

# Forsvarsministeriets IKT-strategi 2008-2011

Indholdsfortegnelse .....	1
1. Indledning .....	2
2. IKT-vision .....	3
3. Forretningens krav til IKT-anvendelsen .....	4
4. IKT-styring og -organisering .....	7
5. IKT-arkitektur .....	9
6. Kompetencer .....	11
7. IKT-sikkerhed.....	13
8. Økonomi, optimering af IKT-driften og indkøb .....	15
9. Handlingsplaner .....	17

## **1. Indledning**

Forsvarsministeriets strategi for informations- og kommunikationsteknologi (IKT) dækker hele ministerområdet og tager udgangspunkt i ministerområdets formål og opgaver.

Strategien gælder i perioden 2008-2011 og fastlægger de centrale principper og målsætninger, der danner grundlag for planlægning, implementering og anvendelse af IKT ved koncernens myndigheder.

Strategien følger Statens It-råds vejledende skabelon for de statslige it-strategier og er udbygget med områder, hvor Forsvarsministeriet har behov for at fastlægge særlige retningslinjer.

IKT-strategien ajourføres som udgangspunkt hvert andet år.

IKT-strategien er godkendt af Forsvarsministeriet i september 2008.

## 2. IKT-vision

Forsvarsministeriets vision for IKT er, at:

***Der rådes over et fælles netværk af netværk, hvor der kan udveksles operative og forvaltningsmæssige informationer, nationalt såvel som internationalt. Informationerne skal præsenteres på én platform, hvor de er tilgængelige sikkerhedsmæssigt forsvarligt, i rette form, på rette tid og sted.***

IKT-strategien skal derfor:

***Tilvejebringe effektive og sikre redskaber til håndtering og udnyttelse af informationer i Forsvarsministeriet.***

Forsvarsministeriet ønsker med IKT-strategien at fortsætte den igangværende effektivisering og optimering af IKT-anvendelsen med henblik på frigørelse af ressourcer til løsning af ministerområdets kerneopgaver. Opgaver for andre offentlige institutioner og private virksomheder skal endvidere kunne løses. IKT-strategien understøtter de initiativer, som Forsvarsministeriets effektiviseringsstrategi fastlægger.

Forsvarsministeriet bidrager til regeringens strategi for digitalisering af den offentlige sektor. IKT-strategien opstiller et konkret mål om, at:

***Forsvarsministeriet vil arbejde og kommunikere digitalt og vil fra 2009 overgå til fuld elektronisk sags- og dokumenthåndtering.***

### 3. Forretningens krav til IKT-anvendelsen

#### Principper og tiltag

Forsvarsministeriets koncern løser operative opgaver som styrkeindsættelse, styrkeproduktion, beredskab, sejladsikkerhed og farvandsopmåling m.m., og skal som en del af centraladministrationen også løse en række forvaltningsmæssige opgaver. IKT-understøttelsen af det operative og forvaltningsmæssige område vil i perioden 2008-2011 foregå i forskellige IKT-systemer. På længere sigt vil den teknologiske udvikling i vidt omfang bevirke, at de to områder kan understøttes af samme IKT-systemer.

Tiltag på IKT-området, fx projekter, standardisering m.m., skal generelt være begrundet i kravet om effektiv anvendelse af ministerområdets ressourcer i lyset af kerneopgaverne eller i specifikke politiske krav til Forsvarsministeriets virksomhed.

"Aftale om forsvarets ordning 2005-2009", herunder omlægning af ressourcerne fra det forvaltningsmæssige funktionsområde til det operative funktionsområde samt opfyldelsen af regeringens strategi for digitalisering, skal understøttes af IKT-projekter. Dette sker bl.a. ved implementering af elektronisk sags- og dokumenthåndteringssystem (ESDH) og sammenkobling af Forsvarets Integrerede Informatiknetværk (FIIN) med Internettet, 1-NET-projektet.

#### Den operative virksomhed

Kravet til IKT-anvendelsen ved nationale operationer er interoperabilitet på nationalt niveau, dels inden for det militære forsvar, dels inden for totalforsvaret i samarbejde med øvrige myndigheder. I forbindelse med internationale operationer er kravet til IKT-anvendelse primært interoperabilitet med NATO-samarbejdspartnere, herunder i henhold til NATO-standarder. Den ønskede effekt er en fleksibel og interoperabel data- og kommunikationsudvikling mellem de deltagende myndigheder/enheder.

Det centrale fokus på det operative område er gennemførelse af netværksbaserede operationer (NBO), der vil kunne opnås ved at sensorer, våbensystemer og beslutningsstøttesystemer i størst mulig udstrækning integreres i et netværk af netværk. Den ønskede effekt herved er, at:

- Informationer kan udveksles på tværs af systemer, klassifikationsniveauer, værn, kommandoniveauer samt til og fra alliance- og koalitionspartnere.
- Informationer er til rådighed for beslutningstagerne i rette tid og sted.
- Enheder og myndigheder kan arbejde og kommunikere digitalt, herunder bl.a. danne grundlag for hurtigere beslutninger, højere operationshastighed, forbedret våbenlevering, og dermed skabe øget effektivitet og sikkerhed.

NBO stiller krav til udvikling af IKT-arkitektur, interoperabilitet, brug af åbne standarder m.m. både i relation til samarbejdet med NATO- og koalitionspartnere samt civile aktører. IKT-systemerne skal producere og formidle den nødvendige information til gennemførelse af den operative virksomhed døgnet rundt, både i relation til nationale og internationale operationer.

Med opbygningen af evnen til at deltage i og gennemføre NBO følger øget kobling gennem "netværk i netværk" på tværs af enheder, værn og nationaliteter. Dermed øges afhængigheden af såvel civile som militære informations- og kommunikationsnetværk for såvel forsvaret som for en potentiel modstander. Den øgede sammenkobling af netværk gør imidlertid også systemets enkelte aktører sårbare over en modstanders angreb i cyberspace. Cyberspace er således en kampplads, hvori forsvaret skal kunne operere og forhindre fjenden i at operere. Ud over fortsat at udvikle evnen til at forsvare egne systemer, skal forsvaret derfor udvikle en militær kapacitet til at gennemføre operationer i cyberspace i form af Computer Network Operations (CNO).

Et første skridt mod NBO er etableringen af 1-NET, som skal understøtte både den operative og forvaltningsmæssige virksomhed.

### **Den forvaltningsmæssige virksomhed**

Inden for Forsvarsministeriets område anvendes som udgangspunkt Dansk Forsvars Management - og Ressourcestyringssystem (DeMars) til Enterprise Ressource Planning (ERP). DeMars-systemet samler styring og forvaltning af økonomi, materiel, personel og struktur samt tilvejebringer ledelsesinformation for størstedelen af ministerområdet. Den fortsatte anvendelse og udvikling af DeMars skal bidrage til en effektiv digitalisering inden for Forsvarsministeriets område.

DeMars er baseret på SAP. Der foretages kun specialprogrammering i de særlige tilfælde, hvor Forsvarsministeriets myndigheder har et forretningsmæssigt behov, som ikke understøttes af SAP-standardfunktionalitet. Hvis der findes SAP-funktionalitet, tilpasses kravene til systemunderstøttelse af forretningsprocesserne som udgangspunkt hertil.

Tredjepartssoftware anvendes, såfremt der ikke findes brugbare SAP-løsninger, eller hvor det ud fra en samlet vurdering er økonomisk fordelagtigt. Tredjepartssoftware i form af IKT-værktøjer anvendes generelt til brug for integration af anden forvaltningsmæssig virksomhed med DeMars eller af de myndigheder, som fx anvender Navision.

Forsvarskommandoen og Forsvarets Koncernfælles Informatiktjeneste deltager i brugergrupper mv., i samarbejde med bl.a. andre nationers forsvar med henblik på at påvirke SAP til fortsat at udvikle forsvarsspecifikt software. Målsætningen vil være, at den operative opgaveløsning efterhånden bliver dækket af standardfunktionalitet.

For at forbedre datakvaliteten, minimere uddannelsesomkostningerne og effektivisere myndighedernes forretningsprocesser, skal myndighederne i størst muligt omfang anvende DeMars funktionalitet ens på tværs af ministerområdet.

Myndighedernes opgaver og ansvar i relation til drift, vedligeholdelse og videreudvikling af DeMars fremgår af bestemmelse for Forsvarskommandoens styringsorganisation vedrørende DeMars (FKOBST 385-2).

## **Digitalisering**

Forsvarsministeriet vil sætte særlig fokus på følgende områder udpeget af regeringen:

- Bedre digital service skal opnås gennem øget selvbetjening, individuel betjening af borgere og virksomheder med udgangspunkt i de enkeltes behov, og betjeningen skal være en del af centraladministrationens samlede service over for borgere og virksomheder. Al kommunikation med medarbejdere, øvrige borgere og virksomheder skal kunne ske digitalt og gennem forskellige digitale kanaler med høj grad af tilgængelighed.
- Øget effektivisering gennem digitalisering skal opnås gennem fortsat udvikling af igangsatte initiativer, herunder effektivisering af arbejdsgange ved anvendelse af fx Lean, business case-værktøjer og systematiske projektstyringsmetoder, udbygning og konsolidering af netværk samt modernisering af systemer, der understøtter styrkeindsættelse m.m.
- Stærkere forpligtende samarbejde om digitalisering skal opnås gennem aktiv deltagelse i Videnskabsministeriets tiltag vedr. standardisering og fælles arkitektur for centraladministrationen samt evt. tiltag afledt af Finansministeriets arbejde med administrative servicecentre i staten.

Ved udarbejdelse af nyt forvaltningsgrundlag samt ved rettelser af det eksisterende må der ikke stilles formkrav, der vil kunne udgøre en hindring for digital kommunikation, eller for at sagsbehandling mv. kan ske digitalt. Dette kan dog fraviges såfremt særlige forhold gør sig gældende, fx i relation til retssikkerhed, militær sikkerhed, lovgivningsmæssige forhold, traktatmæssige forpligtelser eller lignende.

Under hensyntagen til sikkerhedsmæssige og operative forhold skal fastlagte standarder mv. for centraladministrationen i videst mulig omfang følges og indarbejdes i Forsvarsministeriets koncerns IKT-arkitektur. Forsvarsministeriets myndigheder skal endvidere i videst mulig omfang under hensyntagen til sund økonomisk praksis og teknologiske muligheder tilbyde borgere og virksomheder mulighed for selvbetjening mv.

## 4. IKT-styring og organisering

### Organisering

Ansvar for informativirksomheden er fastlagt ved Forsvarskommando direktiv (FKODIR) 380-1. Direktivet gælder for Forsvarskommandoens myndighedsområde samt for andre myndigheder, der anvender ministerområdets IKT-infrastruktur.

Forsvarsministeriets departement fastlægger de strategiske mål samt godkender og iværksætter de væsentligste IKT-initiativer og -projekter inden for koncernen.

Forsvarskommandoens IKT og procesafdeling varetager udmøntningen af IKT-strategien inden for den koncernfælles IKT-virksomhed gennem udarbejdelse af handlingsplaner, varetagelse af projektledelse og implementering af projekter og initiativer på IKT-området samt rådgivning af departementet.

Forsvarskommandoens IKT og procesafdeling forestår den overordnede funktionelle styring af IKT-virksomheden i forsvaret og den strategiske udvikling samt planlægning af ministerområdets fælles IKT-anvendelse. Forsvarskommandoens IKT og procesafdeling sikrer i samspil med de forretningsprocesansvarlige (ansvarlige brugermyndigheder) sammenhængen mellem IKT og Forsvarskommandoens ledelsesprocesser, operative virksomhed og støttevirksomhed.

Forsvarskommandoens IKT og procesafdeling udgør den strategiske forankring af IKT-virksomhedens udførende niveau, Forsvarets Koncernfælles Informatiktjeneste.

Forsvarets Koncernfælles Informatiktjeneste er som koncernens IKT-faglige myndighed ansvarlig for gennemførelse af IKT-virksomheden. Dette indebærer fastlæggelse af de teknologiske og kommercielle rammer for anskaffelse af IKT-produkter og -serviceydelser, for standardisering og konfigurationsstyring, for kontakt til leverandører, indgåelse af kontrakter, forvaltning samt IKT-faglig rådgivning af koncernens myndigheder.

Forsvarets Koncernfælles Informatiktjeneste leverer IKT-serviceydelser til brugerne i henhold til indgåede Service Level Agreements med koncernens myndigheder. Aftalerne tager udgangspunkt i de behov for service den enkelte myndighed har.

Forsvarets Materieltjeneste har det overordnede ansvar for IKT-systemer, der udelukkende støtter styrkeindsættelse eller uddannelse hertil.

Forsvarets Efterretningstjeneste leder og kontrollerer på forsvarschefens vegne den forebyggende IKT-sikkerhed som en del af den militære sikkerhedstjeneste ved myndigheder mv. inden for koncernen.

### Styring

IKT-kvalitetsstyring og -sikring er forankret ved Forsvarets Koncernfælles Informatiktjeneste.

Til understøttelse af ministerområdets overordnede forretningsmæssige mål samles, hvor det er hensigtsmæssigt, IKT-projekter og aktiviteter i programmer, der gennemføres i henhold til programstyringsmetoden Managing Successful Programmes (MSP). I strategiperioden fokuseres især på 3 programmer, DANSWAN, DeMars-programplan og 1-NET.

Styring af IKT-virksomheden følger principperne for Best Practice IT-Governance. IKT-projekter iværksættes på baggrund af en godkendt business case og gennemføres som udgangspunkt ved anvendelse af PRINCE2<sup>1</sup> modellen. Dette gælder for såvel projekter med egen som med ekstern projektledelse.

Herudover skal IKT-sikkerhed indgå som et aspekt i samtlige af projektets faser, og Forsvarets Efterretningstjeneste skal inddrages tidligt i projektet.

Anskaffelse og implementering af større IKT-infrastrukturer og IKT-applikationer, der har karakter af udvikling og gennemførelse af forandringsprocesser, organiseres i projektorganisationer. Sådanne opgaver kræver et samspil af flere kompetencer og vil i vid udstrækning gå på tværs af ministerområdets organisation. Centraladministrationens fastlagte standarder mv. skal i videst mulig omfang anvendes i forbindelse med anskaffelse af nye eller udvikling af eksisterende systemer.

Ved anvendelse af IT Infrastructure Library (ITIL)<sup>2</sup> -processerne sikres, at IKT-ydelser bliver leveret på et veldefineret kvalitetsniveau (Best Practice) med professionalisme og fokus på forretningens mål. ITIL-processerne, herunder Service Level Management, giver grundlag for effektiv løbende vurdering og afstemning af forretningens forventninger, krav og behov.

### **Koordination**

Forsvarsministeriet har etableret koncernfælles Interessentgruppe Informatik (INTIT) til koordination af forhold af generel koncernfælles interesse inden for IKT-driftsfunktionen og behandling af IKT-faglige spørgsmål.

---

<sup>1</sup> PRINCE er en forkortelse af PROjects IN Controlled Environments.

<sup>2</sup> ITIL er en samling erfaringer af "best practices" for driftsledelse.

## 5. IKT-arkitektur

### Den overordnede arkitektur

Med henblik på at skabe sammenhæng og sikre IKT-systemers interoperabilitet, er der opbygget et hierarki af arkitekturniveauer, som er fastlagt i FKODIR 380-2 Arkitektur for Forsvarsministeriets IKT-systemer.

Der anvendes følgende overordnede arkitekturniveauer:

- NBO-målarkitekturen angiver det slutmål, som de samlede IKT-systemer skal bevæge sig mod. Målarkitekturen er udarbejdet i overensstemmelse med NATO Network Enabled Capability<sup>3</sup> Feasibility Study. Dermed sikrer NBO-målarkitekturen ikke kun national interoperabilitet, men også international (NATO) interoperabilitet.
- Forsvarets overordnede systemarkitektur, Defence Overarching Systems Architecture (DEFOSA), er en beskrivelse af sammenhængen i koncernens IKT-systemer, som danner grundlaget for udarbejdelsen af de enkelte IKT-systemers systemarkitektur.
- Systemarkitekturen er arkitekturen i det enkelte IKT-system.

IKT-arkitektur udarbejdes efter principperne for Serviceorienteret Arkitektur (SOA) i regi af NATO og det statslige standardiseringsarbejde.

### Den operative virksomhed

Gennemførelse af NBO i nationalt og internationalt regi, og dermed IKT-visionen "et netværk af netværk", stiller krav til Forsvarsministeriets koncerns IKT-systemer om at sikre den nødvendige interoperabilitet mellem egne IKT-systemer og IKT-systemer hos alliance- og koalitions partnere samt civile statslige og ikke statslige aktører.

NATO Information Infrastructure danner som udgangspunkt grundlaget for interoperabilitet mellem IKT-systemer og muliggør implementering af NBO og NATO Network Enabled Capability. NATO Information Infrastructure inkluderer også nationale netværk, deres muligheder for informationsudveksling, associerede processer og personel til indsamling af information herunder databehandling, lagring, management af information efter NATO behov, som støtte til en NATO-ledet mission. Tilslutning af lokale missionsnetværk til NATO Information Infrastructure sker gennem NATO Information Exchange Gateways.

NATO Network Enabled Capability Feasibility Study er sammen med NATO-arkitekturarbejdet styrende for Forsvarsministeriets IKT-arkitektur for så vidt angår den operative virksomhed. For at sikre interoperabilitet til NATO-arkitekturer vil Forsvarsministeriet gøre brug af NATO militært udviklede rammeværk NATO Architectural Framework samt det engelske rammeværk Ministry of Defence Architecture Framework.

---

<sup>3</sup> NATO-betegnelse for NBO.

Grundlæggende skal den nationale interoperabilitet sikres gennem aktiv deltagelse i nationale og internationale IKT-fora.

### **Den forvaltningsmæssige virksomhed**

Udviklingen af IKT-arkitekturen i nationalt regi sker i tæt samarbejde med Videnskabsministeriet. I den udstrækning det er muligt, skal anbefalede tiltag, der sikrer interoperabilitet mellem centraladministrationens myndigheder, som fx åbne standarder og initiativer i OIO m.m., følges.

De forvaltningsmæssige krav omhandler den bedst mulige udnyttelse af IKT gennem effektivisering og digitalisering af interne arbejdsgange og administrative processer. Dette opnås blandt andet gennem optimering af integrationer mellem systemer, herunder offentlige databaser.

### **Klassificerede netværk**

Forsvarsministeriets koncern vil sikre den nødvendige infrastruktur til understøttelse af udviklingen af NBO. Det eksisterende klassificerede netværk Danish NATO Secret WAN (DANSWAN) vil med implementering af NATO Information Exchange Gateway blive ministerområdets primære netværk til håndtering af data op til og med NATIONAL HEMMELIG samt NATO SECRET. DANSWAN er med NATO Information Exchange Gateway forbundet til NATO Secret WAN, hvorved netværkenes forbindelse til alliancepartneres netværk sikres.

Forsvarsministeriet anvender nationalt regeringens krisestyringsnetværk til hemmeligt (REGNEM) til behandling, opbevaring og transmission af informationer klassificeret til og med hemmeligt. REGNEM giver mulighed for udveksling af klassificerede oplysninger, anvendelse af telefoni og video-konferencer mellem myndigheder. I ministerområdet er REGNEM opstillet ved Forsvarsministeriet, Forsvarets Efterretningstjeneste, Forsvarskommandoen og Beredskabsstyrelsen.

## 6. Kompetencer

### Forsvarsministeriets kapaciteter

IKT-virksomheden i Forsvarsministeriet varetages på det strategiske niveau af Forsvarskommandoens IKT og procesafdeling.

Forsvarskommandoens IKT og procesafdeling er opdelt i to sektioner, hvor IKT-planlægningssektionen forestår den overordnede styring af IKT-virksomheden på det strategiske niveau, og DeMars planlægningssektionen er ansvarlig for strategisk styring af drift, vedligeholdelse og videreudvikling af DeMars.

De strategiske opgaver modsvarer af tilsvarende driftsorienterede opgaver, der bliver udført i Forsvarets Koncernfælles Informatiktjeneste. Ved at forankre Forsvarets Koncernfælles Informatiktjeneste strategisk i Forsvarskommandoens IKT og procesafdeling, sikres bedst mulig koordination. Endvidere sikres, at IKT såvel på det strategiske som på det udførende niveau gennemføres rationelt og driftsøkonomisk forsvarligt i forhold til Forsvarsministeriets opgaveløsning.

Koncernens IKT-kompetencer vedrørende drifts- og vedligeholdelsesmæssige forhold er centreret omkring Forsvarets Koncernfælles Informatiktjeneste. Forsvarets Koncernfælles Informatiktjeneste er organiseret som et videns- og kompetencecenter. Herved udmøntes et organisationsprincip og et ledelsesværktøj, hvor viden og ekspertise kan nyttiggøres på tværs af organisatoriske og strukturelle grænser.

Forsvarets Koncernfælles Informatiktjeneste har egne forretningsorienterede og teknologiske kompetencer. Desuden inddrages kompetencer fra civile leverandører og øvrige funktionelle tjenester.

Koncernens IKT-medarbejdere skal løbende gennemgå den nødvendige kompetenceudvikling inden for IKT-området til understøttelse af koncernens samlede opgavekompleks.

### Den operative virksomhed

Der er behov for, at den operative struktur og støttestrukturen råder over decentrale IKT-kompetencer. Drift af deployerbare IKT-systemer varetages af den operative og logistiske struktur i overensstemmelse med de operative behov ved anvendelse af enhedernes interne ressourcer, der vil kunne virke under de særlige vilkår og risici, den operative virksomhed medfører.

### IKT-arbejdspladsen

For at kunne fastholde IKT-medarbejderne med høje faglige kvalifikationer har forsvaret iværksat en række initiativer. Det er bl.a. initiativer som bedre løn og arbejdsvilkår, mere fleksible arbejdsforhold og personalegoder, der skal sikre medarbejdernes lyst til at blive i jobbet.

Koncernens vigtigste ressource er medarbejderne, og anvendelsen af IKT optager en stor del af deres dagligdag. IKT-systemer skal være brugervenlige og generelt ikke kræve omfattende brugeruddannelser. Der vil dog være krav til medarbejderen om gennem arbejdspladsen at tilegne sig og vedligeholde IKT-kompetencer for til fulde at udnytte de rådige IKT-systemer.

E-learning vil blive anvendt, når dette er muligt og hensigtsmæssigt. E-learning skal i videst mulige omfang anvendes som en integreret del af de uddannelses tilbud, som tilbydes medarbejderne. E-learning giver mulighed for en fleksibel kompetenceudvikling af medarbejderen. E-learning skal i et vist omfang indpasses i den normale arbejdsdag.

## 7. IKT-sikkerhed

### Grundlæggende principper

IKT-sikkerheden er beskrevet i Forsvarskommando bestemmelse (FKOBST) 358-1. Den militære sikkerhedstjeneste har som mål at beskytte koncernen mod trusler, der rettes mod personel, materiel, informationer, informatiksystemer, operationer og etableringer. Dansk standard for informationssikkerhed (DS 484) er indarbejdet i FKOBST 358-1.

Forsvarsministeriets myndigheder er pålagt at følge bestemmelserne for informationssikkerhed som fastlagt i FKOBST 358-1. Heri pålægges myndighederne at udarbejde og vedligeholde IKT-beredskabsplaner, der beskriver nødvendige mod-, opklarings- og genetableringsforanstaltninger, der skal iværksættes ved fysisk nedbrud af IKT-infrastrukturer.

Forsvarets Efterretningstjeneste, der er Forsvarsministeriets sikkerhedsmyndighed, yder rådgivning i forbindelse med den militære sikkerhedstjeneste m.m. Sikkerheden i IKT-systemerne skal være tilstrækkelig til at sikre konfidentialitet, integritet og tilgængelighed i henhold til de krav, der er opstillet til systemerne. IKT-systemer må ikke tilsluttes andre IKT-systemer uden forudgående godkendelse fra Forsvarets Efterretningstjeneste.

Styringen af IKT-sikkerheden er traktatmæssigt knyttet til NATO sikkerhedsbestemmelser og tager udgangspunkt i principperne for Risk Management, herunder PRINCE2.

### Multilateral sikkerhed

Det er et grundlæggende krav til sikkerhed i et netværk, at der foreligger en sikkerhedsmodel, der beskriver, hvilke sikkerhedsmekanismer netværket indeholder. Multilateral sikkerhed i forbindelse med sammenkobling af netværk skal tage udgangspunkt i forretningens krav til funktionelle sammenkoblinger mellem netværkene.

### Den operative virksomhed

IKT-sikkerheden under operationer adskiller sig ikke fra sikkerheden under normale forhold, og FKOBST 358-1 er derfor også gældende for den operative virksomhed.

NATO har påbegyndt etablering af en NATO Public Key Infrastructure (PKI). Der arbejdes på, at NATO PKI og nationale PKI-løsninger i form af Offentlige Certifikater til Elektronisk Signatur (OCES-certifikater) kan videreudvikles til at kunne samarbejde på et ensartet sikkerhedsmæssigt niveau.

### Den forvaltningsmæssige virksomhed

Forsvarets Efterretningstjeneste rådgiver i forbindelse med den militære sikkerhedstjeneste, godkender sikkerhedsmæssige foranstaltninger, varetager sagsbehandling af sikkerhedsspørgsmål, behandler sikkerhedsgodkendelse af personel samt bistår ved uddannelse inden for sikkerhedsområdet. Forsvarets Efterretningstjeneste løser i fornødent omfang ovennævnte opgaver i relation til private virksomheder, der udfører klassificerede opgaver for koncernen, NATO eller de lande, hvormed der er indgået bilaterale industrisikkerhedsaftaler. Den

militære sikkerhedstjeneste varetages i arbejdsgrupper, paneler og møder i NATO og andre internationale organisationer.

Ved udvikling og opdatering af Forsvarsministeriets IKT-systemer skal der anvendes metoder, der sikrer, at dataudveksling sker mellem IKT-systemerne og brugerne på autoriseret og godkendt vis. Det betyder, at IKT-systemerne og brugerne vil få tildelt godkendte digitale identiteter, fx i form af digitale certifikater (digitale signaturer). Forudsætningen for administration af digitale certifikater er, at der etableres infrastrukturer hertil, såkaldt PKI.

## 8. Økonomi

### Grundlæggende princip

Styring og forvaltning af IKT-virksomheden udvikles i overensstemmelse med koncernens styringsprincipper.

### Den operative virksomhed

For IKT-systemer til primær støtte af styrkeindsættelse eller uddannelse hertil i f.m. våbensystemer m.m. er anskaffelse delegeret til Forsvarets Materieltjeneste i samarbejde med de brugende myndigheder.

### Den forvaltningsmæssige virksomhed

Der er etableret en centraliseret IKT-drift med henblik på effektivt at understøtte ministerområdet forretningsprocesser. Den koncernfælles driftsmyndighed, Forsvarets Koncernfælles Informatiktjeneste, har ansvaret for anskaffelse, drift og vedligeholdelse af den koncernfælles infrastruktur og de fælles applikationer, der afvikles på infrastrukturen.

Forsvarets Informatikplan omfatter planlægningsgrundlaget for den centrale informatikvirksomhed i koncernen og indeholder midler til opstilling og drift af informatikkapacitet. Størstedelen af rammerne er bundet til driften af eksisterende infrastruktur og applikationer, og opstilling af ny kapacitet sker på baggrund af godkendte projekter i informatikplanen.

I overensstemmelse med statens regnskabsreform værdifastsættes det kontoradministrative IKT-udstyr og aktiveres i anlægsregnskabet. Forsvarets Koncernfælles Informatiktjeneste varetager som hovedregel denne opgave.

IKT-omkostningerne herunder afskrivninger fra den registrerede værdi af informatikkapaciteten og omkostninger til drift og forvaltning opsamles i en struktur, der afspejler de af FKIT udbudte IKT-serviceydelser. Omkostningerne fordeles til den operative virksomhed, henholdsvis støttevirksomheden ved intern afregning inden for Forsvarskommandoens myndighedsområde og ved fakturering til andre myndigheder samt Forsvarsministeriets departement<sup>4</sup>.

Med baggrund i Forsvarsministeriets udbudspolitik skal placeringen af IKT-opgaverne løbende vurderes, så de løses mest hensigtsmæssigt og effektivt. Det er Forsvarsministeriets samlede mål med udbudspolitikken at sætte fokus på uudnyttet potentiale for udlicitering og derved udnytte konkurrencen på det private marked til at opnå en høj effektivitet og kvalitet i løsning af driftsopgaver. Forsvarsministeriets myndigheder skal i højere grad koncentrere sig om løsning af strategisk vigtige kerne- og myndighedsopgaver. Drift og servicering af IKT-systemer er umiddelbart udbudsegnede opgaver.

---

<sup>4</sup> IKT-omkostninger fordeles til Hjemmeværnet i form af intern omkostningsafregning i henhold til strukturen i DeMars.

Den økonomiske styring af IKT-virksomheden omfatter styring af Forsvarets Koncernfælles Informatiktjenestes interne virksomhed, produktion af IKT-serviceydelser og styring af IKT-projekter.

### **Indkøb og salg**

Som konsekvens af centraliseringen af IKT-driften er indkøbsfunktionen så vidt muligt centraliseret ved Forsvarets Koncernfælles Informatiktjeneste. Derved tilstræbes en stringent og fuldstændig opgørelse af IKT-udgifterne. IKT-anskaffelser over Forsvarets Informatikplan gennemføres ved Forsvarets Koncernfælles Informatiktjenestes foranstaltning. Anskaffelser skal overholde Finansministeriets indkøbsaftaler på det statslige område samt koncernens øvrige rammeaftaler for standard produkter, der baseres på åbne og anerkendte standarder. Endvidere skal anskaffelserne leve op til koncernens krav til sikkerhed og et retvisende udgifts- og omkostningsregnskab. Der afsættes en ramme, inden for hvilken den enkelte myndighed kan prioritere midlernes anvendelse til anskaffelse, drift og vedligeholdelse af pc-relateret IKT-udstyr (skærme, pda, mus, USB-nøgler, scannere, internet udstyr mv.), der ikke er opkoblet på FIIN samt specifikke applikationer, der drives decentralt. Anskaffelser inden for de decentralt prioriterede midler foretages af en central indkøbsfunktion ved Forsvarets Koncernfælles Informatiktjenestes efter anmodning fra myndighederne.

Generelt gennemføres indkøb efter princippet bedst og billigst, idet dog også miljøbelastninger i form af eksempelvis strømforbrug inddrages i de driftsøkonomiske overvejelser.

De samlede omkostninger ved IKT-virksomheden fordeles på de forskellige styringsrelevante serviceydelser og afregnes til de enkelte myndigheder enten ved intern afregning (inden for Forsvarskommandoens myndighedsområde) eller ved udfakturering.

Som offentlig myndighed har Forsvarsministeriet et ansvar for at efterspørge produkter og tjenesteydelser, der belaster miljøet mindst muligt. I forbindelse med indkøb af IKT-udstyr med stort energiforbrug vil der samtidig være god driftsøkonomi i at inddrage miljøbelastninger.

## 9. Handlingsplaner

### **Forsvarets Informatikplan**

Forsvarskommandoen gennemfører planlægning af og disponering inden for IKT-området gennem Forsvarets Informatikplan, som er et tillæg til Forsvarskommandoen Kapacitetstilpasningsplan samt gennem direktiver og bestemmelser på IKT-området.

Forsvarets Informatikplan er på strategisk niveau forankret i Forsvarsstabens IKT og procesafdeling og på udførende niveau i Forsvarets Koncernfælles Informatiktjeneste og skal ses i sammenhæng med Forsvarskommandoens øvrige overordnede strategiske planlægning.

Forsvarets Informatikplan tilvejebringer en fyldestgørende og sammenhængende plan for de samlede aktiviteter inden for IKT-virksomheden og de hermed forbundne økonomiske rammer samt den overordnede ansvarsfordeling i planperioden. Informatikplanen danner grundlag for den løbende implementering og sikrer udviklingen af Forsvarsministeriets IKT-systemer. Planen afspejler de indbyrdes sammenhænge, samt optimering af de anvendte ressourcer på området. I takt med planens udvikling fastsættes den økonomiske ansvarsfordeling for de enkelte projekter i detaljer. I denne forbindelse sikres den ønskede og mest hensigtsmæssige integrering i den fælles infrastruktur. Forsvarets Informatikplan opdateres årligt og tildeles økonomiske rammer fra Forsvarskommandoens Årsprogram.

### **Programmer/projekter**

Højest prioriterede:

#### ***Netværksbaserede operationer***

Udviklingen af NBO er forankret i Forsvarskommandoens Planlægnings- og driftsstab. Styregruppen vedrørende Netværksbaserede Operationer udgør det overordnede forum, hvor NBO udvikling - såvel nationalt som internationalt - følges og med baggrund heri, er det styregruppens opgave at koordinere, indarbejde og forankre NBO i koncernen.

Forudsætningen af gennemførelsen af NBO er, at der etableres et netværk af netværk, hvor informationer principielt kan udveksles frit omend med visse sikkerhedsmæssige begrænsninger. Der skal udarbejdes en samlet plan for udvikling af koncernens højere klassificerede netværk, i regi af DANSWAN og et værnsmæssige kommando-, kontrol- og Informationssystem. NATO Information Exchange Gateway, således at DANSWAN bliver Forsvarsministeriets primære netværk til håndtering af data op til og med NATIONAL HEMMELIG og NATO SECRET og gennem DANSWAN skabes den primære adgang til alliancepartners og NATO netværk.

#### ***Koncernens IKT-arkitektur***

Forsvarskommandoen har nedsat en koncernfælles arbejdsgruppe vedrørende IKT-arkitektur (AG/IKTARK), der har til formål at skabe fælles forståelse for IKT-arkitektur, udarbejde definitioner og begrebsapparat, indstille valg af standarder for hele koncernen, udarbejde FKODIR

380-2, Arkitektur for Forsvarsministeriets IKT-systemer samt vedligeholde forsvarets målarkitektur og forsvarets overordnede systemarkitektur (DEFOSA). Arbejdet med IKT-arkitekturen skal:

- Tilgodese serviceorienterede løsninger.
- Baseres på IP netværk.
- Understøtte evolutionær design og vedligeholdelse.
- Sikre informationsudveksling med internationale partnere.
- Fastsætte nødvendige koncernfælles standarder.
- Tilgodese koncernens IKT-systemers beskyttelse.

AG/IKTARK varetager endvidere rollen som sektorstandardiseringsråd.

### ***Programplan for DeMars***

Der udarbejdes en programplan, der skal være styrende for udviklingen af DeMars i de kommende 4-6 år. Programplanen skal tjene dels som grundlag for fastlæggelse af det forretningsmæssige ambitionsniveau for udviklingen af DeMars, dels som grundlag for at træffe beslutning om hvornår, der skal foretages en opgradering af DeMars. Programplanen skal fokusere på opnåelse af forretningsmæssige gevinster og i den sammenhæng inddrage regeringens strategi for digital forvaltning.

En opdateret teknisk platform for DeMars forventes implementeret ultimo 2008. Med udgangen af nærværende IKT-strategi periode forventes DeMars desuden at være optimeret med den særlige industriløsning, Defense Solution. Defence Solution indeholder funktionalitet, som er særligt rettet mod forsvaret og andre landes militære organisationer, og dermed medvirker til at gøre DeMars mere fleksibel og økonomisk.

### ***1-NET***

Ved gennemførelse af programmet 1-NET åbnes mulighed for, at koncernens medarbejdere kan kommunikere på internettet fra koncernens standardarbejdsplads. Herved forventes opnået en mere effektiv sagsbehandling, bedre muligheder for automatisk dataudveksling og kommunikation med leverandører, borgere, myndigheder mv. uden for ministerområdet. Den øgede effektivitet, kombineret med stordriftsfordele og bedre udnyttelse af eksisterende netværksteknologi forventes at medføre besparelser på koncernens IKT-budget. Hertil kommer forretningsgangsmæssig optimering. Forudsætningen for etablering af 1-NET er, at IKT-sikkerheden i netværket er på et for koncernen acceptabelt niveau, såvel hvad angår krav til fortrolighed, integritet, tilgængelighed og uafviselighed.

Programmet vil tilbyde brugerne internet browsing, internet mail, indhentning af filer samt E-handel fra FIIN computeren. Programmet forventes implementeret ultimo 2008.

### ***Elektronisk sags- og dokumenthåndtering***

Digital sagsbehandling er et centralt område i den digitale forvaltning og elektronisk sags- og dokumenthåndtering (ESDH) er et vigtigt element heri. Med henblik på at overholde fælles-

statslige standarder og sikre den nødvendige informationsudveksling (vidensdeling) og dokumentation inden for koncernen, og på sigt med resten af den offentlige sektor, sker implementeringen af ESDH i rammen af det Fællesoffentlige Elektroniske Sags- og Dokumenthåndteringsprojekt (FESD).

Forsvarsministeriet har ved ESDH-projektets start fastlagt en række effektiviseringsmålsætninger for implementering af det koncernfælles ESDH-system. Der skal opnås effektiviseringer inden for følgende områder:

- Reduktion og automatisering af journaliseringen af dokumenter.
- Reduktion og forenkling i udarbejdelsen af sagsoversigter og -statistik (sagsstyring).
- Reduktion i kopiering til internt brug.
- Forenklet genfindning af sager/dokumenter.
- Reduktion i arbejdet med arkivering og oprydning.
- Minimering af koncernens posthåndtering i forbindelse med afhentning, aflevering, adressering, afsendelse, sortering mv.
- Reduktion af fysiske papirarkiver.

Forsvarsministeriet forventer at ESDH-projektet vil være rentabelt over en 4-årig periode og dermed inden udgangen af indeværende forsvarsforlig. Implementeringen er iværksat og projektet forventes afsluttet med udgangen af 2008.

#### ***Sikkerhedsstandard DS 484***

Regeringen har besluttet, at alle statslige myndigheder skal efterleve de basale krav i Dansk Standard 484 "Standard for informatiksikkerhed" (DS 484). Forsvarets Efterretningstjeneste har fået til opgave at koordinere implementeringen i koncernen og forestår arbejdet med at tilrette de militære bestemmelser på de områder, hvor de ikke lever op til DS 484. Der kan dog være områder, hvor det ikke er hensigtsmæssigt eller muligt at implementere DS 484, fx i operative systemer.

DS 484 er blevet indarbejdet i bestemmelserne for den militære sikkerhed, FKOBST 358-1. Der er dog stadig krav i DS 484, som ikke dækkes af FKOBST 358-1. Disse krav skal dels indarbejdes i andre koncernfælles bestemmelser og dels indarbejdes i myndighedsspecifikke bestemmelser. Forsvarets Efterretningstjeneste vil koordinere og følge op på det fortsatte arbejde med kravene i DS 484 hos myndighederne, bl.a. med indførelse af en ny it-sikkerhedsorganisation. Uddannelser i forhold til den nye it-sikkerhedsorganisation starter op i foråret 2008.

#### Øvrige prioriterede:

#### ***Forsvarsministeriets portal på internettet***

Der etableres en overordnet portal, som samler indgangen til ministerområdets hjemmesider på internettet. Forsvarsministeriets portal skal indgå som en integreret del af borger- og virk-

somhedsportalerne senest fra 2009. Udviklingen af portalens version 1 er i gang, og portalen forventes at blive lanceret i 2008. Portalen skal medvirke til en mere målrettet kommunikation med omverdenen, herunder stille services/tjenester til rådighed til brugerne. Indledningsvis henvises til koncernens øvrige hjemmesider, men på sigt skal kommunikationen på tværs af hjemmesiderne øges. På baggrund af en både intern og ekstern interessentanalyse skal fremtidige behov for udvikling af portalen defineres. I forbindelse med etablering af portalen for ministerområdet skal der:

- Gennemføres en designmæssig koordinering af de eksisterende hjemmesider med henblik på at lette informationssøgningen for brugerne. Koordineringen skal munde ud i koncernfælles retningslinjer for design, herunder "branding" og en mere ensartet navigering og struktur på ministerområdets hjemmesider.
- Udarbejdes en koncernfælles strategi for kommunikation via internettet.

### ***Koncernfælles teknisk platform for internetkommunikation***

Hensigtsmæssigheden af at migrere alle koncernens hjemmesider til en koncernfælles teknisk platform, såvel servermæssigt som applikationsmæssigt, analyseres i 2009.

### ***Telefoniområdet***

Optimering af Forsvarsministeriets telefoni skal med afsæt i forsvarets forvaltningspraksis inden for fastnet- og mobiltelefoni analysere muligheder for fremadrettet opnåelse af et besparelsesprovenu. Udgangspunktet for analysen tages i den eksisterende Koncernfælles Telekommunikationsgruppe (KTG), der omfatter hele ministerområdet. Analysen påregnes afsluttet primo 2008 og vil bl.a. specificere strukturen på telekommunikationsområdet, telefonimønstre, volumen og serviceomkostninger. Dokumentationen vil danne grundlag for den fremtidige telestrategi og benchmarking af alternative teleaftaler samt evt. estimering af et samlet årligt bespareelsepotentiale for koncernen.

### ***E-handel***

Forsvarsministeriet vil, hvor det er muligt og økonomisk fordelagtigt, benytte elektronisk handel til indkøb, som det fremgår af cirkulære nr. 9608 af 20. december 2002, "Cirkulære om indkøb i staten". Målet for E-handel er defineret i Forsvarsministeriets indkøbspolitik af november 2001. Det forudsættes, at DeMars skal indgå som en integreret del af ministerområdets E-handelsløsning. Løsningen skal dog være koordineret med de krav, der er til indkøb ved anvendelse af NATO-kodificering.

### ***Forvaltning af frivilligt og reservepersonel***

Der skal implementeres, og løbende videreudvikles systemer, som muliggør en større grad af selvforvaltning af frivilligt personel, herunder Hjemmeværnets frivillige, samt personel af reserven. Disse systemer skal sikre en høj servicekvalitet samt en effektivisering af denne forvaltning.

### ***Den offentlige virksomhedsportal***

Virksomhedsportalen er den fællesoffentlige servicekanal over for virksomhederne. I 2009 skal virksomhederne kunne anvende alle statslige og kommunale erhvervsrettede digitale indberetningsløsninger via virksomhedsportalen gennem single sign-on med digital signatur. Forsvarsministeriet deltager i udviklingen af den fællesoffentlige strategi for, hvordan de offentlige services skal tilbydes borgere og virksomheder (en kanalstrategi) med henblik på at blive en integreret del heraf.

### ***Tilgængelighed på hjemmesider***

Tilgængeligheden på hjemmesider skal fremmes, bl.a. ved at der indføres obligatoriske krav til tilgængelighed i forbindelse med obligatorisk brug af åbne standarder i det offentlige. Herudover skal IT- og Telestyrelsens publikation "Statens retningslinjer for hjemmesiders og netsteders tilgængelighed" følges.

### ***Indblik i egne ESDH-sager***

Forsvarsministeriet vil indarbejde en løsning til at give borgere og virksomheder overblik over deres sager i ministerområdets sags- og dokumenthåndteringssystemer, når det nødvendige grundlag er tilvejebragt i FESD-regi, forventeligt i 2010, og i det omfang der ikke sker kompromittering af sikkerheden.