

FAKTABOK



2001



ÖCB

Innehåll

Förord	3
--------	---

Kapitel 1

• Projekt TODAKOM	5
• Säkerhetsfrågor	8
• FM IP-nät	9
• Tjänster	10
– TODAPOST	
– TODAKAT	
– CAMA	
• Drift och underhåll av nät och tjänster	12

Kapitel 2

• FM IP-nät	13
• Säkerhet	21
• Regelverk för användning av IP	26
• Tjänster	29
– TODAPOST	
– TODAKAT	
– CAMA	
• Drift och underhåll av nät och tjänster	49
• Utbildning	53
• Förklaring av förkortningar	56

Får kopieras
med angivande av källa och versionsnummer.

Version 2001.01.31

Denna bok finns även elektroniskt publicerad under adress:

Internet. www.todakom.mil.se

FM-IP: todakom.mil.se

Redaktion:

Anders Eriksson/Hans Merilo

Roger Hinders, FMV:FuhDU

Layout:

Kicki Wikström, Text & bildgruppen, ATS, Östersund

Tryck:

Text & bildgruppen, ATS, Östersund 2001

Förord

Denna faktabok har tillkommit för att sprida en samlad information om de tjänster/produkter som utvecklats och införts av projekt TODAKOM. Faktaboken vänder sig till dem inom totalförsvaret, som kommer i kontakt med projektet eller de tjänster/produkter som projektet infört.

Kapitel 1 riktar sig till de som enbart behöver en övergripande information .

Kapitel 2 ger en något djupare information.

Mer ingående information inom vissa delområden finns elektroniskt publicerade på TODAKOM hemsida.

Övrig information från projekt TODAKOM

Strävan från projektet är att all information som utgivits i pappersform även skall finnas elektroniskt på TODAKOM hemsida

TODAKOM hemsida (för både IP-nät och Internet) har adress:

www.todakom.mil.se

Informationskällor som ofta förändras till innehåll eller som är för omfattande har EJ inarbetats i FAKTABOKEN. Principen är i stället att ha en länk till dessa källor (vid elektronisk publicering av FAKTABOKEN vilket sker på hemsidan)

Understrukna ord i denna bok har länkad information i den elektroniska utgåvan (se TODAKOM hemsida)

Referenser står inom []

Den elektroniska utgåvan av boken uppdateras vid behov. Synpunkter på bokens innehåll lämnas på e-postadress: webmaster@todakom.mil.se

I boken används många förkortningar. Förklaringar finns i lista i slutet av boken.

Kapitel I

Projekt TODAKOM

Målsättning för TODAKOM

För att medge ledning och samverkan i fred och kris mellan och inom totalförsvarets civila och militära ledningsfunktioner liksom samverkan mellan olika stridsledningssystem inom det militära försvaret, krävs en generell datakommunikationsarkitektur (omfattande såväl transportmekanism som tjänstedefinitioner) som tillgodoser höga krav på flexibilitet, säkerhet, skadetålighet mm och som kan tillåtas samtrafikera med publika nät under säkra former.

Överstyrelsen för civil beredskap (ÖCB) och Försvarmakten (FM) har utformat en gemensam systemmålsättning för de tjänster som projekt TODAKOM skall införa Systemmålsättning TODAKOM (SYMM TODAKOM).

FM svarar för att bygga ut och förvalta den gemensamma infrastrukturen.

Civila myndigheter bekostar anslutningar och lokal infrastruktur för att ansluta till TODAKOM tjänster.

SYMM TODAKOM revideras regelbundet för att anpassa tjänsterna till utvecklingen av ledningsbehoven och den tekniska utvecklingen.

Införande

FM avser att ansluta samtliga större verksamhetsställen till FM IP-nät. FM kommer att utnyttja TODAKOM tjänster för huvuddelen av det digitala informationsutbytet.

ÖCB avsikt är att ansluta vissa centrala beredskapsmyndigheter och länsstyrelser. ÖCB bekostar länsstyrelsernas anslutningar.

Övriga civila intressenter hänvisas till att kommunicera mot TODAKOM-abonnenter i det särskilt anordnade FM IP-nät via gateways.

De tjänster som införs genom projekt TODAKOM skall kunna användas av totalförsvarsmyndigheter med stort ledningsbehov. Vid många civila beredskapsmyndigheter har likartade tjänster införts för att tillgodose behoven under "normalförhållanden". Inom FM används TODAKOM-tjänsterna som huvudsystem för informationsutbyte under fred och vid beredskapshöjning. Satsningen på att införa tjänsterna har därför varit intensivare inom FM än inom det civila försvaret. Av dessa skäl är FM-nyttjande av tjänsterna för närvarande mer omfattande än nyttjandet från de civila totalförsvarmyndigheterna.

ÖCB har utarbetat en plan som inledningsvis prioriterar möjligheten att nyttja tjänsterna vid kärnkraftlän för att därefter fortsätta införandet inom hela funktionen Civil ledning och för FM viktiga civila samverkansfunktioner.

Projektorganisation

Projekt TODAKOM genomförs gemensamt av FM, ÖCB och FMV.

Projektet är organiserat i delprojekt/beredningsgrupp.

En beredningsgrupp har samordningsansvar för införande vid civila abonnenter.

Projektet överlämnar efterhand ansvaret för att vidmakthålla tjänsterna till linjeorganisationen:

- Försvarsmaktens IP-nät (FM IP-nät) är överlämnat för att ingå i driftorganisationen för Försvarsmaktens TeleNät (FTN)
- trafikalt drift av TODAPOST genomförs av Redovisningsavdelningen Bergslagen/Trafikalt nodstyrning (RAB/TNS)
- lokala TODAPOST-system driftöverlämnas efterhand till abonnenten
- Master för TODAPOST, CAMA och FÄRIST finns vid S 1 i Enköping
- utbildningsresurser för TODAKOM tjänster har skapats vid FM HS/IT-skolan i Halmstad och S1/LedS i Enköping.

TODAKOM-tjänster

”Försvarets internet”

Som bas för datautbytet införs en IP-tjänst. IP står för det protokoll (regelverk) som används. IP-protokollen är den teknik som används för kommunikation över Internet. Den IP-tjänst som införs av projekt TODAKOM innebär att vi inför ett ”Totalförsvarsinternet”. Inom FM skall IP utgöra grund för all kommunikation mellan datorer, även om dessa inte är anslutna till FM IP-nät.

IP-tjänsten styrs genom ett regelverk för datakommunikation, Försvarsmaktens Internet Protocol Suite /Host requirement (FM IPS/H) som beskriver vilka protokoll som får användas vid kommunikation mellan datorer inom FM. Regelverket har tillkommit för att skapa möjligheten till samverkan mellan datorer inom FM.

FM IP-nät är en infrastruktur för IP-kommunikation som byggts inom FTN. Till FM IP-nät ansluts myndigheter och förband. Anslutning till FM IP-nät erfordras för att utnyttja full funktionalitet till TODAKOM-tjänster.

FM IP-nät har en struktur som skall tillgodose höga krav på uthållighet för dataöverföring även under krisförhållanden.

FM IP-nät är byggt av FM. Civila totalförsvarsmyndigheter erbjuds anslutning till nätet till självkostnadspris.

Regelverket skall även användas vid civila totalförsvarsmyndigheters utnyttjande av FM IP-nät.

Elektronisk post

Meddelandeöverföringstjänsten TODAPOST baseras på komersiella produkter. Teknikvalet har baserats på de krav på säkerhetsfunktioner som beskrivits i systemmålsättningen för TODAKOM.

Informationsutbyte

För informationsutbyte mellan datorsystem har utvecklats ett regelverk som stöds av en lösning benämnd CAMA.

Regelverket baseras på överenskommelse mellan myndigheter/förband om villkor och innehåll i informationsutbytet.

CAMA utnyttjar FM IP-nät och TODAPOST för informationsöverföringen.

Katalogtjänst

För att hantera olika typer av adress och nyckeluppgifter har katalogtjänsten TODAKAT införts. TODAKAT kommer att vidareutvecklas för att tillgodose generella behov av katalogtjänst.

Säkerhet

Ett särskilt delprojektet har svarat för stöd i säkerhetsfrågor inom hela TODAKOM-projektet.

Delprojektet har även utvecklat en brandvägg, för skydd av lokala nät som ansluts till FM IP-nät, benämnd Totalförsvarets brandvägg - TODAKOM FÄRIST.



Säkerhetsfrågor

Allmänt

Totalförsvarets användning av FM IP-nät och dess centrala tjänster, ställer krav på säkerhet [Ref SYMM TODAKOM]. Som alltid när man diskuterar säkerhet är det viktigt att först klargöra vad man avser, vilken verksamhet handlar det om, vad konsekvenserna blir om verksamheten inte kan bedrivas som man tänkt, vilken teknik berörs, vilka de tekniska hoten är och vilka som är de potentiella aktörerna.

Säkerhetsfunktioner i IP-nät

Grundläggande krav på FM IP-nät avser tillgänglighet och kapacitet. Nätet skall innehålla funktioner som kan säkerställa dessa krav. Ansvar för säkerheten avseende konfidentialitet (sekretesskydd) och integritet i överförd information ligger hos kommunicerande lokala system.

Säkerhetspolicy

En särskild säkerhetspolicy för drift och användning av FM IP-nät har tagits fram. Denna definierar vilket ansvar som olika aktörer och befattningshavare har. Innan anslutning av lokalt nät till FM IP-nät sker måste även skapas en lokal kommunikationssäkerhetspolicy som närmare beskriver lokala regler, begränsningar etc. Som vägledning har HKV utgett Hotanalys TODAKOM (bilaga 1 till [HKV 12 870:66921](#), 96-06-17). Se även säkerhetsavsnittet i kap. 2.

Allmänt kan konstateras att FM IP-nät kommer att ha hundratals anslutna lokala nät. Det yttersta ansvaret för hur nätets resurser används ligger hos tusentals lokala användare. Delade resurser av alla slag, av vilka FM IP-nät är ett exempel, innebär alltid en potential för missbruk eller oäktsamhet. Det åligger därför alla och envar att utnyttja FM IP-näts resurser på ett hänsynsfullt sätt. Större anspråk på tillgänglig kapacitet skall i förväg anmälas till HKV KRI LED, civila myndigheter anmäler till ÖCB.

Med tusentals användare i samma nät kan insiderhotet inte negligeras. Centrala övervakningsfunktioner måste därför kompletteras med lokala. Misstänkta eller otillåtna aktiviteter skall snarast åtgärdas och anmälas till säkerhetsansvarig.

Trafikkontroll

Vid RAB/TNS sker en kontroll av trafiken i FM IP-nät samt mellan FM IP-nät och externa nät t ex Internet.

Ackreditering

Som ett led i att höja säkerheten och tillgängligheten har HKV (ÖB) beslutat att alla FM system skall ackrediteras.

FM IP-nät - Totalförsvarets internet

Allmänt

1996 fattade FM tillsammans med ÖCB det strategiska beslutet att bygga ett trafik-skyddat IP-nät.

Nätet är utbyggt och har bekostas av FM.

I detta landsomfattande nät skall totalförsvarets datorer kunna kommunicera med varandra enligt den Transmission Control Protocol/Internet Protocol (TCP/IP) arkitektur som används i Internet.

Abonnentnätens omfattning varierar från enbart ett eller flera spridningsnät till ett lokalt stamnät med lokala routar som spridningsnäten ansluts till.

Stamnätet i FM IP-nät, med sina nätnoder och trunkar är en grundförutsättning för data-kommunikation inom TODAKOM-tjänsterna.

Nätet fyller de operativa kraven på:

- funktionalitet i kris
- prioritet
- mobilitet
- redundans

Nätets design är förberett för utbyggnad både avseende kapacitet och omfattning.

TJÄNSTER

Nedanstående tjänster har tagits fram inom projektet

TODAPOST

Allmänt

TODAPOST är benämningen på ett system för elektronisk post. Systemet är avsett för distribution av myndighetspost, mellan verksamhetsställen inom FM samt tjänste-meddelanden till/från befattning eller person. Trafiknätet TODAPOST bildar här en privat domän, sett ur det globala e-postperspektivet.

Förmedling av e-post mellan FM IP-nät och omvärldens Internet sker via särskilt övervakade kopplingspunkter.

Infrastruktur

Vid enheter anslutna till TODAPOST (myndigheter/förband/staber) finns en e-postserver med särskild programvara driftsatt. Denna dator utgör det lokala "postkontoret" till vilket enhetens expedition samt övriga lokala användare (klienter) är anslutna via det lokala nätverket.

TODAKAT

Allmänt

Totalförsvaret i likhet med samhället i övrigt märker av ett snabbt ökande behov av elektronisk kommunikation, såväl internt som externt. Samverkan och informationsutbyte sker i allt större utsträckning på elektronisk väg där aktualitet, säkerhet och kvalitet ges större och större betydelse. För att möta dessa krav finns i dag olika typer av kataloger (register).

Inom projekt TODAKOM finns ett delprojekt för framtagande av en gemensam katalogtjänst. Målet är en katalogtjänst som skall kunna ersätta samtliga nuvarande tele- och datakataloger inom FM. Arbetsnamnet på denna katalogtjänst är TODAKAT.

CAMA

Den primära uppgiften för meddelandeförmedlingstjänsten CAMA, är att på ett enhetligt sätt knyta samman olika slag av system, såväl ledningssystem som administrativa system, lokalt närstående eller på olika platser i landet. Jämför tjänsten TODAPOST som har att göra med personlig post eller myndighetspost.

CAMA bildar sålunda en viktig del av FM infrastruktur. CAMA begränsas ej till autonoma system utan passar väl för direkt samverkande tillämpningar.

CAMA bygger på *elektroniska-, juridiska-, och EDI-avtal* som upprättas mellan involverade parter. De elektroniska avtalen styr adressering, kontrollerar och bevakar överföringen. De juridiska-, och EDI-avtalen är dokument som speglar juridiska förhållanden och beskriver överförd information. *Ett EDI-avtal* skapar förutsägbarhet för både elektroniska affärstransaktioner och ledningssystemmeddelanden samt reglerar villkor och förhållanden som skall gälla i en viss kommunikationsöverföring.

Ett EDI-avtal skall vara enkelt att förändra och förbättra. En EDI-part, exempelvis ett förband, en redovisningsenhet eller motsvarande, skall enkelt kunna läggas till eller tas bort utan att hela EDI-avtalet måste omförhandlas. Vid civil handel utgör FM en part och civila handelsparter andra parter. Då krävs en *juridisk del* som parterna skall underteckna. Som stöd har ett antal mallar färdigställts av projektet TODAKOM.

Drift och underhåll

Allmänt

För varje TODAKOM tjänst/system finns en framtagen underhållsplan system (UHP-S)

Underhållsplan system ger anvisning till berörda verksamhetsställen och myndigheter inom totalförsvaret för planering, styrning och uppföljning av drift och underhåll av materiel (maskin- och programvara) och trafikala funktioner under fred och kris.

Driftstöd kan återfinnas på tre driftstödsnivåer:

- Lokal driftstödsnivå: bestående av lokal IT/ADB-resurs
- Regional driftstödsnivå: bestående av Markteleenheter (MTE) och Underhållsregemente (Uhreg)
- Central driftstödsnivå: bestående av Master TODAKOM , RAB/TNS och FMV

Utbildning av drift- och underhållspersonal

FM HS/IT-skolan och S 1/LedS har gemensamt ansvar för planering och genomförande av TODAPOST-CAMA-FÄRIST-DNS och FM IP-nät-utbildning inom FM. ÖCB ansvarar för att personal inom dess ansvarsområde ges möjlighet till nödvändig utbildning vid FM HS/IT-skolan respektive S 1/LedS.

Kapitel 2

FM IP-nät - Totalförsvarets internet

Allmänt

1996 fattade FM tillsammans med ÖCB det strategiska beslutet att bygga ett trafikskyddat IP-nät. Nätet är utbyggt och har bekostats av FM.

I detta landsomfattande nät skall totalförsvarets datorer kunna kommunicera med varandra enligt den TCP/IP-arkitektur som används i Internet.

De protokoll som får användas i FM IP-nät beskrivs i regelverket FM IPS/H, ett dokument som huvudsakligen refererar till s k Request For Comments (RFC) som är Internet-världens standarder.

FM IP-nät är ett IP router-datanät, vilket innebär att oavsett vilket nät en dator är ansluten till kan olika datorer ha trafik med varandra om alla "talar" TCP/IP, och näten hänger samman med FM IP-nät.

FM IP-nät består dels av ett stamnät, dels accessnätet mellan stamnätet och den accessrouter som ansluts till abonnentnätet.

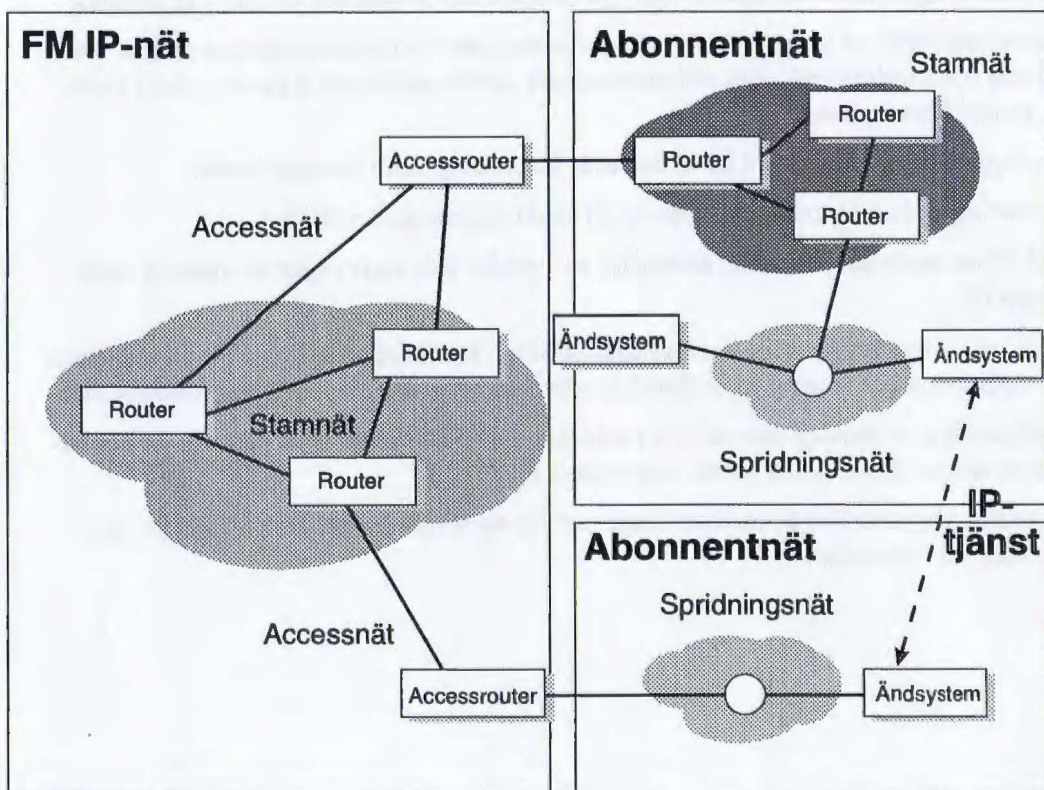


Bild 1.

Abbonentnätens omfattning varierar från enbart ett eller flera spridningsnät till ett lokalt stamnät med lokala routrar som spridningsnäten ansluts till, se bild 1.

Stamnätet i FM IP-nät, med sina nätnoder och trunkar är en grundförutsättning för den datakommunikation som TODAKOM-tjänsterna använder.

Nätet fyller de operativa kraven på:

- funktionalitet i kris
- prioritet
- mobilitet
- redundans

Nätets design medger utbyggnad både avseende kapacitet och omfattning.

FM IP-nät struktur

FM IP-nät består av ett nationellt och flera regionala stamnät som f.n. nyttjar fasta 2 Mbit/s punkt till punkt förbindelser på transportnätsresurser i FTN.

Maskformig topologi ger god redundans.

Nätdesignen tar hänsyn till operativ och taktisk rörlighet, skadetålighet i kris, säkerhet, drift och underhåll.

Dynamisk routing används för att automatiskt hitta bästa framkomliga väg, vilket gör att alternativa vägar inom och mellan regioner automatiskt nyttjas om använd väg förloras.

I första hand väljs att gå genom det nationella stamnätet vid kommunikation mellan två regioner och i andra hand väljs att kommunicera direkt mellan två regioner, eller i vissa fall genom flera regioner.

Routingprotokollet Integrated IS-IS används för routing inom routingdomän.

För routing mellan Autonoma System (AS) används protokollet BGP-4.

I FM IP-nät utgör det nationella stamnätet ett eget AS och varje regionalt stamnät utgör ett eget AS.

FM IP-nät är uppbyggt enligt en hierarkisk struktur. Indelningen är gjord för att underlätta adressplanering och routing samt förenkla administration och skapandet av routing-filter.

Konfigurering av routing-filter är bl a i säkerhetssyfte, att spärra vilka nät som får annonseras ut och att förhindra att fel nät annonseras ut.

I krypteringsapparat 530 finns filterfunktioner för att förhindra otillåten access till centrala resurser i stamnätet.

Övergripande struktur

- Full redundans
- Transportsäkerhet
- Dynamisk "Routing"
- Prestanda
- Säkerhet

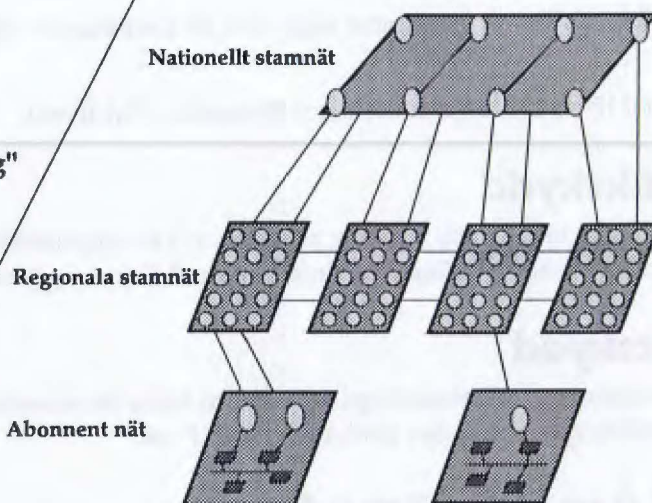


Bild 2.

Följande tjänster erbjudes

IP-förmedlingstjänst:

- Unicast-förmedling, som är bastjänsten i FM IP-nät.
- Multicast-förmedling. IP-multicast, vilket är en punkt till multipunktöverföring av data på ett optimalt bandbreddsbesparande sätt.

Katalogtjänst Domain Name System (DNS):

- se separat avsnitt.

Tidtjänst:

- Tid-servers kommer att finnas i ett par stamnätsnoder vilka distribuerar tid med hjälp av protokollet Network Time Protocol (NTP).
- Tid distribueras genom att stamnätsroutrar formar ett distributionsnät till accessrouterna där abonnenten kan "hämta" tid.

Ansvarsgränser

Ansvarsgränsen för FM IP-nät stamnäts och abonnentnäts funktion går i accesspunkten, vilket innebär att nätövervakningsfunktionen har ansvar fram till och med accessroutern.

Operatören för FM IP-nät lämnar inget stöd för hantering av något annat än IP-baserad trafik.

Protokoll IPv4, Unicast och Multicast förmedlas i FM IP-nät.

Trafikskydd

För att hindra intrång och avsiktlig påverkan av t ex vägvalsinformation i nätet, samt för att försvåra obehörig trafikanalys i nätet används Kryptoapparat 530.

Textskydd

För överföring av sekretessbelagd information krävs att informationen krypteras med textskyddskrypto, innan den sändes över FM IP-nät.

Vad finns på nätnoderna?

Nätnoderna är till största delen installerade på FTN-anläggningar och i anslutning till nätväxlar i FTN. Installationerna är funktionsinriktat utförda i speciella dataskåp, och all utrustning som används, förutom krypto, är standardutrustning.

I Nätnoden finns Cisco-router, Hub och en Unix-dator för name server funktion, DNS. Det finns även krypteringsapparat 530 för trafikskydd.

I några noder kommer även att finnas en "tidsdator" för NTP, vilken styrs av GPS (reserv Rubidium oscillator).

Vad finns hos abonnenten?

Abbonentnoden består av en Cisco accessrouter med Ethernet-gränssnitt (AUI kontakt) mot abonnentens lokala nät (LAN).

Även krypteringsapparat 530, för trafikskydd, placeras hos abonnenten.

Abbonenten anslutes i accessnätet med en kapacitetsanpassad förbindelse från nätnoden. Olika lösningar för förbindelse-framföring/konstruktion förekommer, beroende på abonnentens förutsättningar för anslutning.

Viktiga abonnenter flervägsanslutes.

Nätövervakning

För närvarande sker nätövervakning vid RAB Markteleenhet (MTE) och F 4 MTE. Övervakningen görs vid en nätcentral bestående av en HP arbetsstation, med programmet Open View.

Testnät

Ett testnät är installerat vid FMV, RAB och FM HS/IT-skolan i Halmstad.

Detta testnät är fysiskt och trafikalt skilt från FM IP-nät och skall användas för tester av nya programversioner i router, test av nya applikationer, utveckling och utbildning.

I skrivelse HKV 2000-04-20, 12870:65424 regleras auktorisation och godkännande för system/applikation som får trafikera FM IP-nät.

Se vidare TODAKOM hemsida.

Vad trafikerar FM IP-nät?

Se TODAKOM hemsida.

Utveckling av FM IP-nät

Projekt Todakom har tagit fram ett förslag till utbyggnad/utveckling av FM IP-nät. Principbeslut att bygga ut FM IP-nät enligt detta förslag har tagits av FM.

Förslaget syftar till att vidareutveckla nuvarande flexibla infrastruktur för data-kommunikation på ett sådant sätt att höjda krav från existerande och planerade system och abonnenter kan mötas. Ledstjärnan har varit att anpassa designen efter försvarsmaktens nya krav på flexibel och vidare utbyggbar struktur utan att göra avkall på skäligen redundanskrav.

De huvudsakliga motiven för att uppgradera FM IP-nät är:

1. Möta höjda krav från existerande eller planerade system och abonnenter.
2. Möta ej ännu uppkomna krav. Detta med hänsyn till den relativt långa ledtiden att etablera högre kapacitet i nätet, jämfört med den korta tid det kan ta att introducera en ny tillämpning/applikation.

Övergripande design baseras på ett nationellt stamnät för att avverka långdistans trafik samt ett antal regionala stamnät för att koncentrera trafik för långdistansavverkning samt möjliggöra effektiv trafikavverkning inom regionen. Målsättningen med den nya nätdesignen är att skapa högre tillgänglig bandbredd, minskade fördröjningar samt minskat fördröjningsjitter och på så sätt anpassa bättre mot såväl traditionella applikationer som nya med annan karaktär. Överflyttning av abonnenter mellan den nuvarande nätstrukturen och den nya skall göras på ett sådant sätt att störningar för abonnenterna minimeras.

Allmänt

Den nya strukturen är en utveckling av nuvarande FM IP-nät, samma hierarkiska indelning används och nuvarande routinglösningen bibehålls. Utvecklingen består i att samtliga nivåer uppgraderas med avseende på bandbredden, varvid nuvarande förmedlingsutrustning byts ut. Vidare innebär lösningen en förenkling av nätstrukturen, med färre noder än befintligt FM IP-nätet.

Nätstruktur

Den föreslagna lösningen innebär att ett nytt nationellt stamnät realiseras med 155 Mbit/s trunkar samt ett antal regionala stamnät med 34 Mbit/s trunkar. Abonnenter ansluts till regionala noder, i första hand med 2 Mbit/s.

Den nya strukturen stödjer att abonnenter ansluts med "bashastigheten" 2 Mbit/s samt att vissa abonnenter med högre krav på prestanda (exempelvis Ledningscentraler) skall kunna anslutas med högre hastighet (upp till och med 34 Mbit/s).

Nätstrukturen byggs så att den anpassas efter FM geografiska spridning för att på så sätt tillgodose såväl frestdida behov som erbjuda en funktionell bas för utbyggnad vid eventuell styrketillväxt.

Den nya nätstrukturen innebär en avsevärd reducering av antalet stamnätsnoder jämfört med dagens struktur. Nätet kommer att bli glesare, med lägre logisk såväl som fysisk redundans vad avser förbindelser, jämfört med nuvarande design. Detta bedöms genomförbart då fjärmässig omläggning av transmissionsvägar, med hjälp av digitala korskopplare, mellan FM IP-nätabonnent och FM IP-stamnätsnod är införd i FTN.

Routing

Den strukturella logiken i det uppgraderade FM IP-nät kommer inte att förändras jämfört med idag. FM IP-nät kommer att vara ett hierarkiskt nät med tre nivåer:

Nationellt stamnät

Regionala stamnät

Accessnät

Den routingmodell som finns i FM IP-nät idag har befunnits funktionell och skalbar, varför den kommer att behållas. Vidare uppfyller de idag använda routingprotokollen (BGP och integrated ISIS) kraven som ställs med denna design och alltså kommer de att även fortsättningsvis användas. Således kommer inte routingen i FM IP-nät att påverkas principiellt av den nya nätstrukturen.

Prioritering av trafik

För att tillgodose de krav på garanterad bandbredd, låg fördröjning, jitter mm som ställs av system med högt ställda prestandakrav, finns mekanismer för att åstadkomma prioritering av viss trafik inbyggda i routrarnas operativsystem. Detta, i kombination med att designen av nätet är gjord så att regionala samt nationella trunkars kapacitet överskrider summan av abonnenternas totala kapacitet till en stamnätsnod, gör att prioritetsfunktioner kan etableras.

Nationell nod

De nationella nodernas uppbyggnad har valts så att trafikavverkningsförmåga och redundans maximeras både mot regionala noder och mot andra nationella noder. Varje nationell nod samlokaliseras med en regional nod, för att på så sätt uppnå skadetålighet i

transmissionsgränssnittet och god trafikavvecklingsmöjlighet mot respektive nationellt nät och regionalt nät. Teknologin för nodintern trafikavverkning har tagits fram speciellt för att erbjuda kommersiella operatörer hög avverkningsförmåga och god redundans vid nationella och internationella utväxlingspunkter (D-GIX).

Regional nod

De regionala nodernas uppbyggnad har valts så att abonnenter kan anslutas på ett effektivt sätt och erbjudas goda möjligheter till såväl interregional som intraregional trafik. Trafikavvecklingen inom en fristående nod ombesörjs med vanlig LAN-teknologi; då en regional nod är samlokaliserad med en nationell nod ingår den i den nationella nodens trafikavvecklingsschema enligt ovan.

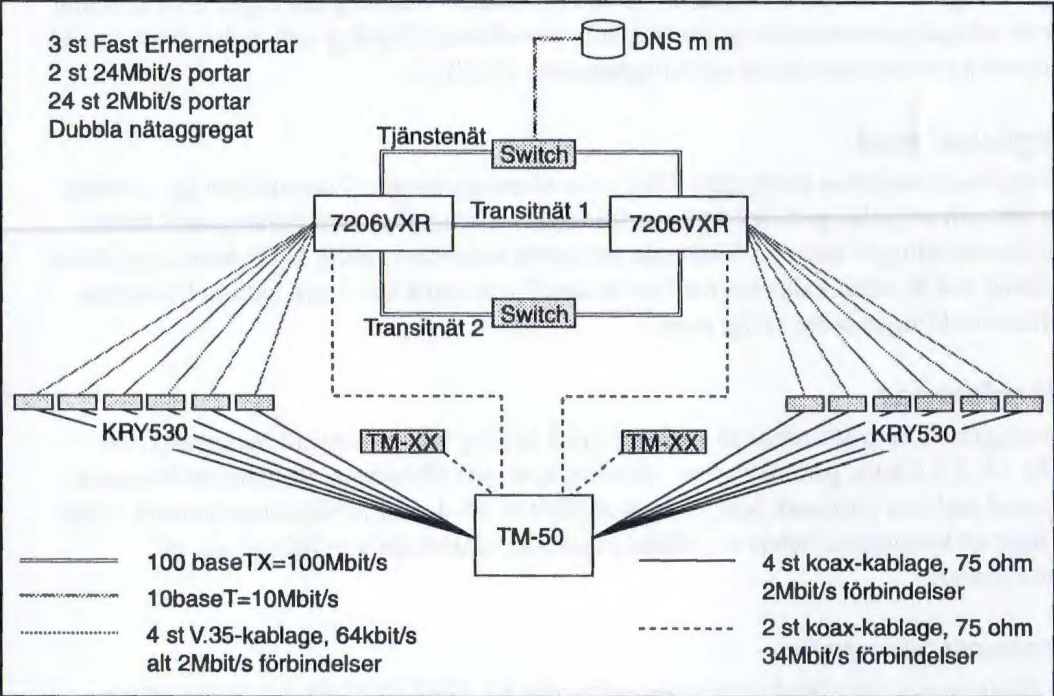
Plattformer

Föreslagna routerplattformar på nationell nivå är idag utbyggbara till maximalt SDH STM-16, 2.5 Gbit/s, genom byte av interfacekort i plattformarna. Routerplattformarna i regional nod kan maximalt bestyckas med SDH STM-4, 622 Mbit/s interfacekort. Detta medger att kommande behov av utökad kapacitet relativt lätt kan tillgodoses på plattformsnivå.

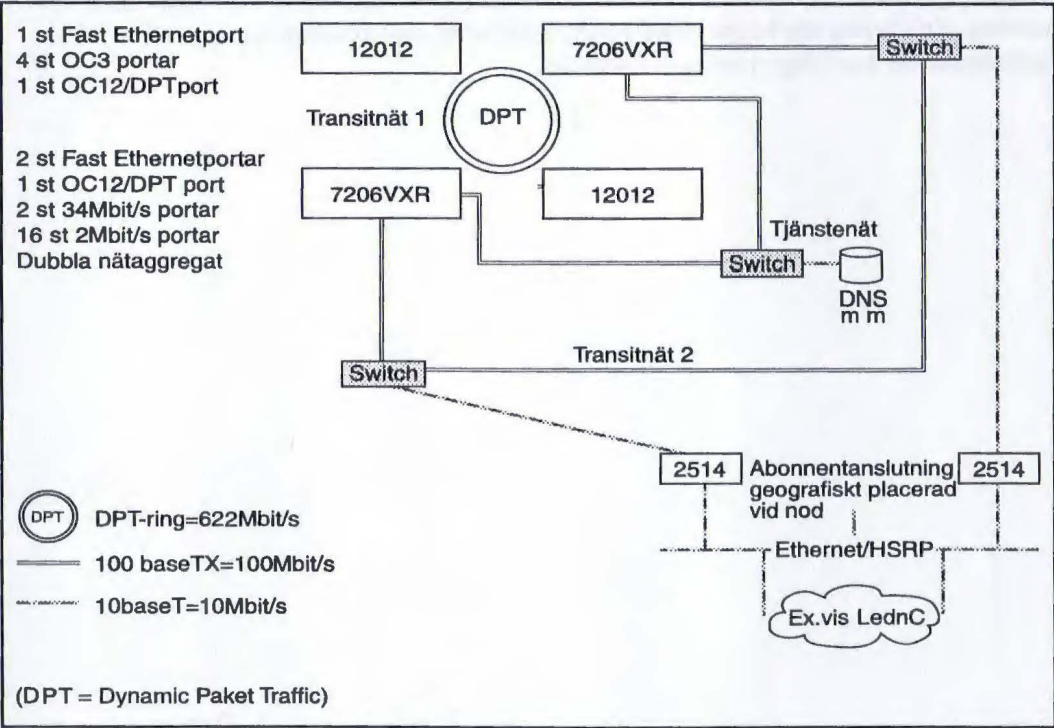
Transmissionsnät

Då fiberresurser utnyttjas kan idag kapacitet upp till SDH STM-64, 10 Gbit/s erhållas och utnyttjas. Tillgänglig radiolänkutrustning har en maximal kapacitet på SDH STM-1, 155 Mbit/s. För att nå högre bandbredd kan hela stamnätet på sikt komma att realiseras med fiberresurser, medan accessnätet realiseras med antingen fiberresurser eller radiolänk-utrustning. En lösning där högre bandbredder realiseras med erhållen kapacitet från radiolänkresurser kan idag ej anses försvarbart.

Regional stamnötsnod



Nationell/Regional stamnötsnod



Säkerhet

Allmänt

Totalförsvarets användning av FM IP-nät och dess centrala tjänster, ställer krav på säkerhet [Ref SYMM TODAKOM] (se även RFC2401). Som alltid när man diskuterar säkerhet är det viktigt att först klargöra vad man avser, vilken verksamhet handlar det om, vad blir konsekvenserna om verksamheten inte kan bedrivas som man tänkt, vilken teknik berörs, vilka är de tekniska hoten, vilka är de potentiella aktörerna.

Låt oss först titta närmare på den för totalförsvaret gemensamma kommunikationsarkitekturens tekniska grund, FM IP-nät.

Säkerhetsfunktioner i IP-nät

Grundläggande krav på FM IP-nät avser tillgänglighet och kapacitet. Nätet skall innehålla funktioner som kan säkerställa dessa krav. Ansvar för säkerheten avseende konfidentialitet (sekretesskydd) och integritet i överförd information ligger hos kommunicerande lokala system.

Vägval

Fungerande IP-nät förutsätter att samverkande, förmedlande komponenter (routers) i nätet har tillförlitlig information om sina grannar och därvid hur mottagna paket skall sändas vidare. Man kan säga att internet (Internet eller slutna Intranät) bygger på en princip om välvillig samverkan där uppgifter om vägval (routing) är korrekta. Om någon annonserar ut felaktig vägvalsinformation uppstår omedelbart störningar i nätet. För närvarande kontrolleras därför denna information noga i FM IP-nät, till priset av den flexibilitet som annars skulle kunna uppnås. För närvarande pågår internationellt arbete mot att försöka skapa säkerhetslösningar för routingprotokollen. Detta är dock inte helt lätt eftersom prestanda hos routrar är en kritisk faktor.

Kan man lita på adressen?

Varje dator har en egen IP-adress. Vilken adress som sätts upp avgörs av den lokale nätadministratören. Det är mycket lätt för användaren att ändra sin IP-adress. Detta kan dock ofta leda till störningar i nätet, t ex om två enheter har samma adress. I andra fall kanske det inte blir några störningar, men i stället uppstår risken för falska avsändaradresser (masquerading). En illasinnad användare (insider) kan ha syftet att försöka få sin dator att se ut som om den var en annan dator, exempelvis en dator som har givits rätt att kommunicera via den lokala brandväggen.

Det finns förslag på hur man skall kunna hantera detta problem. I grunden handlar det om att kunna verifiera identiteten hos avsändande part; autentisering. Detta kan göras med hjälp av en kryptografiskt skyddad hashsumma (kontrollsumma) - under förutsättning att mottagaren har information som gör det möjligt att kontrollera hashsumman [Ref RFC 2402]. Att på förhand distribuera allas nycklar till alla är inte praktiskt hanterbart.

I enstaka fall kan man tänka sig att distribuera nycklar manuellt. I andra fall måste man skapa ett system för automatisk nyckeldistribution som i sig måste ha inbyggda säkerhetsfunktioner. Sådana lösningar kommer att bli aktuella för FM IP-nät på sikt. Se vidare nedan om säker namngivningstjänst.

Vad har Du för adress?

Paket som sänds ut har två IP-adresser, en för avsändare och en för mottagare. Dessa adresser är 32-bitstal och kan representeras som en sifferserie, t ex 192.168.1.12. Precis som med telefonnummer kan det vara besvärligt att lära sig vem som har vilken adress. En funktion som ena dagen ligger på en viss IP-adress kan också plötsligt ha bytt adress genom att den lokala nätstrukturen där funktionen finns har ändrats. Det behövs med andra ord en sorts nummerupplysning. Denna namngivningstjänst heter i Internetvärlden DNS. I IP-nät finns alltid en eller flera DNS-servrar som lagrar aktuell adressinformation. Liksom hos nummerupplysningen kan man fråga vem som har visst nummer (IP-adress) och få svar vilket domännamn som svarar mot detta nummer (www.statskontoret.se). Man kan också fråga vilken IP-adress som en viss domän har.

Uppenbart är att namngivningstjänsten är säkerhetskritisk. Om jag ber om att bli kopplad till en viss tjänst (viss dator) och får ett felaktigt IP-adress-besked är det inte säkert att jag märker detta. Jag kommunicerar då med fel part och lämnar kanske uppgifter som helst inte borde ha gått dit. För sekretessbelagda uppgifter skall detta inte vara ett omedelbart problem; sådana uppgifter får ju bara överföras i krypterad form och kan därigenom i vissa fall ge säker autentisering. Men jag kanske tar emot uppgifter som jag tar för godo och baserar sedan mitt fortsatta agerande på dessa. Vi behöver alltså kunna lita på varifrån uppgifterna kommer. Liksom vid kryptering kan detta ske med hjälp av kryptografiska metoder (antingen genom att kanalen är autentiserad eller genom att själva meddelandet kan autentiseras, genom t ex användning av digital signatur).

Inom TODAKOM studeras säker DNS för ett framtida införande när standard och produkter blir stabila och effektivare. Man har även diskuterat [Ref [RFC 2358](#)] att med hjälp av dnssec kunna distribuera nycklar för autentisering enligt IP-AH.

Vad är klockan?

Många system behöver tillgång till tillförliga tidsuppgifter. Tidskritiska system behöver noggranna tidsuppgifter för att kunna samverka med andra funktioner i t ex vapen- och eldledningssystem. Datorernas loggfiler behöver ensade tidsuppgifter för jämförelser av olika logguppgifter. Vissa överföringsprotokoll använder tiden för att kontrollera ordningsföljden av olika meddelanden som skydd mot återuppspelning (reply). Datorernas interna klockor går visserligen normalt ganska rätt men efter en tid tenderar den lokala tiden att bli alltmer felaktig. Med hjälp av speciella servrar i FM IP-nät kan pålitliga tidsuppgifter enkelt fås med hjälp av NTP [Ref [RFC 1305](#)]. För skydd mot förfälskade tidsuppgifter i nätet skyddas tidsmeddelandena med krypterade hashsummer (med en särskild nyckel). På sikt behövs automatiska metoder för distribution av sådana nycklar.

Länkkryptering

För att försvåra att obehöriga meddelanden (routinginformation mm) eller annan falsksignalering introduceras i FM IP-nät trafikskyddas alla förbindelserna. Trafikskyddet syftar även till att försvåra trafikanalys där någon genom att observera trafikflödet försöker skapa sig en bild av vilka aktiviteter som pågår hos abonnenterna. Trafikskyddet åstadkommes genom signalskyddssystem MGU och Kryptoapparat 530. Krypteringen sker alltså av trafiken mellan respektive router. Det skall observeras att detta kryptosystem således inte skapar något godkänt textskydd för överföring av sekretessbelagd information. Här duger bara av TSA godkänt textskydd etablerat mellan de kommunicerande parterna. Notera att risken för falsksignalering ändå inte helt kan uteslutas. Sådan trafik kan skapas antingen i centrala noderna eller, kanske mer sannolikt, någonstans ute i de anslutna lokala näten. Notera att anslutning till FM IP-nät förutsätter installerad kryptoapparat 530 och att det därvid måste finnas personal som genomgått erforderlig signalskyddsutbildning.

Kontroll och övervakning

Resurser för kontroll och övervakning av FM IP-nät har byggts upp vid RAB och F 4 markteleenheter. Funktioner för normal driftövervakning och uppföljning kompletteras med resurser för spårning och utredning av otillåten trafik. I kontrollfunktionerna ingår även övervakning av e-post-trafik till och från omvärlden (via Internet och Datapak). Se vidare angående "Trafikkontroll av extern trafik".

Säkerhetspolicy

En särskild säkerhetspolicy för drift och användning av FM IP-nät har tagits fram. Denna definierar vilket ansvar som olika aktörer och befattningshavare har. Innan anslutning av lokalt nät till FM IP-nät sker måste även skapas en lokal kommunikationssäkerhetspolicy som närmare beskriver lokala regler, begränsningar etc. Som vägledning har HKV utgett Hotanalys TODAKOM (bilaga 1 till [HKV 12 870:66921, 96-06-17](#)).

Allmänt kan konstateras att FM IP-nät kommer att ha hundratals anslutna lokala nät. Det yttersta ansvaret för hur nätets resurser används ligger hos tusentals lokala användare. Delade resurser av alla slag, av vilka FM IP-nät är ett exempel, innebär alltid en potential för missbruk eller oaktsamhet. Det åligger därför alla och envar att utnyttja FM IP-näts resurser på ett hänsynsfullt sätt. Större anspråk på tillgänglig kapacitet skall i förväg anmälas till HKV KRI LED.

Med tusentals användare i samma nät kan insiderhotet inte negligeras. Centrala övervakningsfunktioner måste därför kompletteras med lokala. Misstänkta eller otillåtna aktiviteter skall snarast åtgärdas och anmälas till säkerhetsansvarig.

Ackreditering?

Enligt HKV regler [Ref [FM Handbok IT](#)] skall informationssystem inom FM ackrediteras före driftsättning. För civila myndigheter har ÖCB med stöd av beredskapsförordningen [Ref SFS 1997:640] utgivit allmänna råd till föreskrifter om Grundsäkerhet för samhällsviktiga datasystem hos beredskapsmyndigheter. Dessa regler innebär att lokalt etablerat IT-stöd måste analyseras och godkännas före driftsättning. I analysen skall bl a ingå identifiering och värdering av hot, beskrivning och analys av vidtagna skyddsåtgärder m m. Detta innebär att lokal chef måste bedöma risken för intrång eller andra störningar. FM IP-nät inkluderar funktioner för att skydda centrala tjänster i nätet. Grundläggande tillgänglighetskrav kan dock inte garanteras utan att ställa krav även på anslutna enheter. Anslutna organisationsenheter (förband, skola, civil myndighet) har därmed ett ansvar att inte störa trafiken i FM IP-nät. Man får inte ansluta eget nät till andra externa nät (som förutom de direkta lokala riskerna detta medför också kan öppna vägen för attacker mot andra användare i FM IP-nät). Det senare innebär att datorer på LAN som är kopplat till FM IP-nät inte utan särskilt tillstånd från HKV får ha förbindelse med externt nät, t ex via modem.

Anslutning av lokalt nät som trafikerar av hemlig, okrypterad information till FM IP-nät får inte ske. Om hela nätet skyddas av kryptosystem 980 (kryptosystem för Virtuellt Privat Nät, VPN) kan dock nätet kommunicera med annat VPN-skyddat nät på annan plats. Även om det lokala nätet skyddas av en brandvägg (se nedan angående Färist) finns risk för att dator som medges kommunikation via brandväggen kan attackeras via de tillåtna protokollfallen och därvid, även om just denna dator inte innehåller hemlig information, vid intrång användas som "språngbräda" för vidare attack mot de hemliga systemen på det egna nätet. Endast genom godkända kryptolösningar i respektive dator kan sådan trafik skyddas och anslutning till FM IP-nät övervägas.

TODAPOST

Allmänna regler för användning av TODAPOST finns utgivna i TODAKOM adresseringsbestämmelser/IP-adresstilldelning ([HKV 1999-10-15, 12870:71879](#)).

Förslag till säkerhetspolicy för drift och användning av TODAPOST framtogets hösten 2000. Integration av försvarsgodkända kryptofunktioner i kommersiella programvaror är besvärlig ur många synvinklar. Krypteringen måste kunna byggas in på ett sätt så att man kan verifiera att inte dess syfte kan kringgå. Detta är svårt såväl från teknisk som kommersiell synpunkt. Inledningsvis har inom FM framtagits ett Filkrypto som arbetar mot Kryptokort 621. Detta filkrypto kan användas i fristående PC för att kryptera enskilda filer. Efter kryptering kan det krypterade meddelandet läggas som bilaga i TODAPOST. Arbeta med att få tillstånd en mer lättanvänd lösning pågår.

Det finns även behov av att kunna utföra s k digital signatur på meddelanden, så att mottagaren kan autentisera avsändare och innehåll. Tekniska lösningar är här beroende av tillgång till öppen-nyckel-certifikat via en gemensam struktur för öppna nycklar (s k PKI; Public Key Infrastructure) för hela försvaret.

Brandväggar

Totalförsvarets brandväggsprodukt, kallad FÄRIST, har utvecklats inom projekt TODAKOM. Färysten är byggd på en konventionell Intel-baserad PC med dubbla nätverksinterface. Som operativsystem har valts en minimaliserad version av Unix. Namnet FÄRIST har avsiktligt valts för att betona att brandväggars normala funktion är att begränsa IP-baserad trafik, snarare än att ge intrycket av att vara ett mycket gediget skydd mot allvarliga, yttre faror (brandvägg). Vidare sker viss loggning av framför allt onormal trafik inklusive försök till att sända otillåten trafik.

All trafik förmedlas via så kallade "ombud" (proxies); Färysten är en kvalificerad typ av brandvägg (applikationsproxy). Det kan noteras att många på marknaden förekommande brandväggar är av enklare, paketfilterande typ som medför större risker.

Alla öppningar som görs i en brandvägg innebär vissa risker. Stora ansträngningar har lagts ner på att tillse att Färysten inte skall kunna korrumpas och därvid fås att åsidosätta konfigurerad policy.

Lokal FÄRIST

Den lokala säkerhetspolicy som skall finnas, skall även inkludera beskrivning av vilken kommunikation som skall tillåtas till och från FM IP-nät. Detta innebär att man lokalt skall beskriva vilka datorer som skall tillåtas kommunicera utåt samt vilka portar och protokoll som tillåtes. Konfigurationen för FÄRIST skall således kunna härledas av dessa lokala regler. Det är uppenbart att utformningen av denna konfiguration är av säkerhetskritisk betydelse. FÄRIST levereras med en uppsättning förberedda "ombud" (proxies) för olika tjänster. Bra och tillförlitliga beskrivningar över de lokala förhållandena (nät, datorer) tillsammans med goda kunskaper i TCP/IP och DNS är nödvändiga för en säker administration av FÄRIST. Utbildning av FÄRIST-operatörer genomförs vid FM HS/IT-skolan, som efter godkänd kurs utfärdar utbildningscertifikat. Stöd åt abonnenterna vid skapande av konfigurationsfiler ges via helpdesk TODAKOM. En bra brandväggsfunktion kräver att någon vakar över funktionen. Centrala regler för konfigurerings av FÄRIST kommer att fastställas.

Abonnenter inom totalförsvaret skall ha FÄRIST vid inkoppling till FM IP-nät. Den utgör lokal organisations "dörrvakt" ut mot det yttre nätet.

Trafik kontroll av extern trafik

Endast e-post tillåts för trafiken mellan FM IP-nät och omvärlden (huvudsakligen Internet). Denna trafik kontrolleras i ett speciellt system (Z-RIST) där flera datorer för övervakning och analys ingår tillsammans med FÄRIST.

Regelverk för användning av IP-protokoll

Allmänt

För att nå målsättningen i SYMM TODAKOM med en gemensam kommunikationsarkitektur, har projekt TODAKOM tagit fram ett regelverk för vilka kommunikationsprotokoll som skall användas i datorer inom FM. Regelverket gäller för ALLA DATORER inom Försvarsmakten, oavsett vilka kommunikationsnät datorerna är anslutna till.

Regelverket som utgår från Internet Protocol Suite (IPS) definierar de tjänster och protokoll som datorer (ändsystem) inom totalförsvaret skall stödja för att uppnå samverkan. Regelverket benämns FM IPS/H.

De begränsningar som införs genom att man exempelvis i andra regelsystem enbart tillåter applikationer Verksamhetsbaserade system (VBS) att utbyta data via CAMA påpekas i dokumentet men har inte lagts in i de avsnitt som mera konkret beskriver FM IPS/H.

Dokumentet beskriver kortfattat tillgängliga tjänster, hänvisar till existerande standarder och ger de kommentarer till dessa som bedöms relevanta i totalförsvarets skilda miljöer. Dessutom definieras för de olika skikten i modellen vilka protokoll och tjänster som skall krävas vid upphandling av ändsystem för att uppfylla IPS/H.

Ytterligare ett syfte är att grovt klargöra hur de olika tjänster och protokoll som ingår i FM IPS/H får användas i FM IP-nät och andra yttre nät.

Definitioner

Tjänster och protokoll i IPS klassificeras efter:

- Krav:** vad som skall krävas vid upphandling av ändsystem
Användning: hur tjänsten/protokollet får användas

Krav

De krav som ställs kan variera mellan olika system varför kraven här på samma sätt som i motsvarande RFC, "Internet Protocol Standards" indelas i:

- A. Skall finnas i alla system.
- B. Bör finnas i alla system. Undantag kan finnas men som regel skall tjänsten/protokollet finnas.
- C. Valbart. Tjänsten/protokollet skall finnas om behov föreligger.
- D. Tjänsten/protokollet skall inte finnas.

Motiv för klassificeringen kan vara funktionell (implementering enligt viss RFC existerar inte eller implementeringar fungerar inte), säkerhetsmässig eller en strävan efter standardisering.

Användning

För varje tjänst/protokoll görs dessutom en klassificering efter hur det får användas. Denna klassificering beror på de säkerhetsproblem som är förknippad med många tjänster/protokoll i IPS. Många tillämpningar/protokoll är förknippade med säkerhetsproblem och är därför inte tillåtna att använda i oskyddade nät. Dock kan användning tillåtas i avgränsade, skyddade nät.

Följande klassificering görs:

I Inom. Tjänsten/protokollet får endast användas inom ett skyddat nät.

U Utom. Tjänsten/protokollet får användas både inom skyddade och oskyddade nät.

Med ett skyddat nät avses ett avgränsat nät. I den mån det finns kopplingar till andra nät skyddas det av en brandvägg.

Dokumentet FM IPS/H finns tillgängligt över Internet och FM IP-nät på:
www.todakom.mil.se

DNS

Vad är DNS?

DNS är en internetjänst vars huvuduppgift är att lösa upp internetadresser i domännamn, exempelvis från 193.44.157.203 till www.mil.se. Tjänsten fungerar såväl fram- som baklänges, det vill säga från namn till nummer eller från nummer till namn. Denna tjänst har tillkommit för att göra det lättare för människor att navigera på ett internet och att administrera detsamma. De allra flesta av oss har lättare att komma ihåg namn än godtyckliga siffror.

DNS är hierarkiskt uppbyggt, som ett upp och nedvänt träd - i toppen finns domänen "punkt" (".") och under denna grenar trädet ut sig i två principiella huvuddelar: framlängesuppslagning, dvs från namn till nummer och baklängesuppslagning (nummer till namn). Direkt under "punkt" finns domäner som exempelvis .se (Sverige) och .com (kommersiell). Hierarkin fungerar på så sätt att närmast överliggande domän delegerar ansvaret för underliggande domäner till respektive registrerade ägare, vilken bestämmer över domänens innehåll och vidare delegering.

Databaserna som DNS använder sig av kan förutom namn-nummerkorrelationen innehålla andra posttyper, exempelvis text, datorinformation och data för styrning av e-post. E-poststyrningen fungerar genom att i databasen anges namnet på en dator som är postkontor för en viss domän och vid förfrågan kommer detta datornamn att sändas till den frågande datorn. Den frågande datorn ställer sedan ytterligare en fråga för att upplösa det erhållna namnet till en adress, varpå den vidarebefordrar brevet till destinationen. De

övriga posttyperna kan förutom att ge allmän information om datorsystem användas för vissa katalogtjänster, bland annat hantering av publika kryptonycklar.

DNS i FM IP-nät

DNS i FM IP-nät är uppbyggt enligt samma principer som Internet, men saknar av säkerhetsskäl direkta kopplingar till denna. Avskildheten gör att FM IP-nät måste försörja sig själv med den del av hela domännamnshierarkin som används. Nätoperatören tillhandahåller och administrerar toppdomänen ”punkt”, subdomänerna .se och .mil.se samt delegering av domäner under dessa. Den korrelerande baklängesuppslagningen handhas på samma sätt av nätoperatören.

Tilldelning av abonnentdomäner i FM IP-nät sker på samma sätt som tilldelningen av adressrymd och domännamnstrukturen och följer i allt väsentligt FM organisation. Samtliga tilldelade domäner inom FM kommer att sluta på mil.se, exempelvis hkv.mil.se. På motsvarande sätt tilldelas de civila myndigheterna abonnentdomäner i FM IP-nät.

Abonentdomänernas skötsel fungerar enligt principen att en abonnent med fler än tre ändsystem i sin domän skall sköta sin egen DNS, såväl fram- som baklängesuppslagning. Nätoperatören bistår abonnenterna med sekundär DNS-server, placerad i FM IP-nät och en del av FM IP-näts generiska infrastruktur. Denna tjänst aktiveras i samband med tilldelning av domännamn till abonnenten.

Tjänster

Följande tjänster har tagits fram inom projektet

- TODAPOST
- TODAKAT
- CAMA
- Förutsättningar för elektronisk handel

TODAPOST

Allmänt

TODAPOST är benämningen på ett system för elektronisk post. Systemet är avsett för distribution av myndighetspost mellan verksamhetsställen inom FM samt tjänstemeddelanden till/från befattning eller person. Trafiknätet TODAPOST bildar här en privat domän, sett ur det globala e-postperspektivet.

Infrastruktur

Vid enheter anslutna till TODAPOST (myndigheter/förband/staber) finns en e-postserver med särskild programvara driftsatt. Denna dator utgör det lokala "postkontoret" till vilket enhetens expedition samt övriga lokala användare (klienter) är anslutna via det lokala nätverket.

Teknisk utformning

De enheter som skall ha anslutning till TODAPOST erhåller en PC med särskild programvara (server med programvara benämnes TODAPOST-server).

Programvaran som är ett paket innehåller operativsystem (FreeBSD), SMTP-server (för e-postfunktionen), DNS, LDAP-server (för katalogfunktionen) och POP (protokoll för e-postklient).

Som klientprogramvara skall i stort sett vilken SMTP-klient som helst (Netscape, Outlook Express, Eudora m fl) kunna användas. FM rekommendationer/krav på klientprogramvaran framgår av FM ITK.

För att varje lokal TODAPOST-server inte skall behöva känna till alla andra servrar i nätet bygger förmedlingen av e-post på DNS som är en slags katalogtjänst i FM IP-nät där en dator kan fråga om och få anvisat hur kontakt med viss annan dator skall etableras.

Skulle mottagande TODAPOST-server tillfälligtvis inte vara ansluten i nätet (exempelvis mobil abonnent under förflyttning) lagras meddelanden till denna i en sekundär

mailserver som finns utplacerad i FM IP-nät. När mottagaren återansluts distribueras lagrade meddelanden till dennes server.

För driftövervakning och administration av trafiknätet finns en organisation, TNS, etablerad vid RAB i Örebro.

Centrala tjänster

I den i FM IP-nät centralt placerade TODAKOM-noden finns särskilda datorer (gateways) för att då så behövs konvertera TODAPOST-meddelanden avsedda att vidarebefordras till mottagare anslutna i andra e-postsystem (eller vice versa).

TODAKOM-noden är för detta ändamål ansluten till Internet (enbart Internet mail) samt 400net (civilt X.400-nät). Det finns även kopplingar för GSM text och minicall text.

Mobila abonnenter erbjuds möjligheten till uppringd brevlåda, vilket kan erhållas efter särskild ansökan.

HKV målsättning är att TODAPOST skall vara huvudsambandsmedel inom Försvarsmakten vad gäller överföring av meddelanden med textinnehåll. Anslutna förband och staber har därmed **krav** på sig att kunna **sända och ta emot myndighetspost**.

För detta ändamål skall samtliga verksamhetsställen ha utbildad e-postregistrator. De verksamhetsställen som tilldelas förvaltningsansvar för TODAPOST-server skall utbilda systemadministratör (SA) samt postmaster (se vidare avsnitt utbildning). Man skall också aktivt hantera förbandets/stabens expeditionsbrevlåda så att myndighetspost i första hand kan befordras via TODAPOST.

Textskydd

I dag finns det inget integrerat textskydd i TODAPOST. För att realisera överföring av krypterade filer med hemlig information har kryptokort 621 distribueras till anslutna förband/stabers huvudexpedition.

Krigssystem

För att svara upp mot krigets krav tas hänsyn till dessa då centrala nätfunktioner utvecklas och driftsätts.

Övrig planering för krigsfunktionalitet sker fortlöpande.

Tjänster i TODAPOST

- Myndighetspost
- Befattnings-/funktionspost (personpost)
- E-post till adressat på Internet
- E-post till Minicall-mottagare med textfunktion
- E-post till GSM-telefon

Adresseringsexempel

Myndighetspost

Expeditionen på Högkvarteret har följande adress:

exp@hkv.mil.se

(Expeditionen är förbandets officiella adress)

Befattnings- / funktionspost

VB på Högkvarteret har följande adress:

vb@hkv.mil.se

Ledningssystem på operativ insatsledning har följande adress:

j6@opil.mil.se

Personpost

Adressen till Pär Åhl vid HKV skrivs:

par.ahl@hkv.mil.se

Adressen till Ann Crona-Vidén vid HKV skrivs:

ann.crona-viden@hkv.mil.se

Tillämpning

För att tydligare visa för mottagaren vem som är avsändare av brevet skall följande göras:

I avsändarens klientprogramvara för e-post konfigureras ett display name (Beskrivande namn). Display name är ingen del av adressen, utan endast för presentation. Detta sänds tillsammans med avsändaradressen. Samma värde används i kataloger och adressböcker för att identifiera en tilltänkt mottagare.

Display name skall skrivas in med nationella tecken. Här får även andra skrivbara tecken som mellanslag, punkt snedstreck etc. användas.

- för personlig profil
- för befattningsprofil
- för funktionsadress

Ex 1 Displayname för personadressen ake.angstrom@hkv.mil.se:

< Åke Ängström HKV >

Ex 2 Displayname för befattnings-adressen postmaster@hkv.mil.se:

< HKV Postmaster >

Ex 3 Displayname för funktionsadressen exp@hkv.mil.se:

< HKV Exp >

Meddelande till Minicall-mottagare med textfunktion

0746123456@minicall.mil.se

Meddelande till GSM-telefon

0705123456@gsmtext.mil.se

TODAKAT

Allmänt

Totalförsvaret i likhet med samhället i övrigt märker av ett snabbt ökande behov av elektronisk kommunikation, såväl internt som externt. Samverkan och informationsutbyte sker i allt större utsträckning på elektronisk väg där aktualitet, säkerhet och kvalitet ges större och större betydelse. För att möta dessa krav finns i dag olika typer av kataloger (register).

Inom projekt TODAKOM finns ett delprojekt för framtagande av en gemensam katalogtjänst. Målet är en katalogtjänst som skall kunna ersätta samtliga nuvarande tele- och datakataloger inom FM. Arbetsnamnet på denna katalogtjänst är TODAKAT (Tele- och datakatalog).

Olika versioner av TODAKAT

En katalogtjänst för e-postadresser behövs bl a för att underlätta användandet av TODAPOST. För detta ändamål driftsattes TODAKAT version 2.

Katalogen utgörs av en central katalogserver. För driften svarar Helpdesk TODAPOST. Katalogen nås av de TODAPOST-användare som är anslutna till FM IP-nät. Respektive lokal postmästare ansvarar för sin del av kataloginformationen.

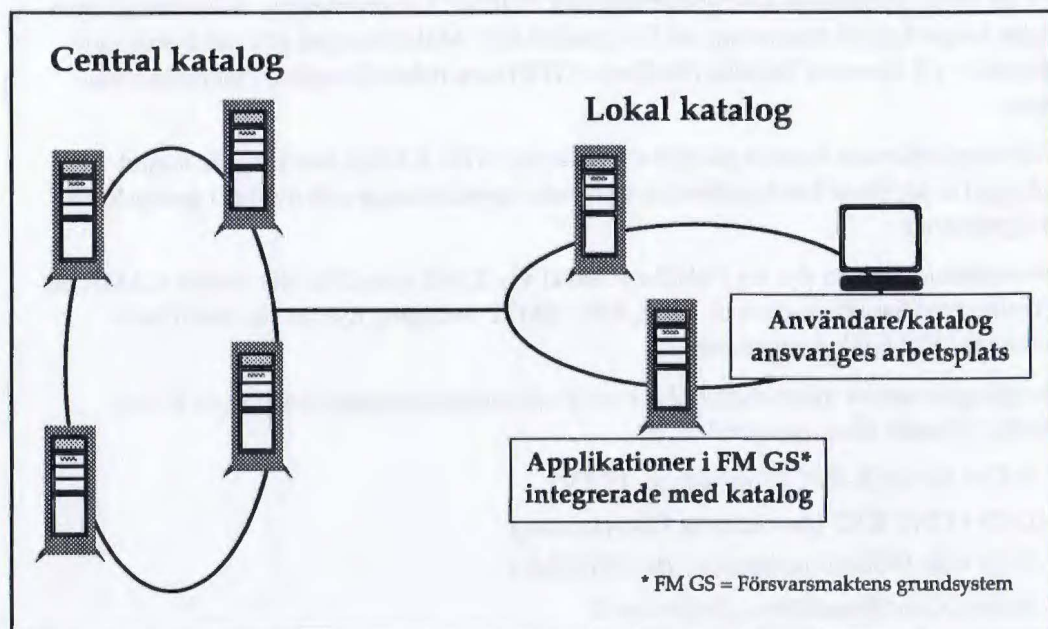
Nästa steg

För att utreda vilket behov som föreligger av katalogtjänst (utöver e-postadresser) genomförs en behovsinventering.

TODAKAT version 3 är beteckningen på nästa steg i utvecklingen av katalogtjänsten. Denna ska till skillnad från TODAKAT version 2 innehålla mer än enbart e-postadresser, baserat på behovsinventeringen.

TODAKAT v3 – baseras så långt som möjligt på internationella katalogstandarder och karaktäriseras av att den skall:

- kunna innehålla all slags information och inte vara begränsad till en viss typ av uppgifter.
- kunna samverka mellan centrala och lokala katalogservrar.
- vara tillgänglig för användare oberoende av geografisk placering.
- ge stora möjligheter att reglera tillgång till information.
- tillhandahålla öppna gränssnitt för integration med andra applikationer och system.



CAMA

Allmänt

CAMA är en produkt för kontraktbaserade tjänster som utvecklats inom projekt TODAKOM. Produkten erbjuder också ett antal kommunikationstjänster för enhetligt meddelandeutbyte mellan autonoma system. Det kan vara elektroniska handelsmeddelanden eller ledningssystemmeddelanden mellan enheter vilka skall kommunicera med varandra även efter omgruppering eller omkonfiguration, med skiftande krav vad avser funktionalitet, överföringshastighet och säkerhet.

Den *primära uppgiften* för CAMA är att knyta samman olika slag av system (egentligen i systemen ingående exekverbara moduler), lokalt närstående eller via WAN. Jämför

tjänsten TODAPOST som har att göra med person- eller myndighetspost. CAMA baseras på principen Store and Forward och i förväg skapade juridiska och elektroniska kommunikationsavtal. CAMA begränsas ej till autonoma system utan passar för direkt samverkande tillämpningar baserade på Client Server. *Skilda slag av system kan kommunicera* via CAMA, på ett enhetligt sätt, vilket kanske ej med befintliga lösningar är möjligt. Replikeringfunktioner enligt ATCCIS håller på att tillföras. *Vid eventuella krav på protokollbyte* påverkas ej tillämpningarna när CAMA används. Detta är de viktigaste incitamenten för användning av CAMA.

Transporttjänsten erbjuder olika slag av bearbetning av informationen, innan den sänds eller tas emot, exempelvis komprimering eller EDIFACT-konvertering. Säkerhetstjänsten bygger i dagsläget på kryptering via Kryptokort 621. Målsättningen påvisar kommande anknytning till Generell Teknisk Plattform (GTP) som måste föregås av tekniska utredningar.

Hårdvaruplattformen baseras på operativsystemet NT4. CAMA version 3 är moduluppbyggd så att dessa kan kombineras i ett antal uppsättningar och nyttjas i godtyckliga konfigurationer.

Kommunikationen kan ske via FM IP-nät såväl via X.400 som IPS. Här nyttjar CAMA ett speciellt utvecklat IPS-protokoll. En X.400 - SMTP övergång nyttjas för elektronisk handel med FM civila handelsparter.

Klientprogramvaran måste nyttja någon av de programmeringsgränssnitt (API) som erbjuds. Följande finns (se tabell 2.1):

- C/C++ för DCE-RPC (Används av IS FV)
- C/C++ ONC RPC (Används av FS-systemen)
- C/C++ för DCOM (används av IS UNDSÄK)
- Active X för: VisualBasic, Delphi m fl
- Filöverföringar

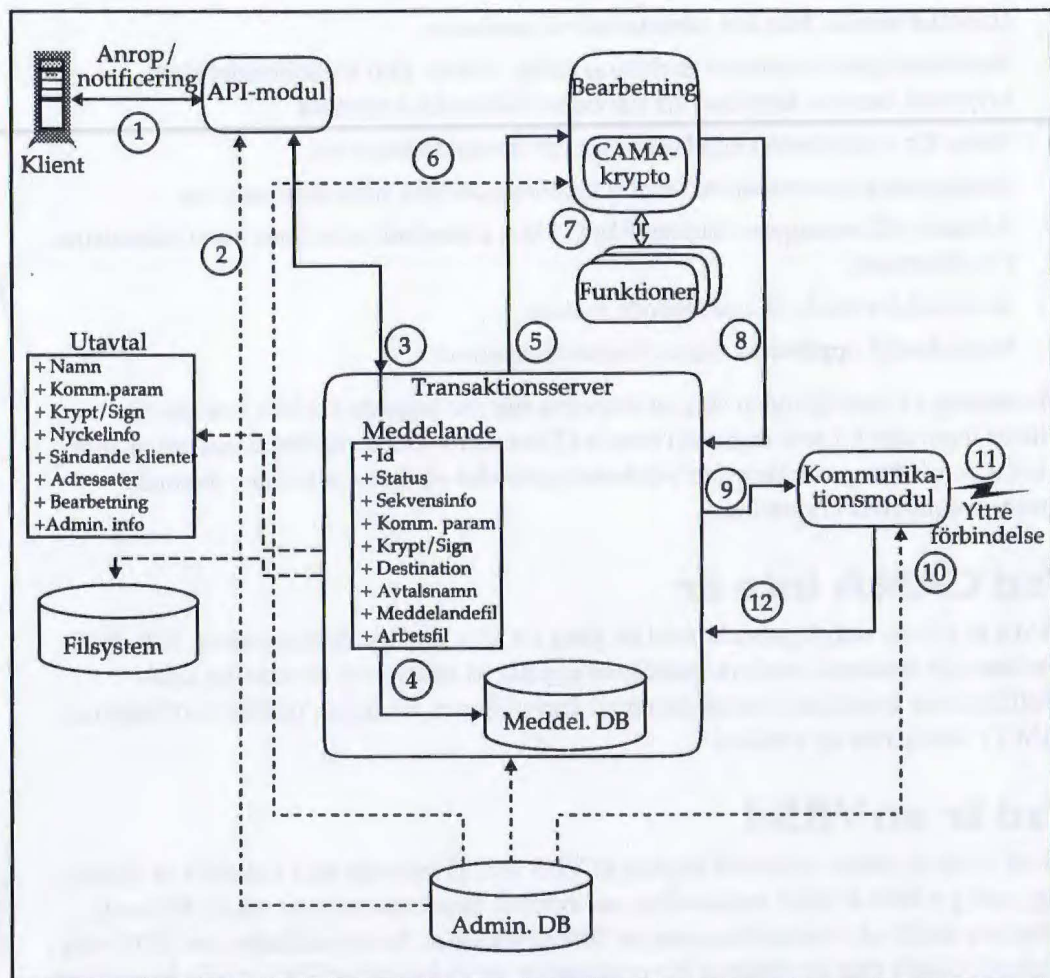
CAMA-tjänsten bygger på *juridiska EDI-avtal och tekniska ("elektroniska") avtal* som upprättas mellan involverade parter. De juridiska EDI-avtalen reglerar juridiska förhållanden och beskriver överförd information. De tekniska avtalen är konfigurerbara parametrar som styr, kontrollerar och övervakar överföringen. En CAMA Server kan betjäna ett eller flera lokalt använda tillämpningar (tidigare kallade VBS).

Tjänster för Elektronisk Handel (EH) Statsmakterna har tidigare bl a genom Toppledarforum (TLF), numera genom Gemenskapen för Elektroniska Affärer (GEA) verkat som en katalysator för införande av Elektronisk Handel inom såväl statliga myndigheter som kommuner och landsting. Införande av EH inom Försvarsmakten sker i samverkan med civila leverantörer. Som bärare av handelsdokument nyttjas CAMA, försedd med en kompilator benämnd EDI-C, och konvertering av handelsmeddelanden allt enligt EDIFACT-standard.

Typiska överföringstider av ett meddelande bestående av 50 tecken via X.400 är 2-5 minuter. Motsvarande överföring via IPS-port sker på sekundnivå.

CAMA meddelandesändning

Detta avsnitt beskriver på ett övergripande sätt hur sändning av ett meddelande hanteras av CAMA.



Figur 1 - CAMA version 3, översiktlig systemskiss

1. Klientsystemet anropar CAMA för att sända ett meddelande som refererar till ett bestämt utavtal.
2. API-modulen kontrollerar att utavtalet finns lagrat i den administrativa databasen. Om avtalet saknas, avvisas anropet.
3. API-modulen anropar transaktionsserver för att skapa meddelandet.
4. Beroende på om avtalet innehåller en eller flera mottagande VBS, skapas ett eller flera meddelanden i transaktionsserver. Varje meddelande lagras som ett objekt i meddelandedatabasen. Det egentliga meddelandet lagras som en fil i filsystemet. Denna fil behålls av systemet tills dess att all hantering av just detta meddelande har

avslutats (Om kvittens efterfrågas, inväntas också denna innan meddelandet anses avslutat). Om avtalet innehåller information och bearbetning, exempelvis komprimering, skapas en arbetsfil som används under bearbetningen.

5. Bearbetningsmodulen hämtar meddelandet från transaktionsserver.
6. Utavtalet hämtas från den administrativa databasen.
7. Bearbetsningsfunktionerna exekveras enligt avtalet. Om meddelandet skall krypteras, anropas kryptoserver varvid meddelandet krypteras.
8. Status för meddelandet uppdateras genom transaktionsserver.
9. Kommunikationsmodulen hämtar meddelandet från transaktionsserver.
10. Adressen till mottagaren hämtas från CAMA adressbok som finns i den administrativa databasen.
11. Meddelandet sänds till mottagande system.
12. Meddelandet uppdateras genom transaktionsserver.

Omsändning av meddelanden sker, exempelvis när mottagande CAMA inte lämnat kvittens inom den tid som angivits i avtalet (Time-Out). Det är transaktions-server som initierar omsändning och beordrar bearbetsningsmodul att klara ytterligare avtalade tjänster, exempelvis kryptering.

Vad CAMA inte är

CAMA är inte en statisk produkt med en gång för alla fastlagd funktionalitet. Allt efter-som krav och önskemål om nya funktioner uppstår så analyseras de varefter krav-specifikationer utvecklas i samverkan med kravställaren. Slutligen tillförs funktionerna i CAMA i form av en ny version.

Vad är en VBS ?

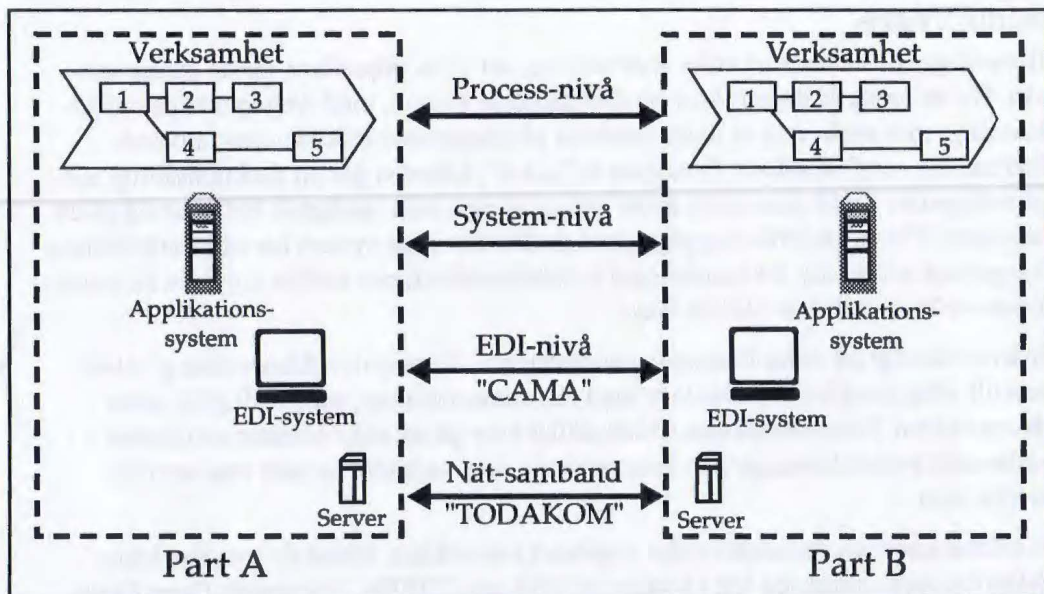
För ett 10-tal år sedan myntades begreppet VBS och då menade man i korthet en tillämpning, som ger stöd åt lokal verksamhet, exempelvis ekonomisystemet vid ett förband. Därutöver skulle all information som var förknippad med funktionaliteten hos VBS vara tillgänglig lokalt med sin databas. En grundtanke var också att en VBS med informations-databasen skulle vara transporterbar och medfölja ett "rörligt" förband som förflyttar sig.

Med den hastighet som Internet-, intranet-, och www-tekniken utvecklas, har begreppet "VBS" börjat vittra och måst tolkas om. Numera sägs i stället "lokalt använd tillämpning" oavsett om den nyttjade informationen finns lagrad lokalt, och nås via LAN, eller finns lagrad på annan plats och nås via ett intranet som det som exempelvis FM IP-nät utgör.

Teknikutvecklingen är på intet sätt begränsande för CAMA som via sitt Hyper Text Transfer Protocol (HTTP) är anpassat till www-teknik och kan överföra alla former av data.

Det måste framhävas att CAMA dock inte utgör en www-server trots att meddelanden kan förmedlas mellan www-server och Browser och omvänt.

Systemgränsnitt



Figuren visar två kommunicerande (system) parter, A och B, som nyttjar TODAKOM och CAMA tjänster. I det här fallet visas på den "lägsta" nivån nätsambandet som utgörs av MTA-enheter (Postkontor). MTA enheterna är i sin tur anslutna till FM-IP-nät vilket dock utelämnats i figuren.

På näst lägsta nivån, finns EDI-samband där CAMA tjänsteutbud kommer med i bilden.

Systemsambandet finns på näst högsta nivån. Då handlar det om anpassning av klient-programvara vilket kan ske på principiellt två olika vägar, antingen via API-programmering eller införande av ett sk fil-API.

Den högsta nivån utgörs av processsamband vilken är verksamhetens ansvar. En tänkt horisontell gräns mellan systemsamband och processsamband utgör den i detta avsnitt avhandlade sk "verksamhetsgränssnittet".

TODAKOM-projektet ansvarar för uppbyggnad av de två lägre nivåerna. Projektet samverkar på näst högsta nivån systemsamband vid integrering med olika system. Det är verksamheten som svarar för rationalisering och uppbyggnad av system anpassat just med avseende på den egna "verksamheten".

Programmeringsgränssnitt

Middle Ware

Tillämpningar utvecklade av olika leverantörer, vid olika tidpunkter, måste kunna samverka. För att uppfylla dagens krav på distribuerade system, med tyngdpunkt på objektorientering, som exekveras av andra moduler på geografiskt åtskilda orter, används principen *Remote Procedures*. Principen är "enkel", klienten gör ett funktionsanrop och exekveringen av funktionen sköts av en annan process som vanligtvis befinner sig på en annan dator. För att underlätta uppbyggnad av distribuerade system har olika arkitekturer och regelverk utvecklats för hanteringen av kommunikationen mellan objekten (klienter och Server's), som kallas Middle Ware.

Det är nödvändigt att dessa lösningar standardiseras. Systemutvecklare måste givetvis känna till vilka direktiv, ej förväxlade med rekommendationer, som skall gälla inom Försvarmakten. Försvarmaktens IP-nät ställer krav på att olika klienter och Server's i distribuerade systemlösningar kan kommunicera med varandra oavsett vem som har tillverkat dem.

Inte oväntat har flera standarder (eller regelverk) utvecklats. Bland de som kan kallas objektorienterade omnämns här i korthet DCOM och CORBA. Microsofts Open Group har fört samman gamla regelverk och distribuerar dem under namnet *Distributed Component Object Model (DCOM)*.

En industriorganisation med fler än 700 olika representanter för företag, forskning och slutanvändare, kallade Object Management Group (OMG), har enats om en standard vid namn *Common Object Request Broker Architecture (CORBA)*. De finns för flera olika plattformar och kan användas tillsammans med flera olika programspråk.

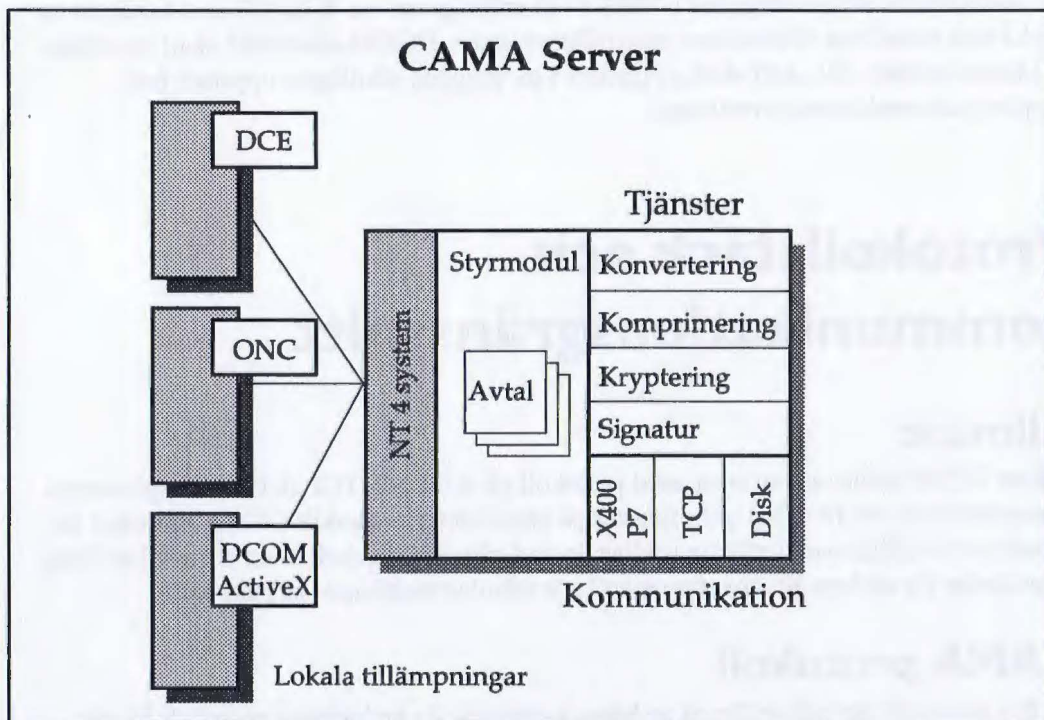
En tredje utbredd standard är Javas *Remote Method Invocation (RMI)* som är plattformsoberoende men kräver just Java som utvecklingsspråk. Därutöver finns ett antal andra lösningar som tangerar Middle Ware i Client Server lösningar exempelvis Sockets eller CGI-skript. Eftersom de ej är objektorienterade eller alltför begränsade för att göra anspråk som programspråks- eller plattformsoberoende, så omtalas de ej här.

Fördelarna med objektorienterade system är flera; välstrukturerade system med samma representation i analys, design och programkod. Felsökning och utbyggnad underlättas. I analys- och designfas kan uppdragsgivare utan kunskaper i programutveckling lättare förstå hur systemet är konstruerat. Kommunikationen underlättas och förändringsarbete förenklas. Återanvändning av kod kan utnyttjas.

För FM är Middleware av typen RPC och ORB aktuella. RPC representeras av två varianter, DCE-RPC och ONC-RPC. ORB representeras av CORBA och DCOM.

Sammanfogning med CAMA

För att kunna kommunicera via CAMA skall klientprogrammen utnyttja någon av de API-er som erbjuds. Beroende på funktionskrav och typ av klient finns olika API-moduler. Två av dem nyttjar RPC (Remote Procedure Control), DCE-RPC respektive ONC-RPC. API för DCE-RPC ger, förutom klientanrop till CAMA, notificeringar om händelser, exempelvis när meddelanden når adressaten. Ett tredje API nyttjar DCOM (Microsoft) som också medger notificering.



Figur 2.1 är en "sprängskiss" som visar CAMA anslutningsmöjligheter med tre st Middle Ware, styrmodul med avtalsdatabas, funktioner och slutligen kommunikationsmöjligheter.

Språk och access	Betyder	Användnings- område
C/C++ för DCE RPC	Distributed Computing Environment - Remote Procedure Call	Ledningssystem
C/C++ för ONC RPC	Open Network Computing Remote Procedure Call	Äldre UNIX- system
C+ för DCOM	C+ för DCOM	Ledningssystem

Anpassning av “äldre” klientsystem

Att fullt ut anpassa tidigare (äldre) utvecklade klientprogram till CAMA kanske ej är ekonomiskt försvarbart beroende på att klientprogrammet (systemet) inom sin tid skall växlas ut. Lämpligt är då att nyttja ett sk fil-API som länkas samman med klientprogrammet. CAMA funktioner kan emellertid då ej nyttjas i sin helhet.

4GL-anpassning i NT4-miljö

I NT4-miljö sker anpassning med CAMA av klientprogram via 4GL API som består av en modul som installeras tillsammans med tillämpningen. DCOM-klientstöd skall installeras på klientsystemet. 4GL-API skall ge tjänster i tre grupper, nämligen: uppstart, nedkoppling och meddelandeöverföring.

Protokollstack och kommunikationsgränssnitt

Allmänt

Bakom TCP/IP döljer sig ett stort antal protokoll på skikt 3-7. TCP-delen utför tjänster på transportskiktet och IP-delen utför tjänster på nätskiktet. Ett särskilt CAMA-protokoll har utvecklats för effektivare trafikavveckling än vad gängse protokoll mäktar med. Det finns inget hinder för att byta till annat protokoll när teknikutvecklingen så påkallar.

CAMA protokoll

CAMA protokoll har införts för att ge högre prestanda, än vad gängse protokoll förmår, med ett antal delfunktioner som ger tjänster för separata delar av TCP/IP-kommunikationen.

- Anslutning till det övriga CAMA systemet.
- Protokoll i CAMA, meddelande eller kvittens.
- Protokoll på TCP/IP nivå t.ex. fönsterstorlek och timeout.
- Protokoll i ett meddelande. Handskakning mellan datapaket och felhantering.
- Flera sessioner i samma socket. D.v.s. uppkopplingen behållas under en given konfigurerbar tid för att sända flera meddelanden om det under denna tid anländer nya meddelanden som skall sändas.
- Felhantering i TCP/IP. Bruten socket, timeout i mottagning.
- Det finns hantering om antalet sockets överutnyttjas så att förbindelser som då utnyttjas mindre måste tas i anspråk.

Protokollet har uppdelats i en sändande och en mottagande del. Nya och godtyckligt antal uppkopplingar kan sättas upp för kommunikationskanaler till andra CAMA enheter.

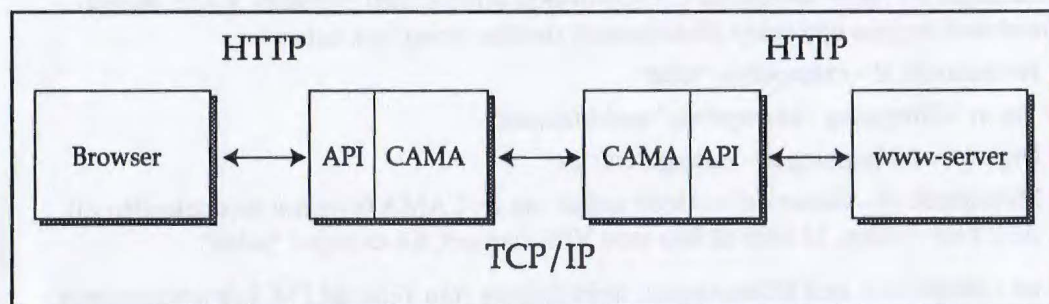
Kommunikation inom samma server sker ej *via socket* utan kopplas upp logiskt och hanteras internt i systemet. (Detta gör att en lokal uppkoppling belastar systemet minimalt). I övrigt skall en lokal uppkoppling vara identisk med en uppkoppling över en socket och skiljer sig ej i sättet att fungera. Högt prioriterade meddelanden har alltid att möjlighet att komma fram.

X.400 och P7-klient

CAMA utväxlar samband med X.400-trafik via P7-protokoll med Försvarmaktens civila handelsparter på såväl samma lokala nät som via WAN. (Se vidare i avsnittet om Clearing House).

HTTP och HTTPS

CAMA utnyttjar HTTP, som är ett högnivåprotokoll speciellt anpassat för WWW, med syftet att effektivt kunna transportera alla former av data med ett minimum av overhead. Betydelsefullt i HTTP är möjligheten att behandla information mellan klienten (Browser) och WEB-Server, även vidarebehandling av informationen. Fördelen med HTTP är att antalet TCP-förbindelser på fjärrlänken minskas, samtidigt som det ger möjlighet att reglera adresseringen på klientnivå. HTTPS är en utökning som innebär HTTP över Secure Socket Layer (SSL).



CAMA som förmedlare av trafik mellan Browser och WWW-server.

Gränssnitt för elektronisk handel

Allmänt

Electronic Data Interchange (EDI) utgör ett led i ett generellt arbete för att effektivisera administration och utbyte av information mellan företag. Med "Business to Business Communication", menas att handelspartners datorsystem direkt, eller via förmedlare av datatjänster, kommunicerar med varandra. Data struktureras på sådant sätt att det blir oberoende av vad mottagaren har för datorsystem. Elektronisk handel kan ske via automatiska processer, där två system utbyter information med varandra utan mänsklig inblandning. I vissa fall är det en människa som initierar dataöverföring eller hämtar (kontrollerar) affärsinformationen hos mottagaren. Ingrepp sker som regel i företagens befintliga datasystem som kompletteras med en kompilator för översättning av handelsdokument enligt en standard benämnd Electronic Data Interchange Format for Administration, Commerce and Trade (EDIFACT).

Mottagande tillämpning

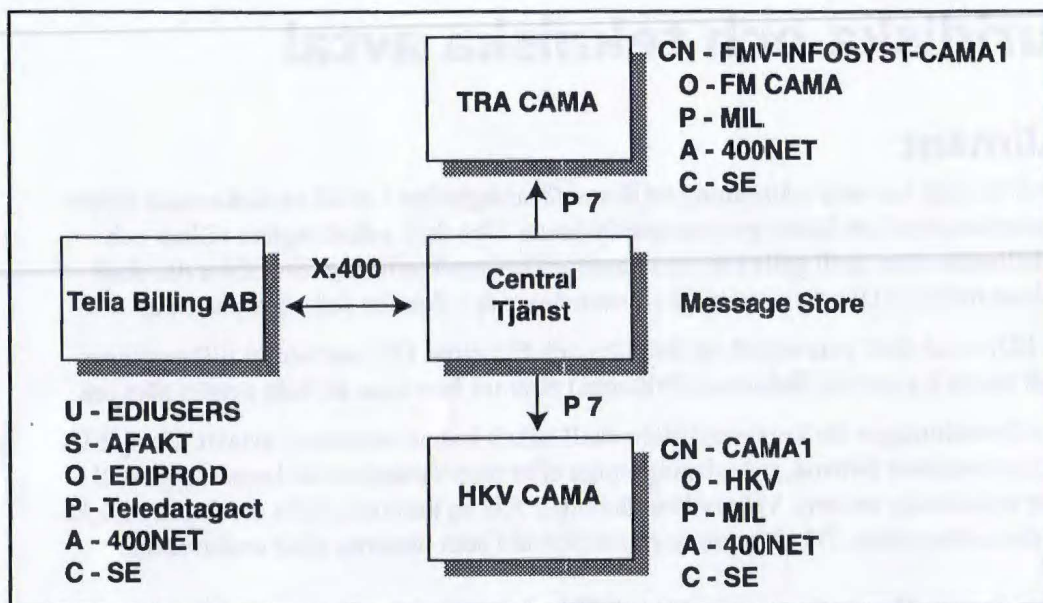
För att avsänd bunt handelsdokument, exempelvis fakturor skall nå fram till avsedd mottagare (VBS), läggs det i CAMA upp ett "avtal" som definierar mottagare. Detta avtal skall ange hur dokumenten ska EDIFACT-mappas. Detta innebär att det avsända meddelandet (fakturabunten) måste innehålla en hänvisning till namnet på ett CAMA-avtal.

Meddelandet inklusive namnet på CAMA-avtalet skickas med protokoll X.435. Avtalsnamnet skall byggas upp enligt fördefinierad struktur kring fyra delar:

- Avsändande id - exempelvis "telia"
- Typ av tillämpning - exempelvis "mobilfaktura"
- Utgåva av tillämpningen - exempelvis "01"
- Mottagande id - Denna del används endast om en CAMA levererar meddelanden till flera VBS-system. Id sätts då lika med VBS-namnet, till exempel "oden".

För att exemplifiera med tillämpningen mobilfaktura från Telia till FM, blir avtalsnamnet lika med "telia-mobilfaktura-01". För de fall flera VBSer sorterar under en CAMA blir namnet lika med "telia-mobilfaktura-01-oden".

En VBS samlar en eller flera redovisningsenheter, som är den egentliga "slutanvändaren" av ett handelsdokument. Redovisningsenheten skall identifieras med en fyrställig numerisk kod. De koder som används, skall framgå av det juridiska avtalet (Interchange Agreement) mellan exempelvis FM och Telia. Även EAN lokaliseringsnummer skall kunna användas för att identifiera mottagande enhet (eller avsändande enhet) enligt SFTI regelverk.



Elektronisk handel- princip för X.400 adressering med Försvarmaktens handelsparter. Mottagande redovisningsenhet.

Gränssnitt för ledningssystem

Ett viktigt exempel på en gemensam begreppsapparat för internationella sammanhang utgör Army Tactical Command and Control Information System (ATCCIS) och som studieprogram finansierat av NATO. Programmet har genomgått fyra faser sedan 1978. Fas IV har avslutats under 1999. ATCCIS övergripande mål är att öka samverkan hos NATO-ländernas ledningsstödsystem att dela och hantera information av gemensamt intresse hos kombinerade styrkor. Samverkan uppnås dels genom en gemensam informationsmodell, dels genom en mekanism för replikering av databaser. ATCCIS förslag till gemensam informationsmodell (Land C2 Information Exchange Data Model) är på väg att bli en NATO Standardization Agreement. Mest känd är ATCCIS informationsmodell som Generic Hub Data Model (GH). ATCCIS-funktionalitet skall nu tillföras CAMA. Det finns goda skäl att anta att ATCCIS kan tillämpas såväl i svenska ledningssystemen nationellt som internationellt.

Juridiska och tekniska avtal

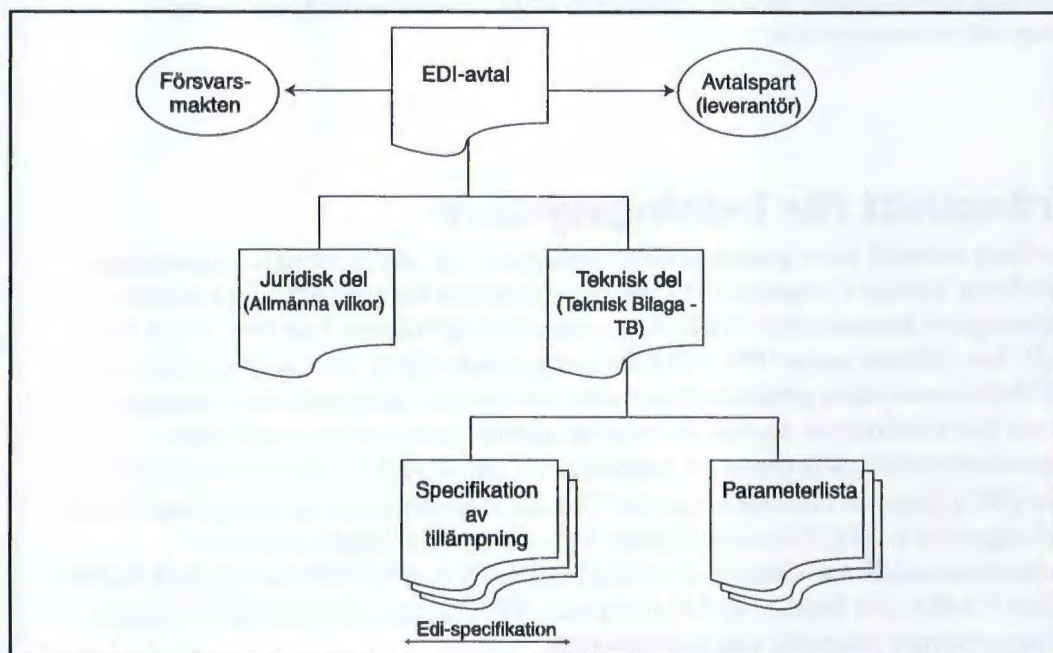
Allmänt

Ett EDI-avtal har som målsättning att skapa förutsägbarhet i såväl en elektronisk affärs-transaktion som i ett ledningssystemmeddelande. Det skall också reglera villkor och förhållanden som skall gälla i en viss kommunikationsöverföring. Ett EDI-avtal skall tecknas mellan EDI-avtalsparter. FM systemägare är i flertalet fall båda parterna.

Ett EDI-avtal skall vara enkelt att förändra och förbättra. Det innebär att tillämpningar skall kunna läggas till, förändras (förbättras) eller tas bort utan att hela avtalet görs om.

Nya förutsättningar för kommunikation skall enkelt kunna inordnas i avtalet. En ny EDI-part, exempelvis förband, redovisningsenhet eller motsvarande skall kunna läggas till eller en befintlig tas bort. Vid civil handel utgör FM en part och civila företag/myndigheter den andra parten. Då tillkommer en *juridisk del* som parterna skall underteckna.

Strukturell uppbyggnad av EDI-avtal



EDI-avtal - ett samlingsdokument

Ett EDI-avtal skall utformas som ett standarddokument med uppgiften att knyta samman avtalets olika delar (bilagor). EDI-avalet refererar sålunda till nedanstående bilagor.

Teknisk bilaga (Rutiner och registervård)

Den Tekniska Bilagan (TB) skall specificera överenskomna tekniska krav på informationssystem och övrig utrustning som används vid utväxling av EDI-meddelanden. Den tekniska bilagan är en del av det EDI-avtal som tecknats mellan parterna. Delar av TB beskrivs av skäl som är förknippade med FM organisation, i separata dokument eller underbilagor, t ex parameterlista. Referens görs härvid från berörda avsnitt i TB.

Förändringar och tillägg kan göras i TB utan att EDI-avtalet behöver göras om. Ändringar bekräftas av berörda parter genom påskrift av försättsblad till TB eller på annat lämpligt sätt. Förändringar i parameterlista eller underbilaga kan göras separat utan att TB ändras.

Juridisk bilaga

Den juridiska delen i EDI-avtalet kan exempelvis basera sig på Single Face To Industry (SFTI) standardavtal (Allmänna villkor) kompletterad och modifierad med nödvändiga tillägg beroende på FM säkerhetskrav. Den juridiska delen skall kunna användas som standardformulering oavsett avtalspart och enbart behöva förändras i undantagsfall, exempelvis vid generella förbättringar. Om det uppstår behov av förändringar i texten är det troligt att berörda delar av texten modifieras i en förhandling och dokumenteras i en särskild bilaga.

Parameterlista (uppgifter för en viss EDI-relation)

Parameterlistan innehåller specifik data för en viss redovisningsenhet. Parameterlistan består av fyra delar;

- administrativ information
- kommunikations- och syntaxdata
- specifikation av tillämpningen
- vad man faktiskt avtalat om

För att hålla ordning på vad man kommit överens om, har varje parameterlista ett unikt dokument- och utgåvenummer. Parameterlistan skall signeras av bägge parter.

Elektroniska avtal

Överföringen av meddelanden mellan klienter styrs av i förväg uppgjorda avtal. Dessa avtal definieras och administreras per CAMA-enhet. Avtalen reglerar mellan vilka klienter meddelandeöverföringen kan ske, hur den tekniskt kan gå tillväga samt hur den hanteras administrativt. Avtalen skall alltid delas upp i ett utgående avtal och ett inkommande avtal. Ett utgående avtal på en CAMA enhet måste alltid korrespondera med ett inkommande avtal på en eller flera andra CAMA Server's för att överföring skall vara

möjlig. I analogi måste ett inkommande avtal på en CAMA-enhet korrespondera till ett utgående avtal på en eller flera andra CAMA Server's.

Den allmänna delen i det elektroniska avtalet kan innehålla namn på involverade parter samt datum från vilket avtalet gäller. Men här finns också en fritextdel (512 tecken) som exempelvis kan hänvisa till juridiska "externa" avtal, förvaringsplats, vilket förband eller enhet som ansvarar för det m fl uppgifter.

Den tekniska delen i det elektroniska avtalet innehåller uppgifter som styr meddelandets behandling: adresser, prioritet, bibehållen sekvensordning, kvittenssvar, Time Out mm.

De tekniska avtalen skapas av CAMA-operatören på plats, eller Off-Line på en PC, och läses senare in till CAMA. Att "knappa" in ett elektroniskt avtal tar c:a en halv till en minut för en driven avtalsbyggare.

Avtalen delas alltid upp i ett utgående avtal och ett inkommande avtal. Ett utgående avtal på en CAMA måste alltid referera till ett inkommande avtal på en eller flera andra CAMA-system för att meddelandeöverföringen ska kunna genomföras. På samma sätt måste ett inkommande avtal på en CAMA referera till ett utgående avtal på en eller flera andra CAMA-system. Kopplingen till ett VBS styrs av CAMA:s in-avtal vid mottagning och ut-avtal vid sändning av meddelanden. En extern part som sänder eller tar emot meddelande har inte nödvändigtvis en CAMA men likväl ett CAMA-liknande system. För att en extern part ska kunna samverka med FM CAMA bör deras system klara av att hantera vissa parametrar, tex CAMA-avtalsnamnet.

För att erhålla ett inkommande CAMA-avtal registreras följande i CAMA:

- Avtalsnamn för inkommande avtal
- Sändande avtalsnamn för ett utgående avtalsnamn
- Om avtalet är aktivt
- Giltighetstid anger avtalets giltiga start och slutdatum
- Om X.435 används
- Administrativa uppgifter såsom namn och adress till respektive sändande och mottagande part
- Mottagande klienter som beskriver mottagande VBS och det API som används
- Notificerade klienter dvs. de VBS:er som ska notificeras
- Funktioner, tex EDIFACT-konvertering och vilket programscript som ska användas
- Säkerhet om kryptering används

För ett utgående CAMA-avtal registreras följande i CAMA:

- Avtalsnamn för utgående avtal och som är unikt begrepp i respektive CAMA
- Mottagande avtalsnamn för ett ev. inkommande avtalsnamn
- Om avtalet är aktivt
- Giltighetstid anger avtalets giltiga start och slutdatum
- Överföringssätt för att definiera hur denna CAMA ska kommunicera med andra adressater vid meddelandeöverföring via detta avtal

- Meddelandeöverföring, dvs. alltid i sekvensordning eller enbart det senaste mottagna
- Prioritet kan väljas
- Om X435 används
- Kvittenser

Juridiska och tekniska avtal - sammanfattning

Det juridiska avtalet, bygger på ett av Toppledarforum utvecklat avtal, som måste anpassas till de system som integreras med CAMA. Det juridiska avtalet gäller sålunda per system, de elektroniska avtalen, gäller per VBS-par. CAMA medger statiska eller dynamiska sändlistor. Då upprättas särskilda CAMA-avtal. För avtal som definierar sändlistor, bör avtalsnamnet vara lika för alla VBS som ingår i grupsändningen. Förvaltning av såväl elektroniska som juridiska avtal sker i samverkan med Master TODAKOM.

Vanligt är att omfattningen av analys- och dokumentationsarbete av verksamheten förbises i samband med införande av elektronisk informationsöverföring. Det finns en logisk uppdelning av EDI, dels ett tekniskt orienterat gränssnitt, dels ett verksamhetsorienterat gränssnitt. Det förstnämnda gränssnittet avser lösningar som för sitt förverkligande kräver teknikintresse. Det senare kräver kunskap och intresse för verksamheten. Den totala lösningen måste vara komplett dokumenterad så att ingen information saknas som omöjliggör driftsättning och förvaltning.

Systems Management

Allmänt

Begreppet Network Management (NM) omfattar såväl fysisk som logisk Network Management. Med det förra begreppet menas angreppssättet att få ett datanät, modem m fl hårdvaruorienterade komponenter, att fungera. Det faktum att komponenterna var för sig fungerar garanterar ej att nätverket fungerar i sin helhet. Begreppet logisk Network Management, har att göra med funktionen hos de logiska kommunikationskanalerna, mellan ändpunkter i systemet, exempelvis mellan en användare och en tillämpning.

Begreppen NM har nu vidgats så att de också täcker in personal som sköter om produktionen, dvs drift, planering och underhåll. Därmed har vi nått begreppet Systems Management.

Administration

En CAMA operatör skall kunna enkelt övervaka en CAMA-server, som finns på det "egna" lokala nätet, via annan arbetsstation under Windows NT (När tillräckligt stark autenticering finnes). Befintlig CAMA-konsol skall köras som en fristående tillämpning som kommunicerar med CAMA-server via CORBA, DCOM eller DCE-RPC/TeS. DCE-RPC Security skall kunna nyttjas. Konsolen skall nås av annan NT-dator.

Larm till operatör

CAMA skall kunna sända larm, när vissa tröskelvärden uppnåts, till en operatör via E-post, Minicall och mobiltelefon.

Fjärrövervakning

Genom speciella avtal skall statusrapporter hämtas från en CAMA-server. Funktionen skall ge möjlighet till central övervakning utan att brandväggar behöver öppnas för annan trafik än CAMA-meddelanden. Operatör vid Master TODAKOM skall kunna nyttja sin konsol och via FM IP-nät kunna avläsa status hos godtycklig CAMA-enhet.

Dubbelriktad testsändning skall kunna ske via brandväggar. Dubbelriktad testsändning innebär att CAMA-systemen automatiskt etablerar förbindelse i båda riktningar. Klienter skall kunna distribuera avtal mellan CAMA-system. Av säkerhetsskäl bör lokal aktivering ske innan avtalen tas i bruk.

Clearing House

Elektronisk handel bör baseras på gängse erfarenheter från industrin och affärsvärlden i övrigt bl a benämnda "Clearing House". Principen innebär i korthet att en central knutpunkt för elektronisk handel byggs upp, som betjänar "egna" verksamheten Försvarsmakten som med standardiserade och i förväg överenskomna protokoll förmedlar handelsdokument med involverade affärsparter. Nuvarande princip med decentraliserad EDIFACT-konvertering överges till förmån för en central konvertering av handelsdokument. Principen med Clearing House ger stora fördelar för elektronisk handel men påverkar i viss mån pågående arbete. FM Clearing House funktion skall verka som en gemensam knutpunkt för elektronisk handel med civila handelparter.

Funktionen skall kunna göra formatkonverteringar från ett antal olika "externa" protokoll och konvertera dem till protokoll som används inom FM.

I det juridiska avtalet skall bland annat beskrivas i vilket format meddelanden skall levereras och tas emot, samt vilket kommunikationsprotokoll som skall användas.

CAMA sköter de meddelandebearbetningar som krävs för att meddelandeformatet skall bli rätt samt växlar till för mottagaren överenskommet kommunikationsprotokoll.

Utbildning

För att klara installation, drift- och underhåll av CAMA erfordras utbildning för lokalt placerad driftpersonal. För mer information se utbildningsavsnittet.

Dokumentation

Dokumentation levereras i PDF-format på CD i samband med CAMA version 3.03 och sedan vid varje ny version.

Mallar förknippade med EDI-avtal levereras av Master TODAKOM i förändringsbar elektronisk form.

Drift och underhåll

Allmänt

För varje TODAKOM tjänst/system finns en framtagna underhållsplan system (UHP-S)

Underhållsplan system ger anvisning till berörda verksamhetsställen och myndigheter inom totalförsvaret för planering, styrning och uppföljning av drift och underhåll av materiel (maskin- och programvara) och trafikala funktioner under fred och kris.

Driftstöd kan återfinnas på tre driftstödsnivåer:

Lokal driftstödsnivå: bestående av lokal IT/ADB-resurs

Regional driftstödsnivå: bestående av Markteleenheter (MTE) och Underhållsregemente (Uhreg)

Central driftstödsnivå: bestående av Master TODAKOM , RAB/TNS och FMV

I detta kapitel beskrivs endast den centrala driftstödsnivån.

RAB/TNS

Vid RAB är den centrala driften för TODAPOST organiserad. Driftledningen utförs vid TNS. Med central drift menas:

- Drift av centrala system för TODAKOM
- Helpdesk
- Trafikkontroll

Centrala system

Omfattar drift av den tekniska plattformen för system ingående i TODAPOST. Övriga centrala system är Försvarsmaktens gateway mot publika nät, POSTBOX, SMS samt TODAKAT.

Helpdesk

Helpdesk TODAPOST svarar för det trafikala stödet till systemadministratörer och postmästare i TODAPOST. RAB/TNS fungerar även som postmaster för den uppringda tjänsten POSTBOX. Vidare administreras FM internet-domän mil.se innefattande tilldelning och registrering av IP-adresser inom FM .

Trafikkontroll

Trafikkontrollen genomför central driftledning och administration av brandväggssystem (FÄRIST, Z-RIST) inom totalförsvaret. Trafikkontrollen genomför trafikkontroll av FM-IP-näts anslutningar mot internet.

Master TODAKOM

Allmänt

Master TODAKOM är produktägarens verktyg för systemintegrering, vidmakthållande och kundstöd (inkl hantering av programlicenser) för tjänsterna:

- TODAPOST
- CAMA
- TODAKAT
- FÄRIST

Master TODAKOM är i fred lokaliserad till Enköping vid Upplands Regemente och är en totalförsvargemensam resurs. Master TODAKOM nyttjas av alla abonnenter inom totalförsvaret.

Verksamhet/ uppgifter

Master TODAKOM löser ålagda uppgifter under såväl fred som kris.

De övergripande verksamhetsmålen är:

- säkerställa att enbart godkända konfigurationer av programvaror och maskinvaror används vid totalförsvarets driftställen.
- kvalitetssäkra programvaror
- att ge ett kvalificerat bakre tekniskt stöd (backdesk TODAKOM)
- driva FM "Clearing House" (tjänst för elektronisk handel av såväl extern som intern omfattning)
- stödja projekt TODAKOM i fortsatt utveckling av TODAKOM funktioner/tjänster

Master TODAKOM deltar i hela processen, från kravfas fram till färdigtestad produkt. Detta för att på ett smidigt och naturligt sätt kunna överföra produkten i vidmakthållandefasen och på så sätt säkerställa att teknisk kompetens byggs upp inom FM stödorganisation i ett tidigt skede.

Master TODAKOM utgör också ett beredande organ för produktägaren, PÅ (HKV KRI LED) vid utarbetande av beslutsunderlag avseende införande av nya/ändrade funktioner i driftsystemen.

Helpdesk

Helpdesk TODAKOM hanterar samtliga felanmälningar och förfrågningar om TODAKOM-tjänsterna TODAPOST, CAMA, TODAKAT och FÄRIST. Felanmälningar och förfrågningar om FM IP-nät ställs till närmaste MTE.

Helpdesk TODAKOM består av två delar, en *frontdesk* och en *backdesk*.

Frontdesk utgör kontaktytan mot lokal driftstödsnivå (systemadministratör, postmaster, etc) och är lokaliserad vid RAB/TNS.

Backdesk är den del som löser felanmälningarna och utgörs av kompetens från RAB/TNS och Master TODAKOM.

Helpdesk TODAKOM ger stöd vid problemlösning genom att:

- ta emot felanmälningar, registrera fel, lösa problem och/eller bevaka att fel åtgärdas av annan instans
- distribuera information omfattande bland annat lösningar på återkommande problem och kommande versioner och funktioner.
- tillhandahålla utbytesenheter (UE) för lokal TODAPOST server och FÄRIST

Helpdesk TODAKOM kan också ge svar på frågor rörande

- register över Internet/X.400-domäner inom mil.se
- register över IP-nät nummer inom FM
- adresseringsbestämmelser
- adresseringsstöd
- centrala tjänster inom TODAPOST.

Felanmälan

Med fel menas brister i såväl programvara som i hårdvaruplattformen. Fel kan uppträda som funktionsavbrott eller begränsningar i funktion.

Felanmälan görs till **frontdesk**, i första hand via e-post:

helpdesk@tns.mil.se

eller telefax:

019 – 39 35 97

Akuta fel kan också anmälas per telefon:

019 – 39 30 70

Av felanmälan ska framgå:

- vem som anmäler (verksamhetsställe + systemadministratör eller postmaster)
- kontaktinformation (telefonnummer, e-postadress, etc)
- felyttring

I samband med felanmälan fås ett ärendenummer, som följer ärendet tills det är löst och kan avslutas. Ärendet prioriteras och placeras i kö hos **frontdesk**. Så snart ledig handläggare finns tillgänglig tas kontakt med felanmälande verksamhetsställe för hantering av ärendet.

Felhantering

Helpdesk TODAKOM säkerställer, tillsammans med aktuellt verksamhetsställe, att TODAKOM-tjänsten fungerar lokalt, i enlighet med gällande installations- och konfigurationsanvisningar.

Om felet kvarstår och det blir aktuellt att kontrollera TODAKOM-tjänsten mot andra system, exempelvis DNS eller FM IP-nät, lämnar Helpdesk TODAKOM över ärendet till MTE, Uhreg, etc för vidare åtgärder.

Alla instanser meddelar sedan vilka åtgärder som vidtagits, så att dessa kan noteras i lösningsdatabasen vid Helpdesk TODAKOM. Först när lösning finns noterad och aktuellt verksamhetsställe vidimerat lösningen, avslutas felärendet hos Helpdesk TODAKOM.

Utbildning av drift- och underhållspersonal

FM HS/IT-skolan och S 1/LedS har gemensamt ansvar för planering och genomförande av TODAPOST- CAMA- FÄRIST och FM IP-nät-utbildning inom FM. ÖCB ansvarar för att personal inom dess ansvarsområde ges möjlighet till nödvändig utbildning vid FM HS/IT-skolan respektive S 1/LedS. (se vidare avsnitt Utbildning).

Utbildning

Allmänt

Ett komplett och heltäckande kursutbud är framtaget.

FM HS/IT-skolan och S 1/LedS ansvarar för planering och genomförande av ett anpassat kursutbud.

Utbildningen är uppbyggd enligt en särskild struktur där vissa kurser utgör förkunskap för andra. För mera detaljerad information om förkunskapskrav, ordningsföljd, kursutbud, certifiering, kostnad och så vidare, kontakta FM HS/IT-skolan resp S 1/LedS.

S 1/LedS planerar och genomför all utbildning avseende TODAPOST och CAMA. IT-skolan planerar och genomför utbildning på Teknisk plattform och FM IP-nät inklusive FÄRIST.

Utbildningen genomförs till största delen med hjälp av speciallektionssalar och utrustningar vid respektive plats.

Sammanställning av utbildning

Utbildningen kan indelas i följande grupper:

- Tekniskt plattform
- TODAPOST
- CAMA
- FM IP-nät inklusive FÄRIST

Teknisk plattform

Kurs 4018C	WAN i FM	IT-skolan
Kurs 4036C	Lokal nät grunder	IT-skolan
Kurs 4071	TCP/IP Teknik	IT-skolan
Kurs 2428	Krypteringsutrustn. 530 för användare	IT-skolan
Kurs 943911	Unix Grundkurs	ATS
Kurs 4085B	Windows NT Administration	IT-skolan
Kurs 4081	Windows NT Installation/Konfigurering	IT-skolan

Genomförs vid

TODAPOST

Kurs 0480	Todakom systemkurs (1 dag för chefer)	LedS
Kurs 0481	Grundkurs Todapost (före 0482-3)	LedS
Kurs 0482	Kurs för systemadministratörer	LedS
Kurs 0483	Kurs för Postmästare & Instruktorer	LedS
Kurs 0485	Tilläggsutbildning för registratorer	FHS

CAMA

Kurs 0440	Översiktscurs CAMA (1 dag för chefer)	LedS
Kurs 0441	Kurs för CAMA operatörer	LedS
Kurs 0442	Kurs för CAMA systemadministratörer	LedS

Försvarsmaktens IP-nät

Kurs 4094B	CISCO ICND	IT-skolan
Kurs 4083	Förnyelse begränsad behörighet	IT-skolan
Kurs 4089A	CISCO BSCN	IT-skolan
Kurs 4095A	Routingprotokoll BGP	IT-skolan
Kurs 4100	Routingprotokoll ISIS	IT-skolan
Kurs 4095CT	Certifiering Allmän behörighet	IT-skolan
Kurs 4084	Förnyelse Allmän behörighet	IT-skolan
Kurs 4099	Felsökning FM IP-nät	IT-skolan
Kurs 4096	Övervakning HP Open View	IT-skolan
Kurs 4078	Sendmail, SMTP	IT-skolan
Kurs 4069	Domain Name System, DNS	IT-skolan
Kurs 4015	Brandväggsadministratör, FÄRIST	IT-skolan
Kurs 4281	Parallellportskrypto Teknik	IT-skolan
Kurs 4282	Parallellportskrypto Fjärr	IT-skolan

För mer detaljerad information angående utbildning

TODAPOST

E-post kursinfo-todapost@s1.mil.se

CAMA

E-post kursinfo-cama@s1.mil.se

FM IP-nät, FÄRIST och DNS

FM HS/IT-skolan:

E-post itsexp@fmhs.mil.se

Tel 035-266 25 00

Elevanmälan

TODAPOST

E-post elevanmalan-todapost@s1.mil.se

CAMA

E-post elevanmalan-cama@s1.mil.se

FM IP-nät, FÄRIST, DNS

FM HS/IT-skolan:

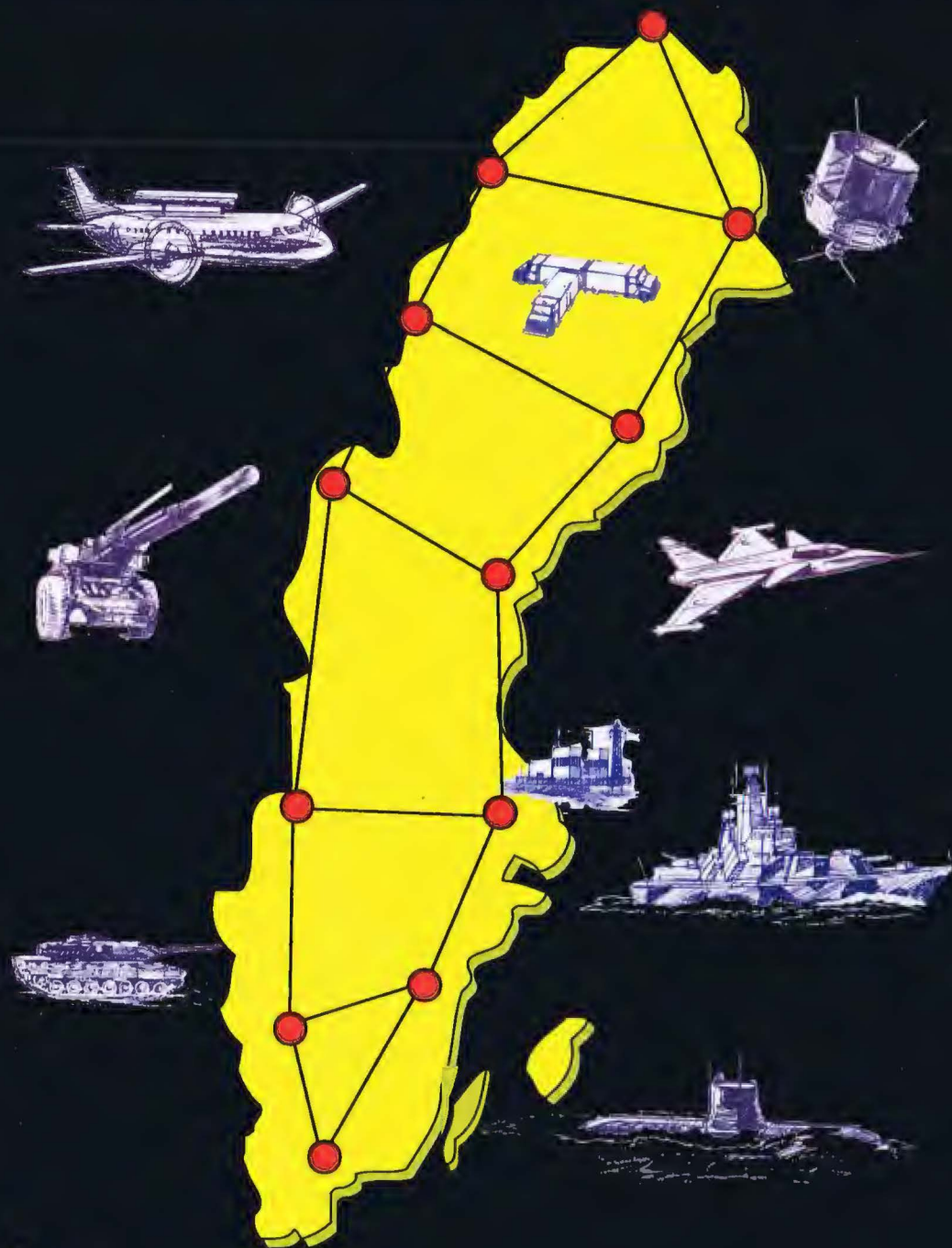
E-post itsexp@fmhs.mil.se

Tel 035-266 25 00

Fax 035-21 19 21

API	= Programmeringsgränssnitt
AS	= Autonoma System
ATCCIS	= Army Tactical Command and Control Information System
CAMA	= Computer Aided Messaging Architecture
CORBA	= Common Object Request Broker Architecture
DCOM	= Distributed Component Object Model
DNS	= Domain Name Ssyetm
DPT	= Dynamic Paket Traffic
EDI	= Electronic Data Interchange
EDIFACT	= Electronic Data Interchange Format for Administration, Commerce and Trade
EH	= Tjänster för Elektronisk Handel
FM IP-nät	= Försvarsmaktens IP-nät (Försvarets Internet)
FTN	= Försvarets TeleNät
FÄRIST	= Totalförsvarets brandvägg
GEA	= Gemenskapen för Elektroniska Affärer
GTP	= Generell Teknisk Plattform
HTTP	= Hyper Text Transfer Protocol
HTTPS	= Utökning av HTTP över SSL
IP	= Internet Protocol
IPS/H	= Internet Protocol Suite
LAN	= Local Area Network
LDAP	= Lighthouse Directory Axxess Protocol (katalogfunktion)
MIME	= Multipurpose Internet Mail Extension
MTE	= Markteleenhet
NTP	= Network Time Protocol
OMG	= Object Management Group
PKI	= Public Key Infrastructure
POP	= Protokoll för e-postklient
PÄ	= Produktägaren
RAB	= Redovisningsavdelning Bergslagen
RFC	= Request For Comment
RMI	= Remote Method Invocation
SA	= Systemadministratör
SFTI	= Single Face To Industry
S-MIME	= Secure – MIME
SMTP	= Simple Mail Transport Protocol (elektronisk posttjänst)
SSL	= Secure Socket Layer
SYMM TODAKOM	= Systemmålsättning TODAKOM
TCP/IP	= Trasmission Control Protocol/ Internet Protocol
TLF	= Toppledarforum
TNS	= Trafikal Nodstyrning
TODAKAT	= Tele- och Datakatalog
TODAPOST	= E-postsystem inom FM
TODAKOM	= Totalförsvarets Datakommunikation
WAN	= Wide Area Network
VBS	= Verksamhets Baserade System
VPN	= Virtuellt Privat Nät
WWW	= World Wide Web
ÖCB	= Överstyrelsen för Civil Beredskap

Försvarmaktens IP-nät



FÖRSVARMAKTEN