera beslut på information som andra kan ha tillhandahållit), så behöver en part säkerställa att samverkan med andra parter uppfyller vissa krav. Genom att ingå ett sådant avtal har de formellt förbundit sig inom koalitionen och tydliggjort vilka rättigheter och skyldigheter som olika parter har i samverkan inom koalitionen. Ett sådant avtal skapar en grund för att den påverkan som parterna ömsesidigt utövar på varandra skall vara acceptabla.

Ett avtal fyller olika funktion i olika delar av livscykeln hos en koalition. Initialt kan koalitionen ta styrning genom att bestämma vilka roller, skyldigheter och rättigheter som olika parter skall ha i den tilltänkta koalitionen. I designskedet dimensioneras processer, resurser och organisationer enligt avtal. Vid genomförandet av koalitionsarbetet utgör avtalet ett underlag för särskilda beslut, så att de beslut som tas är konsistenta med avtalet.

3.4. Användare och identitet

Användare är människor[1] som tar del av information, skapar information och fattar beslut. När dessa användare deltar i samverkan uppträder de som identifierade parter. Identiteter utdelas och administreras inom den administrativa domän (t.ex. företag, myndighet) som användarna tillhör.

Identiteter skall ha mening över administrativa gränser för att användare skall kunna hanteras på ett unikt sätt. Detta krav stöds av de modeller och metoder som underbygger *federerad identitetshantering* (samverkan mellan separat administrerade identitetssystem*)*. Dvs varje part administrerar sina identiteter, men identiteterna har ändå mening i andra parters behörighetskontrollsystem.

Identitetsbegreppet inom IT-området hanteras typiskt i termer av digitala identiteter. När en användare begär information kan det av spårbarhetsskäl eller behörighetsskäl vara viktigt att fastställa vem det är som begär information. Här fyller den digitala identiteten en nyckelroll.

[1] Förutom människor kommer även tekniska artefakter (system, apparater, etc) att utrustas med identiteter.

3.5. Roll-orientering

Såväl av hanterbarhetsskäl (administration av identiteter, rättigheter, skyldigheter, etc.) som av tekniska skäl har begreppet *roll* en viktig funktion i modellering av verksamheter. Detta begrepp fångar upp en allmän karaktärisering av vad som förutsätts av en viss typ av användare.

Till en roll associeras sådant som rättigheter och skyldigheter. Användare som agerar i en verksamhet associeras till de egenskaper som definierar den roll de uppträder i. Detta underlättar administration av rättigheter och skyldigheter, eftersom dessa specificeras oberoende av de individer som kommer att uppträda i denna roll.

Eftersom rättigheter och skyldigheter definieras för roller, så måste en användare kopplas till den roll han vill och får verka i, för att få en möjlighet att genomföra någon verksamhet och därmed åstadkomma effekt. Analogt med administration av identiteter, så skall roller förvaltas i kvalitetssäkrade processer.

3.6. Rättigheter och skyldigheter

Rättigheter och skyldigheter i samverkansperspektivet utgör en särskild infallsvinkel:

- Rättigheter: Vad kan en part kräva av andra? För att samverkan inom koalitionen skall ge de förväntade effekterna, behöver parter få olika typer av stöd från andra parter.
- Skyldigheter: Vad ska en part erbjuda andra parter? Om en part förväntar sig stöd från en annan part, så bör det vara tydligt vad denna förväntan innebär.

Rättigheter och skyldigheter kompletterar varandra och är inte bara två sidor av samma mynt.

I ett informationssamverkansperspektiv fokuseras rättigheter och skyldigheter på informationsutbytet över administrativa gränser. Genom att konfigurera rättigheter och skyldigheter på visst sätt kan man uppnå önskad grad av tillit till att information hanteras på ett ”säkert” sätt.

Rättigheter och skyldigheter skall knytas till roller, och inte till användare. Roller karaktäriserar vad som krävs i (och av) rollen, och ut-

gående från sådan karaktärisering är det lämpligt att fastställa stabila rättigheter och skyldigheter.

3.7. Modellbaserat informationsutbyte

All information skapas, insamlas och representeras av någon enskild aktör. Den informationen kommer att struktureras på ett sätt som är meningsfullt för aktören ifråga – informationen struktureras för att primärt stödja aktörens egna behov.

Eftersom likartad information kan insamlas av olika aktörer som har olika behov, så kan vi förvänta oss att likartad information trots allt kan bli olika strukturerad.

Exempel: En fiskare och en bonde beskriver samma väder på olika sätt, i termer som kan vara optimalt anpassade till de speciella förhållanden som reglerar deras verksamhetsområden.

Men det som är lokalt optimerat, det kan vara globalt suboptimerat. När man skall kommunicera och interagera med gemensam information som grund, då blir det ett problem att olika parter har olika modeller av samma typ av information.

Exempel: Fiskaren och bonden i exemplet ovan har var sin lokalt optimerad begreppsmodell och motsvarande språkbruk. Men om de i samarbete skall utföra t.ex. en transport av boskap genom innerskärgården, så kan genomförandet av deras gemensamma uppgift hämmas av att de inte har ett gemensamt språk (en gemensam begreppsmodell) .

Detta är, inom ramen för en informationsinfrastruktur, en praktisk utmaning. För en konsument med behov av viss typ av information kan det finnas flera möjliga leverantörer som kan tillhandahålla relevant information, men på olika format. Om konsumenten skall kunna dra nytta av att det finns flera leverantörer, då måste informationen – dess struktur – anpassas från leverantörens format till konsumentens format. Det är först då som konsumenten kan mata in och direkt använda informationen i de egna arbets- och processflödena.

Det praktiska problemet att transformera information behöver en principiell ansats, för att det skall kunna hanteras på ett rationellt sätt. En ansats är att basera transformationerna på definierade *informationsutbytesmodeller* – informationsmodeller som utnämns till

auktoriserade modeller av respektive typ av information. En leverantör kan nu implementera en transformation från sitt interna format till utbytesformatet, en konsument implementerar en transformation från utbytesformatet till sitt interna format. Sedan kan godtycklig konsument ta emot denna typ av information från godtycklig leverantör. Detta är ett sätt att betvinga den kombinatoriska explosionen som annars skulle bli en effekt av att fler konsumenter och producenter går med i samverkan.

Exempel: Nyhetskanaler på webben utnyttjar det s.k. RSS-formatet. Detta format är i praktiken en utbytesmodell, eftersom den modellerar informationsstrukturen hos det innehåll som tillhandahålls av leverantören av nyhetsdata.

Användning av utbytesmodeller minskar komplexiteten i själva utbytet mellan parter i en samverkan. Det ställer dock krav på såväl leverantörer som konsumenter att de kan producera och leverera, respektive hämta och tolka, information enligt utbytesmodellen. Som tidigare påpekats är ett starkt krav att informationsinfrastrukturen i så liten grad som möjligt skall begränsa hur en part sköter informationshanteringen inom sin domän. Det betyder att de informationsmodeller som används internt inom en part kan skilja sig från de gemensamma informationsutbytesmodellerna – modeller av informationen när den hanteras internt kan vara bestämda av de affärssystem som används.

Transformationsmodeller överbryggar skillnaden mellan interna informationsmodeller och externa utbytesmodeller. De stöder systematisk transformation av konkret information – information som förekommer enligt ett format översätts till ett annat format. Modeller för transformering underlättar hantering av förändringar i informationsplattformar, genom att information automatiskt kan översättas mellan olika informationsformat. En förändring i hur en part vill betrakta information – t.ex. då en part vill ha viss informationssammanställning istället för en uppsättning enkla grunddata – kan därmed stödjas genom att konstruera en modell som uttrycker transformationen från en modell till en annan.

Exempel: Även om nyhetsinformation kan erhållas enligt RSS-formatet så kan det vara praktiskt för en viss mottagare att få informationen strukturerad som HTML, t.ex. för presentation i en webblä-

sare. Med en informationstranformationsmodell kan man definiera hur RSS-formatet kan översättas till HTML.

Utbytesmodeller och transformationsmodeller bidrar till automatisering av kritiska delar av informationshanteringen. Utbytesmodeller används bl.a. för att upptäcka vilka informationskällor som kan kommas åt via informationsinfrastrukturen, samt att utvärdera egenskaper hos denna information (kvalitet, aktualitet etc.), och detta ger en grund för att organisera väldefinierat informationsutbyte mellan parter. Transformationsmodeller kan användas av automatiserade funktionaliteter för transformering, vilket minimerar arbetet med att anpassa de specifika system som är inkopplade i informationsinfrastrukturen.

4. Slutsatser

Informationsinfrastrukturen är en nyckelkomponent i STIL-ramverket. Infrastrukturens arkitekturmodell har strukturerats på ett sätt som dels tydliggör vilka verksamhetsegenskaper och –krav som kan stödjas av infrastrukturen, dels gör det möjligt att bygga mekanismer som underlättar praktisk anpassning till och användning av infrastrukturen.

I detta avsnitt beskrevs några av de nyckelbegrepp som karaktäriserar STIL:s informationsinfrastruktur och som knyter an till hur en organisations verksamhet organiseras, styrs och uppfattas. Varje sådant begrepp har egenskaper och relationer till andra begrepp, och sådana strukturer kan fångas som modeller. Vi har därför en uppsättning modeller – var och en fokuserad på sitt område – som dels kan användas för att dokumentera perspektiv på en organisations deltagande i en samverkan, dels används som parametrar i infrastrukturen själv.

Lyckad samverkan bygger på delad förståelse för STIL:s informationsinfrastruktur och dess nyckelbegrepp. Vid informationssamverkan kommer också en satsning på att ta fram faktiska avtal, informationsutbytesmodeller och andra modeller att avgöra framgången i samverkan. Med en strävan för en gemensam informationsinfrastruktur kan smidig samverkan, med delad förståelse, ge mervärde för alla inblandade parter t ex i form av gemensam information till högre kvalitet och bättre kostnadseffektivitet.

Grund för tjänstesamverkan

Sammanfattning

För att åstadkomma bästa möjliga flexibilitet för framtiden behövs det en grund av regler, metoder och teknik vid tjänstesamverkan. De samverkande aktörerna behöver bland annat dels kunna förstå beskrivningar av tjänster och dels på ett ordnat sätt få tillgång till de tjänster som är intressanta. Benämningen tjänstedepå rymmer de förmågor som krävs för att ge förutsättningar för tjänstesamverkan. Den gemensamma grunden möjliggör att aktörer på lika villkor och med bibehållen integritet både kan producera och konsumera tjänster som underlättar och effektiviserar såväl egen som gemensam verksamhet.

1. Inledning

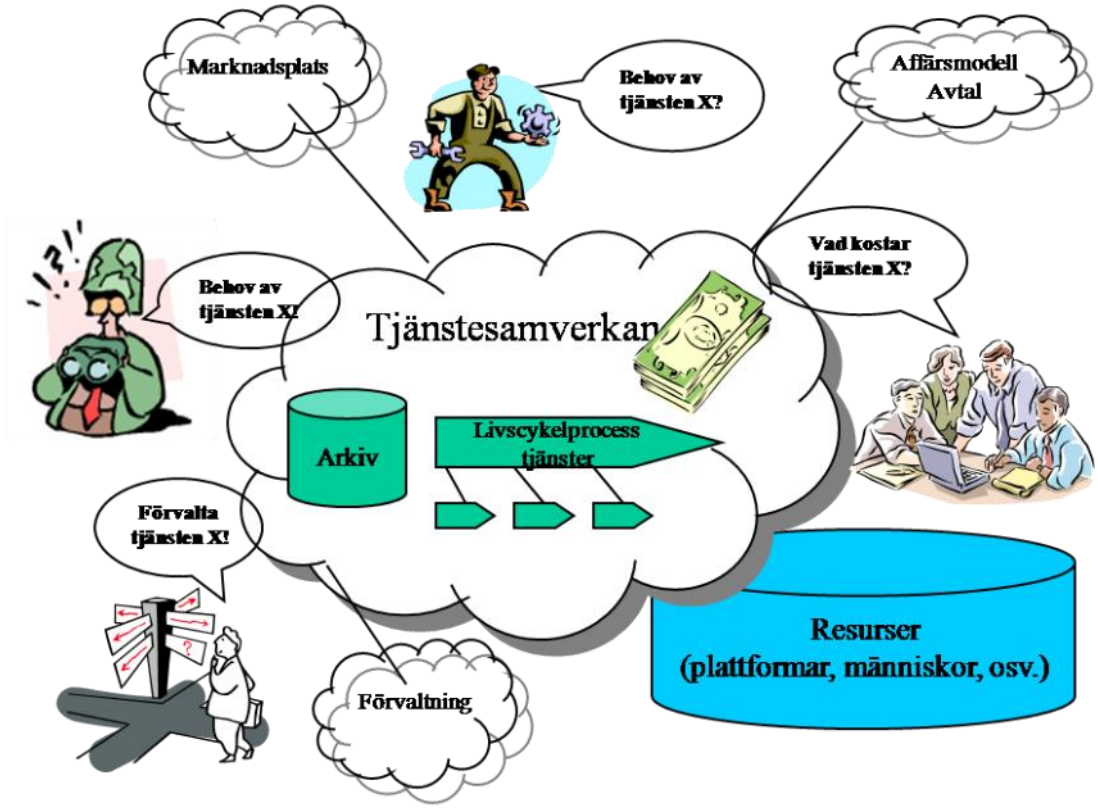
Samverkan mellan aktörer kan underlättas väsentligt genom att utnyttja tjänster för att utbyta information som är av gemensamt intresse. För att åstadkomma bästa möjliga flexibilitet för framtiden behövs det en grund av regler, metoder och teknik vid tjänstesamverkan. De samverkande aktörerna behöver bland annat dels kunna förstå beskrivningar av tjänster och dels på ett ordnat sätt få tillgång till de tjänster som är intressanta. Den gemensamma grunden möjliggör att aktörer på lika villkor och med bibehållen integritet både kan producera och konsumera tjänster som underlättar och effektiviserar såväl egen som gemensam verksamhet.

1.1. Regler, metoder och teknik stödjer grunden

De aktörer som vill samverka kan lyckas allra bäst om de etablerar tillgängliga regler, metoder och teknik som stödjer detta. Vi använder samlingsnamnet ”grund för tjänstesamverkan” för att beskriva detta. I synnerhet omfattar det ett antal modeller, regler och processer. Dessa samverkansregler kan t ex omfatta kvalitets-, informations- säkerhets - och tillgänglighetsfrågor. Överenskommelser underlättar självklart samverkan och sådana kan upprättas såväl bilateralt mellan två parter som i större samverkansorgan, t ex även som standardisering. En grund för tjänstesamverkan stödjer kontinuitet och stabilitet över tiden, med flera samverkande aktörer. Syftet är att bli mer effektiv och ha bäddat för flexibiliteten att på kort varsel utnyttja gemensamma resurser. Andra frågor regleras inte av denna grund, t ex finns stor frihet för producenter av tjänster att använda olika lösningar för att realisera en tjänst.

1.2. En marknadsplats för tjänster

Grunden för tjänstesamverkan ligger i såväl konsumenters som producenter intresse. Med grunden till stöd bör man upprätta en marknadsplats för tjänster, en ”tjänstedepå”, där tjänsteutbudet definieras med listor av tjänster ihop med beskrivningar av dessa. Beskrivningar innehåller information om tjänsterna, s k metainformation. Utifrån stöd av process- och regelverket får bara tjänster som uppfyller vissa kriterier presenteras i ”tjänstedepån”. Detta utgör en kvalitetssäkring för tjänstedepån. I tillägg till det bevakas möjligheter till att inte iden-



Figur 1 ”Tjänstedepån” ger förutsättningar för tjänstesamverkan genom att verka som en marknadsplats för tjänster där producenter möter konsumenter. Här kommer diverse processer, modeller och stödjande regler in för en framgångsrik förvaltning och kvalitet i utbudet. Avtal måste möjliggöras och affärsmodeller formuleras. Genom samverkansorgan beslutas om utformning för bästa användning av ”tjänstedepån” på samverkansarenan samt livscykelhantering för tjänster.

tiska tjänster tas fram på nytt, utan istället återanvändning sker på smidigast möjliga vis.

2. Processer, regler och modeller för tjänstesamverkan

För att kunna använda tjänstesamverkan på ett framgångsrikt sätt behövs det ett antal processer, regler och modeller:

- Begreppsmodeller

  Begreppsmodeller används för att de samverkande parterna skall kunna förstå varandra på ett bra sätt. En begreppsmodell innehåller begrepp och termer som kan användas vid beskrivningar av tjänster.

- Informationsutbytesmodell

  En informationsutbytesmodell definierar informationsobjekt som används dels till att definiera informationsutbytet vid tjänstesamverkan och dels till att definiera metainformation om tjänsterna.

- Gemensamma design- och strukturprinciper

  För att tjänstedefinitioner skall kunna kombineras till fungerande system krävs gemensamma design- och strukturprinciper för tjänsters gränssnitt. Dessa ska redogöra för kompatibilitet och flexibilitet genom t ex arkitektur, tjänsteegenskaper och gränssnittsprinciper. Detta hindrar inte olika realiseringar av tjänster, men förtydligar hur de kan kombineras. Kapitlet *Tjänsternas metainformation* visar på vissa typiska egenskaper för tjänster.

- Sökmetoder och verktyg

  För att tjänstedepåns användare skall kunna söka och finna tjänster i tjänstedepån krävs ändamålsenliga sökmetoder och verktyg, t ex sökmotorer.

- Affärsmodell

  Affärsmodellen skall standardisera de affärsmässiga processerna som krävs för att få använda de tekniskt körbara varianterna av tjänsterna, tjänsteinstanser som utgår från tjänsteimplementationer som depån refererar till (se .(1.3Affärsmodellen måste innehålla avtal och kontrakt, betalning och licenser mm.

- Kvalitetsprocess/kvalitetsnormer

  Tjänstedepåns användare måste kunna känna förtroende för de tjänster som beskrivs där. Det behövs en kvalitetsprocess inklusive regelverk för konfigurationshantering och ändringshantering för att standardisera, versionshantera och kvalitetssäkra beskrivningarna i tjänstedepån. Detta beskrivs senare i detta kapitel.

- Processer för ackreditering

  Tjänsteinstanser som tillhandahålls via tjänstedepån skall vara kvalitetsmärkta ur säkerhetssynpunkt. Det måste finnas processer som definierar hur instanser skall ackrediteras, d v s verifieras och valideras ur säkerhetssynpunkt.

- Modell eller standard för konfigurationshantering (CM) och förvaltning.

  Tjänster i tjänstedepån måste livscykelhanteras enligt en väldokumenterad metod, eller på ett standardiserat sätt. Livscykeln omfattar faser från Identifiering och Formell definition över Användning till Avveckling. (Se vidare i kapitlet Tjänsternas Metainformation). I detta ingår versionshantering av information runt tjänsten under livscykeln (konfigurationshantering).

- Registrering

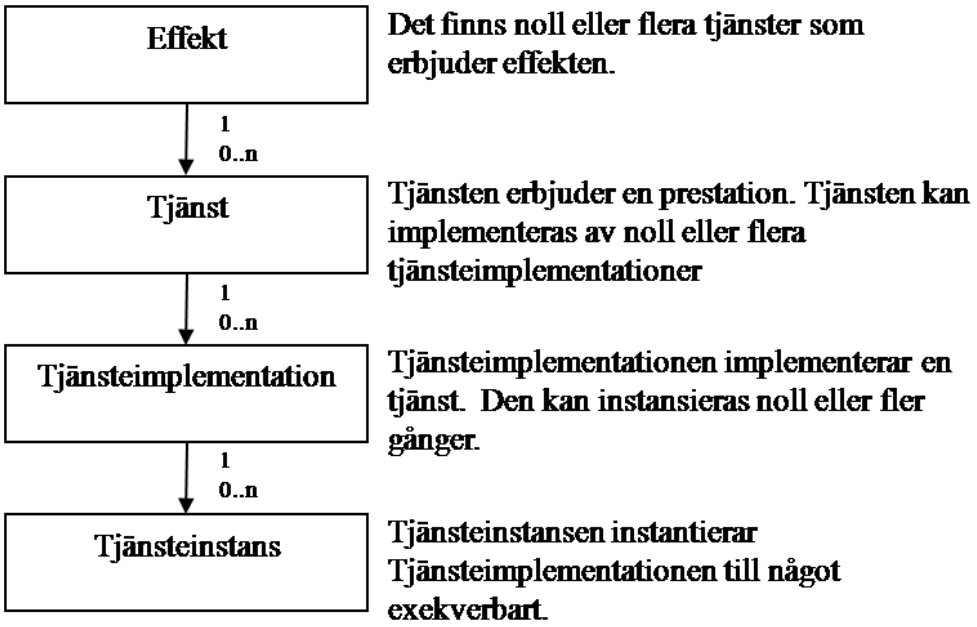
  För att tillhandahålla relevant och aktuell information till intressenter är det viktigt med en form av registrering av såväl producenter av tjänster som konsumenter av tjänster. Tjänsteproducenter måste publicera sina kontaktdata, samt ansvara för uppdateringen av dessa uppgifter.

- Gemensamma tjänster

  Utöver överenskommelser och standardisering av modeller, regler och processer kring tjänstesamverkan finns ett egenvärde att hålla ihop tjänsteutbudet så gemensamt och standardiserat som möjligt.

3. Tjänsterelaterade begrepp

De tjänsterelaterade begrepp som används i detta kapitel förtydligas genom relationerna mellan de olika begreppen i figur 2 nedan.



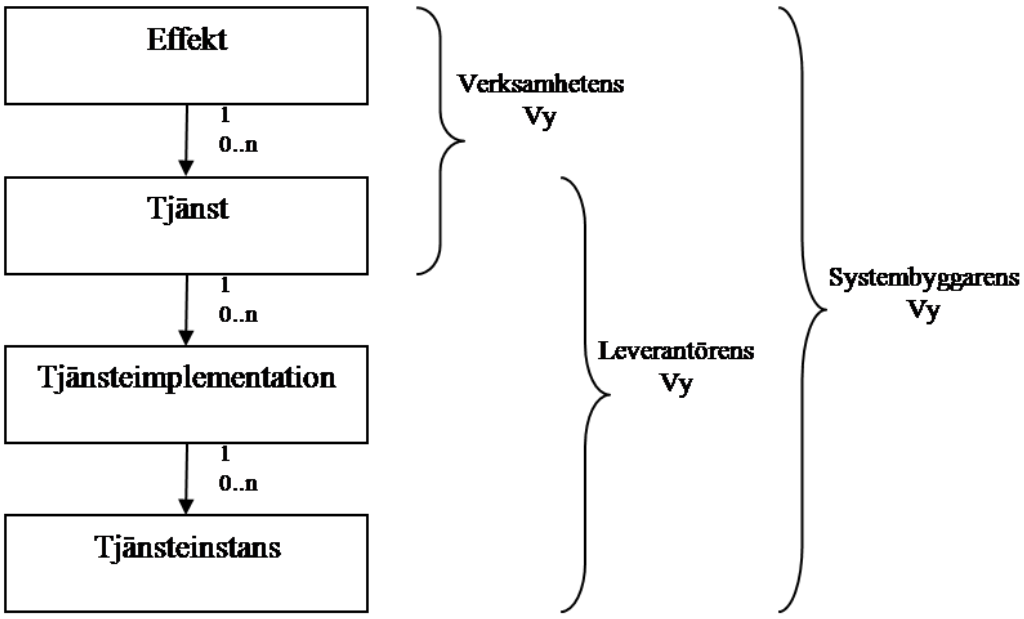
Figur 2 Relation mellan tjänstebegrepp

Något förenklat kan man visa på olika behov av de olika tjänstebegreppen för olika roller. Personal ur verksamheten söker efter tjänster som genererar de effekter som behövs för att lösa verksamhetsuppgifterna medan leverantören söker efter tjänster som kan implementeras och eventuellt instansieras. Därför behöver tjänstedepån möte olika intressegrupper och olika rollers behov.

Ovanstående resonemang illustreras i följande figur. 3.

4. Tjänstedepån

Tjänstedepån skall fungera som en marknadsplats för tjänster, där konsumenter kan söka efter effekter som de har behov av för att lösa sina uppgifter. Tjänstedepån kommer att tillhandahålla referenser till kända, ackrediterade implementationer och instanser av tjänster. Villkoren för att kunna använda dessa tjänster kommer att skilja sig åt, dels behörighetsmässigt, men också affärsmässigt. Dessa villkor más-



Figur 3 Användarnas behovsstyrda vyer av tjänstedepån

te standardiseras och beskrivas i tjänstedepåns anknutna modeller, t ex informationsutbytes- respektive affärsmodell.

Beskrivningar av nya tjänster (nya behov) kommer också att finnas i tjänstedepån. Även dessa kommer att göras tillgängliga på marknadsplatsen för behöriga användare. Med tjänstebeskrivningar kan leverantörer erbjuda nya tjänsteimplementationer av olika kvalitet. Olika leverantörer kan erbjuda samma tjänst med eventuellt olika egenskaper (pris, ser längre, ser mer noggrant etc.).

Ett exempel på hur tjänstedepån kan användas är när ett system ska konstrueras. Vid konstruktion av t ex ett system för samverkan, eller samverkansledning behövs bl.a. geografiskt data för att kunna skapa lägespresentationer med kartbakgrund. När verksamheten har identifierat ett entydigt behov startas en sökning i tjänstedepån efter lämplig tjänst för att tillgodose behovet. Resultatet av sökningen blir en lista på beskrivningar av möjliga tjänster som matchar sökkriteriet. Ur resultatet väljs en lämplig tjänst och sedan är det möjligt att välja leverantör av den valda tjänsten baserat på önskade egenskaper. Det är möjligt att det krävs en kombination av flera tjänster för att tillgodose behovet, till exempel en tjänst för lägesinformation och en för kartbakgrund.

Systembyggaren i exemplet ovan väljer den tjänst som på bästa sätt löser den aktuella uppgiften. För att göra detta krävs tillgång till de egenskaper som beskriver de tjänster han/hon kan välja mellan. Valet av tjänst baseras på hur samverkan med producenten sker och vilka egenskaper som tjänsten erbjuder. En egenskap kan vara vilket format som positionen i lägespresentationen beskrivs med (till exempel RT90 eller WGS84). Nästa steg är att finna den eller de resurser som erbjuder en tjänst som genererar önskad effekt. I detta exempel kan det innebära att insatsstyrkan måste bära en viss typ av GPS-utrustning som levererar tjänsten. Det sista steget innebär att tjänsten instansieras.

I exemplet ovan beskrivs hur tjänstedepån används när ett system konstrueras för att lösa en planerad verksamhetsuppgift med befintliga eller nyutvecklade resurser, vilket motsvarar traditionell systemutveckling. System kan även anpassas/konstrueras för situationer som inte är förutsägbara, vilket kallas situationsanpassad utveckling.

5. Förvaltning

5.1. Livscykelhantering av tjänstedepån

Tjänstedepån måste livscykelhanteras på ett standardiserat sätt. Vald standard skall användas för att driva utveckling, vidmakthållande samt avveckling av tjänstedepån. Det är i första hand inte de implementerade eller instansierade tjänsterna som skall hanteras enligt standarden utan själva informationen om dem och beskrivningarna i depån. Hur implementerade eller instansierade tjänster förvaltas ansvarar leverantörerna för utifrån de krav som ställs på dessa.

5.2. Förvaltning av tjänster

I ansvaret att förvalta tjänstedepån ingår förvaltning av samtliga beskrivningar av tjänster som återfinns där. I förvaltningsansvaret ingår även att se till att implementerade och instansierade tjänster beskrivs på ett standardiserat sätt. Samtliga delar i begreppsstrukturen skall alltså förvaltas, vilket innebär att det behövs processer för att standardisera, versionshantera och kvalitetssäkra beskrivningarna av allt från effekt till instans. En sådan huvudprocess är formell ändringshantering.

5.3. Formell ändringshantering

Kvalitetsnivån hos tjänstedepån skall hållas uppe med en ordnad, formell ändringshantering. Ett ändringshanteringsråd, s k CCB (Change Control Board) instiftas som beslutande organ för vilka tjänster som skall läggas till utbudet i tjänstedepån, vidareutvecklas respektive avvecklas. Dessutom beslutas i rådet om tjänsternas metainformation, t ex beskrivningar och andra egenskaper. Rådets medlemmar bör representera såväl förvaltningsansvarig för tjänstedepån, som konsument (gärna även slutanvändare) och producent.

Tjänsterna i tjänstedepån blir ”certifierade” genom detta formella förfarande och en kvalitetsgaranti följer därmed med tjänsterna som publiceras där. CCB har dock ingen beslutsrätt över affärsmodellerna i tjänstedepån.

6. Kvalitet och spårbarhet

I ansvaret för tjänstedepån ingår att ansvara för kvaliteten på all information depån innehåller, dvs. att beskrivning av effekt och tjänst för samtliga tjänster är korrekta och följer givna mallar. Däremot skall man inte ansvara för kvaliteten på den effekt som erhålls från implementationer och instanser av tjänster. De refererade instansierade tjänsterna skall dessutom vara verifierade och validerade.

I kvalitetsansvaret ingår även ansvar för att all information som tjänstedepån innehåller är spårbar, dvs. att beskrivningarna av effekt och tjänst versionshanteras och dokumenteras så att spårbarhet garanteras.

Ovanstående berör kvalitet på information. När det gäller kvalitet på tjänster blir resonemanget än mer komplicerat. Först och främst gäller det att definiera vad kvalitet innebär i detta fall. Tjänstekvaliteten består av flera olika mått som tillsammans ger en uppfattning om hur bra en implementation eller instans är. Ett mått kan vara hur väl en tjänsteimplementation följer beskrivningen av tjänsten. Ytterligare en egenskap kan vara förmågan hos en tjänsteinstans att leverera utlovad effekt.

När man har definierat ett entydigt kvalitetsbegrepp krävs sedan riktlinjer för hur man applicerar det på olika typer av tjänster. Hur mäter man till exempel kvaliteten på en tjänst som använder sig av andra

tjänsteimplementationer eller tjänsteinstanser i sin realisering? Det krävs alltså vidare arbete även inom detta område.

I överenskommelserna som sätts upp för framgångsrik samverkan är det centralt med regler för säkerhet[1].

[1] I kapitlet **Säkerhet** i Del 1 definieras en arkitektur för informationssäkerhet vid tjänstesamverkan

Tjänsternas metainformation

Sammanfattning

För att hantera tjänster och tjänsterealiseringar under hela deras livscykel behöver man samla in, spara och sprida information av olika slag. I detta dokument beskrivs vilken information som är aktuell, syftet med att spara informationen, var informationen kan lagras, varifrån informationen kommer samt ibland också vilket eller vilka format som kan/bör/skall användas. För olika slags information ges också exempel på hur den kan användas i olika processer.

De tjänster som i huvudsak betraktas är informationstjänster som realiseras med olika slags datoriserade informationssystem.

1. Inledning

Behovet av information om tjänster, tjänsterealiseringar och tjänsteinstanser kan betraktas utifrån deras livscykel. Tjänsterna identifieras, definieras och dokumenteras som ett sätt att översiktligt strukturera ett system av system. Strukturen, i termer av vilka tjänster som finns i systemet, definierar både vad systemet kan utföra samt ger en övergripande bild av vilken flexibilitet som finns i systemet.

De tjänster som i första hand betraktas i detta avsnitt är informationstjänster som realiseras med olika slags datoriserade informationssystem.

Tjänstedokumentationen används när tjänsterna realiseras i form av producenter och konsumenter av tjänsten. Tjänsterna realiseras i ett första steg genom olika former av mjukvara. Denna mjukvara exekveras sedan, i ett andra steg, på ett eller flera ställen på hårdvara av olika slag för att generera de exekverande processer som utgör de egentliga producenterna och konsumenterna av tjänster. Hårdvaran finns placerad på olika former av plattformar.

Detta dokument syftar till att beskriva den information som behövs om tjänster, tjänsterealiseringar och tjänsteinstanser i olika sammanhang och för olika syften. För att konkretisera information ges också exempel på hur denna information kan uttryckas i (halv)formella beskrivningar.

Om man vill uttrycka sig helt korrekt så består information av data tillsammans med en tolkning (interpretation). När man slarvigt uttrycker att man sparar information betyder det oftast att man bara sparar de data som representerar informationen och anser att tolkningen är universell och inte behöver sparas.

2. Sammanhang

Informationen om en tjänst har ett sammanhang där den beskrivs. Sammanhanget utgörs av de gemensamma processer, definitioner etc. som berör informationen för av alla tjänster som hanteras inom en viss verksamhet. Inom denna verksamhet behövs en samordning så att de för organisationen gemensamma arbetsuppgifterna löses på ett gemensamt sätt. Exempel på gemensamma uppgifter inom organisationen kan vara att skapa standards för hur beskrivningar av olika

slag skall se ut, bestämma var information av olika slag skall lagras samt andra beslut som berör tjänsterna i stort.

Inom STIL hanteras många av dessa frågor inom ramen för det som kallas tjänstedepå eller tjänstetorg (beskrivs i dokumentet: **Grund för tjänstesamverkan i Del 2**). Ett annat STIL dokument som avhandlar relaterade frågor är **Informationssamordning för myndighetssamverkan**.

3. Tjänster

I ett initialt skede identifieras behovet av en tjänst, eller tjänstetyp som man ibland säger, och en första skiss av tjänsten tas fram. Detta sker oftast i en första specifikation av ett system eller ett system av system. I detta skede definieras tjänsten i termer av den informationsöverföring och de protokoll och gränssnitttsdefintioner som tillsammans utgör tjänsten. I tjänsten behöver man också uttrycka namnet på de egenskaper som skall kunna användas för att skilja på olika tjänsterealiseringar. Att detta är nödvändigt inses av att t.ex. många olika sensorer kan producera en och samma lägestjänst men i en viss situation är det viktigt att kunna välja den sensor som ser rätt objekt och har rätt täckningsområde.

Ett stort problemområde är att det inte finns någon allmänt accepterad och kommunicerad definition på vad en tjänst är och framförallt vad som skiljer två olika tjänster. Vad krävs för att två tjänster skall anses vara lika? Att de producerar samma effekt? Att de använder samma gränssnitt? Att de använder samma protokoll för informationsöverföring?

I detta avsnitt definierar vi en tjänst som semantiken av de gränssnitt som tjänsten innehåller. Två tjänster är lika om de kan simulera varandra med hjälp av en enkel översättning av gränssnitten.

3.1. Tjänsters livscykel

En tjänst livscykel består av följande faser:

- *Identifiering*, som består i att någon bestämmer ett namn (identifikation) av tjänsten samt producerar någon form av övergripande informell definition av tjänsten. I en given organisation finns det antagligen någon utpekad ansvarig för detta. En frågeställning som

uppkommer här är om en ny tjänst skall identifieras eller om behovet kan lösas av redan identifierade tjänster, eventuellt efter att dessa har modifierats.

- *Formell definition*, består av att ett antal beskrivningselement, som introduceras mer utförligt längre fram i detta avsnitt, definieras och dokumenteras på ett formellt sätt.

- *Användning*. Beskrivningen av en tjänst behöver användas när en producent eller konsument av tjänsten skall implementeras. Tjänsten utgör en del av kravspecifikationen för den som skall implementera en producent av tjänsten. När en konsument av tjänsten skall implementeras används tjänstedefinitionen som ett kontrakt av vad som kan förväntas av producenten. Tjänsternas namn (eller annan identifiering) används också som ett strukturerings- och identifieringshjälpmedel vid konfigurering av situationsanpassade system, dvs. när producenter och konsumenter av samma tjänst kopplas samman med hjälp av ett SitSyst-verktyg.

  Även i andra sammanhang kan man också tänka sig att använda olika delar av tjänstedefinitionen för att söka efter olika slags information om tjänsten, t.ex. tjänstenamnet.

  Under användningen är det möjligt att modifiera och ändra den formella definitionen. Tjänstedefinitionen måste därför CM-hanteras vilket innebär att det samtidigt kan finnas flera olika versioner av en tjänstedefinition.

- *Avveckling*. När det inte finns, eller är tänkt att finnas, några konsumenter eller producenter för tjänsten kan den avvecklas.

3.2. Tjänsters metainformation

3.2.1. Definition av informationsöverföring

En viktig del av beskrivningen av en tjänst är att identifiera den informationsöverföring som behövs mellan en producent av tjänsten och en konsument av tjänsten. Två delar av denna informationsöverföring är av stort intresse:

1. Hur en konsument beställer (avropar, ...) tjänsten.

2. Hur tjänsten ”levereras”. För en del tjänster består effekten av tjänsten av att information levereras till beställaren. Den andra möjligheten är att något tillstånd ändras. Tillståndsändringen är då ”åtkomlig”, dvs. möjlig att upptäcka, både för konsumenten och producenten.

Det finns i dagsläget inget generellt, väldefinierat, formellt beskrivningsspråk för att uttrycka detta informationsutbyte så en enkel beskrivning i naturligt språk kan/bör användas.

Exempel 3.1: Informationsutbytet för en tjänst (eller del av tjänst) som ger ett antal fordons position kan uttryckas på följande sätt:

Konsument	→	Producent:	Information som beskriver identiteten av det eller de fordon vars position är av intresse.
Producent	→	Konsument:	Information som ger fordonens position tillsammans med tiden då positionen bestämdes.

För att standardisera hur man definierar, och kanske också hur man representerar den information som behöver utbytas, används en, för den aktuella organisationen, gemensam informationsutbytesmodell. Beroende på den omgivande organisationen kan denna informationsutbytesmodell definieras och hanteras på olika sätt. I detta avsnitt går vi inte närmare in på detta utan förutsätter att en sådan finns och hanteras inom organisationen.

Flera olika formalismer och språk har introducerats för att definiera olika typer av information och relationen mellan dessa. Exempel på sådana formalismer är Web Ontology Language (OWL) och Resource Description Framework (RDF) som används i Web 2.0 sammanhang. Det återstår att se om man genom att använda något av dessa formella språk för att definiera informationsobjekt kan förbättra beskrivningen av informationsutbytet.

3.2.2. Definition av effekt

För de tjänster vars resultat inte enbart beskrivs av informationsöverföringen mellan konsument och producent utan där effekten består av en (önskad) tillståndsförändring i något tillstånd måste både tillståndet och tillståndsförändringen beskrivas. Exempel på olika tillstånd som kan förändras är tillståndet i konsumenten själv, i någon databas som konsumenten använder eller helt enkelt, genom någon ansluten utrustning, i ”verkligheten”. Några exempel på operationer som ger

tillståndsförändringar är att en beställning skickas, en ventil öppnas, ett värmeelement slås på, eller att någon banktransaktion genomförs.

Om tjänsten har effekter av detta slag skall de definieras. För att beskriva detta formellt måste det finnas en formell beskrivning, t.ex. en formell modell, av det gemensamma tillståndet. Idag finns nästan inga sådana beskrivningar så tillståndsförändringen måste beskrivas i naturligt språk.

Exempel 3.2: Effekten av tjänsten (eller del av tjänsten) som skickar ett uppdrag att till en given polispatrull skulle kunna se ut på följande sätt:

```
Effekt:  Ett uppdrag skickas till den närmaste polispatrullen
         med avseende på händelsen. Uppdraget innehåller föl-
         jande information: ...
```

3.2.3. Protokoll och gränssnittsdefinition

Nästa steg i utvecklandet av en tjänst består av att bestämma hur information skall utväxlas mellan parterna. Detta innebär att man definierar hur olika sorters information skall representeras i form av data, vilka olika meddelanden (metoder) som skall finnas och vilken information (data) som dessa skall innehålla. Allt detta uttrycks i termer av de gränssnitt (interface) som behöver finnas hos konsument respektive producent för att realisera det tänkta informationsutbytet.

I detta sammanhang kan man urskilja två olika skolor. Den ena skolan använder paradigmen med funktioner/procedurer/metoder som en modell för informationsutbytet. Den andra skolan använder paradigmen med write/read/text operationer som modell.

Metodskolan definierar informationsutbytet i termer av gränssnitt medan textskolan hellre vill definiera informationsutbytet i termer av meddelanden. Det finns ingen egentlig skillnad i uttryckskraften i de två skolorna utan definitionssätten kan, åtminstone i princip, översättas till varandra. I realiteten kan väl sägas att metodskolan tar sina intryck främst från matematik medan textskolan mer använder språkliga associationer. I de flesta programspråk kan man använda båda men traditionen är att använda funktioner/procedurer/metoder för informationsutbyte mellan olika delar i ett program och textmetoden för att spara information i filsystemet när man måste linjärisera sina datastrukturer.

Tillsammans med gränssnitten finns också ett tänkt protokoll för informationsutbytet. Protokollet definierar de tillåtna och meningsfulla sekvenser av metodanrop/ meddelanden som finns mellan en konsument och en producent av tjänsten.

En uppsättning gränssnitt och ett protokoll realiserar tillsammans informationsutbytet i en tjänst.

Exempel 3.3: Ett exempel på hur man kan uttrycka representationen av informationen, gränssnitt och protokoll för den tjänst vars informationsutbyte definierades i Exempel 3.1

```
  Module VehiclePositions {
     Structure Position {
          Long lat;
          Long long;
          Long alt;
     }
     Structure Time {
          Longlong ms;
     }
     Structure VehIds {
          Long VehId
     }
     Type ListOfVehIds = Stream of VehId;
     Structure VehPos {
          VehId id;
          Position pos;
          Time t;
     }
     Interface VehiclePositionsProducer {
          ListOfVehIds getAllVehicles();
          VehPos getVehPos(VehId id)
   }
}
```

Motsvarande information kan uttryckas på många olika sätt och i många olika formalismer.

Exempel 3.4: Ett exempel på hur man kan uttrycka protokollet för informationsutbytet av tjänsten VehiclePositions med hjälp av gränssnittet VehiclePositionsProducer är att använda ett reguljärt uttryck. I detta exempel kan metoderna `getAllVehicles` och `getVehPos` anropas i godtycklig ordning.

```
   Protocol VehiclePositions {
     ( getAllVehicles | getVehPos )*
    }
```

3.2.4. Tjänsters egenskaper

Som en del av en tjänst ingår att introducera en uppsättning egenskaper som bland annat gör det möjligt för en konsument att, på ett förnuftigt sätt, särskilja bland de tillgängliga producenterna av tjänsten. Programmeringen av detta val måste ske när konsumenten utvecklas så namnen på egenskaperna måste finnas definierade i tjänsten. Någonstans behöver man också definiera vilka värden, t.ex. i form av strängar (texter), som man kan förvänta sig som egenskapsvärden.

Egenskaperna är emellertid mer generella än så och kan användas i alla sammanhang där man vill spara information om tjänster.

Genom att introducera egenskaper till en tjänst samt ett sätt att definiera och ”värdesätta” dessa har man en generell möjlighet att introducera och hantera metainformation för tjänsten av olika slag och för olika syften.

Exempel 3.5: En sensortjänst kan, till exempel innehålla följande egenskaper:

```
Properties VehiclePositions {
   String    ServiceType;
   String    ServiceId;

   String    HostMachine;
   String    CoverageArea;
   String    Position;
   String    SensorType;
}
```

En del av dessa egenskapers värden kommer inte från tjänstetypen utan från realiseringen av tjänsten eller tjänsteinstansen (se nedan).

Exakt vilka egenskaper som skall finnas för alla tjänster, för olika tjänstetyper, tjänsterealisringar och tjänsteinstanser måste bestäms av den omgivande organisationen. Denna måste också bestämma det tillåtna värdeförrådet för de olika egenskaperna.

4. Tjänsterealiseringar

Givet en definition av en tjänst så är det möjligt att implementera både producenter och konsumenter av tjänsten. Implementeringarna utgörs, i det sammanhang som detta avsnitt behandlar, av olika former av datorprogram.

En förutsättning för en tjänsterealisering är att den tjänst (tjänstetyp) som skall realiseras är identifierad och beskriven.

4.1. Tjänsterealiseringars livscykel

Tjänsterealiseringen har följande livscykel:

- *Design*. Under designen av tjänsterealiseringen behövs tjänstens beskrivning.
- *Implementering*. Implementeringen består i sig av flera olika faser. Först sker en strukturering där tjänsterealiseringen struktureras i olika delar där några av delarna kan utgöras av tjänsterealiseringar av andra tjänster. Det är viktigt att beskriva den tänkta tjänsterealiseringens struktur och vilka krav som finns på andra tjänster och deras realisering. Efter struktureringen sker en realisering av de delar som inte utgörs av tjänsterealiseringar av andra tjänster. Dessutom vill man i en tjänsteorienterad arkitektur att tjänstens ”affärslogik” och tjänstens ”kommunikationslogik” implementeras separat och oberoende av varandra.
- *Användning*. Den övergripande användningen av en tjänsterealisering är att starta den eller de exekverande processer som utgör de användbara tjänsteinstanserna i ett system. De krav som tjänsterealiseringen har på den exekverande och kommunicerande omgivningen i form av datorsystem och kommunikationssystem måste uttryckas i form av omgivningskrav.
- Avveckling.

4.2. Tjänsterealiseringars metainformation

Den information som behövs om tjänsterealiseringar är i första hand följande:

- Namn på (identifiering av) tjänsterealiseringen.
- Namn (identifiering, refererens) till den tjänst (tjänstetyp) som tjänsterealiseringen antingen producerar eller konsumerar.
- Tjänsterealiseringens krav på sin exekveringsmiljö.
- Om tjänsten realiseras av flera olika delar så behövs konfigureringsinformation om tjänsterealiseringen. Ett exempel på detta är när en tjänsterealisering har behov av realiseringar av andra tjänster.

- De värden som tjänsterealiseringen ger till en eller flera av de egenskaper som den realiserade tjänsten introducerar.
- Annan information om tjänsterealiseringen, t.ex. i form av nyckelord som beskriver tjänsterealiseringen och sedvanlig programdokumentation.
- Versionshanteringsinformation.

5. Tjänsteinstanser

För att få göra en tjänst tillgänglig för konsumenter så måste det för det första finnas en tjänsterealisering i form av en producent. Denna utgörs, i det sammanhang som behandlas här, av ett datorprogram. Programmet används tillsammans med lämplig hårdvara för att skapa en exekverande process som utgör en tillgänglig tjänst för alla konsumenter av tjänsten vilka också består av exekverande processer.

En förutsättning för en tjänsteinstans existens är att det finns en definierad tjänst samt en eller flera tjänsteimplementeringar för denna tjänst i form av producenter och konsumenter. Givet dessa förutsättningar så kan en tjänsteinstans skapas genom att tjänsteimplementeringen exekveras i en lämplig datormiljö.

Om tjänsteinstansen är en konsument behövs naturligtvis också en motsvarande tjänsteinstans av åtminstone en producent av tjänsten.

5.1. Tjänsteinstansers livscykel

Följande faser finns i en tjänsteinstans livscykel:

- *Processinitiering*. En sorts information som behöver spridas och som skapas vid processinitiering av tjänsteproducenter är den adress (referens) som behövs av andra tjänsteinstanser (konsumenter) för att komma i kontakt med tjänsteinstansen och därmed kunna använda tjänsten.

  Vid processinitiering genereras ett antal andra egenskapsvärden. Vilka egenskapsvärden som är aktuella i en konkret situation bestäms av vilken tjänst och vilken tjänsteimplementering som är aktuell.

- *Processexekvering*. Om tjänsteinstansen är en producent av tjänsten så kommer den kontinuerligt att användas av olika konsumenter av tjänsten. Dessa behöver information av adressen till producenten samt vilka kommunikationsstrategier och säkerhetsstrategier som kan användas för att kommunicera med tjänsten.
- *Processavveckling* sker när processen slutar att exekvera.

5.2. Tjänsteinstansers metainformation.

Den information som behövs om tjänsteinstansieringar är följande:

- Namn (identifiering, processid) för tjänsteinstansen.
- Namn (identifiering) på den tjänsterealisering som tjänsteinstansen kommer från.
- Namn (identifiering) av den exekveringsmiljö (dator, ”host”, plattform) där tjänsteinstansen exekverar.
- Adress (referens, URI) till tjänsteinstansen.
- Information om vilka kommunikationsstrategier och säkerhetsstrategier som kan användas för att komma i kontakt med tjänsteinstansen.
- Om tjänsteinstansen är en tjänsteproducent så behövs information om de konsumenter som använder producenten. Detta kan utgöras både av de konsumenter som använder producenten just nu och de som har gjort det under tjänsteinstansens livstid.
- Om tjänsten realiseras av flera olika delar så behövs information om de tjänsteinstanser som används för att realisera de tjänster som tjänsteinstansen använder (konsumerar).
- De värden som tjänsterealiseringen ger till en eller flera av de egenskaper som den realiserade tjänsten introducerar. Exempel på sådan information kan vara när tjänsten startades (”uptime”).

6. Ytterligare informationskällor

Inom ramen för Nätverksbaserat Försvar och projektet LedsystT har Försvarsmakten/Försvarets Matrielverk (FMV) arbetat med fråge-

ställningar som har stor anknytning till de frågeställningar som behandlas i detta avsnitt. Många dokument som har tagits fram i detta arbete är fritt tillgängliga. De dokument som framförallt berör ämnesområdet för detta avsnitt är följande referenser:

Informationssamordning för myndighetssamverkan

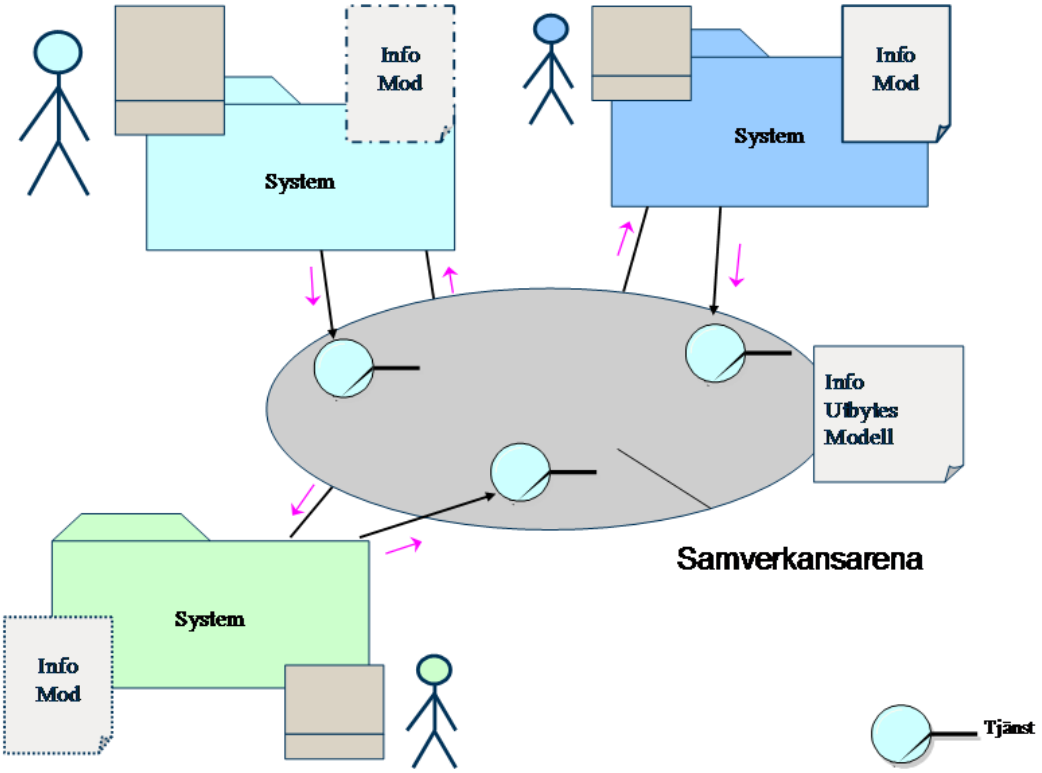
Sammanfattning

I samverkan är det av största vikt att utnyttja och samordna information. Gemensam informationsinfrastruktur utgör grunden för lyckad samverkan. Den kan behöva anpassas och specialiseras till olika samverkanssammanhang, där regler och överenskommelser träffas kring t ex informationsutbud och tillgängliga tjänster, betydelse och säkerhet. Ett verktyg för specifikation av sådana överenskommelser är informationsutbytesmodeller som i stor utsträckning utnyttjar standard. Utifrån vad de olika aktörerna väljer att dela med sig skapas en samverkansarena, som bygger på informationsinfrastrukturen, där tjänster erbjuds som stödjer såväl gemensamma som enskilda behov.

1. Inledning

STIL handlar om stöd för samverkan i ledning mellan myndigheter och andra aktörer baserat på en delad informationsinfrastruktur. En *samverkansarena* upprättas för specifika samverkansbehov med hjälp av ett urval av de tjänster som aktörerna tillhandahåller i informationsinfrastrukturen.

Varje myndighet har sina informationssystem och har utvecklat dessa med stöd av för myndighetens verksamhet relevanta informationsmodeller. Dessa lokala informationsmodeller kan antas ha väsentliga olikheter sinsemellan.



Figur 1. Principskiss över tjänstebaserad samverkansarena som i grunden utnyttjar en informationsinfrastruktur

Ett illustrerande exempel: ett H på skärmen betyder helikopterplatta för räddningstjänsten medan det kan tolkas som hundpatrull av polis. Sådana skillnader skapar ett behov av tolkning/översättning vid flyttning av information mellan olika aktörers system.

En utmaning för parterna i all samverkan är att lyckas förstå varandra! Ju mer sporadisk och extraordinär samverkan är, desto större

är utmaningen, så även när samarbetet skall stödjas med informationsutbyte via IT-system.

Information är en central del av samverkan och behöver särskild uppmärksamhet för att säkerställa ”samfunktion”. Därför behövs också en informationssamordning som grund för tjänster i samverkansarenan. Ett välfungerande och flexibelt informationsutbyte via samverkansarenor med bibehållen integritet för de olika myndigheternas lokala system måste förberedas bland annat genom att etablera gemensamma standarder för information, regler och teknik. En gemensam informationsutbytesmodell etableras för information i samverkansarenor.

En förutsättning för att lyckas med samverkan vid kris är att förbereda grunderna för kommunikation och samförstånd i god tid.

2. Behov av informationssamordning

Samverkan mellan myndigheter vid kriser eller andra extraordinära händelser karaktäriseras av varierande grad av ovisshet. Man vet inte i förväg hur den specifika situationen kommer att se ut och utvecklas och därmed inte exakt vilka behov av samverkan som kommer att uppstå.

Ett effektivt sätt att förebereda för samverkan är att måla upp och utgå från ett antal alternativa scenarier. Dessa scenarier baseras på olika situationer och beskriver de typer av samverkan som krävs mellan aktörerna . Ett antal typfall av samverkan kan då ringas in och utgöra en dimensionerande behovsbild. Baserat på behovsbilden kan man förbereda och skapa tekniska och organisatoriska förutsättningar för effektiv samverkan via informationsinfrastrukturen.

Vi kan här identifiera två olika strategier som kan vara giltiga för respektive typfall:

- Samverkan baserad på likhet

  Scenarier som både har en hög sannolikhet att inträffa **och** där aktörerna har mycket god kunskap om hur de skall samverka kan förberedas i hög utsträckning. Samverkansparter kan i förväg komma överens om aspekter som typiskt är viktiga i *samarbetet i situationen* t ex arbetsformer, ledningsstruktur, beslutsfördelning, informationsdelningsbehov, begreppsapparat, informationsmodeller

samt tjänstebehov. Det kan alltså löna sig att investera i samordning av verksamhets- informations- och tekniklösningar för att *optimera* grunden för samarbete.

- Samverkan baserad på överbryggning

  Scenarier som är svåra att förutsäga **och/eller** då det är svårt att förutsäga hur aktörerna konkret skall samarbeta kan inte förberedas genom likhet eftersom nödvändig kunskap om förhållandena saknas. Dessa scenarier kan istället förberedas genom att aktörerna bygger upp en gemensam förmåga att snabbt utreda samverkansbehov och införa lösningar gemensamt för dessa. Detta innebär att inleda en dialog, identifiera samverkansbehov och därefter flexibelt kunna skapa **nytt** stöd med hjälp av informationsinfrastrukturen. Arbetet avgränsas till de tjänster och informationsutbyten som bedöms realiserbara och bidra till ökad effektivitet i samverkan. Detta ger en förmåga att behovsstyrt överbrygga olikheter mellan aktörernas verksamheter, information och system för att *tillgodose* ett uppkommet behov.

Båda typfallen kan stödjas genom förberedelser men det senare typfallet kräver också en hög handlingsberedskap att skapa ny informationssamverkan utifrån flexibla förutsättningar och identifierade behov.

3. Informationsinfrastrukturens användning för informationssamverkan - introduktion

Myndigheter ansluter till en samverkansarena och erbjuder en delmängd av de tjänster de förberett för samverkan. Varje tjänst har en informationsgränsyta som utgör dess del i informationsinnehållet i samverkansarenan. Tjänsterna kan både lämna och hämta information till/från andra tjänster.

I samverkansarenan kan också etableras tjänster som endast är till för att stötta samverkan mellan myndigheterna i en specifik insats. Det kan t ex vara tjänster för att upprätthålla och presentera lägesinformation som underlag för planering och koordinering av myndigheternas insatser. En sådan kan baseras på lägesinformation från flera av deltagarnas olika interna system.

3.1. Hur gemensam vill man betrakta en samverkansarena?

En viktig fråga för tjänsterna i samverkansarenan är i vilken mån de skall betraktas som gemensamma. Ett par synsätt presenteras här.

3.1.1. Bilateralt (parvis) informationsutbyte mellan aktörer i samverkansarenan

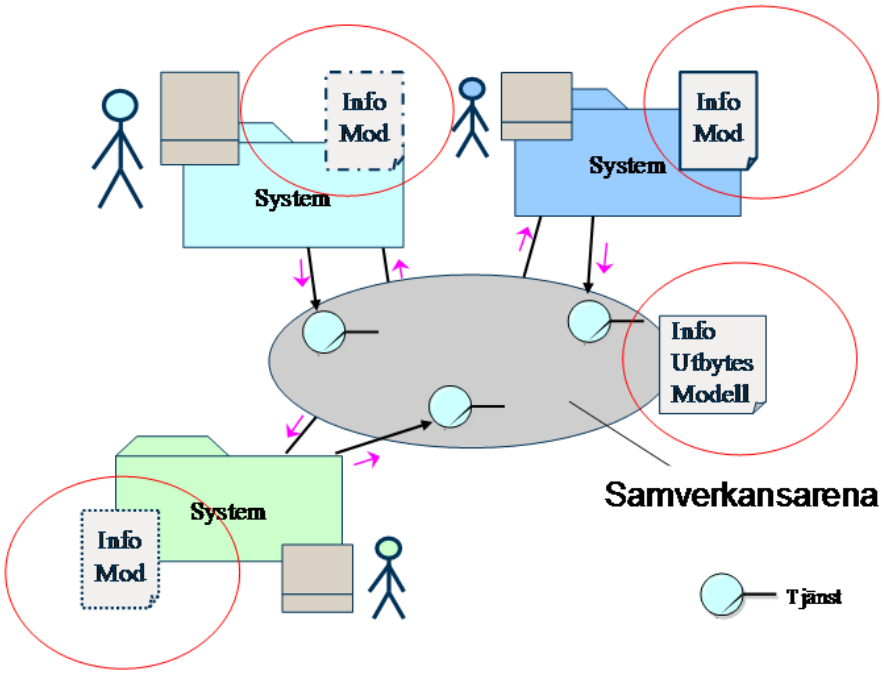
En möjlighet är att samverkansarenan är öppen för alla aktörerna men att dessa bilateralt kommer överens om vilken information och tjänster man skall erbjuda varandra som stöd för den samverkan man skall ha i den aktuella krisen. Då skulle också parterna bilateralt kunna komma överens om regler för betydelse (semantik) och form (syntax) för informations-innehållet i tjänsterna när de uppträder i samverkansarenan. En fördel med detta är ett relativt enkelt förfarande mellan parterna. En nackdel är at det blir svårt för andra (än de två aktörerna i den bilaterala överenskommelsen) att utnyttja tjänsternas information.

3.1.2. Information som gemensam resurs för alla aktörer i samverkansarenan

Informationsinfrastrukturen kommer med tiden att ge tillgång till stora mängder information från en mängd olika aktörer och en mängd olika tekniska system. Det som eftersträvas är att aktörerna i en samverkansarena kan tillgodose sina aktuella informationsbehov genom den samlade informationsresurs som möjliggörs genom samverkansarenan. All information, som man som användare är behörig, till ska kunna nås utan krångligheter eller tekniska restriktioner, såväl för läsning som för hantering och uppdatering.

Det är en fördel om informationen som erbjuds på samverkansarenan har standardiserad betydelse så att alla parter har grundförutsättningar att ta emot och tolka den i sina system. Det ger en betydligt större potential att utnyttja etablerade tjänster för flera syften.

Informationsinfrastrukturen måste stödja att ett stort antal tjänster, tillhandahållna av ett antal olika tekniska system, kan används i kombination. Detta kräver kompatibel information i tjänsternas gränsytor vilket åstadkoms med hjälp av styrande informationsutbytesmodell.



Figur 2. Strukturen av informationsmodeller kring en samverkansarena

3.2. Informationsmodeller och informationsutbytes-modell

Strukturen av informationsmodeller och informationsutbytesmodell markeras i figur 2 nedan och beskrivs i följande text.

3.2.1. Informationsmodeller

Varje aktör som erbjuder tjänster i en samverkansarena har ett eller flera tekniska informationssystem som nyttjas för att utföra tjänsterna. Varje informationssystem byggs och vidareutvecklas baserat på en egen – lokal[1] – informationsmodell som förklarar hur informationsinnehållet är strukturerat och hänger ihop i just det systemet. En aktör med många informationssystem kan alltså också ha många lokala informationsmodeller som inte nödvändigtvis är samstämmiga med varandra.

3.2.2. Informationsutbytesmodell

En informationsutbytesmodell kan byggas upp av modellelement från nationella eller internationella standarder för information och/eller av modellelement som skapas av de samverkande parterna själva. Det finns idag ett stort utbud av standarder och standardiseringsinitiativ i

[1] Vissa myndigheter kan ha nationellt gemensamma typsystem med tillhörande informationsmodell t ex SOS Alarms system Zenit.

olika mognadsfas för information inom diverse domäner till exempel geografisk information, handel (EDIFACT) samt svensk offentlig sektors satsningar på EDI.

3.3. Informationsutbytesbehov

Informationsutbytesbehov (IU-Behov) kan specificeras för informationsutbyten som förväntas förekomma frekvent och/eller mellan flera olika aktiviteter/ verksamhetsenheter i samverkansarenan. Ett informationsutbytesbehov har sin unika specifikation och dess informationsinnehåll baseras på en viss informationsutbytesmodell. Ett IU-Behov kan översättas till flera semantiska områden baserat på deras respektive informationsutbytesmodeller. Detta dokumenteras antingen i ett översättningsdokument eller helt enkelt som en nyupprättad behovsspecifikation för utbytet baserad på annan informationsutbytesmodell.

3.4. Semantiska områden

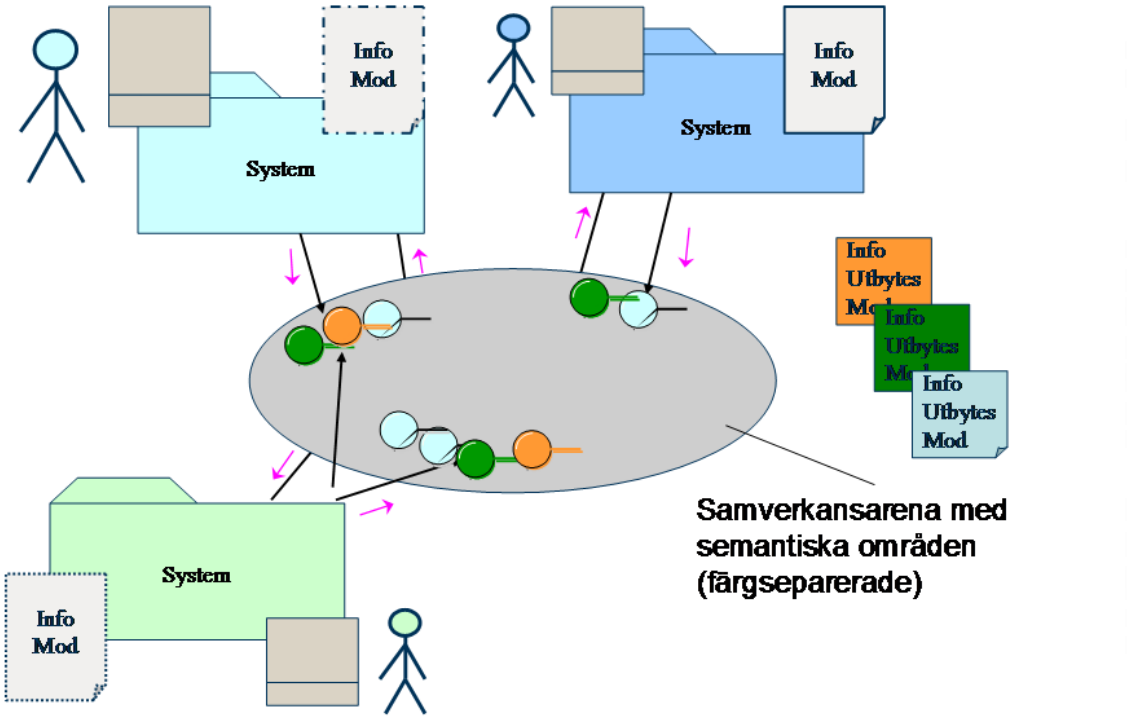
Inom en samverkansarena grupperas tjänster som bygger på en och samma informationsutbytesmodell till semantiska områden. Tjänster inom samma semantiska område kommer då att ha en gemensam bas för informationsinnehållet dvs vara semantiskt och tekniskt kompatibla.

Viss information kan emellertid också komma att behövas i flera olika semantiska områden till exempel i utbyte mellan tjänster i olika semantiska områden inom informationsinfrastrukturen eller i utbyte mellan tjänster inom informationsinfrastrukturen och externa aktörers system. När information skall flyttas/förekomma i tjänster i olika semantiska områden uppstår ett behov av att översätta informationen mellan informationsutbytesmodellerna bakom de semantiska områdena.

3.5. Skyddade informationszoner

Förutom semantiska områden kan det vara relevant att upprätta skyddade informationszoner inom en samverkansarena. Information som skall skyddas till exempel på grund av sekretess kan hanteras inom sk skyddszoner[1] som bara behöriga har tillgång till. Dessa skyddszoner

[1] Referens: LedsystT, LT1K P04-0385 Security Architecture Overview 4.0



Figur 3. Tjänster och informationsutbytesmodeller färgkodade för respektive semantiskt område

har ett starkt skydd och det finns möjlighet att på ett reglerat sätt flytta information mellan skyddsnivåer t ex vid omklassificering från sekretessbelagd till öppen. En skyddad informationszon kan innehålla tjänster från flera semantiska områden och vice versa.

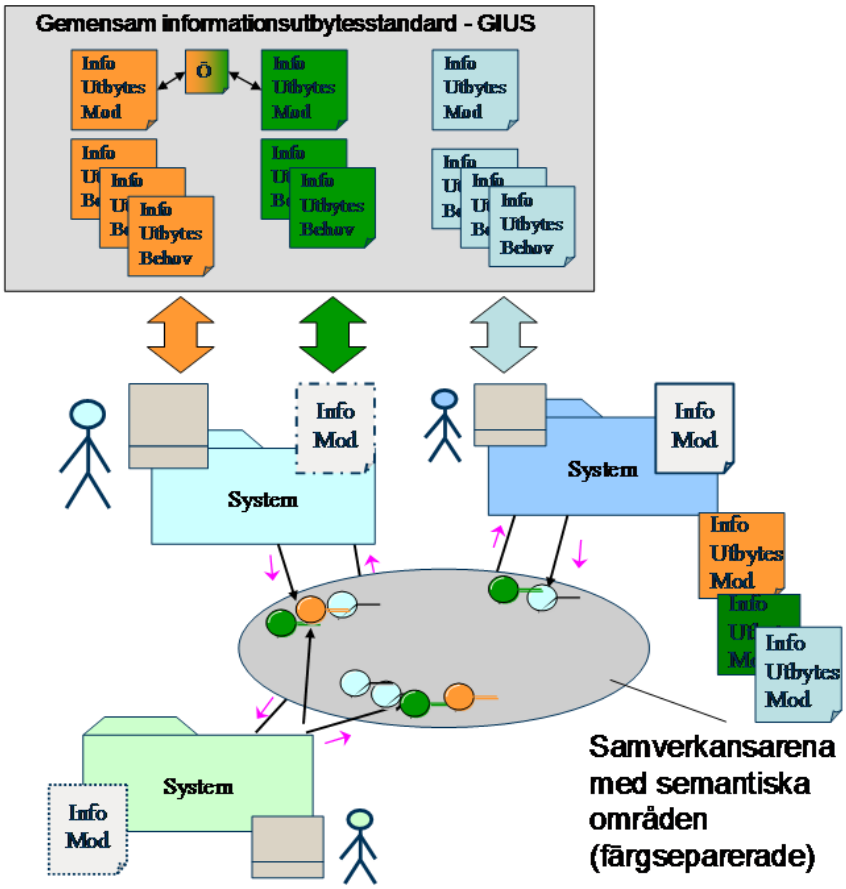
4. Standarder för informationssamordning

Informationssamordningen som stöd för samverkan mellan aktörer i samverkansarenor kan stödjas av en Gemensam InformationsUtbytesStandard – GIUS[1] med ett antal olika komponenter i. Detta avsnitt ger en översikt över GIUS och en kort beskrivning av dess nyckelkomponenter.

Komponentbeskrivning av ingående delar i standarden, GIUS

- Informationsutbytesmodeller inom informationsinfrastrukturen samt relation till standarder, domäner etc.

[1] LedsystT, LT1K P06-0323 Framework for CIES 2.0.



Figur 4. GIUS styr utformning av information i tjänster inom respektive semantiskt område

- Informationsutbytesmodeller för externa informationsutbyten, med aktörer som inte deltar i samverkansarenan.
- Informationsutbytesbehov, specifikationer
- Översättningsspecifikationer och/eller översättningsmekanismer
- Områdesindelningen av semantiska områden i samverkansarenan
- Gemensamt stöd för informationsutbyte i samverkansarenan t ex allmänna information managementtjänster, översättningstjänster och bryggtjänster till externa system (ej till aktörers system)
- Anvisningar (designregler) för att vägleda utformningen av informationsutbyten och dess stödjande standarder

Några av de viktigaste komponenterna av informationsutbytesstandarden beskrivs nedan.

4.1. Informationsutbytesmodeller

En informationsutbytesmodell är en beskrivning av vad information/ data betyder inom ett semantiskt område. Den kan utgöras av bland annat begreppsmodeller, informationsmodeller och datatermkataloger[1].

Informationsutbytesmodeller upprättas och förvaltas knutet till livscykeln för semantiska områden i samverkansarenor. En sådan modells innehåll skall täcka de faktiska informationsutbytesbehoven inom berörda semantiska områden, men inte mer, då det lätt leder till onödig komplexitet.

En informationsutbytesmodell bör födas med innehåll från informations-modeller i nationella eller internationella standarder eller från modeller som utgör de-facto-standard inom en domän om det finns en livskraftig standardiseringsorganisation bakom. Eventuella beslut att upprätthålla ”konsistens” mellan en informationsutbytesmodell och bakomliggande standard innebär ett förvaltningsåtagande då förändring i standarden måste hanteras i relation till modellen **och** de tjänster som baserats på denna.

En informationsutbytesstandard kan baseras på en av flera sätt att hantera informationsutbyten:

- Modellbaserat (med stöd av informationsutbytesmodell) t ex GIS
- Regelbaserat, automatiserad tolkning av data vid utbyte baserat på informationsmodell och tolkningsregler
- Meddelandebaserat (utan entydig bakomliggande informationsmodell) med stöd av specificerat IU-behov, t ex EDIFACT

Den modellbaserade ansatsen rekommenderas i första hand men utvecklingen kring den regelbaserade ansatsen pekar på att även denna kan börja bli realiserbar i nära framtid.

En informationsutbytesmodell dokumenteras i en specifikation med hjälp av en fastställd beskrivningsteknik (notation, till exempel UML) för informationsmodeller. Denna notation bör väljas så att den i görligaste mån liknar eller överensstämmer med de som aktuella aktörer tillämpar för sina lokala system. Det underlättar kraftigt jämför-

[1] Referens: LedsystT LT1K P04-0313, Framework Information Exchange Models 5.0. LedsystT LT1K P05-0080, Framework Information Models 4.0.

barhet mellan informationsutbytesmodell och respektive lokala informationsmodeller.

4.2. Översättningar

Översättningar dokumenteras för specifika behov av samverkan mellan tjänster. Det kan komma att finnas en stor mängd översättningar (av delmängder) mellan två informationsmodeller. Varje översättning baseras på en noggrann analys av berörda modeller och dokumenteras i en specifikation tillsammans med en deklaration av eventuella identifierade innehållsförluster d v s information som inte går att översätta fullt ut mellan modellerna.

Det finns flera principiellt olika sätt att utföra en översättning mellan informationsmodeller:

- Manuell modellmappning, dv s när två informationsmodeller jämförs element för element och beslut tas för hur elementen skall korsrefereras till varandra. Detta är ofta fallet då modellerna är dokumenterade med olika notationer, modelleringsstilar etc.
- Automatiserad modellmappning, dvs när två informationsmodeller jämförs och korsrefereras med hjälp av formaliserade regler. Detta fall kräver gemensamma standarder för notation, modelleringsstil etc och området är fortfarande i fokus för pågående forskning. Automatiserad översättning har potential att tillämpas i runtime och därigenom bidra till högre inbyggd flexibilitet i informationssamverkan.
- Standardiserade meddelanden, dvs när en uppsättning standardiserade meddelandespecifikationer mappas mot tjänsternas informationsgränsyta och /eller mot informationsutbytesmodellen. Denna ansats är tillämpbar när det existerar fristående meddelandestandarder som skall tillämpas i flera semantiska områden och/eller meddelandestandarden i sig saknar en dokumenterad informationsmodell.

Översättningar kan också dokumenteras mellan specifika informations-utbytesbehov och informationsinnehållet i tjänster då dessa i sig innehåller informationsspecifikationer.

Tillämpning av översättningar mellan informationsbeskrivningar (informationsutbytesmodeller, informationsutbytesbehov, tjänstegränsytor etc) bör stödjas av specifika anvisningar i STIL Ramverk.

4.3. InformationsUtbytesBehov

Ett Informationsutbytesbehov – IU-Behov utgör en specifikation av ett informationsutbyte mellan två verksamhetsenheter. Informationsutbytesbehov identifieras och specificeras lämpligen när aktörerna modellerar den verksamhet, information och samverkan som är aktuell att stödja i samverkansarenan.

Specifikationen stäms av mot en specifik informationsutbytesmodell avseende ingående beskrivningar av informationsinnehållet. Nya behov kan identifiera information som inte tidigare ingår i modellen. Då måste ett beslut fattas huruvida informationsutbytesmodellen skall uppdateras med eventuella konsekvenser för andra IU-Behov eller om det nya behovet skall modifieras för att passa befintliga informationsdefinitioner.

Behov kan dokumenteras på samma vis som i LedsystT[1].

4.4. Format

Det finns ett antal format för datakommunikation i bruk idag. Vissa är system- eller produktspecifika medan andra hanteras av någon standardiseringsorganisation, allt från user-groups till nationella och internationella standardiseringsorgan. Något sådant standardiserat format måste ofta användas för att olika system skall kunna fungera tillsammans och byta information. Format inkluderar ofta explicita eller implicita datamodeller, informationsutbytesbehov/meddelanden och/eller överföringsprotokoll för en viss delmängd av information. Det kan därför uppstå behov av att översätta information även mellan en informationsutbytesmodell och den eller de (av andra etablerade) dataöverföringsformat som skall nyttjas för dataöverföringen.

[1] Referens: LedsystT LT1K P06-0624 Framework Information Exchange Requirements 1.0.

5. Livscykel för informationssamordning

5.1. Samband mellan informationsmodeller

Ett effektivt samarbete förutsätter att en gemenskap byggs upp och förvaltas över tiden. I denna gemenskap ingår informationssamordning som en nyckelaktivitet.

De aktörer som ingår i gemenskapen samverkar kring att bygga upp och förvalta en Gemensam InformationsUtbytesStandard (GIUS)[1] för deras samverkansarenor. En GIUS baseras på de faktiska behov av informationssamverkan som identifieras samt på tillgängliga standarder inom relevanta informationsdomäner.

Figur 5. Sambandet mellan GIUS, tjänster och lokal information hos aktörerna.

GIUS styr sedan utformningen av information i de tjänster som erbjuds i samverkansarenan (-orna). Därigenom blir informationen i alla tjänster i samverkansarenan standardiserad vilket underlättar flexibelt utnyttjande av information från olika tjänster och bidrar till att underlätta förståelse och kommunikation mellan aktörerna.

Identifiering av behov av tjänster utgår från vilken information aktörerna behöver ha tillgång till i sin verksamhet och i sina system. Specifikationen av de tjänster som erbjuds i samverkansarenan är styrande för den aktör som via tjänstebryggans skall realisera tjänsten i sitt system. Det betyder att aktören får ta ansvar för eventuell översätt-

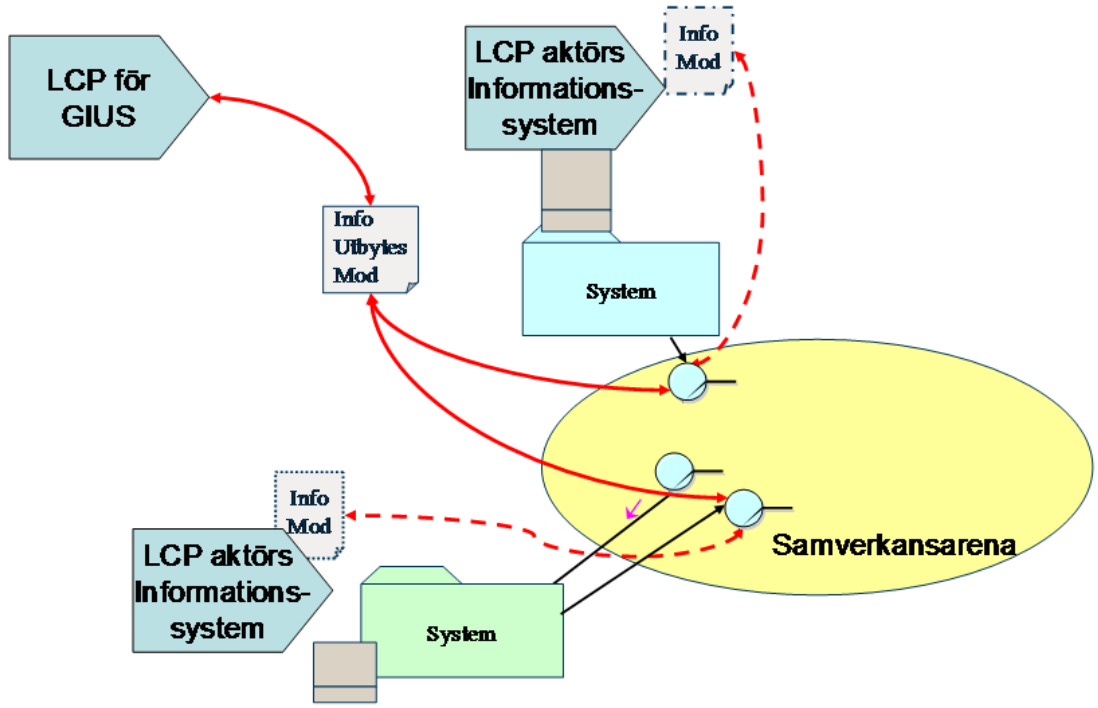
[1] GIUS beskrivs i kapitlet Standarder för informationssamordning

ning av information mellan systemets lokala modell och den form som gäller i tjänstegränsytan baserat på en gemensam informationsutbytesmodell.

Detta innebär att även om samverkan implementeras på ett frikopplat sätt med hög integritet för de myndighetsvisa systemen så skapas ett visst beroende genom de behov av gemensam förvaltning av GIUS som införs.

5.2. Samband mellan livscykelprocesser

För aktörer som vill etablera en långsiktig förmåga att ingå samarbeten via samverkansarenor etableras en gemensam livscykelhantering för en Gemensam InformationsUtbytesStandard inkluderande hantering av informationsutbytesmodeller.



Figur 6. Samband mellan livscykelprocesser (LCP) för GIUS respektive för system/tjänster

Alla aktörers respektive systemförvaltningsprocesser som skall skapa de tjänster aktören kan erbjuda i samverkansarenor kommer att ha ett löpande samarbete med livscykelprocessen för den Gemensamma Informations-UtbytesStandarden.

Utvecklingsprocess för utveckling av situationsanpassade system

Sammanfattning

Detta avsnitt visar översiktligt på en utvecklingsprocess för utveckling av flexibla situationsanpassade system. Avsnittet ger roller som projektledare och systemanalytiker vägledning om hur man utvecklar system av samverkande tjänster.

1. Evolutionär systemutveckling

Moderna system byggs för största möjliga flexibilitet. Gjorda investeringar i befintliga system vill man ta tillvara så enkelt som möjligt. Genom utveckling av tjänstebaserade och situationsanpassade system utnyttjas såväl modern teknik som stabil funktion och informationsresurser från redan befintliga system. Det flexibla angreppssättet möjliggör utveckling evolutionärt, gradvis, där man utgående från behov kan bygga vidare på befintlig funktion och med löst kopplade tjänster göra enkla tillägg till funktionaliteten.

Denna utvecklingsprocess skiljer sig från konventionella processer som grundar sig på fasta produktkravspecifikationer. Den största fördelen med evolutionär utveckling är att systemen tidigt utvärderas till att fylla rätt funktion för användarna. Dessutom kan utvecklingen koncentreras till definition och framtagning av överblickbara delar av programvara.

Den evolutionära systemutvecklingen har en väldig fördel i att körbara systemversioner eller prototyper snabbt kan tas fram för prov och utvärdering. De erfarenheter som användare och utvecklare återmatar, utnyttjas för att så tidigt som möjligt påverka ett ändamålsenligt system med användbara tjänster. Integration av tjänstebaserade lösningar, i små steg, möjliggör att system snabbt kan tas i användning och därefter kontinuerligt vidareutvecklas. Utvecklingen är snabb och enkel och utgår ifrån befintliga tjänster och system, som vidareutvecklas med tjänster på applikationsnivå. Resultatet blir väl situationsanpassade system vars livslängd är beroende av dess funktion.

Upplägg på och beskrivningar av tjänster bör standardiseras, såtillvida att ett enhetligt beskrivningssätt underlättar användningen av en tjänst.

Utvecklingsprocessen behöver ta ställning till förändrade behov och erfarenheter som kan samlas in under provanvändning av sammansatta tjänstebaserade system. Därför passar en evolutionär process, som kan fånga upp behov och krav som förändras och förfinas på vägen. Låsta produktkravspecifikationer som fastställs innan utveckling och är kopplade till affärsöverenskommelser passar inte bra. Istället finns risk att det leder till fel resultat för de som i slutänden skall använda systemen.

2. Hur kravställer man utan kravspecifikation?

Leverantör och mottagare bör bygga sina affärsöverenskommelser på uppfyllande av projekt- och processkrav istället för (som traditionellt) på grundval av produktkravspecifikation. Då flyttas fokus till att ordnat behovsinrikta systemet vartefter ny kunskap byggs i projekten. Alltför många traditionella systemutvecklingsprojekt har slutat med leverans av något som kunden ej velat ha, men som såväl leverantör som mottagare låst sig till genom att sammanblanda krav på produkten med affärsuppgörelsen. På vägen i projektet har annat viktigt bortprioriterats, som ändamålsenlighet och kvalitet. Framförallt är det viktigt att undvika långa projekt utan avstämningar mellan leverantör och kund.

Idéer och kunskap om den slutgiltiga produkten/leveransen/systemet bör givetvis konkretiseras så tidigt som möjligt på ett kostnadseffektivt sätt. Detta görs bäst med hjälp av användarprov med tydliggjord ambitionsnivå. Systemfunktionaliteten kan illustreras utifrån ett liknande system till vilka några nya tjänster läggs till. Då bör system- och funktionsnytta tydliggöras, t ex genom att besvara några väl utvalda verksamhetsnära frågeställningar jämte några centralt systempåverkande. Igenom denna provprocess tar man kontinuerligt hänsyn till omvärlden. Vilka centrala behov och krav påverkar det vi vill åstadkomma i det systemet?

3. Provsystem omvandlas till skarpa

En möjlighet som uppstår, i och med införandet av situationsanpassade system, är mer flexibel systemframtagning och snabbare vidareutveckling av skarpa system. Detta kan ske genom att likställa utvecklingen av skarpa situationsanpassade system med ordnad utveckling av provsystem. När provsystem verifierats och validerats att uppfylla rätt ändamål till rätt kvalitet speglas de över i ett system för skarp drift för en större användargrupp. Det finns en hel del pengar att spara på att korta avståndet mellan system under utvärdering (provsystem) och driftssatta system. Användarmedverkan och täta systemprov är nyckelfaktorer i denna utveckling. Fokus läggs också på vidareutveckling av befintliga system som möjliggörs genom att arki-

tekturarbete för systemen anpassats just till tätare systemförbättringar för ändamålsenliga system genom löst kopplade tjänster.

Förbättrad ändamålsenlighet utgör en viktig besparing för systemets hela livscykel. Huvudsyftet med utveckling av provsystem är just att tidigt utvärdera ett resultat för att kunna förbättra det. De deltagande utvärderarna av systemen har ett stort ansvar att framföra åsikter som stödjer prioritering av de viktigaste förbättringarna för systemen. Därefter kan olika utvecklingssteg planeras.

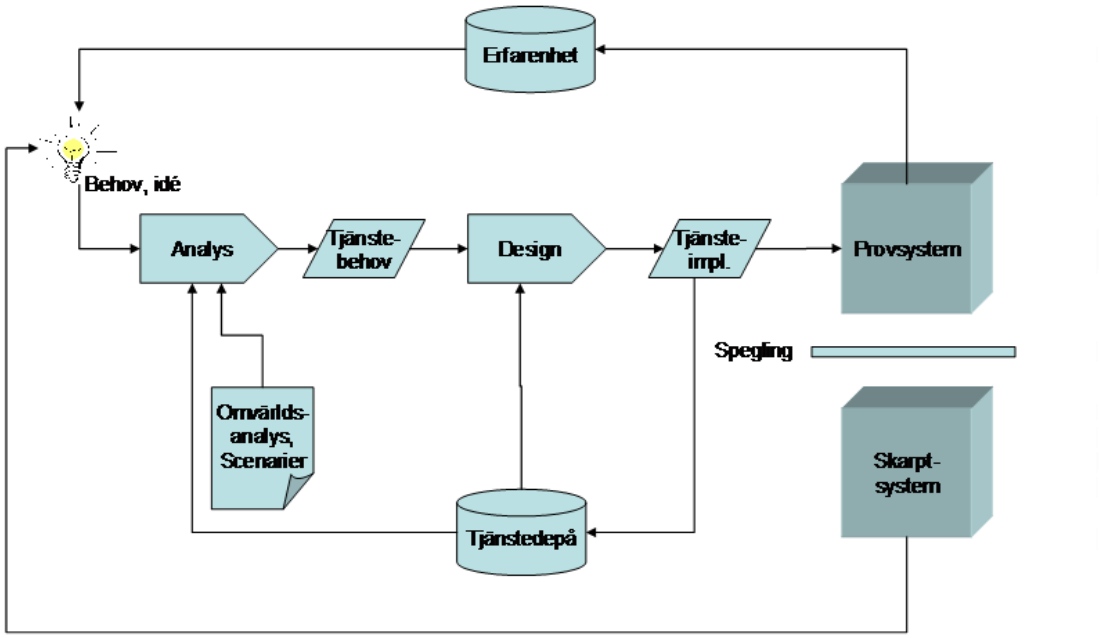
Nästa utvecklingssteg av ett system, som svarar mot nya tjänstebehov, kan därför alltid liknas vid en systemversion som skall utvärderas, till att börja med som provsystem inom denna utvecklingsprocess. Om denna utvärdering faller väl ut, så nyttjas systemet därefter i större skala.

4. Process för tjänstebaserad utveckling

Den evolutionära utvecklingsprocessen för tjänstebaserade system är en iterativ process, som utgår från och anpassas till uppfångade behov.

Utifrån erfarenheter i verksamheten, inklusive skarp systemanvändning, genereras behov och idéer för nästa steg. Användare, utvecklare och ansvariga samverkar kring idéerna i en workshop (Analys) för att konkretisera uppkommet tjänstebehov. Till detta används omvärldsanalys och scenarier för att illustrera verksamhetens behov och idéer. Arbetet resulterar i tydligt beskrivna **tjänstebehov**. Behoven matchas i första hand mot befintliga tjänster och dess tjänstebeskrivningar, för att utnyttja största möjliga återanvändning och hålla nere kostnader. Dessa befintliga tjänster eftersöks på ”Tjänstedepån”, marknadsplatsen för samlade tjänster. Om tjänsten saknas i det befintliga utbudet kan nyutveckling/vidareutveckling bli aktuell.

En nyutvecklad tjänst (Design) görs i första skedet tillgänglig för integration i ett situationsanpassat system för utvärdering, prov och försök. Efter utvärdering i pilotanvändning, verifiering och validering, så kan tjänsten dels sammanföras med andra ”etablerade” tjänster i tjänstedepån och ingå i en skarpare version av ett situationsanpassat system. Producenten av tjänsten bör, när tjänsten är kvalitetsmässigt kontrollerad och innehåller nödvändig beskrivning, gränssnitt etc ansöka om att ”marknadsföra” tjänsten i ”Tjänstedepån”. När tjänsterna



Figur 1. Processen för tjänstebaserad utveckling kopplas tydligt till behov och tjänstebehov som utvärderas med användare under utvecklingen. I botten utnyttjas befintliga tjänster och system så långt som är möjligt.

används skarpt ger de även upphov till ny erfarenhet och nya idéer, som iterativt kan medföra nya behov.

Programutvecklare av tjänsterna jobbar förslagsvis enligt beprövad designmetod (se nästa avsnitt).

Den beskrivna processen har en solklar fördel i tidig validering och verifiering. Eftersom integration av situationsanpassade system görs så smidig, utifrån grundprinciper om arkitektur och flexibilitet, så kan ett system för utvärdering göras tillgängligt på kort tid. System- och funktionsnytta kan tidigt utvärderas mycket lättare än med kravspecifikationer. Diskussions- och kommunikation underlättas och mottagare, användare och kunder till system kan fortare komma till hållbara överenskommelser.

4.1. Beprövad designmetod för utveckling

I FMV:s projekt LedsystT har en designmetod för FMLS (Försvarsmaktens Ledningssystem) tagits fram och använts med gott

resultat[1]. Denna metod är tillämpbar i sin helhet eller som delar i processerna analys och design enligt figur 1. Metoden grundar sig på huvudprinciperna i RUP SE´s disciplin Analysis & Design samt projekterfarenheter från bl.a. LedsystT projektet.

Metoden fungerar som grund för designarbete och är tänkt att användas tillsammans med annan dokumentationen framtagen för FMLS. Metoden är relevant i alla steg i livscykelmodellen ISO/IEC 15288.

Områden som hör till området design men som inte täcks av designmetoden är, design av realisering och arkitektur. Vad gäller design av realisering så kan stöd ifrån vanliga RUP eller motsvarande metodramverk användas som komplement.

Kärnan i designmetoden är de aktiviteter som med ett sammanhållande namn brukar kallas ”Flowdown”. Designmetoden består av fyra huvudprocesser:

- Fånga tjänster (Identify and consolidate services)
    - Identifiera tjänstekandidater utifrån verksamhetsmodeller och krav.
    - Definiera tjänsterna
    - Identifiera vilka designregler som är tillämpliga vid modellering av de aktuella tjänsterna.
- Beskriv tjänster med användningsfall (Describe services /use cases)
    - Beskriv varje tjänst med en kort text
    - Ta fram användningsfall för tjänsten
    - Beskriv användningsfall resp tjänst ur ett black-box perspektiv.
- Realisera tjänsterna (Realize services)
    - Ta fram en white-box design av systemet i fokus genom att göra realiseringar av tjänsterna.

[1] För en detaljerad beskrivning av designmetoden se LedsystT dokumentation: LT1O P06-0293 Designmetod för FMLS.

- Peka ut underliggande tjänster (Consolidate services)
    - Konsolidera de tjänster som identifierats på underliggande systemnivå.

Gemensam lägesinformation

Sammanfattning

Gemensam lägesbild är ett vanligt förekommande uttryck. Tyvärr leder uttrycket till tanken att den traditionella kartan, med information utritad, ska finnas tillgänglig för alla. Här används istället uttrycket ”*gemensam lägesinformation*”, för att poängtera att det inte alls behöver vara en bild som är gemensam. Det är informationen om läget som ska vara gemensam, vilket betyder konsistent och tillgänglig för samtliga parter. Syftet är att ge parterna en gemensam situationsförståelse till grund för eget agerande.

Detta kan säkerställas genom att i förväg planera vilken information man vill ha och beskriva den i en *bruttomodell*. Det gäller inte bara specifik insatsinformation utan även generell information t ex kartdata. När en händelse inträffar gör man ett utdrag ur bruttomodellen som är specifik för insatsen och skapar en *nettomodell*. Nettomodellen definierar vilken information som kan utbytas och vilka tjänster som erbjuder informationen. Den sammanlagda informationen som är tillgänglig via tjänsterna bildar den gemensamma lägesinformationen. Ur denna kan man sedan göra roll och personbaserade utsnitt för att var och en ska få – för sin uppgift – bästa möjliga information.

1. Inledning

Vid en insats, av vilket slag den än är, är det viktigt att samtliga parter[1] har samma uppfattning om vad som händer, vem som gör vad och övriga omständigheter.

Traditionellt har det vid stora händelser funnits en stab som samlat in informationen och delat ut den till dem staben trott ha behövt informationen. För att få överblick har viss information samlats på någon slags bild med en karta i bakgrunden.

De enskilda människorna på fältet har för det mesta arbetat med tryckt karta, papper och penna. Eftersom de befinner sig mitt i händelsens centrum har de den absolut mest aktuella informationen om läget lokalt inom det område de kan överblicka. Däremot har informationen om läget i övrigt inskränkt sig till vad staben eller ledningscentral försett dem med. Vid mindre händelser skapas ingen stab och då får människorna på fältet klara sig med den information de har eller kan få från ledningscentralen (om det finns en sådan).

Arbetsuppgifterna på de olika nivåerna inom en organisation skiljer sig en hel del vilket gör att olika nivåer (utöver gemensam grundinformation om insatsen) vill ha olika information. Detta har, i sin tur, lett till att det allt för ofta har förekommit divergerande information på olika nivåer.

De som arbetar på fältet och de som arbetar inom ledningsfunktioner högre upp i organisationen vill inte ha ”samma information”. De vill ha konsistent information och de vill ha den delmängd av informationen som gynnar och underlättar deras arbete.

För att lösa problemen behövs en annan definition på gemensamt läge än bilden med kartbakgrund. Resten av detta dokument kommer att beskriva en modell för hantering och spridning av information för att uppnå den önskade gemensamma lägesinformationen.

2. Övergripande modell

När en händelse verkligen inträffar finns inte mycket tid att fundera på vilken information man skulle vilja ha och framför allt inte hur man ska få tag i den. För de typer av händelser man kan förutse bör man därför kontinuerligt se över vilken information man tror kommer

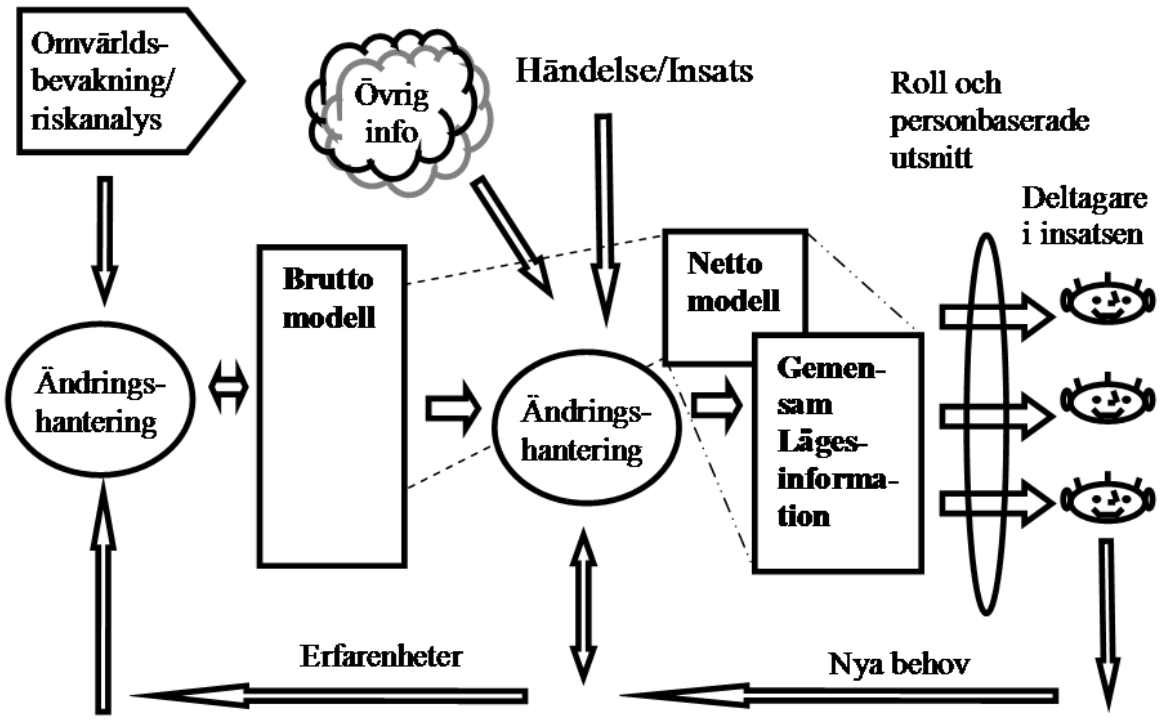
[1] Samverkande myndighet/organisation/företag.

att behövas och säkerställa att den kommer att vara tillgänglig. Inte minst måste avtal om tillgång till information som inte är öppen finnas innan man behöver informationen eftersom lagar, regler och affärsverksamhet påverkar vilken information som är tillgänglig.

Den information som man förutsett ett behov av, kan ses som en samling menyer med önskade rätter (typer av information). Menyn/menyerna är utlagda på en eller flera restauranger (olika leverantörer).

När en händelse inträffar beställer man rätter från de olika menyerna så de tillsammans bildar ett smörgåsbord av information (anpassad för typen av händelse) plus (om det är bra restauranger) ett par rätter (övrig information) utanför menyerna. De som samverkar under insatsen har tillgång till samma smörgåsbord (den gemensamma lägesinformationen) men kan välja rätter och mängd efter eget önskemål.

Figur 1 visar ”smörgåsbordet” lite mer strikt. **Bruttomodellen** (menyn) definierar och beskriver den förberedda informationen. Ur



Figur 1. Övergripande modell över hur förberedd information definieras i bruttomodellen och hur en insats väljer ut en delmängd (en nettomodell) som grund för den gemensamma lägesinformationen (verklig information) ur vilken information kan hämtas efter behov (och behörighet).

denna väljs en delmängd ut till en **nettomodell** (beställning av smörgåsbordet).

Både bruttomodellen och nettomodellen är modeller med beskrivningar av information. Nettomodellen beskriver den information man vill utbyta under den pågående insatsen/insatserna (en informationsutbytesmodell). Bruttomodellen är sammanslagningen av nettomodellerna för de förutsedda händelserna.

Den verkliga informationen kommer att finnas distribuerad över de samverkande parternas system. Den totala mängden information som är tillgänglig (via tjänster) för deltagarna[1] i insatsen är det som bildar **den gemensamma lägesinformationen** (det uppdukade smörgåsbordet).

Under insatsernas gång kan nettomodellen sedan förändras för att uppfylla nya behov hos deltagarna. För att förhindra att nettomodellen ändras fram och tillbaka i onödan sker förändringarna via en styrd ändringshantering som ser till att samtliga deltagares behov uppfylls i så hög grad som möjligt.

De olika deltagarna i insatserna har tillgång till den gemensamma lägesinformationen via tjänster. Åtkomst av dessa tjänster sker via rollbaserad behörighet vilket gör att deltagarna får roll- och personbaserade utsnitt av informationen. Detta för att de ska få den information som just de behöver. Informationen presenteras sedan i deltagarnas egna system på de sätt de finner lämpligt (ett sätt som de känner igen och förstår).

Under varje ny insats får man nya erfarenheter av nettomodellen. När insatsen avslutas återmatas dessa erfarenheter till en ändringshantering för bruttomodellen så att bruttomodellen – och i senare led även nettomodellerna – kan förbättras inför nästa insats.

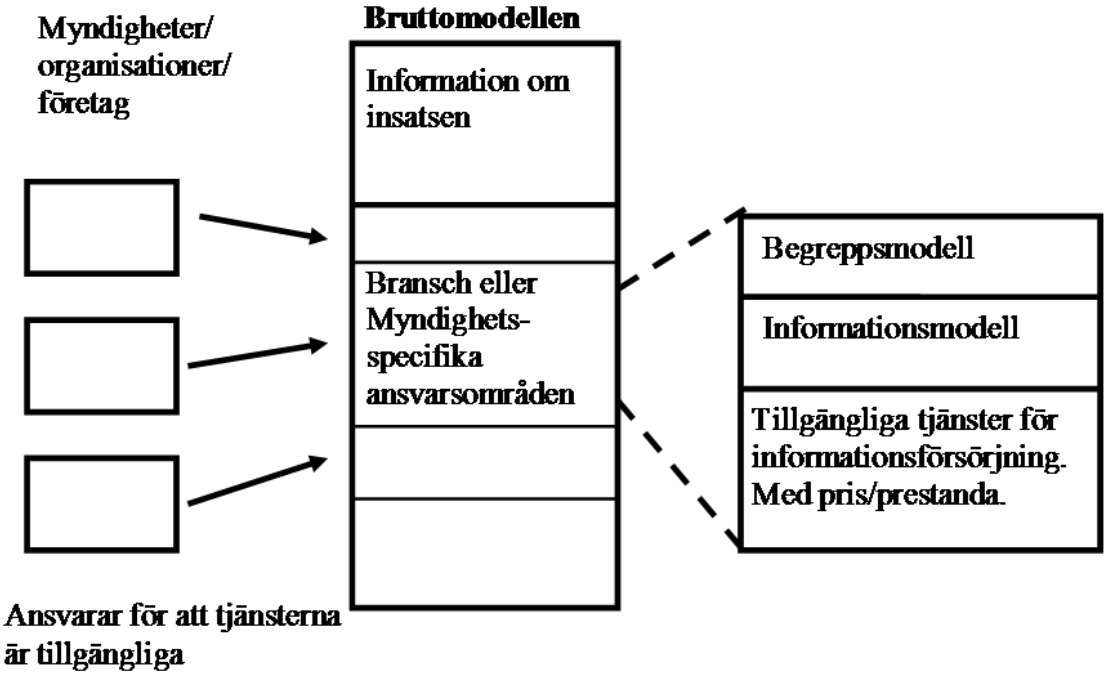
3. Informationsförsörjning

Anledningen till att informationen kontinuerligt ses över och beskrivs i bruttomodellen är bland annat att säkerställa att den är tillgänglig när den behövs. Det betyder att ”någon”, troligtvis myndigheter eller liknande, görs ansvarig för varsin del av informationen. Ansvaret består av två delar[2]: Dels ska informationen finnas tillgänglig när den

[1] Människor som deltar i insatsen, antingen vid händelsens centrum eller på annan plats.
[2] Se även Grund för tjänstesamverkan.

behövs med allt vad det innebär av tekniska lösningar och juridik. Dels innebär det att specificera vilken information som finns, hur den är åtkomlig och hur den ska tolkas.

En mer detaljerad bild av bruttomodellen visas i Figur 2. Som tidigare nämnts innehåller inte bruttomodellen den ”verkliga” informationen utan bara beskrivningar av den verkliga informationen (metainformation).



Figur 2. Bruttomodellen med innehåll och ansvariga.

Bruttomodellen innehåller metainformation för två typer av information: Information *om insatser* respektive för insatser användbar *övrig information* (uppdelad branschvis). När det gäller *information om insatsen* beror den delvis på typen av insats. Eftersom bruttomodellen ska klara många typer av insatser kommer den att innehålla ett flertal alternativ för insatsinformation.

Den *övriga informationen* är strukturerad branschvis efter vilken bransch informationen kommer ifrån. För varje bransch utses en myndighet eller organisation som huvudansvarig för informationen. I ansvaret ingår att ta fram en begreppsmodell som beskriver och definierar de begrepp som används inom den branschen samt en informationsmodell som beskriver hur informationen ser ut och tolkas.

Modeller är bra, men de levererar inte information. Vid en insats behöver verklig information levereras och då via tjänster. Det är den branschansvariga myndigheten/organisationen som ansvarar för att det finns tillgängliga tjänster när informationen behövs. Tjänsterna ska finnas beskrivna i bruttomodellen med vad de erbjuder, med vilka egenskaper, vilken status och vilka resurskrav de har.

De ansvariga myndigheterna/organisationerna behöver dock inte erbjuda tjänsterna själva utan kan lägga ut ansvaret för respektive tjänst och/eller informationsmängd på andra myndigheter, organisationer eller företag. Däremot måste de hålla i den del av ändringshanteringen av bruttomodellen som rör deras respektive område.

4. Insatsinformation och standarder[1]

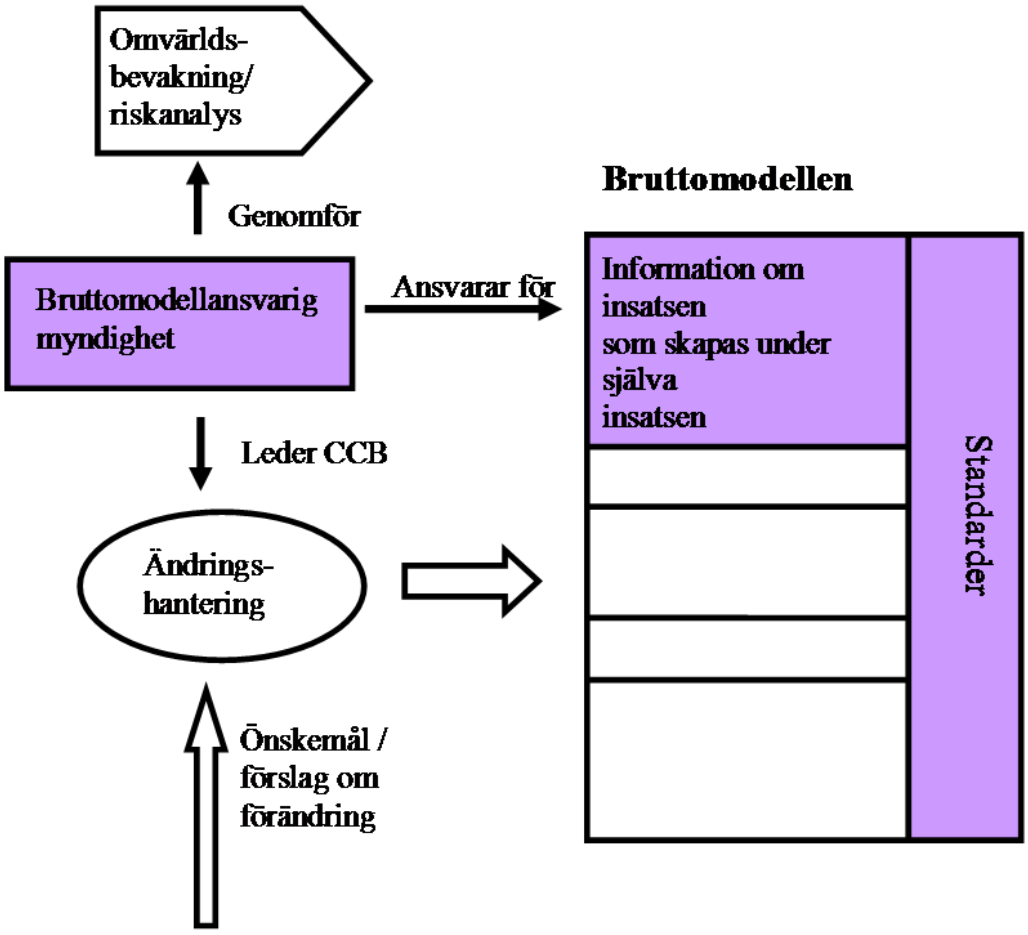
Den branschvisa informationen hanteras av någon ansvarig myndighet eller organisation inom respektive bransch. Men det behövs också någon myndighet som ansvarar för de gemensamma delarna i bruttomodellen. Information om insatser tillhör ingen speciell bransch men måste ändå hanteras på motsvarande sätt som den branschvisa informationen.

Att insatsinformationen inte tillhör någon speciell bransch underlättar inte utan ställer snarare högre krav på ansvar. På samma sätt som för övrig information måste det finnas både en begreppsmodell och en informationsmodell. Men till skillnad från övrig information är fler olika typer av parter och deltagare inblandade vilket leder till en högre risk för motstridiga krav och önskemål.

Det är därför viktigt att en myndighet ansvarar för informationen och förändringarna av den över tiden. Denna myndighet kommer också att ansvara för samordningen mellan förändringarna av den branschvisa informationen. Typiskt sker detta med ett Change Control Board (CCB).

En annan viktig komponent i bruttomodellen är den uppsättning standarder som skall användas. Det gäller både för begreppsmodeller och informationsmodeller och även för beskrivningarna av informationsmodellerna. Standarderna ska helst vara gemensamma för hela bruttomodellen och inte beroende på branschvis information eller insats,

[1] Se även Informationssamordning för myndighetssamverkan.



Figur 3. Användning och hantering av insatsinformation och standarder.

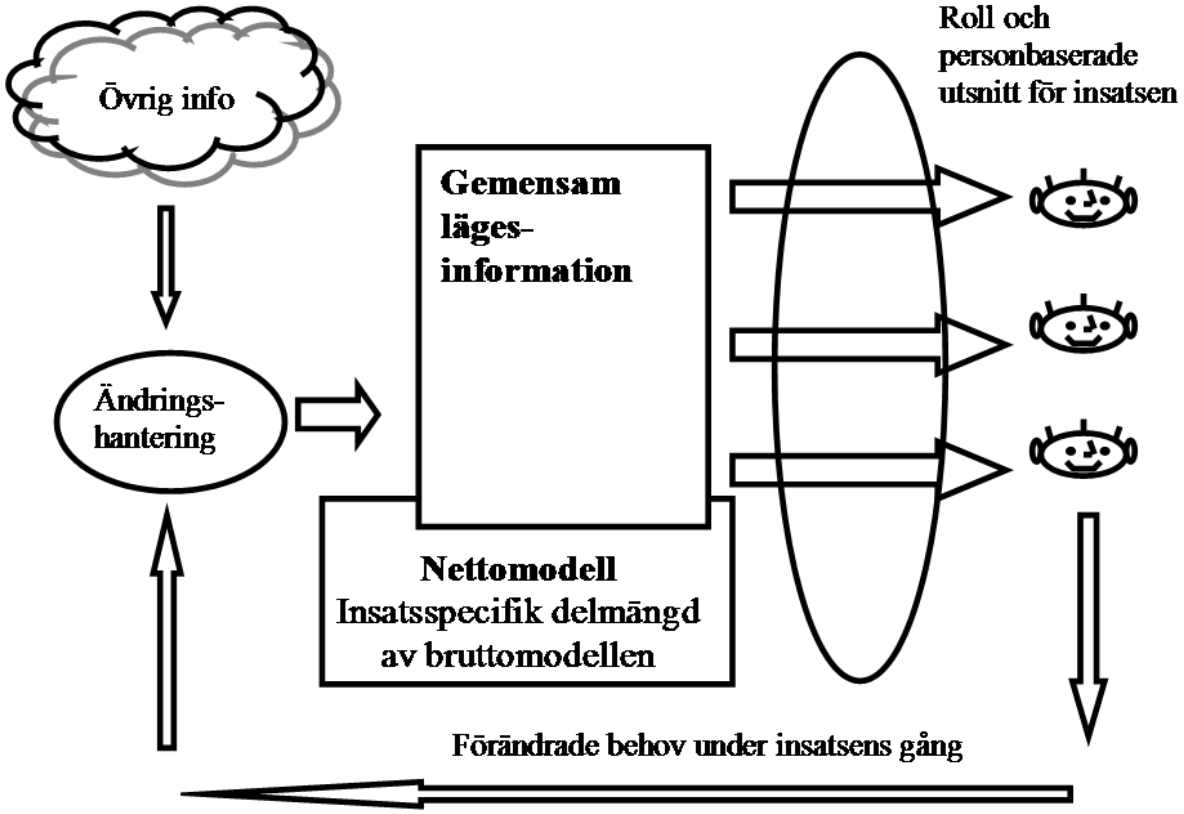
se Figur 3. Det som framför allt ska följa standarder är utbytet av den verkliga gemensamma lägesinformationen under pågående insats.

Urvalet av standarder som skall användas behöver också det ändringshanteras, förmodligen bäst av samma myndighet som har ansvaret för de informationsmodeller som används för att beskriva insatsinformationen.

Ytterligare en arbetsuppgift som faller på ansvarig myndighet är omvärldsbevakning och riskanalys för att se till att de insatser som är troliga finns med i bruttomodellen.

5. Nettomodellen

Bruttomodellen är teoretisk och täcker allt som kan förutses hända. Därför har den alldeles för brett innehåll för att vara användbar i en verklig insats. När en insats startar väljer man därför ut de delar av bruttomodellen som är intressanta för just den insatsen. Den insats-



Figur 4. Den teoretiska nettomodellen och den gemensamma lägesinformationen innehållande verklig information.

specifika delmängden av bruttomodellen bildar då en nettomodell för den specifika insatsen. Nettomodellen är insatsspecifik och innehåller beskrivningar av informationen.

För att skapa den gemensamma lägesinformationen (med verklig information) behövs tjänster som tillhandahåller informationen. Vilka tjänster som ska eller bör användas vid en insats (för att förse deltagarna med rätt information) finns med i den delmängd som väljs ut från bruttomodellen. Dessa tjänster är uttänkta i förväg och det är därför troligt att tjänsterna finns när händelsen inträffar. Om händelsen inte förutsetts finns ett stort antal förberedda tjänster att tillgå (i bruttomodellen) för att göra det bästa av situationen.

För en stab är det naturligt att ”läget” inkluderar flera samtidiga insatser. I de fall insatserna är väsentligt skilda åt kan flera nettomodeller användas parallellt. I annat fall används en gemensam nettomodell vilket ställer krav på att nettomodellen har plats för mer än en insats. Det gör också att de rollbaserade utsnitten (se Figur 4) ur den gemen-

samma lägesinformationen för deltagare, som endast berörs av en insats, enbart ska ge information om ”rätt” insats.

Under insatsens gång kan behov av mer information uppkomma. Det behövs därför en ändringshantering som utifrån vad insatsen handlar om och deltagarnas behov snabbt kan ändra nettomodellen och den gemensamma lägesinformationen för att uppfylla de uppkomna kraven och önskemålen.

Allmänt tillgänglig information, t.ex. från nätet kan också inkluderas i nettomodellen även om den inte finns i bruttomodellen. Om så är fallet kan den informationen se ut hur som helst, d v s den behöver inte följa informationsutbytesmodellens standarder och därför främst vara avsedd direkt för deltagarna. Någon part måste då ta ansvar för att hålla informationen uppdaterad. Detta kan ses som en form av service till övriga deltagare.

6. Slutsatser

För att få ett lyckat resultat under en insats behöver deltagarna i en insats ha information som är:

- Konsistent
- Tillgänglig
- Anpassad efter roll och person

Den modell för gemensam lägesinformation som beskrivits här erbjuder ett strukturerat arbetssätt som förbereder deltagarna för effektiv samverkan via tjänster med situationsanpassad lägesinformation.

Tillämpad säkerhet

Sammanfattning

Detta avsnitt behandlar använd säkerhetsdesign för att uppfylla säkerhetsmål. Exempel på detta är säkerhetsmekanismer för tjänstesamverkan (SSL), för sekretess, integritet och oavvislighet på kommunikation (mellan konsument och producent) respektive X.509 certifikat för identifiering och autentisering. I tillägg till det, behandlas implementering av bryggor för säker design samt regelverk som reglerar rättigheter.

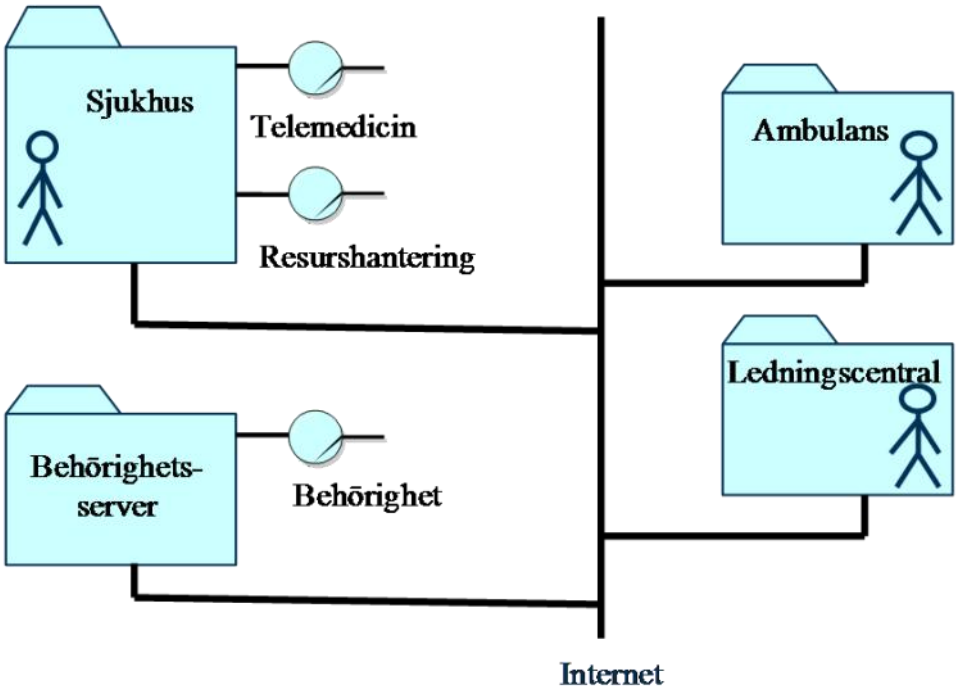
1. Inledning

Detta är ett exempel på en generisk säkerhetsdesign som följer säkerhetsarkitekturen i **Säkerhet** i Del 1. Designen baseras på öppna standarder vilket möjliggör realisering med olika typer av tekniska komponenter, t ex Open-Source eller kommersiella produkter. Utgående från denna generiska design är det tänkt att man kan göra specialiserade designer som i sin tur kan användas för att realisera prototypsystem som skall användas för metodutveckling.

Eftersom det är tänkt att detta exempel även skall kunna läsas av personer som inte har djupa kunskaper om IT-säkerhet så finns det en terminologilista sist i kapitel 7över de IT-säkerhetsbegrepp som används.

2. Systemöversikt

Nedanstående bild visar en systemöversikt över ett exempel där designen är tänkt att användas.



Figur 1. Systemöversikt över exempel.

Ett sjukhus är ett system-av-system som erbjuder två tjänster till behöriga externa användare:

- Telemedicintjänsten kan till exempel användas av ambulanspersonal för att ställa en första diagnos och sätta in lämpliga åtgärder redan på olycksplatsen.
- Resurshanteringstjänsten kan till exempel användas av en ledningscentral för att boka platser för brännskadade personer vid en stor olycka.

Behörighetsservern är ett tekniskt system som erbjuder en tjänst till behöriga användare:

- Behörighetstjänsten kan användas för att avgöra om en användare har behörighet till en viss tjänst eller inte.

Ambulans är ett system-av-system som bland annat kan konsumera tjänsten Telemedicin.

Ledningscentral är ett system-av-system som bland annat kan konsumera tjänsten Resurshantering.

3. Använda säkerhetsmekanismer

3.1. Tjänstesamverkan

X.509 certifikat i kombination med ett challenge response förfarande används för identifiering och autentisering av producenter och konsumenter av tjänster.

SSL (Secure Socket Layer) används för att åstadkomma sekretess, integritet och oavvislighet på kommunikation mellan konsumenter och producenter av tjänster.

Tjänsteproducenter använder sig av en central behörighetstjänst för att kontrollera om konsumenter har behörighet att använda den aktuella tjänsten.

3.1.1. Detaljerad tjänstesamverkan

En tjänstesamverkan mellan konsument och producent sker i följande steg:

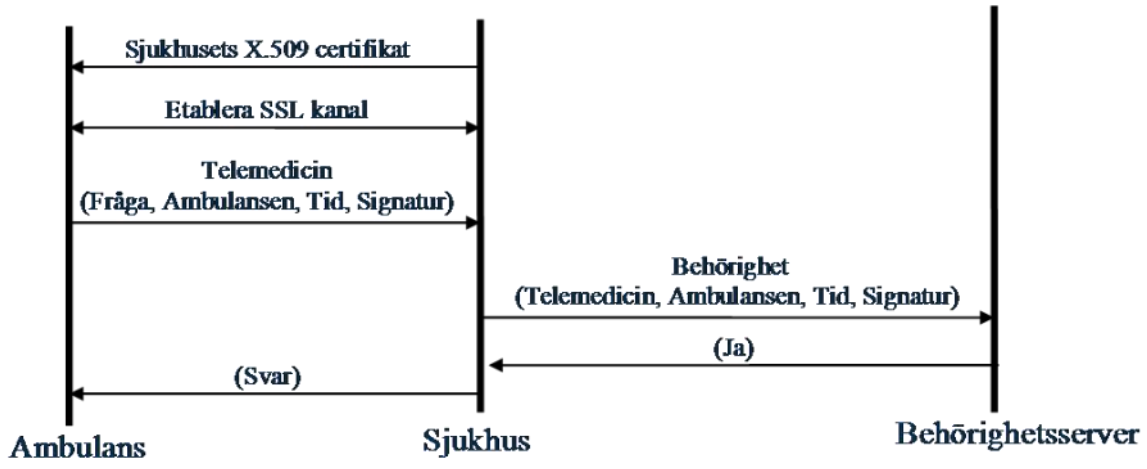
1. En SSL-tunnel mellan konsument och producent skapas m h a producentens X.509 certifikat.

2. I varje operation i varje tjänst läggs det till tre parametrar i linjeprotokollet
   - Konsumentens användarnamn, d v s det som finns i konsumentens X509 certifikat
   - Tidstämpel
   - Id för aktuell tjänsteinstans och tidstämpel krypterat med konsumentens privata nyckel
3. Dessa tre parametrar kompletterat med tjänsteinstansid i klartext skickas av producenten till behörighetstjänsten. (Kommunikationen mellan producenten och behörighetstjänsten skyddas på samma sätt som vid annan tjänstesamverkan förutom att behörighetstjänsten inte behöver fråga någon annan än sig själv om producenten har behörighet eller inte.)
4. Behörighetstjänsten kontrollerar att tjänsteinstansid och tidstämpel är korrekt krypterad med konsumentens privata nyckel, om så inte är fallet så skall konsumenten inte få behörighet att använda tjänsten. (Dessutom krävs det naturligtvis att konsumenten har nödvändiga behörigheter för aktuell tjänst).

Ovanstående illustreras av exemplet i Figur 2.

Behörighetstjänsten har alla användares publika certifikat lokalt lagrade.

De krypterade värdena på tjänsteinstansid är att betrakta som lösenord och skall behandlas som sådana ur säkerhetssynpunkt.

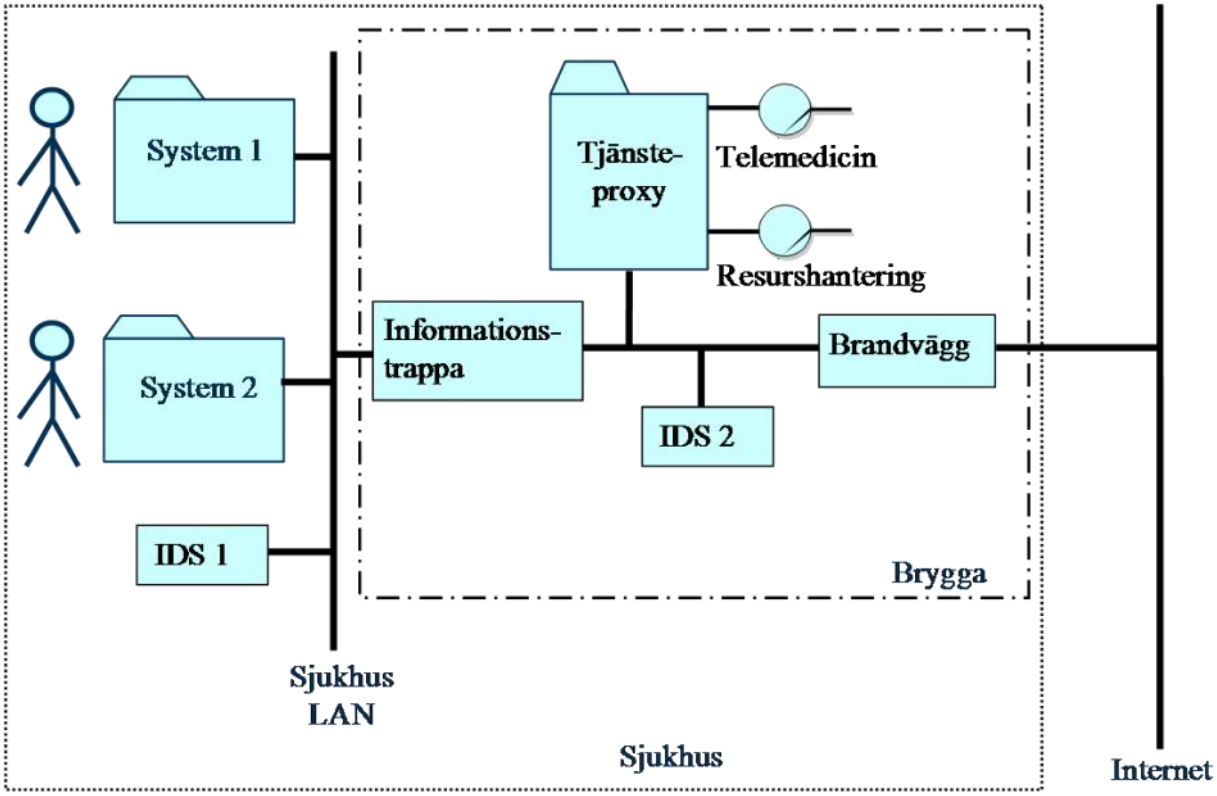


Figur 2. Exempel på en tjänstesamverkan

3.2. Bryggor

Denna design föreskriver att större system så som system-av-system normalt skall använda sig av bryggor när de dels erbjuder tjänster externt och dels använder externa tjänster. Bryggorna bör då uppfylla följande:

- Separering av bryggans nätverk från Internet och interna nätverk (genom t ex brandväggar).
- Kontroll av meddelanden som passerar till och från bryggan.
- Separering av logik som tillhandahåller externa tjänster från back-end applikationer.
- Intrångsdetektion på nätverksnivå (IDS).



Figur 3. Intern struktur för sjukhuset

Figur 3 visar på ett exempel av implementering av en brygga.

All kommunikation mellan sjukhusets lokala nätverk (LAN) och Internet skall gå genom bryggan. Informationstrappan kontrollerar all utgående trafik och säkerställer att all information som kommer externa intressenter tillhanda har en säkerhetsklassificering som tillåter detta.

Brandväggen spärrar all trafik från Internet som inte behövs för att externt kunna konsumera tjänsterna Telemedicin och Resurshantering.

IDS 2 är ett intrångsdetekteringssystem som övervakar nätverkstrafik och andra aktiviteter i bryggan. Alla aktiviteter som inte kan kopplas till konsumtion och produktion av tjänsterna Telemedicin och Resurshantering skall ge upphov till larm.

Tjänsteproxy är ett system som producerar tjänsterna Telemedicin och Resurshantering. Tjänsteproxy använder sig av System 1 och System 2 för att kunna producera dessa tjänster.

System 1 och System 2 är sjukhusets interna system.

IDS 1 är ett intrångsdetekteringssystem som övervakar trafik och andra aktiviteter på sjukhusets lokala nätverk. Detta system skall ge larm om det misstänker oönskade aktiviteter.

3.3. Regelverk

Säkerhetsdesignen föreskriver att följande regler är obligatoriska:

- Alla mänskliga användare får endast ta del av känslig information som de behöver för att kunna fullfölja sina arbetsuppgifter.
- Alla bryggor och andra publika tekniska system så som behörighetsservar skall testas och verifieras så att de uppfyller EAL2 enligt Common Criteria.

4. Uppfyllnad av säkerhetsmål

- Sekretess uppfylls genom att SSL används för att kryptera all extern trafik.
- Integritet uppfylls genom att SSL används för att kryptera all extern trafik.
- Oavvislighet för producenter uppfylls genom att deras X.509 certifikat används för att skapa SSL-kanaler.
- Oavvislighet för konsumenter uppfylls genom att varje meddelande från konsument till producent tidstämplas och signeras med konsuments privata nyckel.

- Identifiering/Autentisering av producenter uppfylls genom att deras X.509 certifikat används för att skapa SSL-kanaler.
- Identifiering/Autentisering av konsumenter uppfylls genom att varje meddelande från konsument till producent tidstämplas och signeras med konsuments privata nyckel.
- Behörighet/Åtkomstkontroll uppfylls genom att producenter först kontrollerar med behörighetstjänsten om konsumenter har behörighet och sedan verkställer behörighetsbesluten.
- Tillgänglighet uppfylls med hjälp av brandväggen och intrångsdetekteringssystemet i bryggan.
- Säkerhet för personer och övrig omgivning hanteras genom att alla bryggor och publika tekniska system skall uppfylla EAL2 enligt Common Criteria.
- Personlig integritet hanteras genom att användare är belagda med förbud att ta del av känslig information som de inte har behörighet.
- Assurans hanteras genom att alla bryggor och publika tekniska system skall uppfylla EAL2 enligt Common Criteria.

5. Identifierade säkerhetsobjekt

Följande säkerhetsobjekt är identifierade:

- Användning av tjänsten Telemedicin
- Användning av tjänsten Resurshantering
- Användning av tjänsten Behörighetstjänst
- Behörighetskrav för tjänster
- Roller och deras behörigheter
- Tilldelning av roller till användare
- Användares privata krypteringsnycklar

6. Säkerhetsadministration

Två stycken områden för säkerhetsadministration har identifierats:

6.1. Övergripande CA (Certificate Authority)

- Skapa/ändra/ta bort användare
- Delegera CA rättigheter
- Godkänna andra CA

6.2. Behörighetsadministration

- Definition av behörighetskrav för tjänster
- Definition av roller och deras behörigheter
- Tilldelning av roller till användare

7. Terminologi

assymetrisk kryptering Innebär att man använder sig av en krypteringsalgoritm som har olika nycklar för kryptering respektive dekryptering av meddelande, d v s krypterar man med den ena nyckeln så måste man dekryptera med den andra och vice versa. I IT-säkerhets sammanhang utnyttjas detta genom att varje användare har ett sådant nyckelpar där den ena nyckeln är privat och den andra är publik.

X.509 Ett protokoll som bland annat definierar format på certifikat för publika krypteringsnycklar.

SSL Secure Socket Layer. Ett protokoll som används för att kryptera TCP/IP trafik ur både sekretess och integritets synpunkt. Det är valbart om bara server eller både server och klient skall autentisera sig. SSL använder sig av assymetrisk kryptering och X.509 certifikat.

CA Certificate Authority. En som utfärdar (signerar) certifikat och därmed på något sätt går i god certifikatinnehavarens identitet.

challenge response Ett challenge response förfarande kan användas för att bevisa användares identitet med hjälp av assymetriska nycklar enligt följande. Användare A bestämmer en utma-

ning i form av ett slumpmässigt tal och skickar detta till användare B. Användare B krypterar utmaningen med sin privata nyckel och skickar det krypterade värdet till användare A. Användare A dekrypterar den krypterade utmaningen med användare Bs publika nyckel och om resultatet av detta blir utmaningen i klartext så har användare B bevisat sin identitet för användare A.

IDS Intrusion Detection System. Ett system som används för att övervaka och upptäcka oönskad nätverkstrafik.

Common Criteria Common Criteria definierar en standard på hur krav på IT-säkerhet skall definieras och verifieras för olika säkerhetsnivåer.

EAL2 Evaluation Assurance Level 2. Innebär att man ur säkerhetssynpunkt testar att system dels fungerar rent funktionellt och dels att de är byggda enligt bästa kommersiella praxis.

Riskhantering

Sammanfattning

För att begreppet risk ska kunna användas till att åstadkomma samverkan behöver ett antal riskrelaterade begrepp ensas. I detta avsnitt ges att antal definitioner för begrepp för riskhantering. En riskhanteringsprocess med aktiviteter presenteras också. Vilka risker man hanterar i en så kallad riskprofil är kontextberoende och tidsberoende.

1. Inledning

Risk är ett begrepp som har många betydelser. Risk används slentrianmässigt i en mängd olika sammanhang utan att vara strikt definierat. För att begreppet risk ska kunna användas till att åstadkomma samverkan behöver ett antal riskrelaterade begrepp ensas. Ansatsen är att här använda ett systemperspektiv som är till för att kunna göra olika typer av analyser och optimeringar.

Här har samlats definitioner på **begrepp** som anknyter till risk[1]. Även aspekter relaterade till värde har tagits med i detta arbete för att underlätta en gemensam syn på risk.

2. Risk

Med risk avser vi en oönskad händelse. Vi kan åsätta händelsen en sannolikhet att den ska inträffa. Vi har också en uppfattning om konsekvensen eller effekten av händelsen.

Definition: Risk är en oönskad händelse med estimerad sannolikhet samt en känd effekt.

3. Riskfaktorer

Att en risk identifierats betyder inte att den betraktas av alla på samman sätt. Till exempel om vi genomför spaningsuppdrag riskerar vi att bli utan förnödenheter. Det tillståndet är en oönskad händelse om den betraktas från det egna perspektivet. Däremot skulle händelsen mycket väl kunna uppfattas som en önskad händelse av motståndaren.

Till de komponenter som används för att bygga situationsanpassade system finns beskrivningar av egenskaper kopplade. Dessa beskrivningar används vid systemoptimeringen. Vissa av dessa egenskaper kan orsaka oönskade händelser, speciellt för tekniska komponenter. T.ex. kan ett fysiskt lagringsmedia för information vid temperaturer över 50 grader börja generera slumpmässiga läsfel. Vi skulle förmodligen säga att risken för läsfel är stor om det blir för varmt.

För att kunna användas vid analys av vilka risker ett visst situationsanpassat system kommer att ha behöver beskrivningarna av de egenskaper som kan orsaka oönskade händelser kompletteras. Med någon

[1] Utgående från Försvarsmaktens arkitektur, FMA.

form av påstående eller värde som gör det möjligt att utgående från det kontext där systemet är tänkt att användas åsätta de oönskade händelserna sannolikheter och bedöma deras effekt. Ex: Det tidigare nämnda lagringsmediet har vid ”normal” temperatur en angiven sannolikhet för slumpmässiga läsfel. Det börjar efter 50 grader generera fler slumpmässiga läsfel. Antalet läsfel fördubblas för var 10:e grad över 50 grader. Denna information gör det möjligt att bedöma risken för slumpmässiga läsfel vid olika användningar.

Riskfaktor: En beskrivning bara knuten till egenskaper hos teknisk komponent som beskriver en egenskapen som kan ge upphov till en oönskade händelse. Detta kompletterat med ett påstående eller värde kopplat till egenskapen som gör det möjligt att bedöma sannolikheterna för de oönskade händelserna och deras effekt beroende på hur systemet skall användas,.

En riskfaktor har ingen sannolikhet åsatt, utan information som gör det möjligt att bedöma hur stor sannolikheten är att oönskade händelser inträffar beroende på hur komponenten används, dvs. på kontext.

Att åsätta en oönskad händelse en bedömd sannolikhet och en bedömd effekt innebär att identifiera en risk.

Riskfaktorer är föränderliga över tiden. De kan sägas spegla den samlade kunskapen om vad man kan råka ut för när man använder den tekniska komponenten.

4. Primära risker

När riskerna med ett system studeras kommer vissa risker att identifieras som ”showstoppers”, dvs. konsekvenserna av dessa oönskade händelser är så allvarliga att de i princip till varje pris måste undvikas. Sådana risker benämns primära risker.

Det situationsanpassade systemets förmåga att avge verkan kan omintetgöras av primära risker. Även de stödsystem som ett situationsanpassat system är beroende av kan ha primära risker. Dvs. det finns risker som om de utfaller medför att ett stödsystem inte längre avger verkan. Detta i sin tur kan bli en risk i det situationsanpassade systemet. Det är dock viktigt att observera att ett stödsystem är ansvarigt för sin egen riskhantering. Dvs. den primära risken hanteras i det stödsystem som har risken men risken att inte få efterfrågad verkan från ett stödsystem hanteras i det situationsanpassade systemet. Om

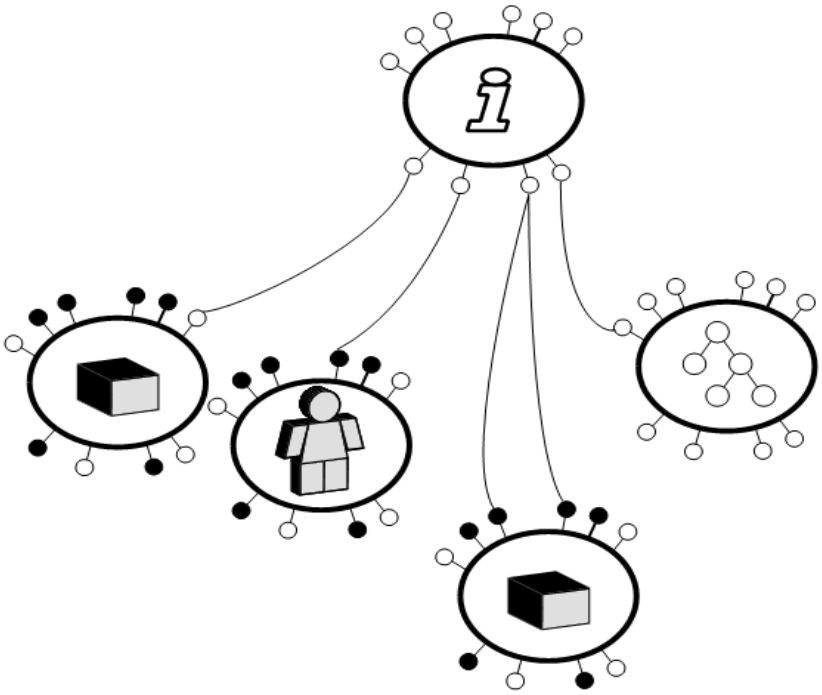
en primär risk i ett stödsystem också skulle medföra en primär risk i det situationsanpassade system har vi byggt ett system som inte har kontroll över sin egen överlevnad. Den ursprungliga primära risken hanteras därför alltid i det stödsystem som äger risken.

Primära risker är en viktig komponent vid systemoptimeringen. Ett system med flera primära risker med icke försumbara sannolikheter är förmodligen ett system som inte kommer att avge förväntad verkan.

5. Deriverade risker

Olika komponenter, både tekniska komponenter och andra typer av komponenter har i ett Situationsanpassat system relationer till varandra. Relationerna används vid systemoptimeringen för att utvärdera hur de tekniska komponenternas riskfaktorer påverkar övriga komponenter i det situationsanpassade system som skall skapas.

Till exempel behöver en informationskomponent ha relationer till de tekniska komponenter som är bärarmedia. Om kartinformationen för ett system är lagrad på ett bärarmedia som är känsligt för låga temperaturer innebär detta en ökad risk att systemet under vissa perioder inte kommer att ha tillgång till kartinformation om systemet används vintertid i övre norrland.



Figur 1. Relationer mellan systemkomponenter innebär även relationer mellan risker.

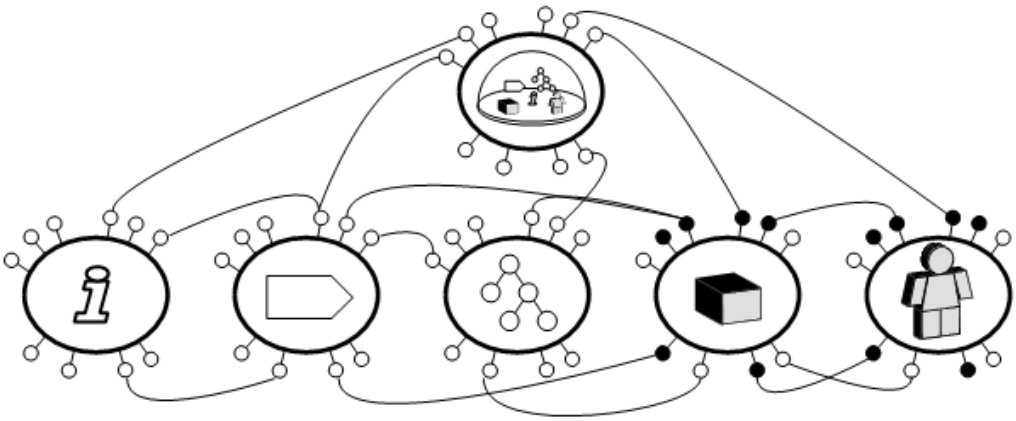
Den typ av association till tekniska komponenter som har risker benämns deriverade risker. I exemplet ovan har den kartinformation som är lagrad på det köldkänsliga bärarmediet en deriverad risk. Det är viktigt att observera att kartinformationen i sig inte har någon risk, byts bärarmediet i exemplet ovan elimineras den deriverade risken.

Även stödsystem bidrar med deriverade risker via sina tjänstegränsytor. Detta innebär att ett situationsanpassat system också kan påverkas av riskhanteringen i de stödsystem som används för olika tjänster.

Den totala mängden risker som påverkar ett system består alltså både av risker som är deriverade från komponenterna i systemet och risker som är deriverade från stödsystemen via de använda tjänstegränsytorna.

6. Sammansatta risker

Varje komponent har ett antal risker kopplade till sig, som i sin tur är beskrivna som riskfaktorer. De risker som är kopplade till en komponent benämns riskkluster. När en komponent väljs för att ingå i ett system kommer komponentens riskkluster att bidra till systemets samlade risker.



Figur 2. Associerade risker till en komponent, s k riskkluster behöver bedömas när komponenten integreras till ett sammansatt system.

En och samma risk kan ingå i olika riskkluster. Alla fordon med luftfyllda däck kan t.ex. få punktering. Detta innebär att en viss risk, som för varje enskild komponent betraktas som försumbar, kan bli väsentlig i ett systemperspektiv.

7. Riskprofiler

Vi har en mängd risker förknippade med vår verksamhet. För de flesta risker är sannolikheten för att risken inträffar så låg, att vi väljer att helt bortse från den. Eller konsekvensen av ett utfall är så liten, att vi väljer att bortse från risken.

Den grad av risk som vi är beredda att bortse från är beroende av hur vårt situationsanpassade system används i ett givet sammanhang. De risker som blir kvar, dvs. de man inte kan bortse från, och som således behöver riskhanteras benämns riskprofil.

Yttre händelser kan förändra sannolikheten för en risk. Även effekten av en risk kan förändras av yttre händelser. Om en risk inträffar som gör att vi tvingas förbruka en del av våra reserver ökar effekten av de övriga risker där ett utfall innebär att vi även nu behöver förbruka delar av vår reserv. Reserven har ju blivit mindre. Detta innebär att ett situationsanpassat systems riskprofil är färskvara. Riskprofilen, eller snarare dess grafiska representation, kan betraktas som ett verktyg för att kommunicera hur yttre händelser påverkar ett SitSyst ur ett riskperspektiv.

Riskprofilen är alltså kontextberoende och tidsberoende.

8. Hot

Ett hot kan beskrivas som en möjlig handling med uppsåt att tillfoga skada. Om ett hot skall tas på allvar måste den händelse som ingår i hotet verkligen kunna inträffa och dessutom vara oönskad.

Hotet ”Om jag inte får xxxxx skall jag få alla Afrikas tigrar att kasta sig över dig” är inte speciellt imponerande även om konsekvensen kan framstå som mindre lockande. Sannolikheten för händelsen är lika med noll. Hotet ”Om inte xxxx så kommer månen att trilla ner i skallen på dig” är inte mycket bättre. Däremot är det mer substans i ”Om inte xxxx så kommer din bil att skadas”. Ett hot som man troligen har anledning att ta på allvar, speciellt om man har en ny bil.

Den sista händelsen, att min bil på något sätt skall komma till skada är både oönskad och har en sannolikhet att inträffa som är större än noll. Det är alltså en risk, som de flesta av oss riskhanterar genom att teckna en försäkring.

Ett hot förstärker en risk, antingen genom att öka sannolikheten för utfall eller genom att öka effekten av utfallet.

Ett hot kan *definieras* som: En utsaga om att öka sannolikheten för effekten av en risk.

Detta innebär att en risk som inte finns med i ett situationsanpassat systems riskprofil efter hotet kan dyka upp i riskprofilen. Att på normalt sätt hantera den nya risken blir en naturlig del av hanteringen av hotet.

Eftersom ett hot ökar väntevärdet för effekten av en risk kan detta användas för att värdera olika hot mot varandra och därmed få ett stöd för beslut om att sätta in motåtgärder.

Ett hot baseras på någon form av ond vilja. Att hantera denna onda vilja är en annan del i hanteringen av ett hot. Detta behandlas dock inte vidare i denna utredning.

9. Osäkerhet

När ett situationsanpassat system skapas föregås detta av en systemoptimering. Syftet är att hitta ”bästa möjliga” konfiguration utgående från de komponenter som finns tillgängliga. Det finns en acceptans för att det situationsanpassade system som skapas inte kommer att kunna avge önskad verkan fullt ut beroende på att vissa av de komponenter som kommer att ingå i systemet inte på alla punkter har önskvärda egenskaper eller prestanda.

I ovanstående resonemang finns varken risk eller osäkerhet, man vet vad man behöver för att få ett situationsanpassat system som kan avge full verkan och man vet också vad som saknas hos de komponenter man väljer.

Verkligheten är inte lika gynnsam, vi kommer inte att med säkerhet veta vilka prestanda de komponenter vi väljer till vårt situationsanpassade system kommer att ha i det kontext där systemet skall verka.

Några exempel:

En positionsbestämningsutrustning har en angiven noggrannhet, +/- 2m t.ex., under vissa bestämda väderbetingelser.

Ett antal fordon som skall användas för transporter har den nödvändiga kapaciteten, men eftersom vi räknar med att ”hyra in” fordonen

från en extern leverantör har vi inte kontroll över underhållsstatus och därför inte heller över vilken tillgänglighet vi kommer få.

Att bygga med komponenter enligt ovan introducerar osäkerhet. Vi vet inte med säkerhet vilken effekt vårt situationsanpassade system egentligen kommer att kunna avge. Det är beroende av osäkra faktorer som vi inte har kontroll över.

Att vädret inte är tillräckligt bra för att vår positionsbestämningsutrustning skall ha fulla prestanda är inte en enskild händelse som kan åsättas en sannolikhet. Vädret kommer att variera över tiden vilket gör att de prestanda vi kan förvänta oss också kommer att variera över tiden.

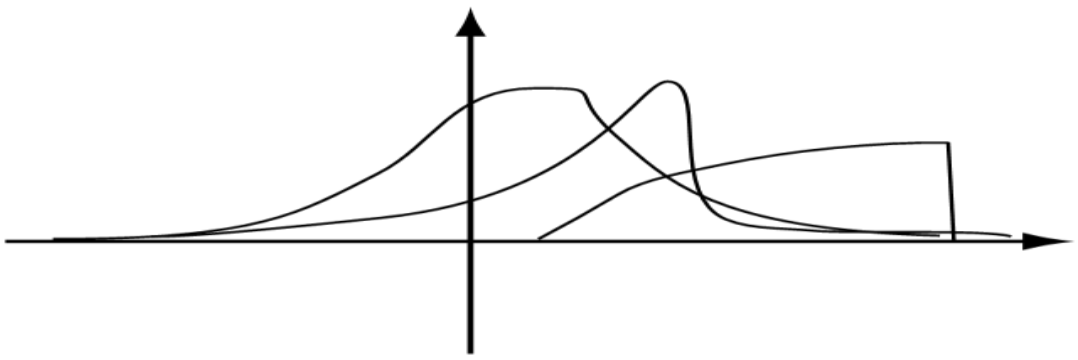
Det oklara underhållsläget av fordonen ovan kommer inte att innebära att ett fordon kommer att stanna vid ett tillfälle, det kommer att medföra att vår transportkapacitet kommer att variera över tiden och påverka vårt situationsanpassade system.

Den prestanda som vi kan förvänta oss från de komponenter som är behäftade med osäkerhet kan beskrivas av fördelningsfunktioner.

Att prestanda hos vissa komponenter kommer att variera till synes slumpmässigt innebär också att den verkan som vårt situationsanpassat system kommer att kunna avge kommer att variera påverkat av de komponenter som är behäftade med osäkerhet.

De fördelningsfunktioner som beskriver osäkerheten i prestanda hos de ingående komponenterna kan vägas samman och användas för att skapa en fördelningsfunktion som gör det möjligt att ange sannolikheten för olika grad av verkan för vårt situationsanpassat system.

Den fördelningsfunktion som beskriver förväntad verkan för vårt situationsanpassade system benämns *verkansvärde*.



Figur 3. Exempel på fördelningsfunktioner.

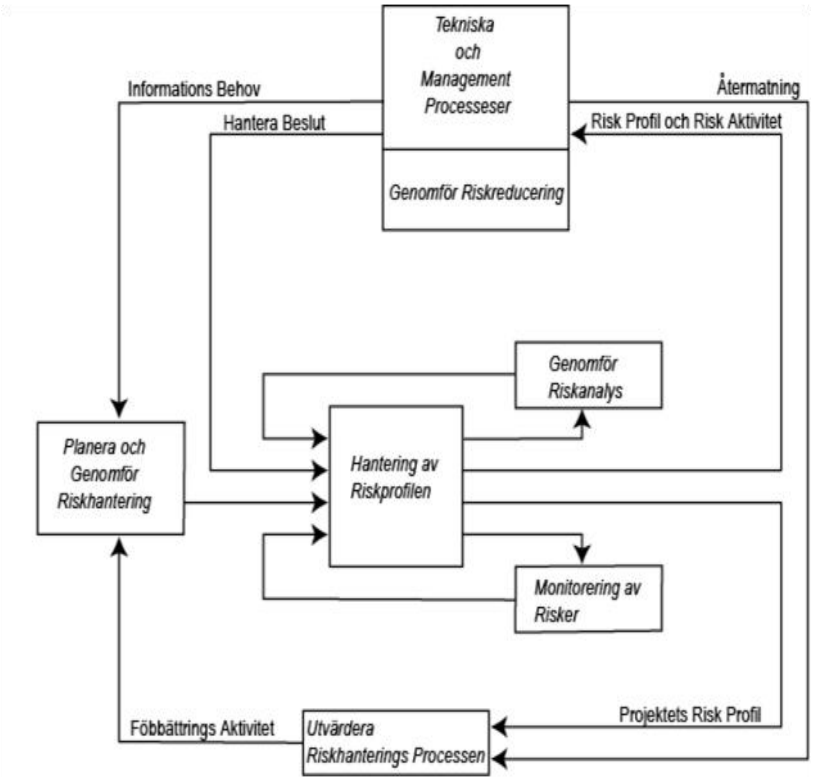
Vid systemoptimeringen kan verkansvärdet användas som en del av det beslutsunderlag som behövs för att avgöra om ett situationsanpassat system, som innehåller komponenter behäftade med osäkerhet, är ”tillräckligt bra”.

10. Riskhanteringsprocess

Riskhantering är en kontinuerlig process för att systematiskt adressera risker som system utsätts för under dess livscykel, i synnerhet där systemet är i aktiv användning. Processen omfattar följande aktiviteter:

- Planera och genomför riskhantering.
- Hantering av riskprofilen.
- Genomför riskanalys.
- Monitorering av risker.
- Genomför riskreducering.
- Utvärdera riskhanteringsprocessen.

Dessa processteg, som visas i figuren nedan, beskrivs översiktligt här.



Figur 4. Aktiviteter eller delsteg inom Riskhanteringsprocessen.

De styrande och tekniska processerna spänner upp krav på information för att kunna fatta beslut som riskhantering omfattar och måste stödja.

Dessa krav på information berör flera aktiviteter som ”Planera och genomför riskhantering” och ”Hantering av riskprofil”. I aktiviteten ”Planering och genomför riskhantering” sätts målsättningen upp för de generella riktlinjerna för riskhantering ska genomföras, procedurer som ska användas, vilka specifika tekniker och så vidare.

Under aktiviteten ”hantera projektet riskprofil” registreras historien och de aktuella sammanhangen och risktillstånden. Projektets riskprofil inkluderar den totala mängden individuella riskprofiler för nuvarande och historisk information rörande en individuell risk, vilket i sin tur omfattar all risktillstånd.

Projektets riskprofil uppdateras kontinuerligt och underhålls genom aktiviteten ”genomför riskanalys” som identifierar risker, bestämmer sannolikheten och konsekvenserna, uppskattar exponeringen samt preparera aktioner för att rekommendera hantering för att få riskerna över deras riskgränser.

Rekommenderade åtgärder tillsammans med status för andra risker och deras åtgärdsstatus överförs till ledningen för granskning. Ledningen beslutar vilken riskhanteringsåtgärder som ska genomföras för alla risker som är oacceptabla. Planer för riskåtgärder sätts upp för samtliga risker som kräver åtgärder. Dessa planer koordineras tillsammans med andra typer av planer och pågående aktiviteter.

Alla risker monitoreras kontinuerligt till dess de inte behöver följas under aktiviteten ”genomför risk monitorering”. Dessutom följs nya risker upp.

Periodisk evaluering av riskhanteringsprocessen krävs för att säkerställa effektiviteten. Under aktiviteten ”evaluera riskhanteringsprocessen” samlas information, inklusive användares åsikter och respons, för förbättring av processen och organisation samt projektets förmåga att hantera risk.

Förbättring definierad som resultatet av utvärdering är implementerad inom aktiviteten ”planering och implementering av riskhantering”.

Riskhanteringsprocessen för programvara används kontinuerligt genom hela produktens livscykel. Aktiviteter och uppgifter inom risk-

hanteringsprocessen interagerar med riskhanteringsprocessen för individuella risker på ett iterativt sätt så fort som riskhanteringsprocessen har tagit sin början. Till exempel kan en risk bli värderad flera gånger under aktiviteten ”genomför riskanalys” för att man har samlat kunskap om risken av genomförd analys. Riskhanteringsprocessen är inte en vattenfallsprocess utan flödettkan ske iterativt med olika fokusering i olika delsteg.

11. Riskhanteringsexempel

Att hantera risker innebär att med olika åtgärder minska väntevärdet för effekten av ett riskutfall. För att åstadkomma detta kan man antingen minska sannolikheten för att en risk utfaller eller minska effekten av ett riskutfall.

Exempel:

Vi skall åka till landet med bilen och vill absolut komma fram i tid. Vi bedömer att det finns två risker som gör att vi kan bli försenade. Bensinstopp är en risk, vi har inte riktigt koll på hur bränslemätaren fungerar. En annan risk är punktering, vi har inte pumpat reservhjulet de senaste fem åren.

För att hantera dessa risker svänger vi in på macken når vi åker. Vi börjar med att tanka, då vet vi att vi kommer fram oberoende av vad bensinmätaren visar. Vi har nu minskat sannolikheten för bensinstopp men inte gjort något åt effekten. Konsekvenserna av att bli stående är fortfarande lika allvarliga men vi känner oss säkra på att det inte kommer att inträffa, p g a bensinstopp.

Sedan pumpar vi reservhjulet och säkerställer att det är i bra skick. Vi har inte på något sätt minskat sannolikheten för punktering men säkerställt att en punktering inte gör att vi blir stående. Vi har minskat effekten av en punktering.

När vi sedan åker vidare känner vi oss rätt säkra på att komma fram i tid, vi har för de båda identifierade riskerna minskat väntevärdet av effekten av riskerna till en nivå som vi bedömt som acceptabel. Absolut säkra på att komma fram i tid kan vi ändå inte vara, två punkteringar t.ex. gör att vi blir stående.

Del 3

Utvecklingsmiljö

Tjänstebaserad utvecklingsmiljö för prov och försök

De tidigare delarna i ramverket har fokuserat på arkitektur och principer mestadels på ett teoretiskt plan. För att fullt ut förstå hur samverkan mellan parter enligt de beskrivna principerna kan fungera i verkligheten och vilka arbetsmetoder som kan användas behöver man även utföra prov och försök.

Att någon utför ordentliga prov och försök och delger resultatet till intresserade är bra. Men ännu bättre är att varje myndighet eller organisation gör prov och försök tillsammans med de parter man skulle vilja samverka med. Därför ingår i detta ramverk även en integrationsmiljö för utveckling och användning av tjänster (OpenSIS) och ett par tjänster som tillsammans med lämplig datorutrustning bildar en teknisk informationsinfrastruktur. Senare i detta dokument finns dessutom tips på fler användbara tjänster.

OpenSIS är framtagen för att testa olika koncept och principer. Den är i sig ett koncept som testats i olika varianter. Det kan därför finnas skillnader mellan beskrivna principer och aktuell implementering i OpenSIS.

Försvarsmakten har vid prov och försök med framgång använt OpenSIS inom ramen för Ledsyst vid UtvC i Enköping. Den har använts för att prova nya (nätverksbaserade) metoder. Dessa övningar har innefattat upp till 300 samtidiga ledningsplatser under en dag. Däremot är OpenSIS i sin nuvarande form inte avsedd för användning i skarp drift.

Här följer en kort beskrivning av OpenSIS. Mer information finns i dokumentationen som medföljer OpenSIS och respektive tjänst.

1. OpenSIS

OpenSIS är den programvara som tillsammans med tjänster och hårdvara bildar en teknisk informationsinfrastruktur. Den består av en kärna, innehållande det som är nödvändigt för säker samverkan mellan system (från olika myndigheter/organisationer/företag) samt verktyg för att hantera samverkan mellan systemen. Dessutom finns ett

antal tjänster som stödjer konceptet med situationsanpassade system (system av system).

1.1. Kärnan

Kärnan är grunden för informationsinfrastrukturen och omfattar den programvara som behövs för säker samverkan, vilket är de två obligatoriska tjänsterna, namntjänst och behörighetstjänst, samt det ”klister” som binder samman alla delar till en infrastruktur. Namntjänst och behörighetstjänst samt funktionalitet för autentisering, sekretess och integritet är utbytbara. Alla applikationer som antingen erbjuder eller utnyttjar tjänster måste köras tillsammans med kärnan.

1.1.1. Namntjänst (Service discovery)

Namntjänsten är informationsinfrastrukturens katalogtjänst där alla tjänster som erbjuds för tillfället (och följer OpenSIS) är registrerade. Den används för att systemen ska hitta tjänster som erbjuds av andra system i runtime.

1.1.2. Behörighetstjänst (Authorization service)

Behörighetstjänsten ansvarar för att hålla reda på vem som får göra vad. Lägga till och ändra behörigheter görs via ett verktyg, behörighetseditorn, som medföljer.

1.2. Sitsystbyggaren

Sitsystbyggaren är ett verktyg för att bygga situationsanpassade system (system av system) och situationsanpassa presentation av information. I båda fallen går det dels att skapa konfigurationer i förväg och spara för att använda vid senare tillfälle och dels att göra anpassningar under drift.

2. Tjänster och presentationskomponenter

För att kunna utföra prov och försök behöver man dessutom ett antal tjänster och presentationskomponenter. Vilka tjänster och komponenter man behöver beror på vilken domän försöken utförs inom. En del tjänster/komponenter kommer det dock att finnas behov av (efter en del justeringar) oberoende av domän t ex karttjänst.

2.1. Tjänster levererade tillsammans med OpenSIS

Förutom de två obligatoriska tjänsterna i kärnan finns ett antal tjänster som levereras med OpenSIS. För att underlätta skapandet av anpassade presentationer innehåller leveransen även en uppsättning presentationskomponenter och ett ramverk för att utveckla presentationskomponenter för Sitsystbyggaren.

2.2. Tjänster, system och MMI-komponenter från Ledsyst

Ledsyst (och då främst LedsystT) har tagit fram ett antal tjänstedefinitioner, system som producerar tjänsterna samt MMI-komponenter som visar informationen. Bland dessa finns det tjänster, system och MMI-komponenter som borde kunna användas i fler domäner än försvarsdomänen, en del direkt, en del med justeringar och andra som inspiration.

Följande är en lista på de tjänster, system och MMI-komponenter framtagna inom Ledsyst som borde kunna användas direkt eller med små justeringar.

Geodata

Inkluderar följande tjänster/MMI:er/system:

- Geo_Analysis (tjänst)
  Gör olika analyser av geodata exempelvis beräkning av fri siktsträcka.
- Geo_Coding (tjänst)
  Adressökning
- Geo_Data_Raster_Map (tjänst)
  Tillhandahåller olika typer av kartdata, t ex sjökort och markkartor.
- MMI_Situation_Picture (MMI)
  Tillåter användare att skapa grafiska planer och målbilder.

I skrivande stund är systemet som tillhandahåller tjänsterna (GIS System Spatial Ace) realiserad med Carmentas kartmotor (Spatial Ace) vilken kräver licens från Carmenta. Eventuellt kan kartmotorn bytas ut och ersättas med en som inte kräver licens (open source).

Rapporter

Inkluderar följande tjänster/MMI:er/system:

- Report (tjänst)
  Skapar och hanterar rapporter.
- Report_template (tjänst)
  Skapar och hanterar rapportmallar.
- MMI_Report (MMI)
  Tillåter användare att skapa rapporter och notifiera befattningshavare om när nya rapporter skapats.
- Report_Server (system)
  Erbjuder tjänsterna Report och Report_template.

Nya (civila) typer av rapporter kan behöva läggas till.

Ritverktyg

Inkluderar följande tjänster/MMI:er/system:

- Geo_Info_Exchange (tjänst)
  Hanterar objekt på en lägeskarta.
- Symbol_Library (tjänst)
  Tillhandahåller symboler.
- MMI_Tactical_Drawing (MMI)
  Tillåter användare att presentera målspår, plottar och olika enheters status.
- Geo_Info_Exchange_Server (system)
  Håller objekt och erbjuder tjänsten Geo_Info_Exchange.

Behöver uppdateras med civila symboler.

Övrigt

Dessutom finns två stödsystem som kan vara användbara:

- NBF-likaren
  Simulerar system som både kan producera och konsumera tjänster.
- http-brygga
  Erbjuder tjänster (enligt OpenSIS) för att hämta webbsidor (vilken som helst).

Referenser

Följande dokument är producerade inom FMV projekt LedsystT. LedsystT är ett projekt för konceptutveckling av den tekniska arkitekturen för Försvarsmaktens ledningssystem. Målsättningen är att huvuddelen av dokumenten skall bli publika (frisläppta och tillgängliga). Vid denna tryckning är ännu så ej fallet. Ett antal av dokumenten är dock frisläppta och tillgängliga i en tidigare utgåva via FMV hemsida. Dessa dokument är namnmässigt lika men LT numret är ersatt med ett FMV nummer.

[1] LedsystT, LT1K P06-0003 *Framework FMLS Metadata* 2.0

[2] LedsystT, LT1K P06-0317 *Description framework for NERE metadata specifications for technical and software systems* 1.0

[3] LedsystT, LT1K P05-0446 Development of *NERE metadata specifications for technical and software systems* 3.0

[4] LedsystT, LT1K P04-0278 *Framework Service Description* 7.0

[5] LedsystT, LT1K P04-0281 *Framework System Description* 3.0

[6] LedsystT, LT1K P05-0026 *SOA for NBD Principles* 3.0

[7] LedsystT, LT1K P05-0075 *Systems Engineering Vision FMLS 2010* 5.0

[8] LedsystT, LT1K P05-0074 *Overarching Architecture* 4.0

[9] LedsystT, LT1K P06-0323 *Framework for Common Information Exchange Standards - CIES* 2.0

[10] LedsystT, LT1K P04-0313 *Framework Information Exchange Models* 5.0

[11] LedsystT, LT1K P06-0145 *Design Overview* 1.0

[12] LedsystT, LT1K P05-0443 *NCES Reference Architecture* 3.0

[13] LedsystT, LT1K P06-0051 *Design Rule Interoperability* 2.0

[14] LedsystT, LT1K P06-0008 *Design Rule Legacy Integration* 1.0

[15] LedsystT, LT1K P06-0050 *Design Rule Flexibility* 2.0

[16] LedsystT, LT1K P06-0106 *Design Rule Mobility* 3.0

[17] LedsystT, LT1K P06-0049 *Design Rule Risk management* 3.0

[18] LedsystT, LT1K-P06-0739 *Design Rule Systems Management* 1.0

[19] LedsystT, LT1K P06-0107 *Design Rule Security aspects of flexibility* 1.0

[20] LedsystT, LT1K P06-0108 *Design Rule Security aspects of information* 1.0

[21] LedsystT, LT1K P06-0359 1.0 *Next Generation Security Architecture for NBD - Overview*

[22] LedsystT, LT1K P04-0385 *Security Architecture Overview* 4.0

[23] LedsystT, LT1K P05-0034 *Infrastructure Overview* 4.0

[24] LedsystT, LT1K P05-0035 *Communication Infrastructure Overview* 4.0

[25] LedsystT, LT1K P05-0100 *Service Approval Process* 1.0

[26] LedsystT, LT1O P06-0293 *Designmetod för FMLS*

[27] LedsystT, LT1O P06-0325 *Arkitekturarbetsflöde*

[28] LedsystT, Framework FMLS Metadata v 2.0.

[29] LedsystT, Description framework for NERE metadata specifications 1.0

[30] LedsystT, NERE metadata specs for tech and softw syst 3.0

[31] LedsystT, Framework Service description

[32] LedsystT, Framework System Description 3.0

Framtagen i samverkan mellan:

FÖRSVARSMAKTEN

KRISBEREDSKAPS
MYNDIGHETEN