

Svenska delen av Internet

INNEHÅLLSFÖRTECKNING

	Sida
1 Statskontorets sammanfattning _____	7
2 Bakgrund _____	12
2.1 Uppdraget _____	12
2.2 Förtydligande och avgränsning av uppdraget _____	13
2.3 Genomförande av utredningen _____	14
2.4 Rapportens innehåll _____	14
2.5 Samråd _____	16
2.6 Propositioner, utredningar och projekt _____	16
3 Vad är Internet? _____	17
4 Dagens och morgondagens situation _____	20
4.1 Internet i dag - fortfarande bara i början på utvecklingen ____	20
4.2 Morgondagens nät _____	21
5 Användning av Internet i Sverige _____	22
5.1 Registrerade domännamn _____	22
5.2 Användningen i Sverige _____	23
6 Tillväxt av Internet i världen _____	24
6.1 Antal datorer _____	24
6.2 Antal användare _____	24
7 Kommunikationsarkitektur för Sverige _____	26

8 Förutsättningar för Internet i Sverige	31
9 Analys av framtida trafikvolym	33
9.1 Syftet med analysen och uppskattningarna	33
9.2 Trafikuppskattning byggd på erfarenhet	34
9.3 Trafikuppskattning - maximialternativ	35
9.4 Bedömning	36
10 Struktur för Internet i Sverige	37
10.1 Huvudkomponenter i den svenska delen av Internet	37
10.2 Operatörens nät med tillhörande stödsystem	38
10.3 Användarens nät	42
10.4 Gemensamma resurser - översikt	43
10.5 Samverkan mellan operatörer	44
11 Internetoperatör, minimal IP-tjänst och ansvarsfördelning	45
11.1 Internetoperatör	45
11.2 Minimal IP-tjänst	47
11.3 Ansvarsfördelning mellan operatörer	47
11.4 Ansvar för regler m.m.	49
12 Nationella knutpunkter för samtrafik	50
12.1 Förutsättningar	50
12.2 Nationell knutpunkt	50
12.3 Nationella knutpunkten i Stockholm	51
12.4 Förslag till utbyggnadsplan	51
13 Gemensamma resurser	55
13.1 Gemensamma resurser utöver knutpunkterna	55
13.2 DNS för toppdomänen .se	56
13.3 Namnserver för DNS-roten	57
13.4 Tidsserver för nationell tid	58

13.5 Vägvalsregister	59
13.6 Indexserver	60
13.7 Whois-server	60
13.8 Drift vid avspärning	61
13.9 Beredskapsdrift av DNS	61
14 Namn- och adressplan	63
14.1 IP-adresser	64
14.2 AS-nummer	66
14.3 Domännamn	67
14.4 Alternativa organisationsformer för domännamnshanteringen	74
14.5 Statskontorets syn på namn- och adresshanteringen	75
15 Finansiering av gemensamma resurser	77
16 Hot mot nätet och nätets tillämpningar	79
16.1 Uppdrag och avgränsningar	80
16.2 Fysiska hot mot infrastrukturen	80
16.3 Kontinuitetsplanering	83
16.4 Logiska hot mot infrastrukturen	83
16.5 Beroendeförhållanden	86
16.6 Organisations- och ansvarsfrågor	87
16.7 Samhällets ansvar	90
17 Säkerhetsarkitektur för Internet i Sverige	92
17.1 Behov av säkerhetsfunktioner	93
17.2 Säkerhetstekniker	95
17.3 Nulägesbeskrivning	106
17.4 Ackreditering av CA	109
17.5 Hinder mot att tillgodose säkerhetsbehovet	110
18 Utbildning och kompetensförsörjning	114

19 Accessnät och tillgång till information	116
19.1 Bakgrund	116
19.2 Nätstrukturen närmast användaren förändras	116
19.3 Bredbandsaccess till hushåll	117
19.4 Tillgång till information	117
20 Telefoni över Internet	118
20.1 Bakgrund	118
20.2 Varför telefoni över Internet?	119
20.3 Problemen med telefoni över Internet	120
21 År 2000-problemet	123

Bilagor

Bilaga	Sida
1 Sammanställning av samrådssvar _____	125
2 Direktiv för uppdraget _____	127
3 Deltagare i utredningen _____	130
4 Ordförteckning _____	132
5 Propositioner, utredningar och projekt _____	138
6 Internet i Sverige - kort historisk och teknisk överblick _	143
7 Tillämpning av Internet inom olika områden _____	168
8 Organisationer i Sverige _____	173
9 Infrastruktur för Internet i Sverige _____	179
10 Användning av Internet i Sverige _____	182
11 Operatörsenkät _____	184
12 Användarenkät _____	188
13 Tillväxten av Internet i världen _____	191
14 Den nationella knutpunkten i Stockholm _____	194
15 Specifikation av minimal IP-tjänst _____	199
16 Hotbilden mot nätet och dess tillämpningar _____	205
17 Säkerhetstjänster _____	216
18 Bredbandsaccess med användning av xDSL-tekniken ____	228
19 Bredbandsaccess via Kabel-TV-nät _____	231
20 Telefoni över Internet _____	233
21 Transmissionsnät i Sverige _____	240

1 Statskontorets sammanfattning

Inriktning av den elektroniska kommunikationen

Statskontoret bedömer att i en nära framtid kommer stora delar av den elektroniska kommunikationen av betydelse att ske via Internet. Därför slår vi också fast att TCP/IP-arkitekturen och Internet kommer att vara den i Sverige dominerande infrastrukturen för elektronisk kommunikation.

Med hänsyn till den stora användningen av Internet inom olika branscher och sektorer, anser Statskontoret att samhället nu måste lägga lika stor vikt vid Internet som hittills lagts vid det allmänna telefonnätet.

Infrastrukturen för Internet består av ett antal delar där vissa delar med fördel kan tillhandahållas i full konkurrens mellan olika aktörer på marknaden. Andra delar, som t.ex. tilldelning av domännamn och databaser för DNS (Domain Name System), måste ske på ett sådant sätt att alla har samma möjligheter och ingen diskrimineras samt att nationella regler följs.

Drift av infrastrukturen skall så långt som möjligt utföras av marknadens aktörer. De regler som skall finnas bör inrikta sig på gemensamma resurser för Internet, minimikvalitet gällande strukturens funktion och på att ange normer för hur de funktioner som påverkar annan operatör och samhällsviktig verksamhet skall utföras.

Utbyggnaden av Internet i Sverige måste ske på ett sådant sätt att nätets sårbarhet minimeras. Internet måste jämföras med andra samhällsviktiga funktioner och fungera inom landet vid svåra påfrestningar på samhället både i fred och i krig. Den svenska delen av Internet måste därför också kunna fungera utan att vara beroende av funktioner placerade utanför Sverige.

Bakgrund till förslagen

Huvudkomponenterna i den svenska delen av Internet är:

- operatörernas nät med tillhörande stödsystem,
- användarnas (kundernas) nät,
- gemensamma resurser för alla operatörer och användare, exempelvis knutpunkter för samtrafik mellan operatörers nät och DNS-servrar för toppdomäner.

Till gemensamma funktioner räknas även hantering av domännamn för toppdomänen *.se*.

Till bakgrunden för Statskontorets förslag hör också att den nationella knutpunkten i Stockholm under juni 1997 har ombildats till en s.k. distribuerad lösning och att en nationell knutpunkt kommer att etableras i Göteborg i december 1997.

En utgångspunkt för förslagen är att regeringen den 25 september 1997 har gett Statskontoret i uppdrag att ta fram en strategi på IT-säkerhetsområdet, som preciserar statens ansvar och anger hur säkerhetsarbetet kan inordnas i det nationella handlingsprogrammet för IT, samt hur arbetet med IT-säkerhetsfrågorna bör organiseras och fördelas mellan olika statliga instanser.

Förslagen

Statskontoret föreslår att ytterligare nationella knutpunkter etableras successivt med början i Malmö/Lund-regionen och därefter i Sundsvall. Nationella knutpunkter skall användas endast av de operatörer som har nationell täckning i Sverige. Vissa av branschen överenskomna regler skall gälla för att operatörerna skall få ansluta sig till de nationella knutpunkterna.

Statskontoret föreslår att nationella knutpunkter för samtrafik mellan operatörernas nät, nätdatabaser m.m. placeras skyddade mot fysiska attacker i bergrum. Möjligheter till utspridning och flervägsanslutningar måste utnyttjas för att öka säkerheten.

Utöver de nationella knutpunkterna föreslår Statskontoret att de gemensamma nätresurserna omfattar följande:

- DNS för landskoden .se och för roten för det globala domännamnsträdet,
- Tidsservrar för nationell tid,
- Vägvalsregister,
- Whois-server,
- Indexserver,
- Domännamnshantering.

Statskontoret föreslår även hur anskaffning och drift av de gemensamma nätresurserna bör ske liksom hur dessa kan finansieras.

Statskontoret föreslår en definition av Internetoperatör och att vissa krav ställs på en Internetoperatör. Statskontoret föreslår också vad den tjänst som operatören levererar till kund minst bör omfatta (minimal IP-tjänst). ISOC-SE (den svenska avdelningen av Internet Society) föreslås ta ett ansvar för att reglerna följs och att reglerna anpassas till kommande behov.

Statskontoret föreslår att införandet av en ny nummerserie för portabla nummer i Sverige utreds av DRS (expertgruppen för Domännamnsregler i Sverige) och att DNS-databaser utnyttjas för lagring av dessa nummer. Statskontoret rekommenderar att DNS utnyttjas för att underlätta samtrafiken mellan telefonnätet och telefoni över Internet.

Statskontoret föreslår att frågan om incidenthantering belyses av en utredning med uppdrag att tillsammans med t.ex. operatörer och användarorganisationer inom offentlig förvaltning och näringsliv utreda och föreslå uppgifter för en organisation för incidenthantering i Sverige och hur den funktionen praktiskt skall utformas.

Statskontoret konstaterar att det för närvarande saknas en övergripande organisation för krishantering för Internet på nationell nivå. Statskontoret föreslår att en sådan organisation pekas ut snarast. Den organisationen skall bemyndigas att besluta om direkta åtgärder för att skydda och vidmakthålla Internet i Sverige. Reaktions tiden behöver vara på nivån minuter eller högst timmar. En plan bör också utarbetas hur den svenska delen av Internet skall drivas fristående från omvärlden vid avspärrning.

Beslut om eventuell isolering av den svenska delen av Internet och åtgärder med omfattande ekonomiska konsekvenser bör fattas av regeringen. Rutiner för detta måste skapas snarast.

Statskontoret föreslår att regeringen snarast låter göra en detaljerad kartläggning över vilka utbildningsområden inom högskoleväsendet rörande teknisk kompetens för uppbyggnad av stora IP-nät som skall vara prioriterade på kort sikt, för att så snabbt som möjligt fylla upp bristerna på kompetent personal.

Bedömningar

Statskontoret anser att:

- Netnod, som har etablerat den nya nationella knutpunkten i Stockholm, även är lämplig för att etablera och ansvara för driften av övriga föreslagna nationella knutpunkter,
- den organisation som ISOC-SE byggt upp för domännamns-hanteringen har förutsättning att fungera bra, dock föreslås att en samrådsgrupp med deltagare från lämpliga myndigheter bildas,
- regelverket för hantering av domännamn för toppdomänen *.se*

är till fyllest.

Synpunkter och rekommendationer

Kritiska noder i systemet bör ha tillgång till reservkraft under en längre tid. Statskontoret anser att vitala delar av nätet i kris- och krigssituationer måste ha utrustning för separat elmatning och tillgång till reservkraft för långa elavbrott, upp till två veckor. Det måste vara en strävan att varje Internetoperatör själv vidtar de åtgärder som fordras för att så långt möjligt upprätthålla sin elförsörjning.

Statskontoret anser att en dokumenterad och verifierad kontinuitetsplan bör vara ett grundläggande krav för samtliga Internetoperatörer. Planerna bör testas minst en gång per år och resultatet av testerna dokumenteras. Kontroll över detta skall utövas av en myndighet.

ÖCB har ansvaret för att säkerställa tillgången till elektronikkomponenter för kris och krig. Statskontoret anser att det därutöver finns behov att analysera leverantörsberoendet för vissa vitala komponenter inom Internet.

Flera av Internetoperatörerna i Sverige har utländska huvudägare vars kunskap om svenska krav under kris och krig är begränsad. Det är viktigt att varje operatör på den svenska marknaden har en etablerad organisation i Sverige.

De myndigheter som har ansvar för kunskaps- och informations-spridning inom säkerhetsområdet bör stimuleras till samordning för att kunna intensifiera sådana insatser.

Statskontoret rekommenderar att den funktion (Försvarsmakten/TSA (Totalförsvarets Signalskyddsavdelning)) som har ansvar för att för försvarsmaktens räkning granska och testa krypteringsalgoritmer i Sverige i ökad omfattning kan användas för civila ändamål.

Statskontoret anser att för bredbandsaccess till hushållen skall användas en infrastruktur som bygger på den som används för övriga Internet, dvs. TCP/IP-arkitekturen. På detta sätt utnyttjas en och samma kommunikationsarkitektur mellan alla änds-system.

Användaren skall ha möjlighet att välja olika operatörer och tjänster och alltid erhålla goda prestanda till olika typer av databaser och informationsservrar. Detta skall även gälla när bredbandsaccess krävs för åtkomst till information.

Genomförande av förslagen

Det finns i utredningen områden där staten har ett ansvar och där förslagen naturligen borde ha kunnat riktas till en myndighet om en lämplig sådan fanns. Statskontoret anser att inrättandet av en myndighet med den kompetens inom Internetområdet som krävs för att kunna hantera frågorna bör övervägas. Eventuellt skulle uppgifterna kunna läggas på en befintlig myndighet, förutsatt att de har möjlighet att bygga upp den kompetens som krävs.

Statskontoret konstaterar att branschen i stor utsträckning är villig att själv reglera och driva de gemensamma nätfunktioner som behövs för ett stabilt Internet och i övrigt ta hand om och vidta de åtgärder som föreslås. Statskontoret anser att detta är ett bra sätt att föra arbetet vidare. Det finns dock skäl att utvärdera hur väl utredningens förslag genomförs och om eventuella nya åtgärder krävs med hänsyn till utvecklingen inom området. Statskontoret föreslår att regeringen hösten 1998 tar initiativ till en sådan utvärdering.

Utredningens arbetsform

Utredningsarbetet har bedrivits i en utredningsgrupp och i ett antal arbetsgrupper. Arbetet har delvis bedrivits som rent utredningsarbete, varvid medlemmarna i gruppen bidragit med utredningsmaterial. Gruppen har också fungerat som ett forum där kunskap m.m. om Internet samlats in och dokumenterats. Dessutom har utredningen varit en samlingspunkt där olika problem kunnat diskuteras och förslag till lösningar kunnat läggas fram.

Statskontoret har kunnat konstatera att branschen under utredningens gång tagit initiativ till och påbörjat genomförandet av särskilt angelägna åtgärder. Åtgärderna har bedömts av Statskontoret.

Utredningsgruppens analyser och bedömningar har legat till grund för Statskontorets förslag.

Utgående från ett utkast till rapport har samråd genomförts under september 1997 med nitton organisationer. En sammanfattning av samrådssvaren finns i bilaga 1.

2 Bakgrund

Under våren 1996 utfördes i SNUS (Swedish Network Users Society) regi praktiska prov för att undersöka efter vilka tekniska principer Internet i Sverige bör utformas. Utgående från proven kontaktades Kommunikationsdepartementet av SNUS med ett förslag på att en utredning om den svenska delen av Internet borde genomföras.

2.1 Uppdraget

Regeringen (Kommunikationsdepartementet) uppdrog genom beslut den 26 september 1996 åt Statskontoret att utreda den svenska delen av Internet.

I regeringens beslut anges:

”Regeringen uppdrar åt Statskontoret att, med utgångspunkt i bifogade riktlinjer och vad som anförts i proposition 1995/96:125, beskriva Internet i dagsläget, göra en analys av framtida krav och komma med förslag till åtgärder. Statskontoret skall undersöka behovet av och förutsättningarna för att öka säkerheten och användbarheten i den svenska delen av Internet. Uppdraget skall redovisas för regeringen senast den 1 oktober 1997”.

I regeringens direktiv för uppdraget till Statskontoret anges bl.a. syftet med utredningen:

”Syftet med översynen är bl.a. följande:

- att med bibehållande av nätets öppna karaktär, öka uthålligheten i den organisation av gemensamma, konkurrensneutrala funktioner, som krävs för administration och utveckling av Internet,
- att minska nätets sårbarhet för störningar,
- att öka nätets användbarhet genom att överväga om det behövs ett fastare regelverk och en mer utvecklad struktur för den svenska delen av Internet,
- att, med bakgrund av föregående punkt, se hur regelverk och struktur bör utformas”.

I direktiven för uppdraget anges dessutom:

”Förslag som rör regelverket och strukturen skall ligga i linje med internationella rekommendationer och standarder, vara ändamålsenliga från teknisk synpunkt och behandla frågor

som bl.a. namn- och adressplan, utveckling av vägvalsregister, administration av säkerhetsnycklar samt utveckling av en nationell sökstruktur. Utgångspunkten skall vara att bygga vidare på den kompetens inom Internetområdet som byggts upp på olika håll i Sverige”.

I direktiven anges vidare att:

”Utgångspunkten för utredningen skall vara att staten endast i undantagsfall ingriper med reglering. Branschen skall i så stor utsträckning som möjligt ta ansvar för krav på nätoperatörer etc.”

Vad gäller finansiering anges i direktiven att utredningen skall ge förslag till hur utbyggnad och finansiering av gemensamma och kritiska resurser skall göras och att utgångspunkten är att operatörerna själva skall svara för finansieringen.

I direktiven anges slutligen att Statskontoret skall genomföra uppdraget med stöd av expertorganisationer som SNUS (Swedish Network Users Society) och SEIS (Säkrad Elektronisk Information i Samhället) med flera. Vidare anges att Statskontoret skall samråda med företrädare för telemarknaden samt med representanter för berörda myndigheter och organ.

Direktiven (riktlinjerna) för uppdraget anges i sin helhet i bilaga 2.

I denna rapport redovisas resultatet från uppdraget.

2.2 Förtydligande och avgränsning av uppdraget

Statskontoret vill här framhålla att enligt direktiven avser uppdraget frågor som har samband med datatransmission (transmission av s.k. IP-paket) och inte tillämpningsfrågor. Dock behandlas frågor gällande telefoni över Internet som är samtrafik på applikationsnivå och enligt direktiven skall dokumenteras.

Statskontoret vill också framhålla att uppdraget *inte* omfattar exempelvis offentlighetsrättsliga (yttrande- och tryckfrihet), straffrättsliga och upphovsrättsliga frågor.

Övriga avgränsningar av uppdraget anges i rapporten i samband med att respektive fråga behandlas.

2.3 Genomförande av utredningen

Utredningsarbetet har bedrivits i en utredningsgrupp och i ett antal arbetsgrupper. Utredningsgruppen har även svarat för planering och uppföljning av arbetet. Arbetet har delvis bedrivits som rent utredningsarbete, varvid medlemmarna i gruppen bidragit med utredningsmaterial. Gruppen har också fungerat som ett forum där kunskap m.m. om Internet samlats in och dokumenterats. Dessutom har utredningen varit en samlingspunkt där olika problem kunnat diskuteras och förslag till lösningar kunnat läggas fram.

Statskontoret har kunnat konstatera att branschen under utredningens gång tagit initiativ till och påbörjat genomförandet av särskilt angelägna åtgärder. Åtgärderna har bedömts av Statskontoret. Utredningsgruppens analyser och bedömningar har legat till grund för Statskontorets förslag.

I utredningsgruppen har deltagit representanter från Statskontoret, SNUS och STUPI (Svensk Teleutveckling och Produktinnovation AB). I arbetsgrupperna har deltagit representanter från nämnda organisationer samt bl.a. från SEIS. Av bilaga 3 framgår vilka personer som deltagit i utredningsarbetet.

Med hänsyn till utredningens tekniska karaktär har SNUS undergrupp Swedish Operators Forum (SOF) använts som referensgrupp. I SOF, som är ett öppet forum, deltar alla större operatörer i Sverige.

Två seminarier har genomförts under utredningstiden, det första i november 1996 och det andra, med säkerhet som tema, i april 1997.

Utredningsarbetet har bedrivits med en stor öppenhet och som ett led i utredningsarbetet har en mängd olika kontakter tagits med företrädare för myndigheter, företag och andra organisationer. Uppdragets bakgrund, syfte m.m. har presenterats vid ett flertal seminarier under utredningstiden.

2.4 Rapportens innehåll

Som nämnts ovan har utredningsarbetet bedrivits i en utredningsgrupp och i ett antal arbetsgrupper. Utredningsgruppen har redovisat sitt resultat till Statskontoret, varvid Statskontoret har ställt sig bakom de bedömningar och förslag som framförts av utredningsgruppen. Undantag gäller vissa säkerhetsfrågor som

redovisas i avsnitt 17, där Statskontoret väljer att i huvudsak redogöra för utredningsgruppens förslag och rekommendationer med hänsyn till att dessa frågor är föremål för behandling inom Regeringskansliet. I avsnitt 17 är det förutom Statskontorets bedömningar och förslag också *utredningsgruppens bedömningar och förslag* som redovisas.

I rapporten lämnar Statskontoret förslag till åtgärder. I rapporten anger Statskontoret också rekommendationer, bedömningar och liknande. För att tydligt skilja mellan förslag och rekommendationer m.m., anges i rapporten alla **förslag inom ram** och alla rekommendationer och bedömningar med *fet kursiv stil*. Med hänsyn till vad som ovan sagts gällande avsnitt 17 anges där i stället ”utredningsgruppen föreslår ...”.

Disposition av rapporten

Innehållet i avsnitten 3 till 6, inklusive bilagor, ger i första hand bakgrunden till och förutsättningarna för utredningen.

I avsnitt 7 behandlas vad en öppen kommunikationsarkitektur omfattar och vad det innebär ett en sådan utnyttjas och i avsnitt 8 beskrivs kortfattat förutsättningar för Internet i Sverige.

I avsnitt 9 finns en uppskattning av framtida trafikvolymerna för Internet i Sverige och i avsnitt 10 beskrivs strukturen för Internet i Sverige.

I avsnitt 11 föreslås vilka kriterier som definierar en Internetoperatör och vad en IP-tjänst minst bör omfatta, liksom vilken ansvarsfördelning som bör gälla mellan operatörer.

I avsnitt 12 föreslås var och när nationella knutpunkter för samtrafik bör etableras och i avsnitt 13 vilka nätresurser som bör vara gemensamma och konkurrensneutrala för alla operatörer och användare.

I avsnitt 14 behandlas bl.a. nätadresser (IP-adresser) och domännamn för toppdomänen .se, dvs. toppdomänen för Sverige.

I avsnitt 15 föreslås hur de gemensamma nätresurserna kan finansieras.

I avsnitt 16 beskrivs hotbilden mot nätet och i avsnitt 17 behandlas vad en säkerhetsarkitektur för Internet bör omfatta.

I avsnitt 18 föreslås att en kartläggning bör genomföras över vilka utbildningsområden som bör prioriteras.

I avsnitt 19 behandlas bredbandsaccess till hushållen och där lämnas förslag till efter vilken teknisk princip sådan access bör vara utformad.

I avsnitt 20 beskrivs problem och möjligheter med telefoni över Internet.

I avsnitt 21 behandlas år 2000 vad gäller Internetrelaterade frågor.

Rapportens bilagor innehåller i huvudsak bakgrundsbeskrivningar och fördjupningar till de olika problemområden som har behandlats av utredningen.

2.5 Samråd

Enligt direktiven för uppdraget skall Statskontoret samråda med företrädare för telemarknad samt med representanter för berörda myndigheter och organisationer.

Utgående från ett utkast (1997-09-04) till denna rapport har samråd genomförts under september 1997 med nitton organisationer. I föreliggande rapport har så långt möjligt hänsyn tagits till erhållna synpunkter. Samrådsvaren har sammanställts och redovisas i bilaga 1.

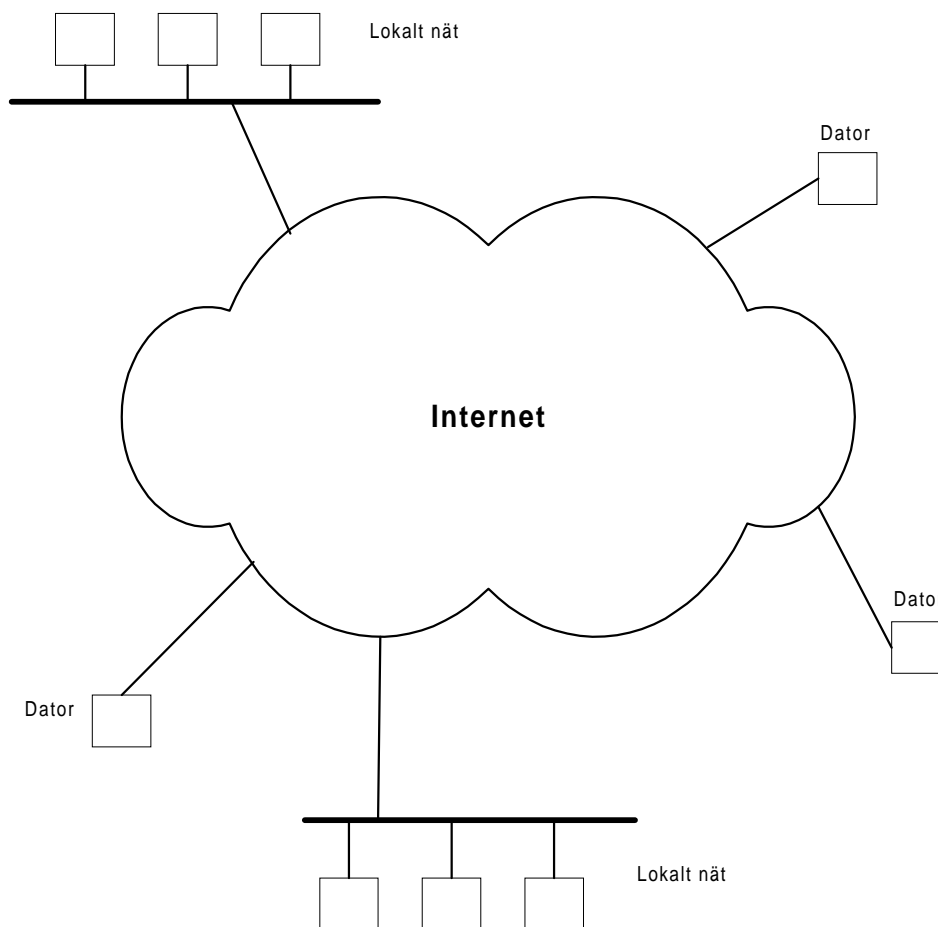
2.6 Propositioner, utredningar och projekt

I bilaga 5 sammanfattas vad som anges i propositioner och utredningar vad gäller Internet. Där beskrivs också projekt med anknytning till Internet.

3 Vad är Internet?

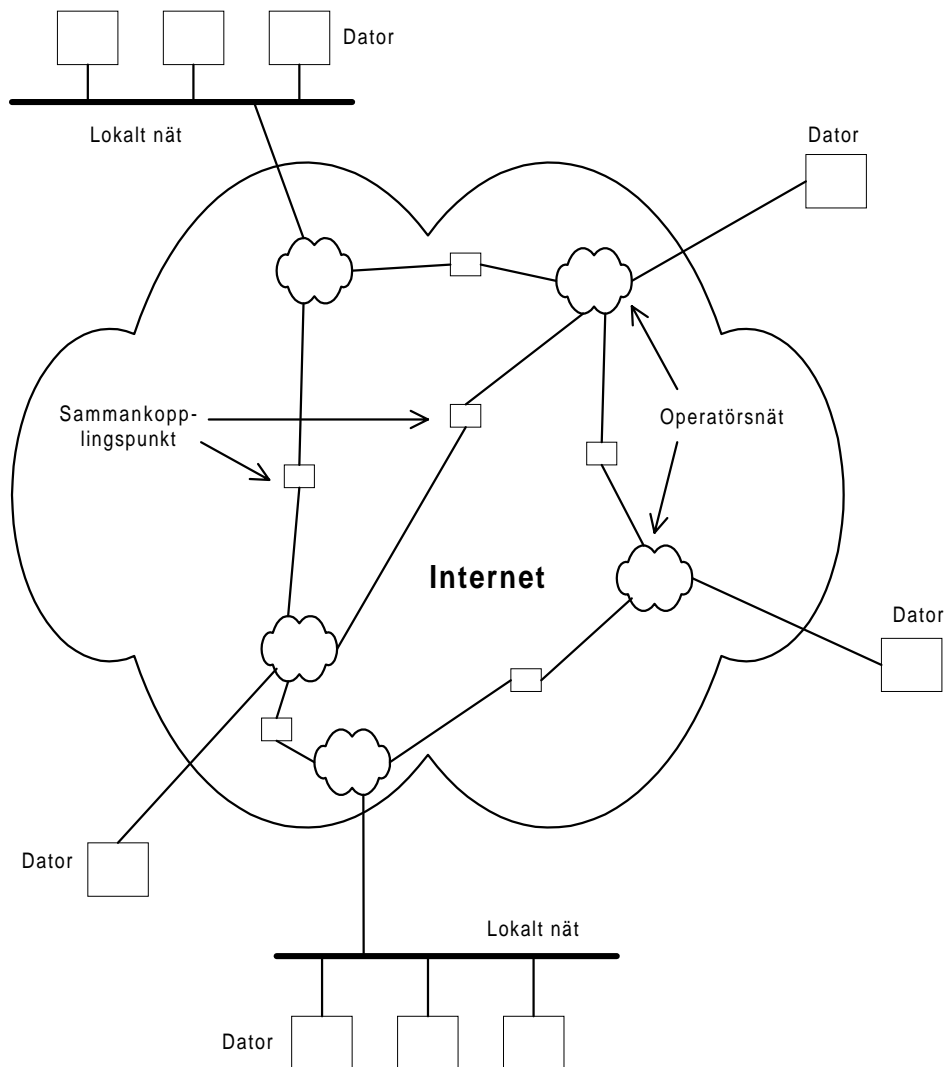
Ett "internet" kan tekniskt sett betraktas som en *samling* datornät som är sammankopplade med hjälp av ett antal datorer (routrar), vilket tillåter dem att fungera som *ett* enda stort virtuellt nät. Det finns flera sådana nät. Ett av dessa kallas Internet. Internet är det största nätet i världen enligt ovanstående definition.

Användarna ser Internet som ett enda stort nät till vilket varje dator är ansluten, direkt eller via ett lokalt nät:



Figur 3-1

Det som användaren ser som ett nät består emellertid av ett stort antal sammankopplade delnät. De olika delnäten utgörs i stort sett av olika operatörers nät. Till operatörernas nät ansluts olika organisationers (lokala) nät och datorer:



Figur 3-2

För att olika typer av datorsystem som är anslutna till Internet skall kunna kommunicera med varandra krävs gemensamma regler för det, så kallade kommunikationsprotokoll. Internet är ett paketförmedlande nät som använder IP-protokollet (Internet Protocol) för förmedling av trafiken. IP-protokollet används vanligen tillsammans med protokollet TCP (Transmission Control Protocol), därav den vanliga beteckningen TCP/IP.

För att Internet skall fungera finns ett antal stödsystem. De viktigaste stödsystemen är det logiska vägvalssystemet (routingssystemet) och DNS (Domain Name System).

Trafiken i nätet förmedlas via noder (routrar) som vanligen är sammankopplade med fasta förbindelser. Trafikvalet i nätet sker med hjälp av det logiska routingsystemet som har till syfte att finna den bästa trafikvägen till en viss destination i nätet. Det

logiska routingsystemet beskrivs mer detaljerat i avsnitt 10.

För att ett användarsystem automatiskt skall kunna översätta mellan domännamn och nätadress (IP-adress) och omvänt, används DNS.

I bilaga 6 "Internet i Sverige - kort historisk och teknisk överblick" förklaras de viktigaste grundfunktionerna för Internet och speciellt vad som gäller för Internet i Sverige. Dessa grundfunktioner omfattar såväl organisatoriska som tekniska frågor.

Där beskrivs även exempelvis olika typer av kundanslutningar (uppringda och fasta) till Internet, huvudkomponenterna i en operatörs nät, principen gällande knutpunkter för samtrafik mellan operatörers nät, IP-adresser och autonoma system. Vidare beskrivs användning av domännamn och den hierarki som gäller för dessa liksom DNS. I bilagan ges även en kort tillbakablick vad gäller Internet i Sverige.

I bilaga 20 "Telefoni över Internet" beskrivs den principiella skillnaden mellan Internet och telefonnätet.

4 Dagens och morgondagens situation

Syftet med detta avsnitt är att ge en koncentrerad bild av dagens och morgondagens användning av Internet.

4.1 Internet i dag - fortfarande bara i början på utvecklingen

Internet har, även om det funnits i mer än tio år i Sverige, endast börjat användas av en bredare krets av användare de senaste 2-3 åren. Antalet användare har ökat starkt under 1996 och 1997 såväl i Sverige som globalt. I dagsläget uppskattar man att nästan hälften av Sveriges vuxna befolkning på något sätt har tillgång till Internet. Tillväxten i nätet, mätt i såväl antal användare som trafikvolym, är fortfarande exponentiell totalt sett.

De nya möjligheter som det globala Internet och Internettekniken ger, har hittills utnyttjats endast till en liten del. Internet och IT används mest för att kommunicera inom respektive företag och organisationer och inom respektive samhällssektor. Tekniken ger emellertid möjlighet att bedriva verksamhet i helt nya former på alla områden, från näringsliv, offentlig förvaltning och utbildning, till sjukvård och konsumenttjänster. Hela underhållningssektorn har tagit till sig Internet i stor utsträckning. Denna förändring har bara börjat. Många olika försöksverksamheter bedrivs. Man har dock ännu inte till fullo lärt sig att ta tillvara möjligheterna utan använder tekniken och organiserar verksamheten på i stort sett samma sätt som före IT och Internet.

Det politiska intresset i olika länder för Internet har tilltagit under de senaste 1-2 åren, varvid intresset har fokuserats på vilken typ av information som finns tillgänglig i olika databaser anslutna till nätet. Ett andra intresse är Internet som en ekonomiskt intressant företeelse. Flera länder funderar över hur användningen av nätet skall kunna beskattas. Lagstiftningsfrågorna utreds i flera olika sammanhang. Bland frågorna märks integritetsfrågor samt kopplingen till mediapolitiken. Lagstiftningen lider också av att tekniken sätter gamla principer och lagar mer eller mindre ur spel. Den tekniska utvecklingen gör att exempelvis dagens lagstiftning inom tryckfrihetsområdet kommer i direkt konflikt med den spridning av oetiskt material som förekommer på Internet.

Det politiska intresset har också resulterat i att många nationella IT-program har tagits fram. Man kan nu räkna upp allt från de första stora politiska initiativen i USA och Bangemannrapporten från EU, till rapporter från FN:s olika organisationer som väl-

signar IT-satsningar i u-länder. Inom i-länderna talar man mest om IT och Internet för att utveckla näringslivet genom att med IT bl.a. lösa kompetensutvecklings- och arbetslöshetsproblem.

Det är självklart att det för Sverige, och för andra länder, är av avgörande betydelse för utvecklingen, att en god infrastruktur för telekommunikation och Internet kan utvecklas om de politiska målsättningarna om exempelvis distansundervisning, utveckling av glesbygden och en effektivare offentlig förvaltning skall kunna uppnås.

4.2 Morgondagens nät

Den tekniska utvecklingen ger upphov till en vision om att det går att tillhandahålla "Internet-tjänster" överallt genom ett kommunikationsnät som integrerar radio, satellit, fiber och koppar-kablar som förmedlare av tjänsterna. Rent tekniskt *kan* detta komma att baseras på Internets protokollösningar (vad det är, behandlas i avsnitt 7). Drivkraften i denna tekniska utveckling ligger i dag hos marknaden.

Under de närmaste fem till tio åren kommer det att utvecklas ännu mer komplicerade lösningar som ur användningssynpunkt kommer att vara enklare att använda. För att möjliggöra dessa tillämpningar behövs högre nätkapacitet än dagens. Nya tekniska lösningar och koncept kommer att behöva utvecklas.

Med ökad kapacitet på fiberområdet och med den nya dator-tekniken så kan dagens "burklösningar", dvs. TV, radio, video, telefon, fax, dator, komma att smälta samman. Utvecklingen av intelligenta hus, där all utrustning kan styras ligger nära i framtiden. Inom tio år är det vanligt att ha ett "multinet" inom bostaden kopplat till antingen ett fibernät eller med kommunikation via satellit så att alla de gamla tjänsterna och många nya erhålls, allt sannolikt baserat på Internets protokollösningar. Denna utveckling har redan påbörjats.

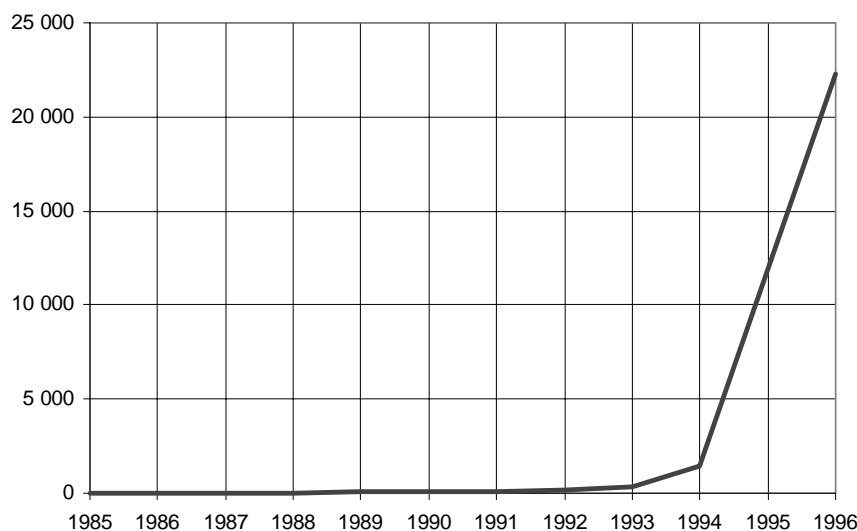
5 Användning av Internet i Sverige

Enligt direktiven för utredningen skall en beskrivning av Internet i dagsläget göras. I detta avsnitt ges en bild av hur Internet nu används i Sverige och i nästa avsnitt behandlas användning och tillväxten av Internet i världen. I bilagor till rapporten redovisas

- Tillämpning av Internet inom olika områden (bilaga 7)
- Organisationer i Sverige (bilaga 8)
- Infrastrukturen för Internet i Sverige (bilaga 9)
- Operatörsenkät (bilaga 11)
- Användarenkät (bilaga 12)

5.1 Registrerade domännamn

Utvecklingen av antalet registrerade domännamn kan tas som ett mått på hur företag, myndigheter, kommuner, skolor och organisationer i ökande utsträckning använder Internet. Det är nämligen i huvudsak dessa som registrerar egna domännamn medan privatpersoner, i den mån de registrerar egna domännamn, i stor utsträckning har Internetadress som underdomän till en operatör. Figur 5-1 visar hur antalet årligen registrerade domännamn för Sverige har utvecklats sedan 1985.



Figur 5-1

Källa: Internic-SE

Som synes har ökningen varit mycket stark de senaste åren. Mellan 1993 och 1994 var ökningen över 300 % och mellan 1994 och 1995 över 700 %. Mellan 1995 och 1996 var ökningen 86 %. Åren innan dess ökade antalet domännamn i allmänhet med 50–100 %

per år. Den starka ökningen under 1994 och 1995 sammanfaller i stort sett med att den nya tjänsten World Wide Web introducerades och snabbt blev mycket populär.

I juli 1997 var det totalt ca 50 000 domännamn registrerade för Sverige.

5.2 Användningen i Sverige

Infratest Burke AB och Expressen AB genomförde i april 1997 en studie "Det Svenska Internetanvändandet 97:1". En sammanfattning av studien finns i bilaga 10. I detta avsnitt redovisas kortfattat några av resultaten.

5.2.1 Tillgång till Internet

Andelen svenskar som har tillgång till Internet via arbetet, skolan, hemmet eller vänner och bekanta var i april 1997 46 %, vilket motsvarar 2,9 miljoner personer. I oktober 1996 var motsvarande siffra 30 %. Detta innebär att på ett halvår har tillgången ökat med cirka 1 miljon personer.

Hela 23 % av alla som har tillgång till Internet är studerande. De studerande utgör bara 12 % av befolkningen.

78 % av de tillfrågade hade tillgång till dator.

5.2.2 Användningen av Internet

Vid senaste tillfället de tillfrågade använde Internet var de uppkopplade i genomsnitt cirka 50 minuter. 39 % av användarna behöver Internet i sitt arbete.

5.2.3 Användningsområden

De vanligaste användningsområdena uppges vara

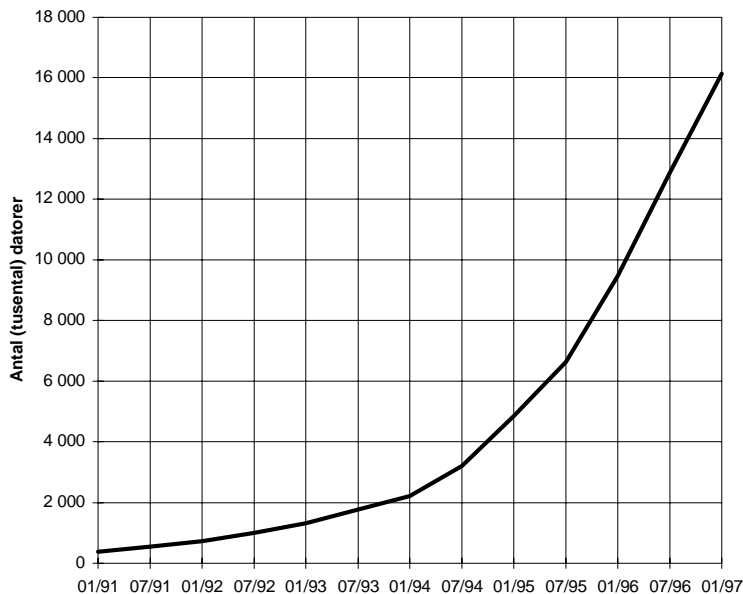
- Söka och hämta information.
- E-post.
- "Surfa" för nöjes skull.

6 Tillväxt av Internet i världen

Syftet med detta avsnitt är att ge en bild av tillväxten av Internet i världen. Nedan redovisas några av de kartläggningar som finns tillgängliga via Internet. I bilaga 13 redovisas ytterligare ett antal liknande kartläggningar.

6.1 Antal datorer

Network Wizards är ett av de mer kända företag som kartlägger användningen av Internet. För att få en bild av antalet datorer på nätet anges av Network Wizards de datorer som finns registrerade i DNS, se figur 6-1. Detta ger en minimibild av Internets storlek. I verkligheten är antalet datorer högre eftersom ett anslutet lokalt nät endast räknas som en dator.



Figur 6-1: Tillväxt i antal datorer på Internet enligt Network Wizards
Källa: Network Wizards, <http://www.nw.com>

Analys av den procentuella tillväxten i antal datorer per år utifrån figur 6-1 ger en tillväxt under perioden på mellan 40 % och 55 %. Någon klar trend syns inte i förändringen av tillväxttakten.

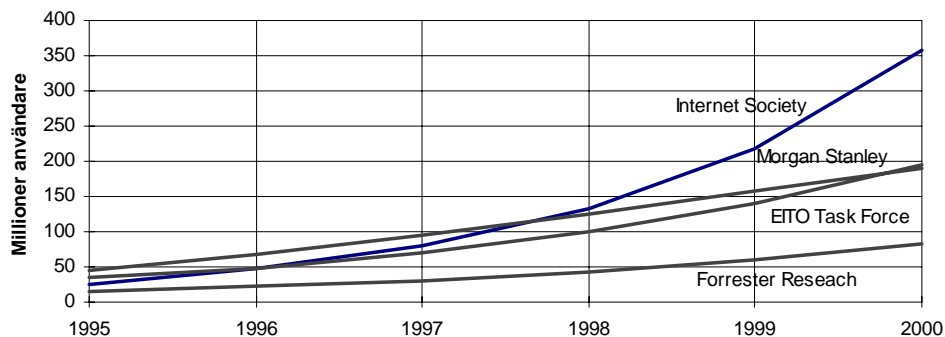
6.2 Antal användare

Svårigheten att uppskatta antal användare på Internet gör att de resultat som redovisas bör ses mer som försök till goda gissningar. Definitionen av en Internetanvändare är troligen heller inte entydig.

Fem olika försök att under första halvåret 1996 uppskatta antalet Internetanvändare i USA resulterade i värden mellan 9 och 42 miljoner användare, där den högre siffran erhöles via telefonintervju med ett mindre antal (1 000 st) utvalda personer.

Enligt EITO (European Information Technology Observatory) Task Force fanns det ca 68 miljoner Internetanvändare i världen i slutet av 1996.

Figur 6-2 visar några olika uppskattningar av antalet framtida användare av Internet.



Figur 6-2: Prognos över antalet användare av Internet

Källor: Internet Society, Morgan Stanley, EITO Task Force, Forrester Research (sammanställt av EITO)

Prognoser över antalet framtida användare innehåller stora osäkerheter. Framför allt gäller detta svårigheten att uppskatta intresset för nya tillämpningsområden som ännu inte börjat användas allmänt eller ännu inte existerar. Hittills har dock den verkliga tillväxten av Internet ofta överträffat de flesta prognoser.

7 Kommunikationsarkitektur för Sverige

Statskontoret anser att det i dag endast är TCP/IP-arkitekturen som uppfyller de väsentligaste kraven på en öppen kommunikationsarkitektur.

Statskontoret bedömer att i en nära framtid kommer stora delar av den elektroniska kommunikation av betydelse att ske via Internet. Därför bedömer Statskontoret att TCP/IP-arkitekturen och Internet kommer att vara den i Sverige dominerande infrastrukturen för elektronisk kommunikation. Vid utveckling av nya tillämpningar för elektronisk kommunikation rekommenderas att TCP/IP-arkitekturen används.

Syftet med detta avsnitt är att beskriva behovet av och nyttan med en stabil infrastruktur i Sverige för elektronisk kommunikation baserad på en öppen kommunikationsarkitektur.

För att kunna erbjuda alla medborgare, företag, offentlig sektor och andra organisationer i Sverige möjlighet att på ett säkert sätt utbyta elektronisk information med varandra krävs en väl fungerande infrastruktur. Denna infrastruktur kan jämföras med vägnätet för bilar, järnvägen för tåg etc.

En kommunikationsarkitektur för vägnät anger hur man skall trafikera vägnätet, vilka trafikregler som gäller, utformning av vägskyltar, hur mycket last man får framföra m.m. På samma sätt som man har riktlinjer och normer för vägtrafik krävs att man har riktlinjer och normer för det elektroniska (väg)nätet.

I det elektroniska nätet finns det olika bredd, lastförmåga och hastighetsbegränsningar. I det elektroniska nätet sätts dessa begränsningar antingen av beskaffenheten hos vald transmissionsmetod eller, än vanligare, av förmågan hos "väghållaren".

Den allra viktigaste komponenten sett från dem som koordinerar ett lands IT-infrastruktur är att det klart och tydligt anges vilka trafikregler som skall gälla för datautbyte, dvs. vilken *kommunikationsarkitektur* som skall användas för elektronisk kommunikation.

I kommunikationsarkitekturen finns också de funktioner som behövs för att kunna "lasta om transporterat gods" från en vägtyp till en annan, t.ex. från kommunikation över fiber till kommunikation via kopparkabel eller från förbindelse via uppringd an-

slutning i allmänna telefonnätet till fast anslutning.

Kommunikationsarkitektur

Utgångspunkten är att en kommunikationsarkitektur skall vara öppen och omfatta minst följande komponenter:

- Regler för kommunikation, s.k. protokoll, för både transport av data och för olika tillämpningar
- Regler för fördelning av nätelement som identifierar änds-system så att identifieringen blir globalt unik, ofta kallas detta (nät)adressplan
- Regler för fördelning av logiska änds-systemsidentifierare, exempel på detta är domännamn, telefonnummer och e-postadresser
- Stödsystem för styrning av trafik och vägval (routing)
- Stödsystem för översättning mellan logiska och fysiska änds-systemsidentifierare (t.ex. mellan domännamn och nätadress)
- Stödsystem för övervakning, felsökning och drift
- Stödsystem för säkerhetsfunktioner; autentisering, signering och kryptering (som också måste stödjas av kommunikationsprotokollen).

I övrigt krävs att arkitekturen är definierad i en internationellt accepterad öppen standard och likaså att arkitekturen stödjer användning av olika typer av transmissionsresurser (dvs. kan användas över olika typer av transmissionsnät).

Likaså måste det finnas väl fungerande produkter från ett flertal leverantörer att tillgå på marknaden och dessa olika produkter måste kunna kommunicera med varandra (interoperabilitet) utan problem.

På marknaden måste det även finnas väl spridd kunskap om regler, system och produkter samt hur man lämpligast fogar samman dem för att på effektivaste sätt få fungerande system för avsett ändamål.

I en väl fungerande kommunikationsarkitektur är också möjligheten att använda kryptering och andra säkerhetsfunktioner fundamentala.

Öppna systemlösningar

Genom att utveckla och använda system som bygger på en öppen kommunikationsarkitektur uppnås sådana effekter som dels en enhetlig miljö för att olika datorsystem skall kunna samverka samt en enhetlig miljö för utveckling och drift av tillämpningsprogram, dels en gemensam miljö för säkerhetsfrågor. Genom konkurrensen mellan olika leverantörer erhålls kostnadsbespa-

ringar jämfört med att anskaffa produkter som bygger på leverantörsspecifika lösningar. Även nackdelar finns, men fördelarna anses överväga.

Utveckling av tillämpningar

Tidigare byggde man vanligen sin elektroniska kommunikation ända från grunden (från transmissionsnätet) till den tillämpning man egentligen hade för avsikt att utveckla, se figur 7-1.



Figur 7-1

Att bygga på det sätt som beskrivs ovan har som effekt att det blir mycket svårt att byta transmissionsnät eller ändra i en tillämpning utan att behöva göra om allt från början. Möjligheten att kommunicera med andra system blir i det närmaste obefintlig. Man tvingas i stället bygga speciella översättare som överför information från ett system till ett annat.

Ett exempel, vilket man kanske inte tänker på, är det allmänna telefonnätet som är uppbyggt på detta sätt, se figur 7-2.



Figur 7-2

Val av kommunikationsarkitektur

Vid utveckling av tillämpningar för elektronisk kommunikation rekommenderar Statskontoret att en kommunikationsarkitektur används som bygger på öppna standarder och som i övrigt omfattar de komponenter som anges ovan under rubriken Kommunikationsarkitektur. Det finns i dag endast två öppna och leverantörs-

oberoende kommunikationsarkitekturer att välja mellan. Den ena bygger på OSI (Open Systems Interconnection) och den andra är TCP/IP-arkitekturen.

För TCP/IP finns väl fungerande produkter till alla typer av datorsystem av betydelse från ett stort antal leverantörer. Likaså finns det en väl spridd kunskap på marknaden om hur dessa produkter kan användas. Motsvarande kan inte sägas föreligga för OSI, även om det för vissa tillämpningar, såsom elektronisk post, finns produkter som i begränsad omfattning används i praktiken. Även OSI-tillämpningar kan använda TCP/IP för datatransporten.

Statskontoret anser att det i dag endast är TCP/IP-arkitekturen som uppfyller de krav som kan ställas på en öppen kommunikationsarkitektur.

TCP/IP-arkitekturen

För Internet används TCP/IP-arkitekturen. Internet och TCP/IP-arkitekturen utvecklas fortlöpande med nya protokoll och tillämpningar, som exempel kan nämnas protokoll för multicasting och garanterad bandbredd. Utöver nu vanliga tillämpningar såsom e-post och World Wide Web kommer TCP/IP och Internet allt mer att också användas för telefoni, videoöverföring och videokonferenser.

Statskontoret bedömer att i en nära framtid kommer stora delar av den elektroniska kommunikationen av betydelse att ske med användning av TCP/IP-arkitekturen och Internet. Vid utveckling av nya tillämpningar rekommenderas att TCP/IP-arkitekturen utnyttjas för den elektroniska kommunikationen. Detta ger grunden för att utveckla nya och effektivare funktioner för samhället.

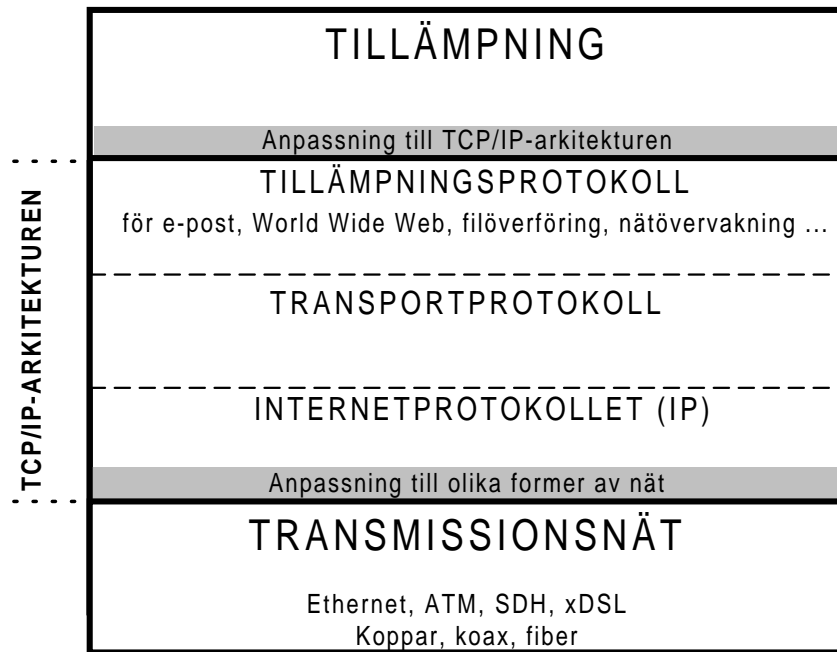
TCP/IP-arkitekturens princip anges förenklat i figur 7-3.



Figur 7-3

Av figur 7-4 framgår principen med att använda TCP/IP-arkitek-

turen för utveckling av tillämpningar och att olika typer av transmissionsnät kan utnyttjas.



Figur 7-4

Slutsats

Statskontoret bedömer att TCP/IP-arkitekturen och Internet kommer att vara den i Sverige dominerande tekniken för elektronisk kommunikation.

8 Förutsättningar för Internet i Sverige

Med hänsyn till den stora användningen av Internet inom olika branscher och sektorer, anser Statskontoret att samhället nu måste lägga lika stor vikt vid Internet som hittills lagts vid det allmänna telefonnätet.

Drift av infrastrukturen skall så långt som möjligt utföras av marknadens aktörer. De regler som skall finnas bör inrikta sig på gemensamma resurser för Internet, minimikvalitet gällande strukturens funktion och på att ange normer för hur de funktioner som påverkar annan operatör och samhällsviktig verksamhet skall utföras.

I detta avsnitt behandlas översiktligt förutsättningarna för Internet i Sverige.

Internet som bas för elektronisk kommunikation

Som tidigare framförts i rapporten anser Statskontoret att det i dag inte finns något verkligt alternativ till Internettekniken som kan utgöra en bas för elektronisk kommunikation mellan system i Sverige. Det är därför viktigt att den svenska delen av Internet fungerar på ett för samhället tillfredsställande sätt. Detta innebär att centrala delar i nätet måste vara utförda på ett sådant sätt att erforderlig stabilitet och uthållighet erhålls.

Med hänsyn till den stora användningen av Internet inom en mängd olika branscher och sektorer, av vilka många kommer att vara viktiga för samhällets funktioner, anser Statskontoret att samhället nu måste lägga lika stor vikt vid funktionen hos Internets infrastrukturen som hittills lagts vid det allmänna telefonnätet.

Önskad inriktning

En infrastruktur för Internet består av ett antal delar där vissa delar med fördel kan tillhandahållas i full konkurrens mellan olika aktörer på marknaden. Andra delar, som t.ex. tilldelning av domännamn och DNS-tjänster för toppdomäner, måste ske på ett konkurrensneutralt sätt och följa nationella regler. Domännamn behandlas i avsnitt 14 och DNS behandlas bl.a. i avsnitt 13.

Drift av infrastrukturen skall så långt som möjligt utföras av marknadens aktörer. De regler som skall finnas bör inrikta sig på gemensamma resurser för Internet, minimikvalitet gällande strukturens funktion och på att ange normer för hur de funktioner som påverkar annan operatör och samhällsviktig verksamhet skall utföras. Se vidare i avsnitt 11.

Utbyggnadsmöjlighet

På grund av att nya användningsområden tillkommer och att användningen av befintliga tillämpningar ökar skall vid dimensionering och vid konstruktion av nationella knutpunkter och gemensamma nätresurser sådan teknik användas så att systemen utan större svårighet kan utökas till att klara en kraftigt ökad belastning. Nationella knutpunkter och gemensamma nätresurser behandlas i avsnitt 12 respektive 13.

9 Analys av framtida trafikvolymer

Statskontoret bedömer att den beräknade trafiken för år 2002 redan i dag skulle kunna klaras av med tillgänglig teknik.

9.1 Syftet med analysen och uppskattningarna

Det är viktigt att här framhålla att utredningens uppdrag inte omfattar dimensionering av IT-infrastrukturen i Sverige, vilket är en uppgift för marknadens aktörer. Emellertid ingår det i utredningsuppdraget att kunna specificera omfattning av gemensamma nätresurser och funktioner för den svenska delen av Internet såsom knutpunkter för samtrafik och övriga gemensamma nätresurser. Dessa behandlas längre fram i denna rapport.

Det finns minst två skäl till att det är angeläget att göra de i detta avsnitt redovisade uppskattningarna av den förväntade trafikvolymen; dessa skäl är:

1. Vilka trafikvolymer kommer att erhållas om den största delen av Sveriges elektroniska kommunikation sker via Internet? Denna punkt är viktig, då utredningen behöver göra en rimlighetsanalys om detta är tekniskt och praktiskt möjligt.
2. Vilka trafikvolymer kommer att behöva hanteras *mellan* de olika aktörerna (operatörerna) via någon form av sammankopplings- eller knutpunkt?

Genom att ha en uppfattning om trafikbehovet är det möjligt att undersöka om teknikutvecklingen väntas leda till produkter och tjänster inom områden som är relevanta för att bygga dessa nät och knutpunkter. För att säkerställa funktioner som är viktiga för samhället är det angeläget att man bygger dessa funktioner baserat på beprövad och standardiserad teknik och utrustning.

Nya tillämpningsområden

Förutom att användningen av "dagens" tillämpningar kommer att öka, bl.a. genom att nya användare ständigt tillkommer, kommer Internet i allt större utsträckning att användas för "nya" tillämpningar som ljud (telefoni, radio), rörliga bilder och stillbilder (TV, video, grafik). Många av dessa nyare tillämpningar kräver tillgång till bredbandsanslutning. Trafikuppskattningarna i detta avsnitt förutsätter en sådan utveckling av tillämpningarna.

Förändrat trafikmönster

Användarnas Internettrafik sker i dag till övervägande del utanför den egna regionen (närområdet), dvs. trafiken sker via respektive operatörs stamnät i Sverige och dess utlandsförbindelser. Exempelvis "hämtas" stora mängder webb-information från USA.

Dagens trafikmönster kommer sannolikt att förändras mot mer regional trafik när det finns mer intressant information för användarna att ta del av inom den egna regionen. Detta kommer t.ex. att ske genom att man speglar innehållet eller temporärt lagrar kopior regionalt av exempelvis ofta efterfrågade webbsidor från avlägsna platser. I framtiden kommer dessutom en stor del av trafiken att distribueras till en region *i en kopia* och sedan spridas till många användare *inom* regionen med användning av multicastteknik, vilket kan jämföras med vad som nu gäller för vanlig TV-distribution.

I takt med att användarna kommer att utnyttja mer avancerade grafiska funktioner än de som ingår i dagens tillämpningar, kommer man att vilja distribuera dessa till speciella resursdatorer. Syftet med detta är inte bara att spara bandbredd för kommunikation över långa distanser, utan också att få den totala beräkningsresurs som krävs för komprimering, animering och interaktiva tjänster.

9.2 Trafikuppskattning byggd på erfarenhet

Trafikuppskattning i detta delavsnitt bygger på erfarenheten att trafiken fördubblas ungefär var nionde månad. Här uppskattas trafikutvecklingen under en tidsperiod på 63 månader, dvs. under sju stycken niomånadersperioder (drygt fem år), räknat fr.o.m. april 1997 t.o.m. juli 2002 utgående från startvärdet 60 Mbit/s. Startvärdet 60 Mbit/s är *genomsnittsvärdet* av den trafik som i april 1997 passerade den nationella knutpunkten i Stockholm.

Förutom den trafik som sker mellan operatörer via knutpunkten finns även trafik inom respektive operatörs nät vilken inte passerar knutpunkten. Likaså kan trafik utväxlas direkt mellan operatörer utan att passera knutpunkten. Hur stor denna trafik totalt är har dock inte kunnat uppskattas.

Värde i Mbit/s	Datum när trafikvolymen beräknas inträffa	Antal månader räknat från starttiden
60	April 1997	0
120	Januari 1998	9
240	Oktober 1998	18
480	Juli 1999	27
960	April 2000	36
1 920	Januari 2001	45
3 840	Oktober 2001	54
7 680	Juli 2002	63

Av tabellen ovan framgår att trafiken efter 63 månader uppskattas till 7 680 Mbit/s. Utgående från startvärdet 60 Mbit/s gällande för april 1997, är trafiken 128 gånger så stor i juli 2002 ($7680/60 = 128$).

9.3 Trafikuppskattning - maximalalternativ

Trafikuppskattningen i detta delavsnitt bygger på ett scenario där 2 miljoner användare (dvs. användare i hushåll, företag, offentlig sektor och andra organisationer) i Sverige utnyttjar Internet och har tillgång till s.k. bredbandsaccess. Här antas att detta förhållande inträder ungefär vid samma tidpunkt som använts i beräkningarna i föregående avsnitt, dvs. i mitten av år 2002.

För trafikuppskattningen antas att varje användare har ett trafikbehov på 400 kbit/s i medeltal över dygnets 24 timmar (400 kbit/s är således ett medelvärde per användare). Att använda medelvärden är en metod som har visat sig användbar vid dimensionering av nät i Internetsammanhang.

Denna uppskattning av trafiken är ett *maximalalternativ*, dvs. det är ett försök att uppskatta vilken trafikvolym som erhålls när användarna i framtiden konsumerar maximalt.

Antagandet bygger vidare på att det finns en annan typ av access till Internet än dagens, dvs. en typ som möjliggör överföring av stora datamängder under mycket kort tid (bredbandsaccess).

Antagandet är således baserat på att alla hushåll, företag osv. kan använda någon accessmetod som stödjer TCP/IP-arkitekturen och har en tillräcklig genomströmning för att hantera dels medelbelastningen, dels den skurvisa trafik som kommer att förekomma för sådana tillämpningar som kräver att en stor datamängd

överförs under kort tid till användaren.

Uppskattningen är också baserad på antagandet att användarna har lika tillgång till tjänsterna på Internet oberoende av vilken operatörer som tillhandahåller anslutningen till tjänsten och oberoende av vilken operatör som svarar för accessförbindelsen.

Nätet belastas således i medeltal med:
 $2 \text{ miljoner användare} \times 400 \text{ kbit/s} = 800\,000 \text{ Mbit/s} .$

Antag att 10% av trafikvolymen passerar genom den nationella knutpunkten och att det bara finns en sådan knutpunkt. I så fall behöver knutpunkten dimensioneras för 80 000 Mbit/s . Denna trafik kan man redan i dag klara med att använda tillgänglig teknik.

Som framgår av avsnitt 12 "Nationella knutpunkter för samtrafik" föreslås att ett antal nya nationella knutpunkter etableras under de närmaste åren. Detta innebär att den uppskattade trafiken enligt ovan kommer att fördelas över ett antal knutpunkter liksom över ett antal operatörers stamnät.

9.4 Bedömning

Bedömningen är att trafikvolymen genom knutpunkterna år 2002 kommer att befinna sig någonstans *mellan* det värde som erhålls genom att extrapolera värden byggda på erfarenhet för trafikillväxten cirka fem år framåt, dvs. 7 680 Mbit/s (enligt avsnitt 9.2), och det värde som erhålls genom att försöka uppskatta vad användarna *maximalt* väntas konsumera i framtiden och som passerar knutpunkten, dvs. 80 000 Mbit/s (enligt avsnitt 9.3).

Slutsatsen blir att oavsett den stora skillnaden mellan dessa värden så skulle den beräknade trafiken i mitten av år 2002 redan i dag kunna klaras av med tillgänglig teknik.

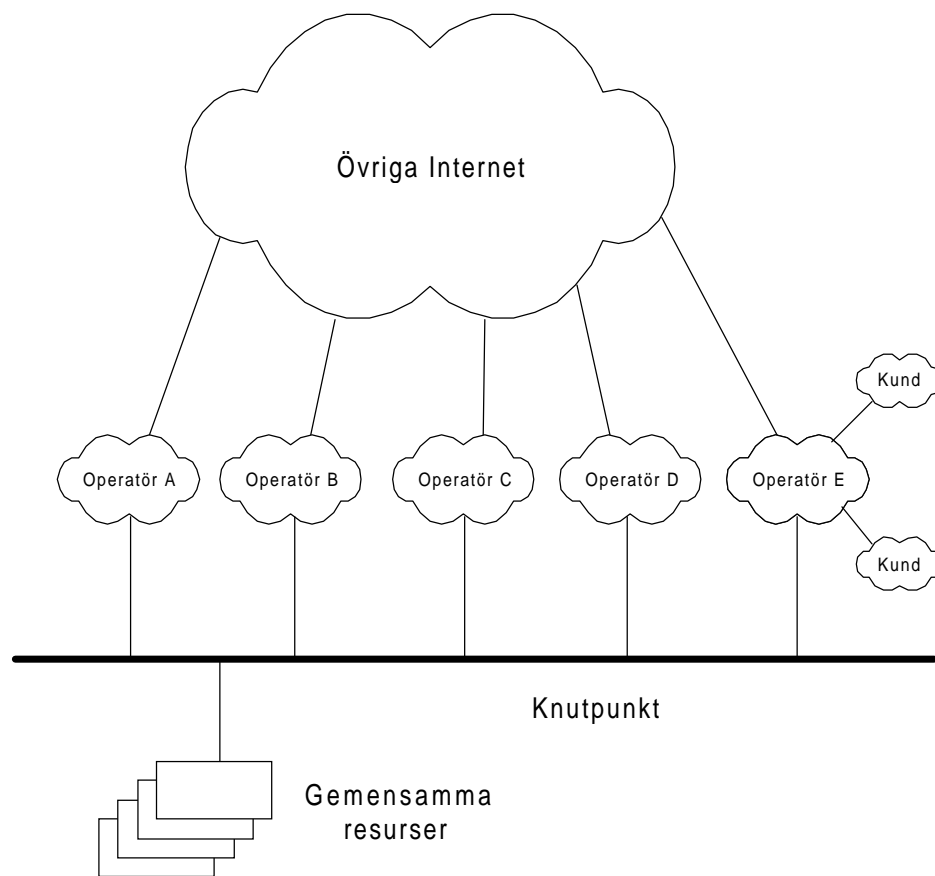
10 Struktur för Internet i Sverige

10.1 Huvudkomponenter i den svenska delen av Internet

Nyckelkomponenter i den svenska delen av Internet:

- operatörernas nät med tillhörande stödsystem,
- användarnas (kundernas) nät,
- gemensamma resurser för alla operatörer och användare, exempelvis knutpunkter och DNS-servrar för toppdomäner.

Se principskissen i figur 10-1.



Internet i Sverige - principskiss

Figur 10-1

10.2 Operatörens nät med tillhörande stödsystem

En typisk operatör på Internet bygger sitt nät runt ett stamnät som kan ha en varierande topologi. För stamnätet väljer man ett medium som har en överföringskapacitet som väl överstiger den genomströmning man avser att ha genom nätet för fjärrtrafik. Exempelvis är det vanligt med switchad FDDI eller switchad 100 Mbit/s Ethernet.

Operatören behöver sedan ordna så att samtrafik kan ske med andra operatörer inom Sverige, vilket enklast sker genom att ansluta sig till de nationella knutpunkterna, samt avtala med de andra operatörerna om trafikutbyte via knutpunkten (se nedan).

För trafik till övriga Europa är det vanligt att operatörerna köper kapacitet från någon av dem som driver de pan-europeiska näten (som Ebone, UUnet eller BT/Concert).

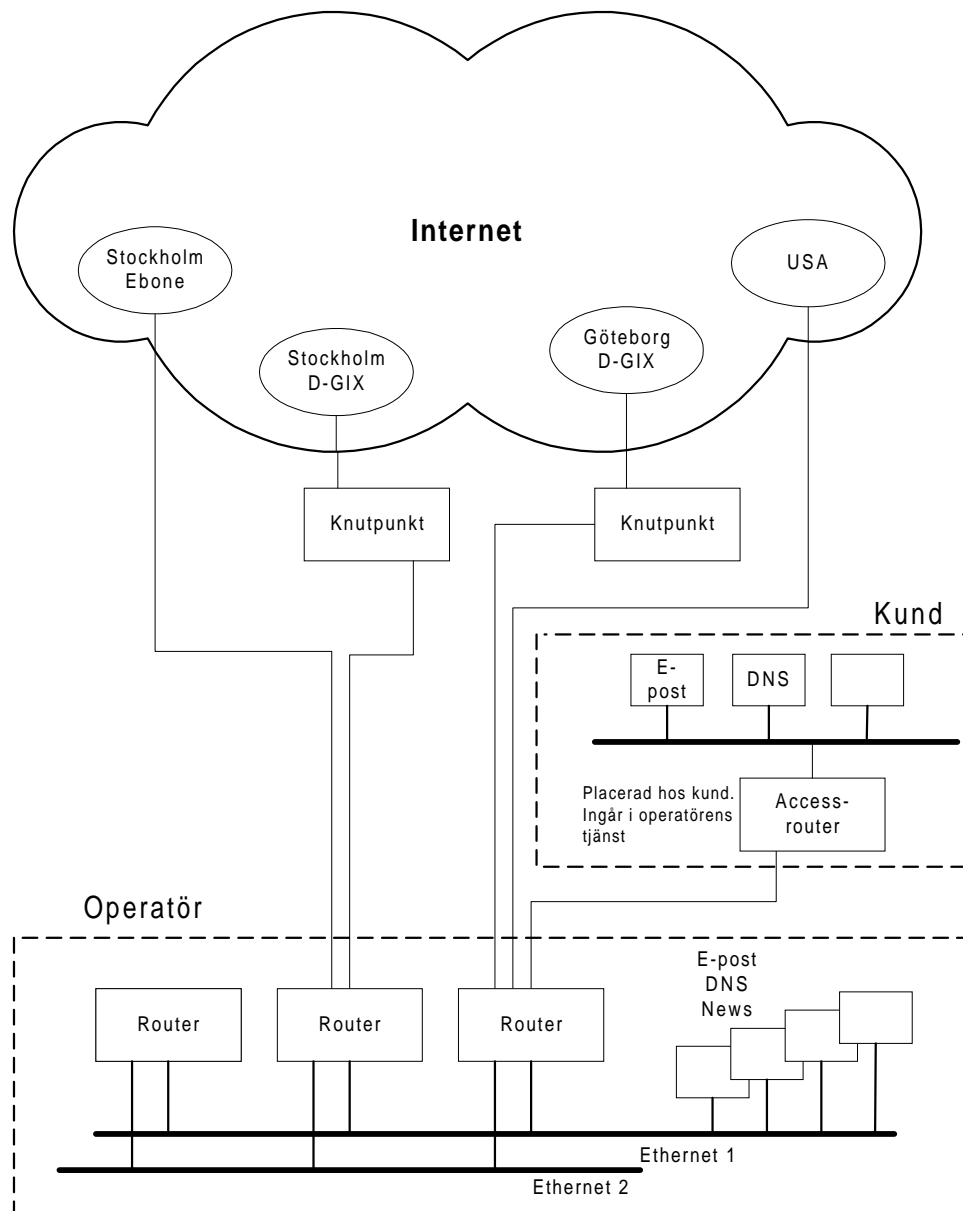
För trafik till Nordamerika och destinationer i Asien är det vanligast att operatörerna endera köper en reguljär kundanslutning av en amerikansk operatör eller en transitanslutning från en internationell transitoperatör.

Till sina stamnätsroutrar ansluter operatörerna fasta accesslinjer till sina kunder (uppringda kundanslutningar behandlas inte här).

I figur 10-2 (se nästa sida) består operatörens nät av två Ethernet. Till detta nät är routrar och stödsystem för DNS, e-post och News anslutna. Till höger i figuren visas en kunds nät med accessrouter för den tjänst som operatören levererar. Till kundens nät är server för e-post respektive DNS anslutna. I detta exempel är operatören ansluten till två nationella knutpunkter (D-GIX i Stockholm respektive Göteborg). Operatören har även en anslutning till det europeiska nätet Ebone och en till USA.

Domain Name System (DNS)

I operatörens nät behövs ett antal datorresurser vilka används för att tillhandahålla DNS-information. Beroende på operatörens storlek etc. kan de använda datorresurserna vara utformade på olika sätt. Operatören behöver minst tillhandahålla DNS för de domännamn som används för operatörens egen utrustning vad gäller översättning namn-till-nummer och omvänt. I det fall operatören tillhandahåller DNS för sina kunder antingen i form av primär eller sekundär DNS tillkommer resurser för detta.



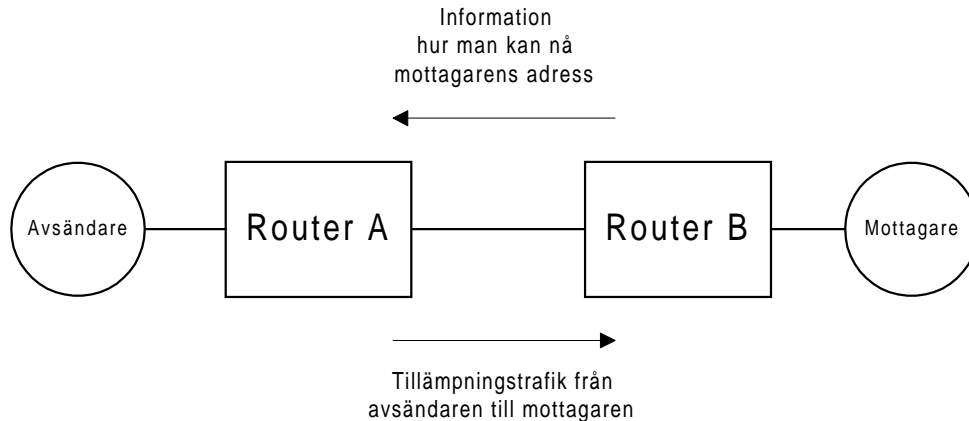
Figur 10-2

Minimikravet är att man för varje domän har minst två separata DNS-servrar placerade och anslutna på ett sådant sätt att dessa inte samtidigt drabbas av avbrott (vilket skulle innebära att de inte kan nås från huvuddelen av Internet och svara på de ställda DNS-frågorna).

Det logiska vägvalssystemet (routingsystemet)

Trafikvägval i Internet sker med hjälp av ett stödsystem som vanligen benämns "routingsystemet". Ändamålet med det logiska routingsystemet är att finna bästa trafikväg till en viss destination i nätet. Detta sker genom att routrarna i nätet berättar för sina "kollegor" vilka andra destinationer de känner till. Routinginformation skickas i nätet via routingprotokoll på samma sätt som all annan trafik, dvs. vanligen som IP-paket.

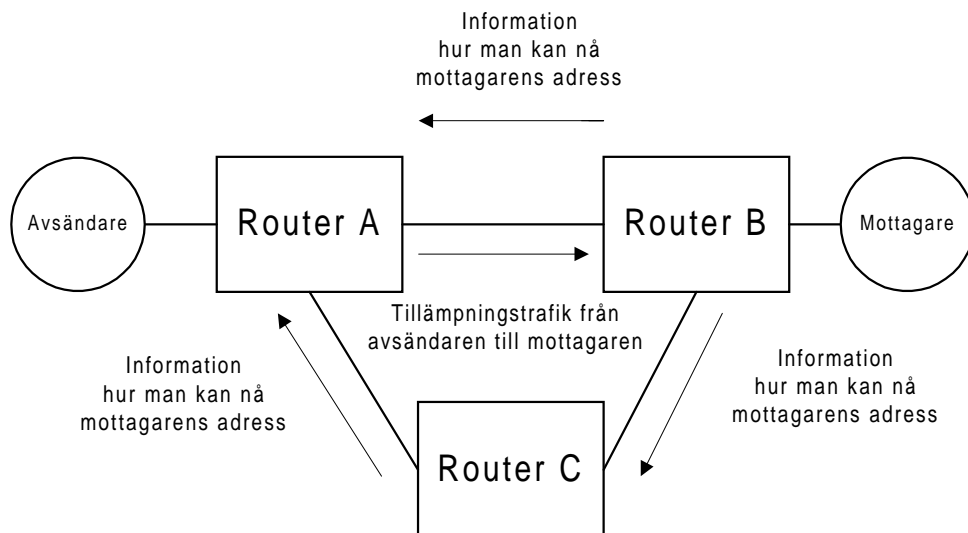
Det finns olika huvudtyper av routingprotokoll: interna routingprotokoll (Interior Gateway Protocol), som exempelvis OSPF (Open Shortest Path First) och externa routingprotokoll (Exterior Gateway Protocol), som exempelvis protokollet BGP (Border Gateway Protocol). (Även i bilaga 6 behandlas routing.)



Figur 10-3

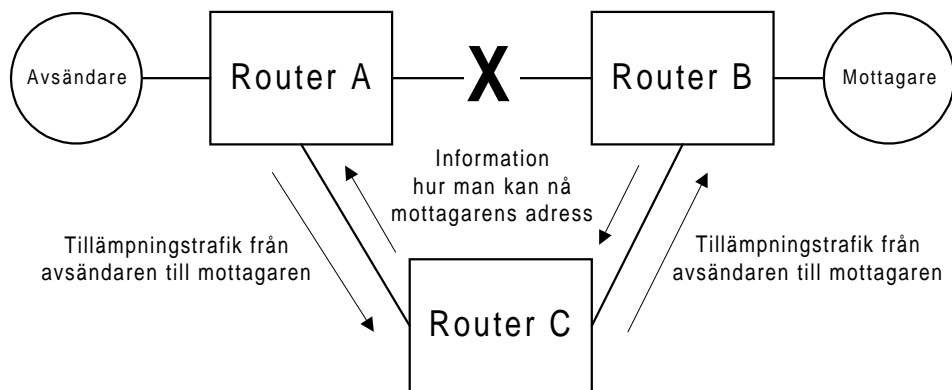
Förloppet är sådant att router B med hjälp av ett routingprotokoll berättar för router A hur man kan nå adresser inom mottagarens nät. Router A bygger ett dynamiskt register över närliggande destinationer och till vilken granne man skall skicka trafik för vidarebefordran till slutdestinationen/mottagaren. (Det omvända sker också, att router A berättar för router B om adresser inom avsändarens nät.) Se figur 10-3.

Om man i operatörens nät har redundanta (ung. alternativa) vägar, skickas routinginformationen vidare genom alla tänkbara vägar. Router A kommer således att höra talas om möjlig väg till mottagaren via router B och router C och kommer att välja den utifrån ett antal olika parametrar bäst fungerande vägen till mottagaren. Se figur 10-4.



Figur 10-4

Om den fysiska trafikvägen mellan router A och B drabbas av ett avbrott, kommer ingen ny routinginformation fram, utan bästa väg som router A ser till router B och mottagaren är nu via router C, vilket gör att registret över hur man kommer till en destination i router A uppdateras och trafiken skickas via den nya vägen. Se figur 10-5.



Figur 10-5

Varje enskild operatör ansvarar för routing inom sitt nät och för den information de med hjälp av externrouting skickar över till andra operatörer med vilka de har samtrafik. Regeln är att en operatör motsvaras av ett AS (Autonomt System) och att operatören presenterar en konsistent bild av sin insida mot andra operatörer i det fall att det finns mer än en förbindelse mellan två operatörer. De autonoma systemen identifieras med s.k. autonoma systemnummer. (I bilaga 6 förklaras begreppet autonomt system.)

Routing från en operatörs nät till en annan operatörs nät sker oftast enligt principen att man tar den kortaste vägen i sitt eget

nät till anslutningen mot destinationens operatör.

E-post

Operatören har ett eller flera datorsystem för hantering av e-post till och från operatören samt för mellanlagring av e-post för kunder i det fall kundens system av någon anledning inte är näbart från det avsändande systemet. E-postsystemen kan även omfatta system som medger läsning och sändning av brev från användarprogram hos användaren.

News

Om operatören tillhandahåller News som tjänst till sina kunder finns ett eller flera datorsystem som används för att ta emot, lagra och vidarebefordra News till datorsystem hos användarna. Operatören kan även ha datorsystem för läsning och avsändning av News från användarprogram.

Kund

Operatören har oftast någon form av utrustning placerad nära tjänstens avlämningspunkt hos kunden. Den kan t.ex. vara utförd som en kundplacerad router med Ethernetanslutning samt transmissionsutrustning för att ansluta routerns fjärrsida till operatörens stamnätsfunktion.

Access till hushåll

Även anslutning av hushållsanvändare bör, för att det skall vara effektivt, bygga på en infrastruktur som till fullo stödjer TCP/IP-arkitekturen. Det bör finnas möjlighet för användaren att fritt välja bland operatörer och tjänster samt erhålla goda prestanda oberoende av vilken operatör som tillhandahåller accessen till hushållen. Se även avsnitt 19 "Accessnät och tillgång till information".

Redundans

Centrala delar av utrustningen inom en operatörs nät bör dubbleras. Reservvägar bör finnas med minst 50% av den nominella kapacitet som gäller för den aktuella förbindelsen. Normal funktion måste kunna upprätthållas under veckolånga avbrott i elförsörjningen och på nätets huvudvägar. Se vidare avsnitt 16.

10.3 Användarens nät

Användarens (kundens) lokala nät (LAN) ansluts vanligen till operatörens tjänst (IP-tjänsten) via en s.k. accessrouter och en fast anslutning. Tjänsten levereras till kunden på accessrouterns LAN-sida. (Här behandlas inte anslutning av användarens utrustning via uppringd förbindelse, inte heller de fall när en an-

vändares nät är anslutet till flera operatörer.)

Till användarens lokala nät ansluts persondatorer och servrar för olika tillämpningar. För att förstärka skyddet mot obehörigt intrång i användarens datorsystem placeras vanligen en brandvägg (firewall) mellan accessroutern och det lokala nätet.

I användarens lokala nät finns normalt serverfunktioner för elektronisk post och DNS.

Om användarorganisationen inte själv tillhandahåller (den primära) DNS-servern, kan denna funktion normalt upphandlas som tjänst från operatören. Normalt är att varje användarorganisationen även har en sekundär DNS-server som är placerad skild från den primära servern. Vanligen kan operatören även tillhandahålla den sekundära DNS-servern som tjänst. Likaså kan operatören tillhandahålla serverfunktion för lagring av extern e-post till organisationen i de fall den ordinarie e-postservern tillfälligt inte är nåbar.

Man kanske inte alltid tänker på att nätets (Internets) funktion sträcker sig ända fram till respektive persondator och server. Den funktion som användaren erhåller är inte starkare än den svagaste länken mellan de kommunicerande ändsystemen. Problem hos användare beror ofta på orsaker som är "nära" användaren och som ligger helt utanför operatörernas kontroll.

En organisations lokala driftstöd och implementeringar av kommunikationsfunktioner och tillämpningsprogram måste således hålla en viss minimikvalitet. Vilken denna miniminivå skall vara sätts av respektive organisations krav på funktion och driftsäkerhet. I dag är det dock självklart att den lokala telefonväxeln alltid skall fungera, men det är inte alls lika självklart för många organisationer att dess datorsystem, med intern och extern kommunikation, alltid skall fungera, även om det kanske för många användare är lika viktigt eller viktigare för verksamhetens bedrivande än telefonerna.

10.4 Gemensamma resurser - översikt

Till gemensamma resurser hör de system som alla användare och operatörer är beroende av. De olika delsystemen behandlas i detalj i avsnitt 12 och 13.

En *knutpunkt* utgör en sammankopplingspunkt, en fysisk transportväg, mellan flera olika operatörers nät. Knutpunkter placeras oftast på ett sådant sätt att de har ett bättre fysiskt skydd än

många andra nätkomponenter. Detta gör att det i många fall kan vara lämpligt att placera de gemensamma systemen vid dessa knutpunkter. Det främsta verktyget för att åstadkomma uthållighet är också att man har ett flertal kopior av de gemensamma resurserna placerade på olika platser i nätet.

Det är dock möjligt att de olika operatörerna även anordnar förbindelser mellan varandra utan att passera en knutpunkt.

Till gemensamma resurser räknas även de *DNS-system* som hanterar toppdomäner och domäner ned till den nivå där ansvaret för DNS-system har överförts till respektive användarorganisation eller till dess operatör.

För att kunna erhålla enhetlig *tid* för dokument, transaktioner och för säkerhetsfunktioner, hanterade inom olika delar av infrastrukturen, krävs att det finns tillgång till en sådan tid vilken kan användas av alla system anslutna till Internet.

I det fall man önskar ta reda på hur det är tänkt att trafiken skall styras (routa) till en viss nätadress, som för tillfället inte annonseras ut i routinginformationen från en operatör, skall det vara möjligt att kunna utnyttja ett *vägvalsregister*. I vägvalsregistret dokumenteras hur all routing mellan olika operatörer skall ske.

Whois-server (centralt domänregister) används för att hitta administrativ och teknisk information gällande viss domän under landskoden *.se*.

Index-server för elektroniska kataloger, "white pages" är en gemensam indexeringstjänst från vilken en användare kan erhålla hänvisning till den katalogtjänst i Sverige där man kan hitta bl.a. e-postadressen till en viss person.

10.5 Samverkan mellan operatörer

Svenska operatörer har, som en undergrupp till SNUS, bildat ett gemensamt, informellt, forum kallat Swedish Operators Forum (SOF). Avsikten med SOF är att operatörerna där skall kunna behandla gemensamma frågor.

11 Internetoperatör, minimal IP-tjänst och ansvarsfördelning

Statskontoret föreslår att definitionerna enligt 11.1.1 och kraven enligt 11.1.2 skall gälla.

Statskontoret föreslår vad en minimal IP-tjänst bör omfatta och vilken ansvarsfördelning som skall gälla mellan operatörer.

Statskontoret föreslår att ISOC-SE tar ett ansvar för att reglerna i detta avsnitt följs, liksom att reglerna anpassas till kommande situationer.

Statskontoret har för avsikt att tillsammans med SOF-gruppen ta ett ansvar för och utveckla den generella specifikationen gällande en IP-tjänst.

I direktiven för utredningen anges att ”det är av stor vikt att se till att privata och kommunala operatörer har samma gränssnitt mot användaren”. Med gränssnitt avses här nätoperatörens tekniska gränssnitt på IP-nivå, dvs. vilken IP-tjänst som levereras till kunden i anslutningspunkten. Vid fast anslutning till tjänsten är anslutningspunkten vanligen LAN-sidan på anslutningsroutern.

Statskontoret anser att det måste finnas sätt att garantera en viss minimifunktion så att en kund vid varje tillfälle kan utgå från att en IP-tjänst fungerar och, om detta inte är fallet, att man på ett entydigt sätt kan identifiera var ett fel uppstått och vem som är ansvarig för att åtgärda felet.

De definitioner, krav och ansvarsfrågor som anges i detta avsnitt har utredningsgruppen arbetat fram i samarbete med SOF-gruppen.

11.1 Internetoperatör

11.1.1 Definition av Internetoperatör

Utredningsgruppens förslag till definition:

Med *operatör* avses här en juridisk eller fysisk person som för annan juridisk eller fysisk persons räkning vidarebefordrar IP-paket enligt RFC 791 (och motsvarande för IP version 6), där IP-paketets avsändar- eller mottagaradress disponeras av tredje fy-

sisk eller juridisk person.

Ovanstående innebär att de organisationer som transporterar IP-paket från avsändare utanför den egna organisationen till tredje part definitionsmässigt är operatörer.

Operatörer delas in i kategorierna huvudoperatör och Internetoperatör.

Huvudoperatör - En huvudoperatör är direkt ansluten till alla nationella knutpunkter enligt de regler som finns i avsnitt 12 under "Nationell knutpunkt". En huvudoperatör skall också uppfylla de krav som ställs nedan på en Internetoperatör.

Internetoperatör - En Internetoperatör uppfyller de krav som finns angivna i avsnitt 11 under "Krav på Internetoperatör". Observera att en Internetoperatör som inte är huvudoperatör måste köpa transit (förklaras i bilaga 6) från en huvudoperatör för att nå en nationell knutpunkt.

11.1.2 Krav på Internetoperatör

Följande krav ställs på en Internetoperatör:

1. En Internetoperatör skall leverera en IP-tjänst som uppfyller kraven enligt "Specifikation av minimal IP-tjänst" (se nedan).
2. En Internetoperatör är skyldig att ordna trafiken så att trafik till och från IP-adresser inom respektive operatörs nät och samtliga nationella knutpunkter i Sverige är möjlig, antingen genom egen anslutning till nationell knutpunkt eller genom annan operatör (transit).
3. En Internetoperatör är skyldig att vid alla nationella knutpunkter, direkt eller indirekt via transitoperatör, utväxla trafik med alla andra Internetoperatörer som begär detta. Detta gäller dock endast för trafik till destinationer vilka ligger inom operatörens nät där leveranspunkten finns inom Sveriges gränser. Undantaget från samtrafik är destinationer inom operatörernas interna infrastruktur.
4. Trafik mellan kunder och Internetoperatörer i Sverige får endast i undantagsfall (t.ex. vid fel på huvudväg) förmedlas över förbindelser vilka går via annat land.
5. En Internetoperatör skall, direkt eller indirekt via transitoperatör, bidra till drift och finansiering av gemensamma

resurser, exempelvis av DNS för .se-domänen.

6. En organisation som vill bli undantagen från någon av ovanstående punkter får framställa begäran om detta hos knutpunktsleverantören.

11.2 Minimal IP-tjänst

Ur Statskontorets PM "Generell specifikation av IP-tjänst" har "Specifikation av minimal IP-tjänst" utformats (se bilaga 15). I denna föreslås vad en minimal IP-tjänst bör omfatta. Syftet med denna specifikation är att på en detaljerad nivå ange de komponenter och prestanda som en IP-tjänst minst skall omfatta. Det innebär att de komponenter och prestanda som anges i nämnda specifikation är den absolut lägsta nivån på en IP-tjänst som en kund kan förvänta sig från en Internetoperatör (leverantör). Man bör observera att detta inte är en kravspecifikation för upphandling av en IP-tjänst.

Tjänsten skall kunna utnyttjas av kunden 24 timmar per dygn under årets alla dagar. Eftersom specifikationen anger vad som skall kunna levereras från operatören till en kund, omfattar den inte de fall då en kund är ansluten till flera operatörer.

Statskontoret har för avsikt att tillsammans med SOF-gruppen ta ett ansvar för och utveckla den generella specifikationen gällande en IP-tjänst.

11.3 Ansvarsfördelning mellan operatörer

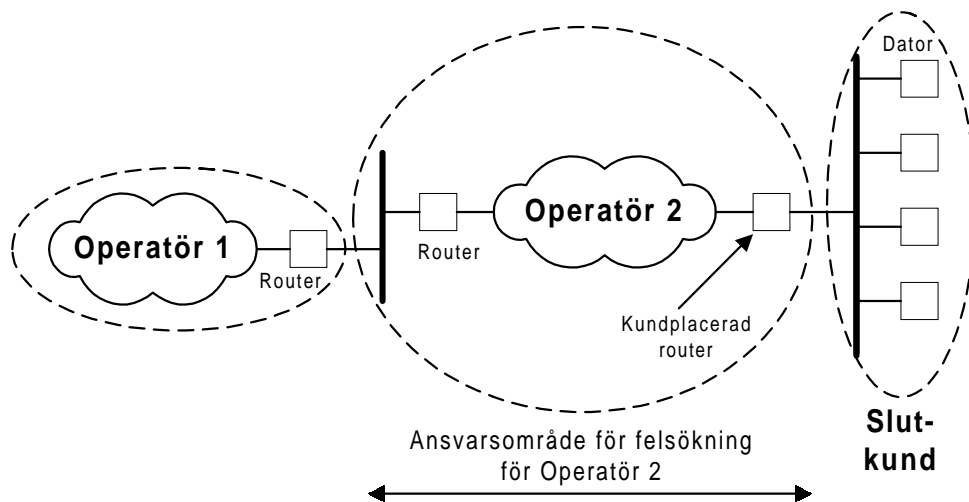
Bakgrund

I de fall en slutkund erhåller sin Internettjänst via en lokal operatör och den lokala operatören är ansluten till övriga Internet via en annan operatör, finns risk att det råder oklarhet i respektive parts ansvarsområde och vilka rutiner som gäller vid felsökning. I detta avsnitt lämnas ett förslag till ansvarsfördelning och sådana rutiner.

Ansvarsfördelning och procedur för felsökning.

I figur 11-1 beskrivs ansvarsområden för operatörer vad gäller felsökning.

Konfigurationen i figuren är exemplifierad med routerteknik, men skulle kunna utgöras av ett system med switchutrustning eller där slutkunden ansluts via uppringd modemförbindelse.



Figur 11-1

Procedur för felsökning är följande:

- Slutkunden skall göra felanmälan hos operatör 2, varvid slutkunden skall erhålla en s.k. trouble ticket (dvs. en kvittens på felanmälan med ett referensnummer).
- Operatör 2 skall analysera felsituationen för att klarlägga om felet ligger hos Internetoperatör 1, hos slutkunden själv eller om det finns fel i IP-förmedlingen från Internetoperatör 2.
- Vid fel hos operatör 1 skall operatör 2 felanmäla detta till operatör 1 på uppdrag av slutkunden. Operatör 1 skall på motsvarande sätt lämna trouble ticket och felsöka. Detta innebär att slutkunden aldrig skall ta direktkontakt med operatör 1. I annat fall åtgärdas felet av operatör 2 alternativt av slutkunden när det är slutkunden själv som har orsakat felsituationen.

Krav på felsökningen hos operatör 2 är bl.a.:

- Operatör 2 skall kunna ta emot och administrativt hantera felanmälningar från slutkund.
- Operatör 2 skall kunna upprätthålla de servicenivåer som finns angivna i "Specifikation av minimal IP-tjänst".
- Omfattningen av felsökning skall sträcka sig från det fysiska gränssnittet mot operatör 1 till motsvarande gränssnitt hos slutkunden. Beroende på avtal mot slutkund kan felsökningsområdet även omfatta slutkundens nät.

Det är väsentligt att varje operatör har kunskap om TCP/IP och överliggande stödprotokoll som DNS etc. så att denne kan avgöra om ett fel är att hänföra till operatör 1, slutkunden eller om det är fel i den egna logiska eller fysiska IP-förmedlingen (exempelvis i det bärande transmissionssystemet, routingsystemet eller DNS).

11.4 Ansvar för regler m.m.

Statskontoret föreslår att ISOC-SE tar ett ansvar för att reglerna i detta avsnitt följs, liksom att reglerna anpassas till kommande situationer.

12 Nationella knutpunkter för samtrafik

Statskontoret föreslår att nationella knutpunkter endast skall användas av de operatörer som har nationell täckning i Sverige. Vidare föreslår Statskontoret att vissa regler skall gälla för att operatörerna skall få ansluta sig till knutpunkterna.

Utöver den nationella knutpunkten i Stockholm och den planerade knutpunkten i Göteborg, föreslår Statskontoret att ytterligare nationella knutpunkter etableras successivt med början i Malmö/Lund och därefter i Sundsvall.

Statskontoret anser att Netnod är lämplig organisation för etablering av nationella knutpunkter utöver i Stockholm och Göteborg.

12.1 Förutsättningar

I direktiven för uppdraget anges det att Statskontoret skall "föreslå flera regionala knutpunkter för sammankoppling av datanäten". Med detta förstås nationella knutpunkter för samtrafik mellan operatörer som etableras på regional nivå.

Likaså anges i syftet med utredningen följande: "Att med bibehållande av nätets öppna karaktär, öka uthålligheten i den organisation av gemensamma, konkurrensneutrala funktioner, som krävs för administration och utveckling av Internet".

Utöver de nationella knutpunkterna kommer det troligen i Sverige att etableras andra knutpunkter på regional eller lokal nivå. Dessa knutpunkter behandlas inte i denna rapport.

12.2 Nationell knutpunkt

En *knutpunkt* utgör en fysisk transportväg, i form av en sammankopplingspunkt, mellan fler än två operatörers nät. Trafik mellan olika operatörers nät kan alltså utväxlas över knutpunkten.

Med nationella knutpunkter avses de knutpunkter som etableras enligt avsnitt 12.4. Statskontoret föreslår att *nationella knutpunkter* endast skall användas av de operatörer som har nationell täckning i Sverige. Undantag gäller för de operatörer som inte har kunder i Sverige. Nationella knutpunkter etableras med god geografisk spridning på orter med stor trafiktäthet. Genom att ha

flera nationella knutpunkter erhålls såväl redundans som lastdelning.

Varje nationell knutpunkt skall ha sådan kapacitet att den kan hantera trafiken mellan operatörernas nät. Detta kan ske genom gemensam sammankopplingsutrustning. I de fall den gemensamma sammankopplingsutrustningen inte har kapacitet nog att hantera trafiken mellan vissa operatörers nät, etablerar knutpunktsleverantören kompletterande bilaterala transportvägar direkt mellan dessa operatörers nät.

För att få ansluta sig till de nationella knutpunkterna har knutpunktsleverantören (se 12.4) fastställt att operatörer bl.a. skall uppfylla följande krav:

- ha eget AS-nummer,
- inte använda defaultrouting,
- ha routingutbyte med minst två andra operatörer via de nationella knutpunkterna,
- endast skicka trafik till destination med vilken man i förväg kommit överens om trafikutbyte, samt
- vara ansluten till samtliga nationella knutpunkter.

Statskontoret stödjer att dessa krav skall uppfyllas.

12.3 Nationella knutpunkten i Stockholm

I Stockholm finns i dag den enda nationella knutpunkten i Sverige.

Under juni 1997 ombildades denna knutpunkt från en samlokaliserad lösning till en distribuerad lösning med utrustning placerad på två platser i Stockholm. Den tidigare knutpunkten har varit placerad på KTH. (Se vidare i bilaga 14 "Den nationella knutpunkten i Stockholm".)

12.4 Förslag till utbyggnadsplan

Syftet med ytterligare nationella knutpunkter

Genom att etablera ytterligare nationella knutpunkter utöver den i Stockholm erhålls redundanta förbindelser och en lastfördelning av trafiken inom Sverige.

Varianter av nationella knutpunkter

För den tekniska lösningen har utredningsgruppen kommit fram till att följande två varianter av nationella knutpunkter är lämpligast:

1. Distribuerad lösning med centrala delar dubblerade.
Variant 1 innebär en dubblering av central utrustning och att denna är placerade i två skilda lokaler. Kommunikationen mellan de centrala delarna sker via optisk fiber. Den yta som krävs på respektive plats är en lokal om minst 10 m². Respektive operatör har sin utrustning placerad på annat håll, dvs. i egen lokal skild från den centrala delen. Operatörens utrustning ansluts till båda de centrala utrustningarna via optisk fiber
2. Samlokaliserad lösning med centrala delar dubblerade.
Variant 2 innebär att de centrala delarna är dubblerade och att dessa är placerade inom samma lokal. Respektive operatör har också sin utrustning placerad i denna lokal eller i nära anslutning till de centrala delarna. Operatörernas utrustning ansluts till båda de centrala utrustningarna. Den yta som krävs för den gemensamma lokalen är minst 40 m².

För båda varianterna gäller att lokalen för de centrala delarna skall ha elkraft och kylanläggning med reservgång för drift under 14 dagar.

Som exempel på utrustning för de centrala delarna kan nämnas att för den nya (1997-06) knutpunkten i Stockholm utgörs de av två FDDI-växlar och dubblerade fiberoptiska förbindelser till respektive operatörs utrustning.

Utgångspunkt

En viktig utgångspunkt för de nationella knutpunkterna är att behovet av samtrafikskapacitet mellan operatörer alltid skall kunna tillgodoses. Detta innebär bl.a. att den tekniska lösningen för knutpunkterna skall vara utbyggbar och flexibel. Etablering av knutpunkterna föreslås ske successivt (se nedan).

Kriterier för val av ort för knutpunkt

Kriterier för val av ort för placering av nationell knutpunkt:

- alla Internetoperatörer har (eller vid driftstart har) infrastruktur till den aktuella orten (detta anger grovt var kunderna finns),
- transmissionsnätets topologi; nuvarande och planerad utbyggnad av fiberoptiska nät; speciellt gäller det tvärförbindelser,

- lokal för utrustning med lämpligt fysiskt skydd t.ex. bergtrum,
- för distribuerad lösning (variant 1) kräver tillgång till fiberoptiskt nät inom orten.

Förslag till etablering av nationella knutpunkter

Statskontoret föreslår att etableringen av knutpunkterna sker successivt utgående från behovet. Bedömningen är att det under en överblickbar tid är aktuellt med maximalt åtta stycken nationella knutpunkter för Sverige. En utgångspunkt för etableringen är att den nya knutpunkten i Stockholm har tagits i drift under juni 1997 och att knutpunkten i Göteborg kommer att tas i drift under december 1997.

Nedan anges förslag till etablering av knutpunkt nummer 3-4. För den femte knutpunkten anges endast tänkbar ort.

Nr	Placering	Driftstart	Nationell knutpunkt	Status
1	Stockholm	1997-06	Variant 1	Etablerad
2	Göteborg	1997-12	Variant 1	Etableras
3	Malmö/Lund	1998-07	Variant 2	Förslag
4	Sundsvall	1999-01	Variant 2	Förslag

På samtliga angivna orter ovan är de större Internetoperatörerna representerade med sin infrastruktur, dvs. det finns ett kundunderlag.

Enligt uppgift från knutpunktsleverantören (se nedan) kommer knutpunkt i Göteborg att vara en distribuerad lösning (variant 1 ovan) och uppbyggd på samma sätt som knutpunkten i Stockholm. Detta innebär att utrustningen kommer att vara installerad två lokaler i Göteborgsområdet och att optisk fiber utnyttjas för kommunikation mellan dessa lokaler samt mellan lokalerna och respektive operatörs lokal.

För etablering av knutpunkten i Skåne finns tillgång till bergsumsanläggning. Med hänsyn till att det ur beredskapssynpunkt kan vara mindre lämpligt att placera nationella knutpunkter i storstadsregioner föreslås att knutpunktsleverantören tillsammans med operatörer samt försvars- och beredskapsmyndigheter ytterligare överväger val av ort för placering i Skåne.

För etablering av den första knutpunkten i Norrland föreslås Sundsvall som lämplig ort, där bergsumsanläggning finns. Alternativ som övervägts är Lycksele och Älvsbyn där det också finns bergtrum för placering av utrustningen. Det är dock inte kommer-

siellt försvarbart att etablera en knutpunkt på någon av dessa orter i januari 1999. Dock bör man ur beredskapssynpunkt även överväga alternativen Lycksele och Älvsbyn och möjligheten till statlig finansiering av dessa knutpunkter. PTS har uppgett att medel för sådana åtgärder finns.

Med hänsyn till den förväntade trafiktillväxten är Örebro tänkbar ort för etablering av den femte knutpunkten. Ytterligare knutpunkter, dvs. från den sjätte knutpunkten, etableras vid behov.

Organisation för etablering och drift av nationella knutpunkter

Utredningsgruppen kan konstatera att för etablering av den nationella knutpunkten i Stockholm har Stiftelsen för telematikens utveckling bildat Netnod Internet Exchange i Sverige AB (Netnod). (Se bilaga 8.) Netnod kommer också att svara för den planerade etableringen av knutpunkten i Göteborg.

Eftersom det redan finns en organisation för etablering och drift av knutpunkter, dvs Netnod, anser Statskontoret att den organisationen även är lämplig för etablering av övriga nationella knutpunkter enligt ovan. Etableringen föreslås ske i ett nära samarbete med de Internetoperatörer som har eget stamnät i Sverige (via SNUS undergrupp SOF), PTS och andra eventuella knutpunktsleverantörer. Denna samarbetsgrupp anger också vilken teknisk lösning och utrustning som skall väljas samt lämplig lokal för utrustningen. Knutpunktsleverantören ansvarar för planering och installation samt för drift av knutpunkterna.

Övergripande regel för nationella knutpunkter

Statskontoret föreslår att alla Internetoperatörer med eget stamnät i Sverige och med nationell täckning skall vara anslutna, direkt eller via annan operatör, till samtliga nationella knutpunkter. I de fall en sådan operatör väljer att inte ansluta sig direkt till en nationell knutpunkt är den operatören att betrakta som kund till den andre operatören. En sådan operatör betalar för sin transittrafik till den vars nät operatören utnyttjar. Undantag gäller för de operatörer som inte har kunder i Sverige men som har anslutning till knutpunkt.

I övrigt gäller de regler som utformats av knutpunktsleverantören.

Vilka krav som bör ställas på Internetoperatörer framgår av avsnittet 11.1.2 "Krav på Internetoperatör".

Finansiering

Se avsnittet 15 "Finansiering av gemensamma resurser".

13 Gemensamma resurser

Statskontoret föreslår följande gemensamma nätresurser:

- DNS för landskoden *.se* och för roten, dvs. för ”.”
- Tidsservrar för nationell tid
- Vägvalsregister
- Whois-server
- Indexserver
- Domännamnshantering (se avsnitt 14)

Statskontoret föreslår att lämplig myndighet i kontakt med Net-nod tar initiativ till en plan tas fram så att den svenska delen av Internet kan drivas fristående från omvärlden vid avspärrning. Detta föreslås ske i samarbete med PTS, ÖCB, Säkerhetspolisen, Försvarmakten och berörda operatörer (SOF-gruppen). Statskontoret har inte kunnat identifiera någon myndighet som är lämplig för detta och har omfattande kompetens inom Internet-området.

Vid planering och utbyggnad är det viktigt att vissa av de för strukturen gemensamma funktionerna dimensioneras så att dessa kan hantera *minst den dubbla trafiken* av den uppskattade vid varje tidpunkt. Detta gäller inte bara dimensionering av överföringskapacitet utan också vid konstruktion av logiska system exempelvis för omvandling av logisk till fysisk nätadress.

13.1 Gemensamma resurser utöver knutpunkterna

Statskontoret föreslår att de gemensamma nätresurserna, utöver de nationella knutpunkterna, för drift av den svenska delen Internet skall vara:

- DNS för landskoden *.se* och för ”.” (dvs. roten för det globala domännamnsträdet) samt de delar som behövs för att erhålla nummer-till-namnuppslagning.
- Nationell tid via protokollet NTP.
- Vägvalsregister gällande hur routing skall ske till adress med visst prefix. Vägvalsregister används vid felsökning och konfigurering av operatörernas routrar.
- Whois-server för domännamn under *.se*.

- Indexserver för elektroniska kataloger, "white pages". Detta är en gemensam indexeringstjänst från vilken en användare automatiskt kan få en hänvisning till den katalogtjänst i Sverige där man kan hitta e-postadresser.

Dessutom anser Statskontoret att det krävs reservsystem för drift av resurser som finns utanför landets gränser vilka den svenska delen av Internet är beroende av. Detta omfattar bl.a. DNS och tidsdistributionssystemet.

De gemensamma resurserna föreslås bli placerade och drivas så att de erhåller bästa skydd mot olika former av störningar, såväl vad det gäller fysisk miljö som olika former av attacker och in-trång via nätet självt.

13.2 DNS för toppdomänen .se

DNS och domännamnsstrukturen beskrivs i bilaga 6 "Internet i Sverige - kort historisk och teknisk överblick".

Varje dator som är ansluten till Internet behöver kunna skaffa information om vilka IP-adresser och domännamn andra datorer har genom att slå upp dem i DNS-databasen.

Det är viktigt att de namnservrar för DNS-roten och de som tillhandahåller information om vilka huvuddomäner som finns under toppdomänen .se gör detta på ett konkurrensneutralt sätt och att driften av dessa sköts effektivt och säkert.

I dag hanteras .se av följande datorsystem, varav tre är placerade i Sverige (anges med kursiv fetstil):

NS.UU.NET
 SPARKY.ARL.MIL
I.ROOT-SERVERS.NET
 NS.EU.NET
NIC.LTH.SE
 DNS.CIT.CORNELL.EDU
SUNIC.SUNET.SE

Den organisation som fr.o.m. hösten 1997 kommer att ha ansvaret för toppdomänen .se behandlas i avsnitt 14, "Stiftelsen för Internetinfrastruktur" (II-Stiftelsen). (Se bilaga 8.)

Knutpunktsleverantörerna bör vara de som kontrollerar driften av DNS-servrarna. Detta kan ske via kontraktering av driften till lämplig organisation. NIC-SE som fr.o.m. hösten 1997 kommer att föra registret över domäner inom .se skall på lämpligt sätt se

till att primärservern för .se uppdateras med korrekt information minst en gång per arbetsdag. Se avsnitt 14.

Statskontoret föreslår att namnservrar för toppdomänen .se placeras på följande platser:

- Stockholm (vid nationell knutpunkt)
- Göteborg (vid nationell knutpunkt)
- Malmö (vid nationell knutpunkt)
- Norra Sverige (vid nationell knutpunkt)
- Centraleuropa
- Nordamerika, östkusten
- Nordamerika, västkusten
- Japan

Knutpunktsleverantören skall ansvara för driften av namnservrarna vid de nationella knutpunkterna. Genom ett internationellt samarbete och med ett ömsesidigt utbyte av tjänster arrangeras driften av övriga namnservrar. Ansvaret för driften av respektive namnservrar skall ligga hos en operatör som har direktanslutning till respektive knutpunkt.

Dessutom föreslås att två stycken DNS-servrar för .se placeras vid en totalförsvarsorganisation.

Respektive namnservrar får inte vara ur drift mer än en dag per år.

Statskontoret stödjer vidare SOF-gruppens förslag att samtliga DNS-servrar för .se, som är placerade i Sverige, skall klara av att hantera "secure DNS" enligt RFC 2065 och 2137 fr.o.m. den 15 november 1997.

13.3 Namnservrar för DNS-roten

Namnservrar för DNS-roten hanterar den översta nivån i det globala domännamnsträdet. Sedan 1989 har Sverige haft den enda namnservern för DNS-roten utanför Nordamerika. Det har tidigare funnits tolv servrar. Maj 1997 startade den trettionde namnservern för DNS-roten i världen. (Domännamnsstrukturen beskrivs i bilaga 6 "Internet i Sverige - kort historisk och teknisk överblick".)

Nu hanteras roten i domännamnsträdet av nedanstående system. Dessa är placerade på olika platser i världen, varav

I.ROOT-SERVERS.NET är placerad i Sverige:

A.ROOT-SERVERS.NET	(Virginia, USA)
B.ROOT-SERVERS.NET	(California, USA).
C.ROOT-SERVERS.NET	(Virginia, USA)
D.ROOT-SERVERS.NET	(Maryland, USA)
E.ROOT-SERVERS.NET	(California, USA)
F.ROOT-SERVERS.NET	(California, USA)
G.ROOT-SERVERS.NET	(Virginia, USA)
H.ROOT-SERVERS.NET	(Maryland, USA)
I.ROOT-SERVERS.NET	(Stockholm, Sverige)
J.ROOT-SERVERS.NET	(Virginia USA)
K.ROOT-SERVERS.NET	(London, England)
L.ROOT-SERVERS.NET	(California, USA)
M.ROOT-SERVERS.NET	(Fujisawa, Japan)

Det är ur beredskapssynpunkt mycket viktigt att Sverige även i fortsättningen inom landet kan behålla en av Internets namnserverar för DNS-roten. Det gör det enklare att klara en avspärrning. Därför är det viktigt att drift och underhåll av denna server görs på ett klanderfritt sätt, likaså att det alltid finns kvalificerad representation i relevanta samarbetsforum.

Statskontoret föreslår att namnservern för DNS-roten som är tilldelad Sverige skall placeras vid den nationella knutpunkten i Stockholm. Netnod föreslås vara den som kontrollerar driften av denna namnserver. Detta kan ske genom kontraktering av driften till lämplig organisation.

13.4 Tidsserver för nationell tid

För olika datortillämpningar kan det krävas tillgång till enhetlig och exakt tid, exempelvis för elektroniska dokument, elektronisk post, transaktioner och för säkerhetsfunktioner. Tillgång till enhetlig och exakt tid kan erhållas från tidsserverar anslutna till Internet. Till datorsystemen förmedlas tid med protokollet NTP. (I bilaga 6 förklaras närmare hur tidsfunktionen fungerar för Internet.)

För att göra det möjligt att erhålla rätt nationell tid föreslår Statskontoret att tidsserverar och högstabla klockor anskaffas och att de placeras vid var och en av de nationella knutpunkterna. Respektive tidsserver erhåller sin tid från klockan.

Sveriges Provnings- och Forskningsinstitut (SP) i Borås är riksmätplats för tid, tidsintervall och frekvens och har tre atomur som tillsammans utgör den nationella tidsskalan. Inom ramen för ett internationellt samarbete mellan tidslaboratorier världen runt och ett omfattande forskningsarbete, ingår SP:s atomklockor i bildandet av den internationella tidsskalan, UTC. SP bedöms ha den

kompetens som krävs för att på Internet erhålla en tidsfunktion av eftersträvad kvalitet och atomklockorna vid SP kan utgöra tidreferens för de klockor som är placerade i de nationella knutpunkterna.

Statskontoret föreslår att SP får till uppgift att dels utforma en infrastruktur för tidsdistribution, dels i samarbete med Netnod, anskaffa lämpliga klockor för placering vid knutpunkterna. Likaså föreslås att SP i en driftsituation får till uppgift att kontinuerligt kontrollera klockornas noggrannhet och funktion. Tidsfunktionen bör vara så utformad att den vidmakthålls i händelse av att Sverige blir avspärrat från omvärlden och vid segmentering av Internet.

Metodiken att distribuera tid är att utgå från en primär klocka (den nationella klockan med sin server) som ger tid till klockor på sekundär nivå (de nationella knutpunkterna). Dessa i sin tur ger tid till nästa underliggande nivå och så vidare i ett antal nivåer till den vanlige användaren. På vilken nivå som tiden hämtas beror på tillämpningen. Tidhållningen inom Internet är en allmän nyttighet som kommer alla användare till gagn.

Genom den hierarkiska uppbyggnaden av hur tiden distribueras är det omöjligt att debitera kostnaden för den nationella tidhållningsresursen på de enskilda användarna.

Statskontoret föreslår att Netnod skall ansvara för finansiering, anskaffning och drift av tidsservern. Likaså föreslås att Netnod finansierar anskaffningen av de klockor som föreslås placeras vid respektive knutpunkt. Förslag till finansiering av driften av klockorna anges i avsnitt 15.

13.5 Vägvalsregister

Ett vägvalsregister dokumenterar hur routing av trafiken skall göras till adresser med visst prefix (se avsnitt 14, "IP-adresser") och, i de fall det finns flera vägar, i vilken ordning dessa vägar skall användas.

Vägvalsregistret skall således dokumentera det totala trafik- och routingutbytet mellan alla operatörer som är anslutna till knutpunkterna. Registret används vid felsökning och konfigurering av operatörernas routrar.

Vägvalsregistret skall även innehålla information om kontaktpersoner hos de olika operatörerna för felavhjälpning. Vägvalsregistret skall vara indexerat med AS-nummer.

Statskontoret föreslår att vägvalsregister upprättas och placeras vid minst två av de nationella knutpunkterna. Netnod föreslås ansvara för anskaffning och drift av vägvalsregistren. Operatörerna skall ansvara för att informationen i registren är aktuella.

13.6 Indexserver

Med hjälp av en indexserver skapas en central tjänst till vilken en producent av information kan skicka ett index (dvs. en summering av den information som producenten tillhandahåller). Indexeringstjänsten ger i sin tur kunderna till tjänsten referenser tillbaka till producenten när information som beskrivs av detta index söks.

Detta innebär att en producent av information inte behöver skicka ut komplett information till en indextjänst, eller göra all information tillgänglig för anonym access (som sker i dag med traditionell robot-teknik). I stället uppstår efter hänvisningen ett kund – producentförhållande vilket i sin tur möjliggör för producenten att ge olika service till olika kunder, utgående från vad som avtalats.

Statskontoret anser att gemensamma indexeringstjänster skall stödjas och att Netnod ansvarar för driften av indexservern. Med hänsyn till att indextjänsten är en distribuerad lösning får Netnod finna en lämplig fysisk placering av respektive indexserver.

Till bastjänsterna hör sökning efter en persons elektroniska post-adress, utgående från personens namn och adress. Detta problem undersöks i projektet TISDAG (Technical Infrastructure for Swedish Directory Access Gateways). Projektet stöds av Stiftelsen för Kunskaps- och Kompetensutveckling (KK-stiftelsen), och kommer att beskriva hur en sådan central indextjänst skall realiserar. (Projektet TISDAG beskrivs i bilaga 5.)

Statskontoret anser att gemensam indexering av webbinformation inte är en gemensam nätfunktion och endast bör skapas om marknaden själv tar ett sådant initiativ. Vilken information som skall tillhandahållas genom gemensamma söktjänster kan fortsätta att diskuteras i forum som ISOC-SE eller SOF.

13.7 Whois-server

Whois är en s.k. white pages-tjänst. Sådana tjänster kan användas för att, utgående från uppgifter gällande en kontaktpersons namn, organisation, geografisk lokalitet eller en kombination av sådan uppgifter, hitta mer uppgifter om personen. En white pages-tjänst kan realiserats på olika sätt med olika protokoll. Det är vanligt att använda Whois-funktionen för att erhålla information om personer som administrerar Internet.

Statskontoret anser att det måste finnas en gemensam whois-tjänst som utgör ett centralt domänregister för att hitta administrativ och teknisk information gällande viss domän under landskoden *.se*. Med hänsyn till NIC-SE:s verksamhet (se avsnitt 14) anser Statskontoret vidare att NIC-SE skall ansvara för anskaffning och drift av whois-servern samt vara ansvarig för att uppgifterna i whois-serverns register uppdateras fortlöpande. Whois-servern föreslås bli placerad vid den nationella knutpunkten i Stockholm.

13.8 Drift vid avspärning

Statskontoret föreslår att lämplig myndighet i kontakt med Netnod tar initiativ till att en plan upprättas för hur den svenska delen av Internet skall drivas fristående i händelse av avspärning eller vid attack via nätet mot för nätet centrala resurser utanför Sveriges kontroll. Detta arbete skall ske i samarbete med PTS, ÖCB, Säkerhetspolisen, berörda operatörer (SOF-gruppen) och Försvarsmakten. Statskontoret har inte kunnat identifiera någon myndighet som är lämplig för detta och har omfattande kompetens inom Internetområdet.

Syftet med dessa åtgärder är att kunna bibehålla driften nationellt och att med hjälp av lokala resursdatorer placerade i Sverige simulera kritiska resurser för drift av Internet. Dessa kritiska resurser finns vanligen i nätet utanför Sverige.

13.9 Beredskapsdrift av DNS

Man förvänta sig att även i fortsättningen andra toppdomäner än *.se* kommer att användas av svenska organisationer. Exempelvis använder nu vissa operatörer i Sverige för adresser till kunders e-postkonton domännamn inom *.com*- och *.net*-domänerna. Dessutom använder vissa företag i Sverige adresser utanför *.se*-domänen. Det finns ingen svensk organisation som har kontroll över dessa domäner.

Utgående från att Sverige kan bli avspärrat från omvärlden bör

man se till att under alla omständigheter nödvändig drift av namnservern för toppdomänen *.se* kan klaras inom Sverige.

I avsnitt 13.2 föreslås att namnserver för toppdomänen *.se* hanteras inom Sverige. Detta är även lämpligt ur beredskapssynpunkt.

Ur beredskapssynpunkt kan det däremot vara direkt olämpligt att enbart ha domännamn registrerat utanför *.se*-domänen, beroende på att dessa domännamn inte med säkerhet kan nås vid avspärning.

14 Namn- och adressplan

Statskontoret föreslår att ISOC-SE bildar en samrådsgrupp med deltagare från lämpliga myndigheter.

Statskontoret anser att den organisation som ISOC-SE byggt upp för domännamshanteringen har förutsättningar att fungera bra.

Statskontoret anser vidare att regelverket för hantering av domännamn för toppdomänen .se är till fyllest.

I direktiven för uppdraget till Statskontoret ingår bl.a. att behandla namn- och adressplan. I direktiven anges även att "ett tekniskt sunt regelverk avseende bl.a. namn- och adressplan skall tas fram" samt att "bedöma om den nuvarande administrationen av Internet är adekvat, eller om den bör organiseras på annat sätt". Likaså anges att utgångspunkten skall vara att staten endast i undantagsfall ingriper med reglering.

Namn- och adresshantering har hittills fallit utanför gällande lagstiftning. Frågan har dock behandlats och kommenterats i samband med revideringen av telelagen (SFS 1993:597). På sid 198-199 i Ds 1996:38, Moderna telekommunikationer åt alla, resonerar utredaren kring de namn- och adressplaner som finns och konstaterar att vad gäller X.400 så har Post & Telestyrelsen (PTS) ett samlat ansvar medan för Internets namn- och adressering ligger ansvaret för detta på en tjänsteman på KTH (Inter-nic.se). Denne tjänsteman har uppdraget att förvalta den svenska namn- och adressplanen för Internet av IANA. Slutligen drar man slutsatsen att "Mot bakgrund att PTS redan har ansvaret för namn- och adressplanen för X.400 är det naturligt att det samlade ansvaret för ovannämnda planer åläggs myndigheten".

I regeringens proposition (1996/97:61) om översyn av telelagen (SFS 1993:597) görs sedan bedömningen att "Med hänsyn till en pågående utredning om Internet avvaktar regeringen med ställningstaganden till förslagen om en samlad databas med elektroniska postadresser och om ansvaret för namn- och adressplan på Internet".

I detta avsnitt om namn- och adressplan beskrivs de typer av adresser som här är aktuella: IP-adresser, AS-nummer samt domännamn. Dessutom beskrivs hur hanteringen har fungerat hittills i Sverige, samt de initiativ som marknaden tagit under

våren 1997 för att formalisera hanteringen. Enbart den svenska delen av Internet behandlas.

I bilaga 6 "Internet i Sverige - kort historisk och teknisk överblick" förklaras vissa grundfunktioner för Internet, bl.a. behandlas IP-adresser, AS-nummer och domännamn liksom organisationer för operatörssamarbete.

Adresstyper

Inom Internet finns tre typer av adresser, IP-adresser, AS-nummer och domännamn. För de två första typerna sker tilldelning på internationell nivå och det är adresser som enskilda användare inte "ser". Den sistnämnda är den adress som användaren direkt använder vid exempelvis elektronisk post och som det har varit en del debatt kring under de senaste åren. Det är också domännamshanteringen som dominerar detta avsnitt.

14.1 IP-adresser

IP-adressen är varje terminals (dators) unika nätadress. Den består av 4 bytes, dvs. av 32 bitar (ettor och nollor) och som brukar översättas i decimala tal med en gruppering om fyra siffergrupper. Varje siffergrupp kan ha värden inom intervallet 0-255. Den kan till exempel se ut som: **192.36.125.2**

Denna adress är topologiskt indelad i vad som kallas prefix och lokaldel. Den totala siffersekvensen är alltid lika lång men prefixet kan variera i längd. Med långt prefix blir lokaldelen kort och tvärtom. Prefixen tilldelas operatörerna som därefter delar ut underprefix eller lokaldelar till sina kunder. Det innebär att ju kortare prefix en operatör får desto fler kunder kan denne ha bakom sitt prefix. Ett speciellt adressutrymme är reserverat för privata nät (beskrivs i RFC 1918) och som kan återupprepas. Att adressutrymmet kan återupprepas medför att vid ett eventuellt byte av operatör kan enskilda terminalerna inom det privata nätet behålla sina IP-nummer och det är enbart de första siffrorna som pekar mot det privata nätet som behöver ändras. Detta underlättar ett eventuellt operatörsbyte för ett enskilt privat nät. En komplikation är dock att adresserna måste översättas till riktiga adresser vid gränsen till operatören.

Vad som är värt att notera är att IP-adresser är icke-geografiska men operatörsberoende. Om man byter operatör så måste man således också byta IP-adress. Operatörsportabilitet är inte möjlig enligt det dokument som RIPE (RIPE-159) gett ut om IP-adresser.

Tilldelningen av IP-adresser sker på internationell bas och hante-

ras alltså inte centralt i Sverige. En operatör i Sverige får adresser från RIPE NCC i Amsterdam att fördela till sina kunder. För Europa, Mellanöstern, Afrika, f.d. Sovjetunionen och delar av Asien är det RIPE NCC som har ansvaret för IP-adresser. InterNIC och APNIC är systerorganisationer som delar ut adresser för resten av världen. Dessa tre organisationer sorterar under IANA. RIPE har beskrivit hur IP-adresser skall tilldelas för att erhålla ett effektivt utnyttjande. Beskrivning av vad som menas med effektivt utnyttjande av IP-adresser finns dokumenterat i RIPE-159.

Information om vilka adresser som har tilldelats vilken operatör finns tillgänglig på Internet i databaser som förs av RIPE NCC och dess systerorganisationer.

Tilldelningspolicy

Totalt finns i IPv4 plats för ca 4,3 miljarder IP-adresser på Internet. I praktiken är en stor del av detta adressutrymme tomt. Stora delar av adressutrymmet används aldrig eller försvinner vid uppdelning av befintligt adressutrymme i delnät. Före Internets popularitet var det lätt för en organisation att få tag på adressutrymme. Man delade tidigare ut stora mängder adresser utan ordentlig eftertanke och analys, eftersom Internet var ganska litet och adressutrymmet ansågs vara väl tilltaget. Resultatet ser vi i dag genom de mycket stora routingtabeller som orsakar ökad administration, dyrare centrala anslutningar, dyrare linjer, försämrad kapacitet samt organisationer som har väldiga mängder outnyttjat adressutrymme.

För närvarande finns det ungefär 40 000 routingentryn på Internet. Ett routingentry anger vilken väg en router skall skicka IP-paket för att nå en destination i ett specifikt logiskt IP-nät. Ett routingentry lagras i ett register i routern. Registret uppdateras dynamiskt med användning av routingprotokoll. Grovt kan man säga att routers placering i nätet avgör hur många värden som lagras i routers register. En centralt placerad router innehåller vanligen ett större antal värden än en lokalt placerad t.ex. en accessrouter.

Vad man vill uppnå genom de regleringar som finns är dels en minskad belastning på Internets centrala utrustningar, dels ett effektivare utnyttjande av befintligt adressutrymme. Detta uppnår man främst genom följande två tillvägagångssätt:

1. Genom omfördelning och omstrukturering av redan utdelade adressutrymmen och aggregering av detta adressutrymme kan man minska antalet routingentryn i routingtabellerna.
2. Genom samarbete mellan operatörer försöker man dela upp

14.3 Domännamn

14.3.1 Principen för domännamn

Antalet domännamn i Sverige ökar kraftigt. Det finns i dag omkring 50 000 st och antalet nyregistreringar uppgår till ca 2 500 per månad och ökar i takt med användningen av Internet i Sverige. Det kommer allt fler frågor från användare, vilket ökar belastningen på domänregistreringsfunktionen på Internic.se.

Toppdomänen för Sverige är *.se*. Domännamnshanteringen i Sverige omfattar därmed allt som sorterar under toppdomänen *.se*. Tilldelning sker idag av s.k. huvuddomäner till företag och andra organisationer som därefter kan indela den tilldelade huvuddomänen i subdomäner. För privatpersoner har huvuddomänen *.pp.se* bildats och för telefonnummer *.6.4.tpc.int*. Under våren 1997 beslöts inom AG12 (se nedan) dessutom att bilda länsvisa huvuddomäner genom strukturen *.länsbokstav.se*.

När det gäller tilldelning av domännamn så finns det en grundläggande princip som har överskuggat alla diskussioner under de senaste åren. Det är principen om portabilitet. Det finns två typer av portabilitet som man pratar om, geografisk portabilitet och operatörsportabilitet. När man pratar om Internet och domännamn så är geografisk portabilitet automatiskt inbyggt i systemet (även om jag flyttar geografiskt så behåller jag samma domännamn) och operatörsportabilitet erhåller man genom att det inte finns någon identifierare för operatören i domändelen. Exempelvis domänen statskontoret.se innehåller ingen information om vilken operatör som används och Statskontoret har möjlighet att byta operatör utan att tvingas byta domännamn.

14.3.2 Nuvarande organisation för domännamnshantering

Under hösten 1995 arbetade ITS, SNUS och PTS tillsammans fram en policy för hur domännamn skall tilldelas i Sverige. Samtidigt gjordes också en samordning med meddelandehanteringssystemet X.400 och en överenskommelse om tre grundprinciper:

1. Namn- och adressportabilitet

Organisationen som identifieras av namnet skall ha rätten till namnet, och skall fritt kunna välja eller byta operatör vid godtycklig tidpunkt. Namnet skall därför inte innehålla någon relation till en eventuell operatör eller annan extern organisation.

2. Näbarhet

Det skall vara möjligt att befordra e-post med användning av enbart det unika namnet och landskoden. Detta nås eftersom namnet är unikt i Sverige.

3. Adresskonvertering

En X.400-adress skall kunna konverteras helt och hållet till en Internet e-postadress respektive omvänt, utgående enbart från adressen själv, utan tillgång till yttre information, såsom databaser eller register.

En överenskommelse om dessa principer nåddes genom ett gemensamt remissförfarande från ITS, SNUS och PTS och där principerna stöddes av följande organisationer: France Telecom, GE Information Services, IBM Svenska, ITS, Postnet, SNUS, SUNET, Telenordia, Tele2, Telia, Unisource och VM-data. I samband med överenskommelsen bildades en arbetsgrupp (AG12) inom ITS. Medlemmar i arbetsgruppen är ovannämnda organisationer samt SNUS och Statskontoret, dock har inte alla deltagit aktivt i arbetsgruppen. Under våren 1997 har gruppen utökats med representanter från användarsidan. ITS håller med teknisk och administrativ sekreterare. Ordförande utses av ITS styrelse och har sedan starten varit Patrik Fältström, SNUS.

I gruppen har regler som skall gälla för tilldelningar av domännamn diskuterats fram. Gällande regler för tilldelning finns publicerade (<http://www.internic.se>) tillsammans med anvisningar om hur man går tillväga för att registrera ett domännamn.

För att registrera ett domännamn vänder man sig till en operatör, vilken sedan hjälper till ansökan om registrering av domännamn. Registreringen sköts av Internic.se. Internic.se kontrollerar att det sökta domännamnet inte är upptaget sedan tidigare, att namnet svarar mot organisationsnamnet m.m., i enlighet med de regler som formulerats av AG12. Om Internic.se finner att namnet inte kan tilldelas den sökande så avslås ansökan. Om sökanden anser att avslaget inte är motiverat kan denne begära att få avslaget granskat av AG12. AG12 ger därefter ett utlåtande och den diskussion som uppstår inom AG12 kan också ge upphov till att regelverket utvecklas.

Det föreligger också en möjlighet att någon eller några vill klaga ytterligare på hanteringen och få sin fråga prövad rent rättsligt, vilket kan medföra ett mycket ovisst, arbets- och kostnadskrävande förfarande som inte gagnar vare sig de klagande eller de många instanser som skulle kunna bli indragna i en sådan process.

I samband med att Internet vuxit i popularitet har allmänhetens och massmedias intresse för domännamnsfrågor vuxit. Detta har inneburit att principerna för tilldelning och även enskilda fall har diskuterats i massmedia. En av de frågor som diskuterats är att det inte i formell mening går att överklaga ett beslut om tilldelning. Det råder också stor osäkerhet om hur tilldelningen egentligen går till och vem som beslutar. När domännamnsregistreringen i Sverige började 1986 gavs ansvaret från IANA för .se till en anställd på Enea Data AB som sedan tog med sig uppgiften till Internic.se. Under de år som gått har utvecklingen av Internet tagit en ofattbar fart. Att ansvaret för registrering av domännamn ligger på en enskild person är funktionellt och organisatoriskt inte längre tillfredsställande.

14.3.3 ISOC-SE

I mars 1997 bildades ISOC-SE, ett nationellt "chapter" till ISOC (Internet Society). Inom ISOC-SE har man uppmärksammat att det finns problem med ansvaret för domänen .se och därför har man under våren 1997 arbetat fram förslag till en ny organisation för att hantera domännamn i Sverige. Förslaget till ny organisation har ISOC-SE diskuterat med ITS/AG12, SNUS, SOF m.fl. Ansvaret för .se kommer i samband med att den nya organisationen startar att överföras från Internic.se till Stiftelsen för Internetinfrastruktur (II-Stiftelsen) i samförstånd med IANA.

ISOC-SE och II-Stiftelsen beskrivs i bilaga 8.

14.3.4 ISOC-SE:s förslag gällande domännamshantering i Sverige

Avsikten är att domännamnsfrågor skall hanteras av branschen och så långt som möjligt genom självreglering. Den organisation som har ansvaret för hanteringen redovisar öppet sin verksamhet, volym, kvalitet och tillgänglighet för användarna, allmänheten och myndigheter.

I hanteringen av domännamn ingår fyra olika funktioner - tillsyn, regler, operation och prövning. Varje funktion har sitt tydliga ansvar i hanteringen och dessa beskrivs nedan.

Se även figur 14-1.

- Tillsyn - en stiftelse som har ansvaret för toppdomänen .se. Stiftelsen är den funktion som därigenom har huvudansvaret för att domännamshanteringen fungerar i Sverige. Med ansvaret följer att genom avtal/outsourcing organisera den operativa hanteringen samt att verka för att regler för hur domännamn skall tilldelas kontinuerligt vidareutvecklas, så

att nationella såväl som användarnas intressen tas tillvara.

- Regler - en expertgrupp, gruppen för domännamnsregler i Sverige (DRS), som ansvarar för vidareutveckling och underhåll av regler för domännamnstilldelning. Gruppen är sammansatt av experter med kunskap om juridik, namn- och adresstilldelning och Internet.
- Operation - ett aktiebolag, som på uppdrag av stiftelsen har det ekonomiska, juridiska och operativa ansvaret för hanteringen av tilldelningar. Aktiebolaget skall vid tilldelning av domännamn följa de regler som utarbetats av DRS. Aktiebolaget upphandlar en registerhållare, som utför många av de operationella uppgifter som erfordras för att verksamheten skall fungera.
- Prövning - prövningsinstanser, som tar ställning till och avgör klagomål vid om- och överprövning både vad gäller tillämpning av regler och tilldelning av domännamn.

De funktioner som beskrivs ovan har också relationer till kunder m.fl. Nedan följer en utförligare beskrivning av hur relationerna mellan de ovan beskrivna funktionerna samt från dessa mot andra berörda fungerar.

Tillsyn

Stiftelsen för Internetinfrastruktur (II-Stiftelsen)

II-Stiftelsen har det yttersta ansvaret för domänen .se. Med det ansvaret följer ett tillsynsansvar för hur .se används och att själva hanteringen fungerar tillfredsställande. Den har således allt ansvar vad gäller domännamshanteringen. II-Stiftelsen är stiftad av ISOC-SE. I urkunden står att "stiftelsen skall särskilt främja utvecklingen av hanteringen av domännamn under toppdomänen .se och andra nationella domäner avseende Sverige".

Branschen har tagit på sig ansvaret för självreglering av denna fråga och ser det som av yttersta vikt att rättigheten till .se-domänen skyddas från enskilda ekonomiska och kommersiella intressen eller annat som innebär att .se-domänen skulle kunna användas på ett sätt som inte gagnar de nationella intressena.

Medel för att starta verksamheten kommer från marknaden och från Internetoperatörerna. Styrelsen kommer att vara sammansatt av representanter för marknaden och kommer att bestå av tre representanter valda av ISOC-SE, varav en skall vara ordförande i styrelsen, 1 representant för SNUS samt en representant för Swedish Operators Forum, SOF.

För att täcka de utgifter som finns för att sköta registrering och tilldelning av domännamn kommer kunderna att få betala dels en engångsavgift vid registrering, dels en årlig summa för underhåll. Om något överskott uppstår kommer det att användas till de infrastrukturella investeringar som erfordras för att domännamnsbehandlingen skall fungera på ett tillfredsställande sätt och uppfylla de krav (exempelvis portabilitet) som ställs på adresseringsstrukturen.

II-Stiftelsen kommer att licensiera ut hanteringen av domännamn till Aktiebolaget NIC-SE. (II-Stiftelsen och NIC-SE beskrivs i bilaga 8.)

Regler

Domännamnsregler i Sverige (DRS)

Utveckling och underhåll av regler tas självständigt fram av DRS på uppdrag av II-Stiftelsen. DRS fungerar dessutom som en remissinstans samt skall vara berett att avge yttranden såväl i omprövnings- som överprövningsärenden. Ledamöterna i DRS utses av en valberedning som utses av II-Stiftelsen. I DRS skall finnas kompetens från områdena juridik, Internet och namn- och adresshantering. Kompetensprofilen i DRS kan förändras efter behov.

DRS skall också verka för att vid behov informera en vidare krets om utvecklingen. Under arbetet bör också en dialog föras med ett intresseforum som har en bred representation av Ombudskandidater, journalister, föreningar, operatörer, jurister, patentbyråer, offentlig förvaltning, studerande m.fl. Detta intresseforum är att jämföra med det hittillsvarande ITS/AG12. Syftet är att informera och göra regler kända samt att ta emot och behandla intryck om användning och synpunkter på regelverket och tilldelningsprinciper.

Operation

Kund

Kund är den som ansöker om ett domännamn. Kunden ansöker via ett Ombud (se nedan). Kunden är skyldig att uppdatera sina uppgifter (namn på kontaktperson, fysisk adress mm) om de ändras.

Ombud

Ombudet agerar å Aktiebolaget NIC-SE:s vägnar gentemot Kund. Ett Ombud tar emot såväl nyregistreringar som uppdateringar från Kund och vidarebefordrar denna information till Registerhållaren. En traditionell operatör kan vara Ombud men även

andra kan bli Ombud. Ett Ombud måste uppfylla vissa villkor, vilka har specificerats av NIC-SE.

Ombuden är licensierade av NIC-SE och ett mellan NIC-SE och Ombud avtal reglerar vilken service som Ombuden skall ge Kunden. I avtalen regleras också vilka regler som Ombuden skall följa när det gäller domännamnstilldelning. Det är viktigt att alla Ombud följer samma avtal.

Ombud som inte uppfyller kraven i avtalet med Aktiebolaget får en varning. Om ingen förbättring kommer till upphör avtalet med Ombudet, som därmed inte längre har mandat att skicka in uppdateringar och nyregistreringar till Registerhållaren.

Aktiebolaget NIC-SE

Aktiebolaget NIC-SE är ett helägt bolag till II-Stiftelsen. NIC-SE:s ansvarsområde är att se till att olika register är aktuella, att avgifter betalas samt att registerföringen sker med hög service-nivå och till rimlig kostnad. Register som är aktuella är kundregister, domännamnsregister, DNS m.fl. De tjänster som behövs för att dessa uppgifter skall kunna fullgöras kommer att upphandlas enligt god affärssed.

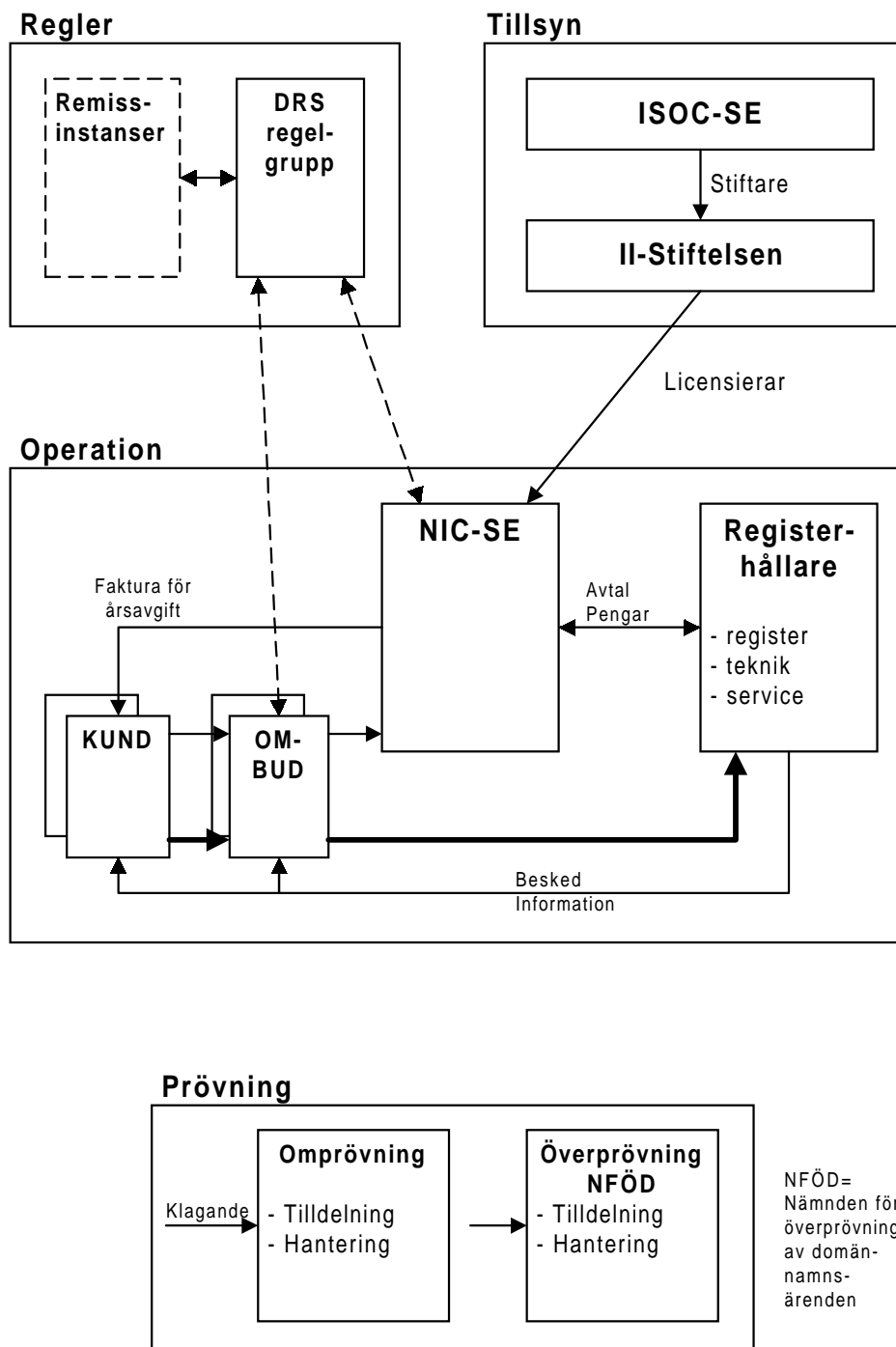
II-Stiftelsens styrelse utser styrelsen i NIC-SE. Det skall finnas en verkställande direktör på deltid samt ett mindre kansli.

II-Stiftelsen i egenskap av ägare prioriterar hur eventuellt ekonomiskt överskott i NIC-SE:s verksamhet skall användas.

Registerhållare

Registerhållaren sköter på uppdrag av aktiebolaget det praktiska arbetet med registrering av domännamn i Sverige och håller register över domäner m.m. uppdaterade. Licensierade Ombud har rätt att hantera registrering av domännamn och gör det genom att skicka in ifyllda blanketter till Registerhållaren. Kund kan inte registrera domännamn direkt hos Registerhållaren.

Registerhållaren och NIC-SE tecknar ett avtal som specificerar pris samt service och kvalitet för bemanning och utrustning för att klara den volym ansökningar och förfrågningar som uppkommer. NIC-SE avser att teckna separat avtal avseende omprövning med Registerhållaren. Omprövningsbeslut skall vara motiverade. Omprövningsbesluten skall månatligen delges DRS och NIC-SE:s kansli.



Figur 14-1

Prövning

Prövning av hantering och tilldelningsfrågor kan ske i två nivåer, omprövning och överprövning. Överprövningen sker genom s.k. skiljedomsförfarande och avgör slutligt målet. Reglernas utformning är inte möjliga att pröva. Man kan dock sända synpunkter och idéer till förändringar av reglerna till DRS som ger svar efter behandling av ärendet.

Omprövning

Omprövning av tilldelningsfrågor riktas till NIC-SE, som sänder det vidare till Registerhållaren. Registerhållaren avgör frågan och sänder svar, vid avslag med en motivering, till NIC-SE som informerar Kunden. Omprövning av hanteringsfrågor riktas till NIC-SE som avgör frågan och sänder svar till Kunden, med kopia till Ombudet.

Överprövning

Kund som inte är nöjd med omprövningsbeslutet skall ha rätt att begära överprövning därav. Överprövning skall ske genom anmälan till en grupp kallad Nämnden för Överprövning av Domännamnsärenden (NFÖD). Nämnden skall vara helt fristående från II-Stiftelsen och Aktiebolaget och kommer att ha ett eget kansli. Överprövning kan ske alternativt genom ett förenklat skiljeförfarande varvid nämnden består av tre personer. Dessa skall besitta kompetens inom immaterialrätt, Internet och domännamns-hantering. Förfarandet är kostsamt och förlorande part får stå för båda parter kostnader. Andra alternativet är ett on-line förfarande där överprövningen sker av en från II-Stiftelsen och NIC-SE oberoende person, troligtvis en jurist.

14.4 Alternativa organisationsformer för domännamns-hantering

Som ansvarig för .se-domänen har en stiftelse bildats av ISOC-SE vilken i sin tur äger ett aktiebolag som driver den operativa verksamheten. Man kan tänka sig alternativa organisationsformer för att driva samma funktionella verksamhet.

Det finns fyra organisationsformer som kan vara aktuella: Myndighet, stiftelse, aktiebolag, ideell förening.

Myndighet

I direktiven för uppdraget anges att staten endast i undantagsfall skall ingripa med reglering. Därmed är en organisation med en myndighet som är ansvarig för .se-domänen sannolikt inte aktuell.

Stiftelse

Stiftelse är en organisationsform som är självägande och vars syfte framgår av stiftelseförordnandet. Stiftelsen förvaltar en självständig förmögenhet för ett bestämt ändamål. En föreskrift i ett stiftelseförordnande kan endast ändras, upphävas eller i särskilt fall åsidosättas om de på grund av ändrade förhållanden inte längre kan följas eller har blivit uppenbart onyttiga eller uppen-

bart stridande mot stiftelsens avsikter eller om det finns andra särskilda skäl.

Aktiebolag

Även för ett aktiebolag finns en urkund som reglerar exempelvis bolagsordningen och verksamheten. Bolagsordningen för ett aktiebolag kan ändras av bolagsstämman, vilket innebär att en högre grad av flexibilitet nås relativt vad som gäller för en stiftelse. Detta kan vara en fördel då man vill förändra verksamheten, men en nackdel om man vill att verksamheten skall vara svår att förändra.

Ideell förening

En ideell förening samlar personer som har ett gemensamt intresse. Den har stadgar, styrelse och medlemmar. Stadgarna styr hur föreningen skall fungera. Årsmötet granskar vad föreningen gjort och väljer styrelse, inriktning m.m. Vad som sagts om aktiebolag om förändring av verksamheten, gäller även för ändringar av stadgarna för en ideell förening.

14.5 Statskontorets syn på namn- och adresshanteringen

Organisation för hantering av domänen .se

Statskontorets uppfattning är att man bör göra en organisation enkel och robust. Robust så att man inte får följd effekter, dvs. om en del faller, faller alltsammans. Vidare bör man i möjligaste mån se framåt i tiden. Man bör ha ett tidsperspektiv på minst fem år. Vad gäller den organisation som driftsätts från ISOC-SE:s sida innehåller den de funktionella komponenter som måste finnas för att verksamheten skall fungera.

Ett godkännande från IANA krävs för att ansvaret för .se skall kunna flyttas. Om utvecklingen påkallar att ansvaret för .se i en framtid måste flyttas från II-Stiftelsen till någon annan organisation så måste även IANA godkänna att ansvaret flyttas. Vid eventuell oenighet inom landet kan det då bli problem med att övertyga IANA men om enighet råder torde det gå relativt enkelt.

Sammanfattningsvis kan sägas att Statskontoret anser att den organisation som ISOC-SE byggt upp kommer att fungera bra.

ISOC-SE:s ambition är att samarbeta med relevanta myndigheter för att skapa en domännamshantering som fungerar bra för Sverige. Statskontoret föreslår att ISOC-SE bildar en samrådsgrupp med deltagare från lämpliga myndigheter. ISOC-SE bedöms ha skapat en hantering som undanröjer de problem som hittills

funnits samtidigt som marknaden själv tar hand om verksamheten. Detta måste sägas ligga i linje med det direktiv som utredningen haft att endast i undantagsfall ingripa med reglering.

Regelverket för domännamn

Arbetet med att utarbeta ett regelverk för hanteringen av domännamn sker fortlöpande. Hittills har det skett inom AG12 men med den nya organisation som börjar aktivt arbeta under hösten 1997 kommer DRS att få en tung roll. Med de ambitioner som finns från ISOC-SE:s sida att samarbeta med relevanta parter på marknaden (myndigheter såväl som privata organisationer) anser Statskontoret att det regelverk som föreligger är till fyllest och att det finns goda förutsättningar att det kan vidareutvecklas.

IP-adresser och AS-nummer

Tilldelning av IP-adresser och AS-nummer sker på en internationell nivå och hanteras inte centralt av någon organisation inom Sverige. Detta skapar inga problem inom landet. Dessa frågor behöver därför inte behandlas av denna utredning.

15 Finansiering av gemensamma resurser

Enligt utredningsdirektiven skall Statskontoret ge förslag till hur finansiering av gemensamma resurser skall göras.

Statskontoret föreslår att de gemensamma resurserna/funktionerna finansieras enligt nedanstående tabell.

Resurs/funktion	Finansieringsform		
	A	B	C
Nationella knutpunkter	X		
DNS för .se och roten	X		
Reservsystem för DNS för .se och roten	X		
Nationell tid (tidserver) Anm: Finansieringen avseende drift av klockorna anges även under A	X		
Reservsystem för nationell tid (tidserver)	X		
Vägvalsregister	X		
Domännamnshantering		X	
Whois-server		X	
Indexserver			X

A. Nationella knutpunkter, drift av DNS för .se och roten, nationell tidsgivning och vägvalsregister

Dessa funktioner skall finansieras av de huvudoperatörer (se avsnitt 11.1.1) som är anslutna till de nationella knutpunkterna. Finansieringen skall täcka de kostnader som finns för anskaffning, drift av funktionerna liksom för den vidareutveckling och de förstärkningar samt de nyinvesteringar som krävs. Finansieringen skall inte ge någon vinst.

Dessa funktioner skall drivas av knutpunktsleverantören som anskaffar utrustning, hyr lokaler, hyr förbindelser, lägger ut driftuppdrag etc.

Respektive operatör föreslås betala en fast avgift som endast är beroende av hur operatören ansluts. I nuläget (september 1997) då den enda nationella knutpunkten finns i Stockholm och består av två FDDI-växlar placerade i olika lokaler samt ev SDH-förbindelser mellan par av operatör finns det två avgifter. Alla operatörer betalar för dubbla FDDI-anslutningar, dvs. en FDDI-ring till vardera växeln. Den operatör som behöver dubblera sin FDDI-anslutning betalar dubbel avgift. De operatörer som bilateralt behöver SDH-förbindelser betalar en extra avgift som täcker kostnaderna för SDH-förbindelserna och dess utrustning.

När ytterligare knutpunkter etableras i landet finansieras dessa enligt samma princip som för knutpunkten i Stockholm.

Anskaffningskostnaden för klockor och övrig utrustning uppskattas till ca 600 000:- per knutpunkt.

Finansiering av driftskostnader för klockorna

Driften av klockorna placerade vid respektive nationell knutpunkt föreslås bli finansierade via statliga medel. För Sveriges Provnings- och Forskningsinstitut (SP) kostnader för personal, drift och utveckling av samtliga klockor m.m. föreslås att SP erhåller, via statliga medel, 1 200 000:- per år. Detta föreslås bli finansierat via anslag från "Anslaget B6 Bidrag till standardisering, provnings- och mätteknisk FoU m.m." inom utgiftsområde 24 Näringsliv.

B. Domännamnshantering och whois-server

Hur registrering av domännamn och därmed sammanhängande funktioner föreslås utföras finns närmare beskrivet i avsnitt 14.3.4. Finansieringen föreslås ske genom en engångsavgift och en årlig avgift per registrerad domän. Avgiften betalas av den som har ansökt om respektive domännamn.

Eventuellt överskott i verksamheten med domännamnsregistrering föreslås användas till att finansiera utveckling av gemensamma Internet-funktioner i Sverige.

C. Indexserver

Drift och vidareutveckling av indexserverar för kataloger med bl.a. e-postadresser föreslås finansieras av de organisationer som tillhandahåller kataloginformation. Avgiften föreslås vara beroende av antalet e-postadresser som respektive organisation tillhandahåller.

16 Hot mot nätet och nätets tillämpningar

Statskontoret anser att det är av största vikt att utbyggnaden av Internet i Sverige sker på ett sådant sätt att nätets sårbarhet minimeras. Internet måste jämföras med andra samhällsviktiga funktioner och fungera inom landet vid svåra påfrestningar på samhället både i fred och i krig. Den svenska delen av Internet måste därför också kunna fungera utan att vara beroende av funktioner placerade utanför Sverige.

I takt med en allt mer spridd användning av Internet har säkerhetsfrågorna aktualiserats. För att kunna bredda och utveckla användningen av Internet i Sverige är det viktigt att öka medvetenheten om den sårbarhet som kan finnas inbyggd i nätet och nätets tillämpningar och om vilka åtgärder som ger ett ökat skydd.

Den traditionella hotbilden har förändrats p.g.a. Internet. Nätet har skapat nya förutsättningar för att sprida kunskap om brister i maskin- och programvara i såväl datorsystem som i olika nätfunktioner. På nätet förmedlas idag, till en allt större krets av intresserade, kunskapen om hur man utnyttjar teknikens brister för att genomföra t.ex. intrång via bl.a. Internet. I takt med att det ekonomiska utfallet av brott på nätet kan tänkas öka så ökar sannolikt också intresset för området. Hotbilden skiftar ständigt då ny teknik och nya programvaror introduceras dagligen.

De flesta exempel på incidenter på Internet idag beror emellertid på dålig säkerhet i användarnas ändsystem, och den situationen kommer inte att förändras av att bra säkerhetsmekanismer införs på nätnivån.

Ett resultat av den snabba teknikutvecklingen inom området och en avreglerad marknad är att operatörerna på den svenska marknaden hamnat i en situation med hård konkurrens. Låga kundkostnader och ett stort tjänsteutbud prioriteras för att snabbt vinna marknadsandelar. Detta sker på bekostnad av bl.a. säkerhetsfrågorna. Kunderna ställer sällan krav på säkerhet, och uppföljning och kontroll av operatörernas åtaganden sker också sällan.

Den avreglerade marknaden har många aktörer, och det medför att det inte längre finns någon som har överblick över helheten.

För att förbättra den situationen är det viktigt att de politiskt an-

svariga ger signaler om att säkerhetsfrågor är viktiga. Det måste bli självklart att näringslivets och offentlig sektors beslutsfattare får insikt om hot och risker och tar ansvar för dessa frågor.

16.1 Uppdrag och avgränsningar

I direktiven anges att utredningen skall inventera hotbilden mot nätet och nätets tillämpningar. Arbetet har bedrivits i en mindre arbetsgrupp inom utredningen. Inventeringen omfattar en definition av begreppet hotbild, samt en beskrivning av olika typer av hot med exempel. Gruppens arbete omfattar inte kundernas ändsystem, outsourcing av funktioner från ändsystem, såsom webbhotell etc.

En viktig utgångspunkt har varit SOU 1995:19, Ett säkrare samhälle, huvudbetänkande från Hot- och riskutredningen.

I bilaga 16 har utredningsgruppen definierat begreppet svåra påfrestningar, för att med den definitionen som utgångspunkt kunna definiera hotbilden för svåra påfrestningar så att extraordinära situationer i fred kan urskiljas från normala driftstörningar. I bilagan beskrivs också tänkbara aktörer bakom fredstida aktioner och deras motiv samt en bedömning av dessa olika aktörer.

Observera att det inte existerar någon exakt motsvarighet mellan de hot som beskrivs i detta avsnitt och den säkerhetsarkitektur som beskrivs i nästa avsnitt. Avsikten med denna beskrivning av hotbilden är endast att ge en antydning om komplexiteten i de överväganden som måste göras för att minimera Internets i Sverige sårbarhet.

16.2 Fysiska hot mot infrastrukturen

För att kunna svara mot dagens kommunikationsbehov är tillgången till olika typer av kommunikationsnät av vital betydelse. Den ökade tillgången till nät bidrar till ökad komplexitet och större risker. Avbrott och andra störningar kan uppstå genom brister i elförsörjning, brand, vatten, intrång, explosioner m.m. Även naturliga företeelser som åska, spänningsvariationer i elnäten m.m., kan orsaka avbrott och gör det dessutom förhållandevis ofta.

När det gäller att fysiskt skydda infrastrukturens alla delar, med kabelförbindelser, antenner och centraler, måste vi ändå utgå ifrån att det är en omöjlig uppgift, främst på grund nätets omfatt-

ning och utbredning och att det därmed existerar ett stort antal svaga punkter. Men dessa risker kan minimeras genom noggrann analys och åtgärder vid utbyggnad och utveckling.

16.2.1 Svagheter i transmissionssystem och utrustning

Statskontoret föreslår att nationella knutpunkter för samtrafik mellan operatörers nät, nätdatabaser m.m. som är av vital betydelse placeras skyddade mot fysiska attacker i bergskyddade anläggningar. Möjligheter till utspridning och flervägsanslutningar måste utnyttjas för att öka säkerheten. Det kan finnas skäl att överväga huruvida vissa vitala funktioner inom Internet i Sverige skall vara föremål för SUA-upphandling (Säkerhetsskyddad upphandling med avtal). Vidare bör övervägas om Internetoperatörer skall betraktas som K-företag (krigsviktiga företag).

Statskontoret föreslår att frågor om SUA och klassificering av Internetoperatörer som krigsviktiga företag hanteras inom ramen för den utvärdering av genomförandet av utredningens förslag som Statskontoret föreslår skall äga rum hösten 1998 alternativt inom ramen för det uppdrag om strategi för IT-säkerhet som Kommunikationsdepartementet lagt på Statskontoret i september 1997.

Nätet består av flera olika delar som var för sig kan slås ut. Om nätet är rätt uppbyggt kan man avsevärt minska risken för en total utslagning. Detta innebär krav på samverkan mellan aktörerna (t.ex. operatörer och transmissionsleverantörer) och användning av parallella transmissionssystem samt att viss kritisk utrustning ges en säker placering, rätt konfigurering och dubblering.

16.2.2 Avbrott i elförsörjning

Kritiska noder i systemet bör ha tillgång till reservkraft under en längre tid. Statskontoret anser att vitala delar av nätet i kris- och krigssituationer måste ha utrustning för separat elmatning och tillgång till reservkraft för långa elavbrott, upp till två veckor. Det måste vara en strävan att varje Internetoperatör själv vidtar de åtgärder som fordras för att så långt möjligt upprätthålla sin elförsörjning.

I bilaga 16 beskrivs några exempel på incidenter vad gäller avbrott i elförsörjning.

16.2.3 Brand och översvämning

Skador orsakade av brand och vatten utgör hot som är bland det värsta som kan inträffa. Förödelsen kan bli total och verksamheten lamslås under längre tid. Erfarenheter visar att lämpligt brandskydd ofta saknas. Operatörerna måste själva ta ansvar för att ha ett godtagbart skydd mot dessa hot för att inte brand- eller vattenskadorna i operatörernas utrustning skall utgöra något större hot utan kan anses vara begränsat.

16.2.4 Obehörigt tillträde

Att någon obehörig fysiskt skulle kunna bereda sig tillträde till vitala delar av operatörernas utrustning får betraktas som ett mindre sannolikt hot. Statskontoret förutsätter att sådan utrustning finns placerad i lokaler som har ett genomtänkt tillträdeskydd.

Även behörig personal som t.ex. användare, driftpersonal, systemutvecklare, underhållspersonal och övervakningspersonal utgör en risk. Personkvalitet i sådana befattningar kan åstadkommas genom placering i säkerhetsklass och genomförd registerkontroll i kombination med god personkännedom.

16.2.5 Avbrott i transmissionsnätet

Det är ett mycket vanligt problem att t.ex. kablar skadas vid grävning och annan åverkan. Om en sådan skada drabbar regionala eller rikstäckande delar av nätet kan omkopplingar i idealfallet ske så snabbt att de flesta användare inte blir berörda. Avbrott i de lokala förbindelserna kan få större konsekvenser.

Det finns stora möjligheter att avsiktligt skada delar av transmissionsnätet som t.ex. fiber, kopparkabel och radio-/radiolänk-anläggningar p.g.a. deras placering. Förutsättningarna att skydda sådana anläggningar mot fysiska angrepp är små.

Även om slutkunden ställer krav på operatören på alternativa vägar i transmissionen så har kunden ingen möjlighet att säkerställa att det verkligen existerar sådan redundans. Inte ens operatörer kan till hundra procent försäkra sig om att deras trafik har tillgång till alternativa vägar, t.ex. om de köper transmission av en annan nätleverantör. Detta är en fråga mellan kund och leverantör, dvs en Internetoperatör skall kräva att transmissionsleverantören (Telia, Banverket, Svenska Kraftnät, Teracom) redovisar hur en förbindelse går.

Möjligheterna att erhålla faktisk redundans i den egna trafiken ökar med användning av olika transmissionsnät parallellt. (Se bilaga 21 om olika transmissionsnät i Sverige). Det är inte säkert att det blir högre tillgänglighet p.g.a. att en abonnent anlitar olika operatörer. Mindre operatörer hyr ofta förbindelser av de större operatörerna så det kan i praktiken vara samma kabel.

16.3 Kontinuitetsplanering

Statskontorets slutsats är att en dokumenterad och verifierad kontinuitetsplan bör vara ett grundläggande krav för samtliga Internetoperatörer. Planerna bör testas minst en gång per år och resultatet av testerna dokumenteras. Kontroll över detta skall utövas av en myndighet.

Vilken denna myndighet är, är en fråga som kan belysas i det uppdrag som Kommunikationsdepartementet lagt på Statskontoret i september 1997, att ta fram en sammanhållen strategi för samhällets datasäkerhet.

I bilaga 16 ges en definition av vad utredningsgruppen menar med kontinuitetsplanering.

Kraven på att kontinuerligt kunna bedriva verksamheten är grundläggande för samtliga operatörer. Behovet av att analysera hot och risker får i nuläget bedömas vara lågt prioriterat. Avsaknad av plan är särskilt vanligt i mindre och medelstora organisationer med stor dynamik i verksamheten och hög tillväxttakt. Innebörden av en allvarlig störning i verksamheten är sällan definierad och dokumenterad. Planer och andra förberedelser saknas ofta. Detta, i kombination med begränsat fysiskt skydd för driftställen, beroenden av nyckelpersonal och ett inbördes beroende mellan operatörer kan medföra oönskad förlängning av avbrott, med mycket allvarliga konsekvenser.

16.4 Logiska hot mot infrastrukturen

Före den stora Internetexpansionen återfanns de största IT-säkerhetsproblemen i att användare hade dåliga lösenord och delade användarkonton med varandra. Många lever fortfarande i övertygelsen om att det förhåller sig så. Det fanns också en rad brister i de vanligaste programvarorna, vilka kunde utnyttjas för missbruk och intrång.

Många av dagens incidenter har dock mer än tidigare drabbat Internets infrastruktur. Hoten mot Internet avser i första hand tillgänglighet.

Nedanstående tabell ger en överblick över olika typer av attacker och vad de medför:

Typ av attack	Resultat
Nätavlyssning	Avlyssning av lösenord och känslig information
IP-spoofing	Förfalskning av avsändaradress
Övertagande av logisk förbindelse	Används för att ta över befintliga sessioner, t.ex. telnet
Data spoofing	Ändrar information i befintlig kommunikation mellan två datorer.
Trafikanalys	Analysering av trafik för att se vilka som kommunicerar, trafikmönster m.m.

Alla Internetanslutna organisationer utstår hela tiden ett grundhot på grund av att flera verktyg existerar som möjliggör attacker. En del verktyg medger mer urskiljningslösa attacker medan andra verktyg medger en koncentration mot vissa IP-adressområden eller grupper av domännamn (t.ex. veckans domännamnsregistreringar).

Vissa attackerande personer har ett bestämt mål med sina gärningar, t.ex. politisk eller annan övertygelse. Idag så bryr sig merparten personer som håller på med intrång på Internet inte om organisationen i sig utan är mer intresserade av själva intrånget, eller att intrånget bara är en del i en annan aktivitet, t.ex. att sprida piratkopierad programvara.

16.4.1 Exempel på logiska hot

Det finns inte utrymme för att beskriva alla kända typer av attacker mot Internetprotokollen. Det finns och kommer alltid att finnas oförutsägbara hot. Det är därmed viktigare än någonsin att vedertagen säkerhetspraxis tillämpas konsekvent.

De logiska hoten omfattar bl.a.:

- Felaktiga riskbedömningar
- Oupptäckta beroenden
- Felaktiga antaganden
- Mänskliga fel och brist på säkerhetstänkande
- Resursblockering/Mätta nätet/Denial-Of-Service/Fördröjning av data
- Trafikanalys
- Felaktiga implementationer av IP
- Attacker med uppsåt

- Programmerade/programmerbara attacker
- Någon inom Internetvärlden som inte följer gängse konventioner
- Attacker mot nyckelpersoner

Några av dessa behandlas mer utförligt i bilaga 16.

16.4.2 Säkra och provade produkter och system

Det är att ta en stor risk att anta att de produkter som finns tillgängliga på marknaden är säkra, och det ställs allt starkare krav från användare på tillgång till produkter, system och tjänster för IT-säkerhet som är provade och certifierade.

För att ett svenskt system för provning och certifiering av produkter och system för IT-säkerhet skall kunna inrättas krävs att det finns ett svenskt grundläggande regelsystem för olika former av teknisk provning och kontroll. Detta regleras i lagen om teknisk kontroll. Genomförandet av säkerhetsutvärderingen bör lämnas åt marknaden. För detta bör finnas minst ett organ inom landet vars kunskaper, miljö, arbetssätt och verktyg kontrolleras av en myndighet.

En producent eller konsument av produkter och system för IT-säkerhet får själva bekosta utvärderingen. Resultaten granskas i efterhand och ges en formell stämpel, ett certifikat, som utfärdas av en myndighet eller annan utpekad instans.

Ett svenskt system för utvärdering och certifiering av system och produkter för IT-säkerhet skall vara marknadsorienterat och överensstämja med principerna om öppna system. Alla organ som bedöms inneha kompetens för detta skall ha möjlighet att starta och bedriva provnings-, utvärderings- eller certifieringsverksamhet. Ackreditering är det sätt på vilket deras kompetens bekräftas. Ackreditering görs för svenskt vidkommande av SWEDAC, vilket också innebär att de som ackrediterats blir godkända på europeisk bas då SWEDAC i sitt arbete med ackreditering använder sig av de standarder och arbetssätt som man enats om inom Europa.

Aktörerna i ett svenskt system skall delta i det arbete som bedrivs i samförstånd mellan provnings- och utvärderingslaboratorier och/eller certifieringsenheter i Europa, för att säkerställa ömsesidigt erkännande av varandras provningsresultat och certifikat. Produktcertifiering är ett komplement till systemcertifiering. SWEDAC har tagit initiativ till att skapa möjligheter för certifiering på den svenska marknaden.

16.5 Beroendeförhållanden

De tjänster som operatörerna levererar till slutkund är ofta i något led beroende av andra; operatörer, transmissionsleverantör etc. En slutkund är därför också beroende av säkerhetsåtgärder inom hela kedjan. I de avtal som tecknas mellan operatör och slutkund redovisas sällan dessa förhållanden och kunden blir därför inte medveten om vilka risker som finns. En förutsättning för att kunna samordna flera aktörer är att ansvarsgränserna mellan inblandade aktörer är klarlagda.

16.5.1 Utrustning och komponenter

Logisk datakommunikation bygger på att underliggande fysiska komponenter måste fungera. I tidigare hotutredningar talas det mycket om beroenden av elförsörjning och telekommunikation. För att datakommunikation skall fungera måste **både** den elförsörjning och telekommunikation som används för transmissionsdelarna **och** publik och privat datakommunikationsutrustning fungera.

Datakommunikation beror på flera andra komponenter:

- Underliggande transmissionsutrustning
- Felfri programvara
- Felfri maskinvara
- Rätt konfiguration och parametersättning av kommunikationssystem
- Organisatoriska problem

Att säkerställa alla dessa, t.ex. undvika fel i maskin- och programvara är omöjligt, däremot kan man förbereda och planera inför dessa typer av händelser.

Ett annat beroende som kommer upp är vid sammankoppling av operatörer. För att en operatör skall kunna ge sina kunder några garantier om servicekvalitet så måste operatören också kunna förvissa sig om att de som operatören är beroende av uppfyller de krav som ställs. En utbyggnad av modempoolen hos en operatör genererar behov av motsvarande utbyggnad på sammankopplingspunkterna hos andra operatörer. För att undvika prestanda- och säkerhetsproblem måste operatörerna inte bara ställa krav på varandra utan också reglera sådana frågor i avtal.

ÖCB har ansvaret för att säkerställa tillgången till elektronikkomponenter för kris och krig. Statskontoret anser att

det därutöver finns behov att analysera leverantörsberoendet för vissa vitala komponenter.

Merparten av dagens Internet och därtill anslutna nät består av utrustning tillverkad av ett fåtal företag främst baserade i USA. Handelshinder, distributionsproblem eller andra typer av restriktioner på export, import eller användande av denna typ av utrustning skulle direkt få konsekvenser på nätinfrastrukturen. Kostnaden för t.ex. en router är hög och lagerhållningen i Sverige begränsad.

16.5.2 Nyckelpersoner

Flera av Internetoperatörerna i Sverige har utländska huvudägare, där kunskapen om svenska krav under kris och krig är begränsade. Statskontoret rekommenderar att varje operatör på den svenska marknaden har en etablerad organisation i Sverige.

Beroendet av nyckelpersoner för viktiga funktioner i verksamheten ökar med den snabba teknikutvecklingen och den hårdnande konkurrensen. Få av dessa nyckelpersoner är krigsplacerade i sina befattningar och få operatörer har begärt uppskov för aktuell personal

Konsekvenserna av detta kan bli mycket allvarliga eftersom många operatörer drabbas samtidigt med påföljd att den totala möjligheten att driva Internet i Sverige under kris och krig påverkas.

16.6 Organisations- och ansvarsfrågor

16.6.1 Incidenthantering

Statskontoret föreslår att frågan om incidenthantering belyses av en utredning med uppdrag att tillsammans med t.ex. operatörer och användarorganisationer inom offentlig förvaltning och näringsliv utreda och föreslå uppgifter för en organisation för incidenthantering i Sverige och hur den funktionen praktiskt skall utformas.

I USA har sedan länge funnits en organisation kallad CERT (Computer Emergency Response Team) som sammanställer och distribuerar larm och varningar relaterade till drift av nätanslutna datorer. Incidenthantering är en funktion som beroende av ambitionsnivå kan göra allt från att åtgärda och koordinera åt-

gärder mot incidenter och andra hot till att endast ta emot rapporter om incidenter, sammanställa statistikinformation och framskriva trender baserat på dessa rapporter.

Hos varje operatör krävs det en organisation som kan upptäcka och ta hand om attacker riktade mot infrastrukturen, dvs själva nätet. En nära kontakt mellan operatörerna är en viktig förutsättning för att samordnade och effektiva motåtgärder snabbt skall kunna komma till stånd. Initiativ till sådan samverkan mellan operatörerna har också tagits under hösten 1997.

Det förekommer också ofta att intrång sker från personer som befinner sig i ett annat land och hoppar i flera steg. För att kunna hantera och åtgärda den typen av incidenter och få till stånd rättslig prövning så krävs det också samarbete mellan incidenthanteringsorganisation, polisväsende, operatörer och rättsväsende på en internationell nivå.

16.6.2 Krishanteringsorganisation

Statskontoret konstaterar att det för närvarande saknas en övergripande organisation för krishantering för Internet på nationell nivå. Statskontoret föreslår att en sådan organisation pekas ut snarast. Den organisationen skall bemyndigas att besluta om direkta åtgärder för att skydda och vidmakthålla Internet i Sverige. Reaktionstiden behöver vara på nivån minuter eller högst timmar.

Beslut om eventuell isolering av den svenska delen av Internet och åtgärder med omfattande ekonomiska konsekvenser bör fattas av regeringen. Rutiner för detta måste enligt Statskontorets uppfattning skapas snarast.

Varje operatör och organisation med samhällsviktiga funktioner måste ha upprättat en plan som beskriver hur verksamheten skall genomföras under kris och krig.

Bemanningen för kris och krig måste vara planerad och säkerställd, och personalen vara krigsplacerad på sina ordinarie arbetsplatser.

Den säkerhet som fordras för att den svenska delen av Internet skall fungera i alla situationer måste vara grundad på den fredstida nivån. Flera åtgärder behöver vidtas inom säkerhetsområdet

för att Internet i Sverige skall uppnå en sådan robusthet att det kan motstå påfrestningar av olika slag. Det finns inte utrymme för att utveckla och införa nya system för informationshantering och kommunikation när störningar uppstår.

Det finns behov av ökad central ledning och samordning vid förberedelser för kris och krig. För att lättare kunna samordna mellan operatörerna måste den "grundfunktionalitet" som krävs i en krissituation definieras. Det är viktigt att operatörer och berörda myndigheter gemensamt formulerar hur verksamheten kan bedrivas i det samlade perspektivet fred-kris-krig.

En effektiv informationsverksamhet är avgörande för om myndigheter och andra vid svåra påfrestningar skall kunna genomföra de åtgärder som är planerade. Det finns behov av att finna en elektronisk motsvarighet till "Viktigt Meddelande". Den som har mandat att gå ut med allmänna varningar, mobiliseringsorder etc. elektroniskt måste kunna förvanskningsskydda och signera den informationen.

Var och en som får informationen måste också kunna verifiera signaturen. Det innebär att information som möjliggör en äkthetskontroll av signaturen måste finnas publicerad och spridd på ett sätt som gör det nära nog omöjligt att förfalska, t.ex. att den publiceras på första sidan i telefonkatalogen, eller något lika vanligt förekommande material. Man måste kunna förutsätta att ingen klarar av att manipulera hela upplagan, medan däremot begränsade delar av upplagan kan förvanskas. Var och en kan ändå till rimlig förvisning verifiera genom att jämföra med någon annan persons version av informationen för äkthetskontroll.

I komplexa system är det särskilt vanligt att drift och underhållsåtgärder får oavsiktliga och oanade konsekvenser. I ett krisläge bör sådana åtgärder begränsas till ett minimum och löpande underhållsarbete eventuellt avbrytas.

Statskontoret anser att en bättre samordning av resurser behövs i en krissituation. Operatörerna bör ha avtal om utnyttjande av varandras nät i en krissituation. Eventuell möjlighet till samutnyttjande av personal och övriga ledningsresurser bör stimuleras. Det är också önskvärt med tillgång till redundanta drifts- och övervakningsplatser.

Beslut om att konstruera beredskapsnät, där t.ex. debiteringsfunktioner tas bort och filtrering tillfogas för att största möjliga kapacitet skall uppnås kräver klara regler för prioriteringen. Statskontoret anser att dessa regler bör formuleras på en politisk

nivå och i samförstånd med operatörerna.

Ansvar för skydd av det egna systemet är ofta underskattat. Detta utgör också ett hot mot andra system, då det första systemet kan vara en sprängbräda mot andra mål (som kan vara huvudmålet för en attack). En kunskapshöjande aktivitet med information om konsekvenser och risker med datanät bör genomföras.

De myndigheter som har ansvar för kunskaps- och informations-spridning inom säkerhetsområdet bör enligt Statskontoret stimuleras till samordning för att kunna intensifiera sådana insatser.

16.7 Samhällets ansvar

Regeringen har i september 1997 gett Statskontoret i uppdrag att ta fram en strategi på IT-säkerhetsområdet, som preciserar statens ansvar och anger hur säkerhetsarbetet kan inordnas i det nationella handlingsprogrammet för IT, samt hur arbetet med IT-säkerhetsfrågorna bör organiseras och fördelas mellan olika statliga instanser. Uppdraget skall avrapporteras senast den 29 maj 1998. Internetutredningens förslag och rekommendationer är ett viktigt underlag i detta arbete.

Ansvar inom regeringskansliet för IT-säkerhetsfrågor bör tydliggöras och det departement som har ansvar för IT-frågor skall också ha ett naturligt ansvar för de frågor som har att göra med säkerhet inom IT-området.

Flera myndigheter inom statsförvaltningen har bl.a. till uppgift att kräva att andra skall vidta åtgärder för att skapa skydd och uppnå säkerhet i verksamhetens informationssystem. Alla bidrar genom att ta ansvar inom sitt område.

Det kan vara en fördel med många aktörer inom säkerhetsområdet. Mångfalden kan leda till att en åtgärd inom ett område ger impulser inom andra. Det finns å andra sidan en uppenbar risk för att en helhetssyn på säkerhet förknippad med informationsförsörjning går förlorad om det inte finns någon med ett utpekat ansvar för att ha överblick, och som kan ta initiativ till åtgärder, rapportera iakttagelser, bl.a. till regeringen.

Framför allt kommuner, landsting och näringsliv är annars hänvisade till impulser från branschorganisationer, ideella föreningar och enskilda företag.

Många olika bransch- och intresseorganisationer engagerar sig för att hitta lösningar på bl.a. säkerhetsproblemen på Internet, t.ex. SNUS, SEIS, Swebizz, EDIS, Dataföreningen Sig Security. Dessa utgörs i huvudsak av ideella föreningar med begränsade resurser och med små möjligheter till resultatspridning och genomförande utanför den egna intressesfären.

Det finns några nyckelbegrepp som är avgörande för utvecklingen:

Distansarbete - vi vill bli rörligare i vår yrkesutövning och vi vill kunna styra var och när vi gör det som ålagts oss.

Internet/intranät, TCP/IP-dominans - den ökade öppenheten, ökade funktionaliteten och de allt mer generella verktygen för med sig ökad sårbarhet.

Avsaknad av säkerhetsfunktioner får inte lägga hinder för en sådan utveckling. Syftet med en IT-säkerhetsstrategi är att åstadkomma och bibehålla en säkerhetsnivå som ger hög kvalitet.

17 Säkerhetsarkitektur för Internet i Sverige

Arbetet med att beskriva säkerhetsarkitekturen har bedrivits i en mindre arbetsgrupp inom utredningen.

I gruppens uppgifter har ingått att göra en inventering av befintliga standarder på säkerhetsområdet och en uppskattning om vilka som används. I nuläget finns det ett flertal parallella, helt olika standarder på området. Det har ännu inte utkristalliserats någon "vinnare". Därför är det viktigt att se till att de olika systemen kan samarbeta och interoperera i en för detta gemensam infrastruktur. Gruppen lämnar också förslag om administration av säkerhetsnycklar.

På nästa sida finns en skiss över den säkerhetsarkitektur gruppens uppdrag omfattar. Det krävs skydd på olika nivåer i arkitekturen.

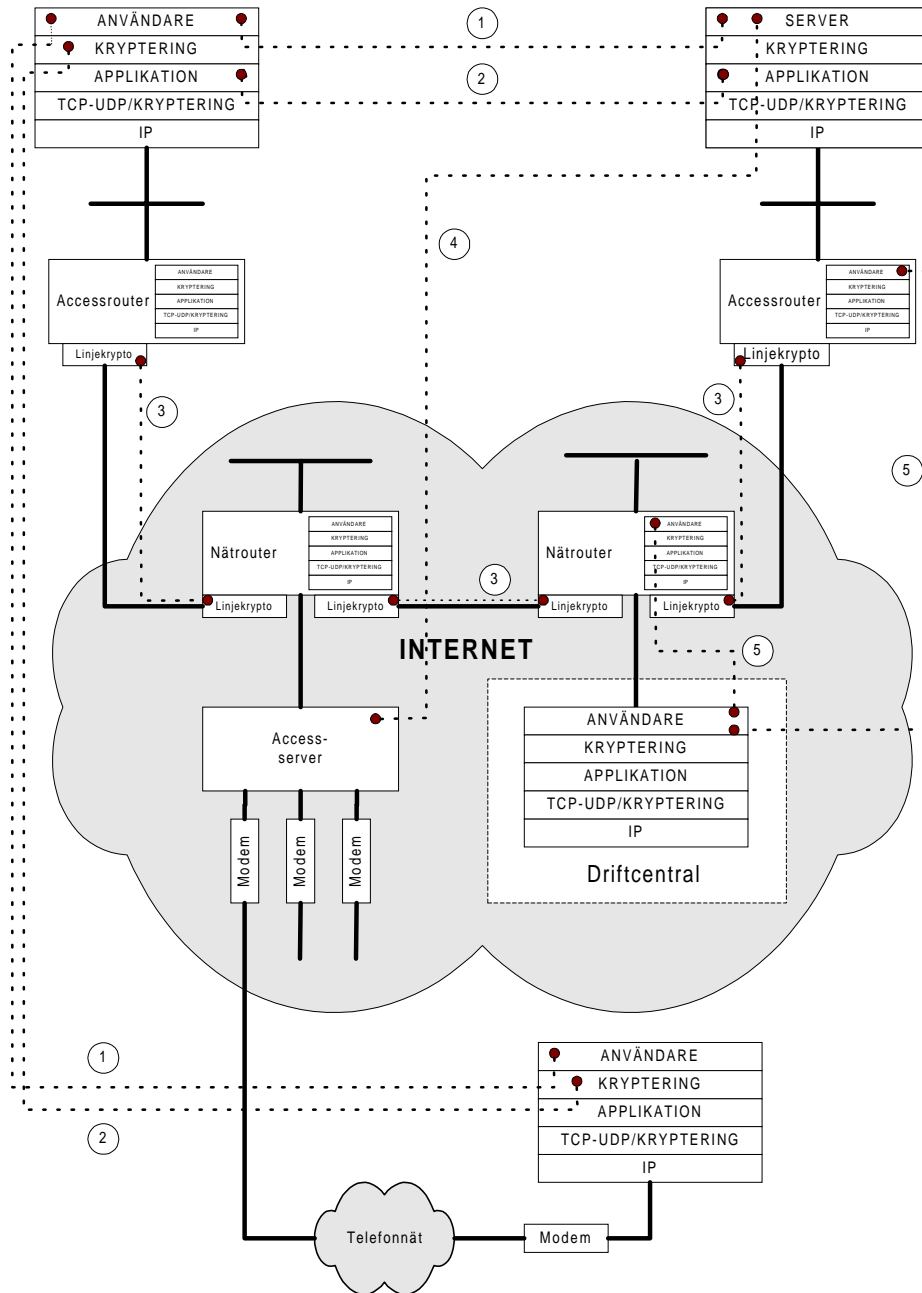
På tillämpningsnivån krävs textskydd, och det är den nivån som oftast diskuteras när frågor om digitala signaturer och kryptering kommer upp. På underliggande nivåer och på stamnätsnivån behövs emellertid också olika typer av säkerhetsfunktioner. Här finns exempelvis behov av att skydda själva nätet och nätets gemensamma funktioner som t.ex. adressinformation (DNS) och vägvalsinformation (routinginformation, routinguppdateringar).

I skissen anges kryptering på fem nivåer (siffrorna har sin motsvarighet på bilden):

1. kryptering av brev/meddelanden respektive signering av brev/meddelanden samt autentisering mellan användare och applikation,
2. skydd av data under transport utan autentisering av användare (förvanskningsskydd),
3. skydd av förbindelse mot angrepp,
4. autentisering (säker identifiering) av användare,
5. övervakning och konfigurering av materiel/utrustning fysiskt belägen inom ett område man inte har kontroll över (t.ex. fjärr-konfiguration av routrar).

Skissen är en beskrivning av var säkerhetsfunktionerna skall placeras i arkitekturen.

De säkerhetsfunktioner som krävs bygger på identifiering, signering och kryptering och är fundamentala.



Förslagen bygger på internationella standarder, men rör enbart den svenska delen av Internet, förutom de delar där svenska Internet ingår i ett globalt sammanhang som t.ex. när det gäller DNS.

17.1 Behov av säkerhetsfunktioner

Allt eftersom nya tillämpningar utvecklas ställer vi allt högre krav på att kommunikationen skall vara säker. De säkerhetsfunktioner som efterfrågas i den ökade användningen av Internet bygger i de allra flesta fall på någon användning av kryptoteknik. Fram till helt nyligen har kryptering varit viktigt enbart för

statsmakterna, och då framför allt för militärer och diplomater. Vad som på kort tid har ändrat på detta förhållande är att andra aktörer ser behov av att skicka känslig information via tele- och datakommunikationsnät. Företag, myndigheter och enskilda utövar ett allt starkare tryck på leverantörer av IT-produkter och operatörer av nättjänster att kunna genomföra elektroniska affärer, elektronisk ärendehantering och service, distansarbete, kommunikation mellan privatpersoner etc, på ett säkert sätt, både inom och utanför Sverige.

17.1.1 Varför behöver vi säkerhetsfunktionerna?

All kommunikation är i grunden osäker. Näten är flexibla, samtidigt som de gör det möjligt att t.ex. avlyssna meddelanden och skicka meddelanden i andras namn. Användare kan alltså inte förvänta sig att öppna och allmänna nät är säkra och måste därför själva vidta åtgärder för att skydda sin information och därmed också kunna få säkerhet hela vägen från avsändare till mottagare. En del åtgärder måste emellertid också appliceras på själva nätet och de gemensamma funktioner som har att göra med drift och underhåll av nätet.

De som har det tekniska ansvaret för nät drift kan räkna upp en lång rad situationer där information som kommuniceras mellan datorer måste skyddas från avlyssning eller modifiering. Några exempel:

Routing

- En operatör måste kunna signera routinguppdateringar så att andra operatörer kan verifiera att dessa är korrekta.
- Det måste finnas ömsesidiga avtal om routingutbyte mellan operatörer.
- En operatör behöver ha en säker förbindelse till kunders routrar, och en kunds router måste vara skyddad.
- För att ta reda på vem som äger en viss IP-adress skall varje operatör kunna gå till en gemensam databas för att se vilka nät som varje operatör annonserar (routing registry).
- Det finns behov av distribuerad autentisering av uppringande kund (roaming).

DNS

Informationen i DNS på olika nivåer måste skyddas mot förvanskning. Hur kan vi skydda DNS-noden *.se*? I dag finns det inget enkelt sätt att verifiera att den information som har hämtats från DNS är autentisk och inte har ändrats. Detta gör det möjligt att lura användare genom att lägga in falsk information i DNS och på så vis ge sig ut för att vara någon annan.

Tidstjänst

En gemensam tjänst som bör finnas tillgänglig i Sverige är tillgång till en tidsserver där man kan få tillgång till exakt tid. Tidsstämpling är en viktig fråga när det gäller exempelvis spårbarhet, giltighet för kryptonycklar m.m. Mer om en sådan tjänst finns i avsnitt 13.

17.2 Säkerhetstekniker

Det finns olika tekniska lösningar för att realisera olika säkerhetstjänster. De säkerhetstjänster som är förknippade med elektroniskt informationsutbyte är integritet och autenticitet, oavvislighet samt konfidentialitet. Dessa säkerhetstjänster beskrivs i bilaga 17.

Så gott som alla tekniska lösningar för att realisera säkerhetstjänsterna har inslag av kryptering. Vad kryptering är och olika metoder för detta beskrivs också i bilaga 17. Det finns symmetrisk kryptering respektive asymmetrisk kryptering. Digitala signaturer förutsätter i nuläget användning av asymmetrisk kryptering.

17.2.1 Krypteringsalgoritmer

Statskontoret rekommenderar att den funktion (Försvarmakten/TSA (Totalförsvarets signalskyddsavdelning)), som har ansvar för att för försvarmaktens räkning granska och testa krypteringsalgoritmer i Sverige, i ökad omfattning kan användas för civila ändamål.

En bra krypteringsalgoritm är en algoritm där det inte finns något enklare sätt att forcera den än att prova alla befintliga nycklar, och där antalet nycklar är så stort att det inte är realistiskt att prova dem alla.

Det är naturligtvis viktigt att den svenska delen av Internet har starka krypteringsalgoritmer. Detta åstadkoms bäst genom att använda öppna standardalgoritmer som har blivit testade och undersökta av kryptografer världen över under en tillräckligt lång tid och då visat sig motståndskraftiga mot attacker. Dessutom är det angeläget att använda internationellt kända algoritmer så att det går att kommunicera med parter utanför Sverige.

Hemliga algoritmer är inte lämpliga att använda då det inte går att få reda på vare sig hur de fungerar, hur de skall implementeras i programvara eller användas vid kommunikation med någon

utanför landets gränser.

Ett problem är att det inte går (med få undantag) att bevisa att en algoritm är bra, utan bara att den inte är dålig på något känt sätt. Detta gör att standarder och tillämpningar inte bör vara låsta till en viss algoritm, utan att det skall vara enkelt att välja vilken algoritm som skall användas och att byta ut en algoritm som börjar visa sig tveksam.

Det finns anledning av överväga hur många algoritmer som skall vara i bruk samtidigt. Vid användning av endast ett minimum av algoritmer blir skadan stor om någon av dem skulle visa sig vara osäker. Vid många algoritmer får man dålig kompatibilitet, samtidigt som risken teoretiskt ökar för att någon skall visa sig vara osäker.

I varje verksamhet måste det finnas ett åtgärdsprogram om en algoritm blir tveksam eller central nyckel skulle röjas. Om tillämpningen är sådan att skadorna blir stora om nyckeln röjs, måste det dessutom finnas särskilt starka metoder att skydda den centrala nyckeln.

17.2.2 Checksummealgoritmer

Checksummealgoritmer, eller hashfunktioner, är en funktion som tar en godtyckligt lång bitföljd och beräknar en checksumma, dvs en kortare bitföljd med fix längd. Hashfunktioner bör vara kollision-fria, det vill säga det skall vara i det närmaste omöjligt att hitta två olika bitföljder som ger samma checksumma.

Hashfunktioner kan användas för signering och verifiering. Secure Hash Algoritm 1 (SHA 1) respektive Message Digest 5 (MD5) är de i dagsläget två dominerande algoritmerna. Tillgängliga programvaror måste både kunna känna igen och kunna verifiera båda.

Utredningsgruppen rekommenderar att generering av checksummor sker enbart med SHA1 i nya tillämpningar.

Pseudokollisioner har påträffats i MD5, vilket gör att man kan befara en viss osäkerhet.

17.2.3 Nyckellängder

Ett villkor för att en krypteringsalgoritm skall kunna stå emot försök att analysera (forcera) kryptotext är alltså att det finns många nycklar till algoritmen. Om det bara finns ett fåtal nycklar så är det lätt att prova att dekryptera med alla nycklar och på det

sättet återskapa klartexten. Antalet nycklar måste således vara tillräckligt stort för att det inte ens med mycket snabba datorer skall gå att hitta rätt nyckel inom överskådlig tid.

I stället för att ange antalet nycklar brukar man prata om nyckellängder. Den enhet som nyckellängden anges i kallas för bitar. Varje extra bit i nyckeln innebär att det blir ytterligare dubbelt så många nyckelkombinationer att testa. En 8-bitsnyckel ger 256 kombinationer, en 16-bitsnyckel ger över 65 000 möjliga nycklar, en 30-bitars nyckel motsvarar ungefär en miljard. DES-algoritmen (Data Encryption Standard) är ett exempel på en symmetrisk algoritm, och har med 56 bitars nyckel 72 058 000 miljarder möjliga nycklar.

Om nyckeln är lika lång som den krypterade texten blir det omöjligt att utföra kryptoanalys, dvs att forcera och tolka kryptotexten. Ju kortare nyckel, desto lättare att analysera kryptot.

Nyckellängd är avhängigt av krypteringsmetod (asymmetrisk eller symmetrisk) och inte direkt jämförbara. Säkerheten i ett symmetriskt kryptosystem beror på nyckelns längd och algoritmens konstruktion. Det går att beräkna hur lång tid det tar att prova alla nycklar.

För att uppnå ett starkt textskydd med dagens använda algoritmer, kryptoanalyser och datakraft bör nyckellängden i ett symmetriskt kryptosystem uppgå till minst 70 bitar.

För asymmetriska krypteringsalgoritmer (öppen nyckel-system) används en annan metod vid kryptoanalys varför nyckeln måste vara betydligt längre. För RSA bör den helst vara minst 1024 bitar lång.

17.2.4 Nyckelhantering

Om en nyckel lagras tillsammans med den information den skall skydda spelar det inte någon roll hur bra en krypteringsalgoritm är. Att säkert överföra nycklar mellan kommunicerande parter är en av de största utmaningarna när det gäller kryptering.

Det är viktigt att klargöra alla komponenter och funktioner i nyckelhantering, innan det går att skapa en nyckeladministration för något ändamål.

Det är också viktigt att klargöra hur man skall gå tillväga i de olika situationerna:

- Söka/Hitta öppen nyckel(distinguished name, namngivning)
- Hämta öppen nyckel(katalog, nyckelaccess)
- Kontrollera/verifiera öppen nyckel(revokeringslistor/spärrlistor)

Namngivning av nycklar

Varje nyckel måste kunna identifieras unikt. Det måste alltså stå klart från början vilken information som skall finnas i ett certifikat (I bilaga 17 beskrivs certifikat). Nyckeln namnges när den skapas, och den identitet den får behöver inte vara samma som när den distribueras. Dvs, nyckel-identitet behöver inte bytas ut för att man byter lagringsplats för distribution. Ett visst certifikat kan unikt identifieras med en kombination av utfärdarens identitet och ett serienummer. En person kan ha flera certifikat så det måste också gå att unikt identifiera personer. En enhetlig standard för hur innehavarens identitet anges är att föredra. I Sverige har vi personnummer som skulle kunna användas för det ändamålet.

Hårda och mjuka nycklar

Krypteringsnycklarnas längd och tekniska kvalitet är av stor vikt. Men samtliga moment från skapande, paketering, distribution och slutligen användning, är lika viktiga för att helheten skall ge det "bevisvärde" som är grunden för införande av säkerhetstjänsterna identifiering/verifiering av individer samt framställning av elektroniska dokument försedda med digitala signaturer. För att belysa skillnaden mellan två säkerhetsnivåer beskriver vi detta genom att tala om "hårda" respektive "mjuka" nycklar.

Med hårda nycklar menas de fall där krypteringsnycklarna efter framställning lagras och exekveras i maskinvara. Det är vanligtvis utrustning gjord för ändamålet som t.ex. "black box" PC-kort eller aktiva kort. Med mjuka nycklar menas följaktligen att krypteringsnycklarna skapas, lagras och används i ren programvara.

Tekniskt sett skiljer sig inte dessa nycklar från varandra. Det kan t.o.m. vara enklare och snabbare att administrera längre nycklar i programvara än i maskinvara. Men i det fall en tredje part skall ta ansvar för hur en viss nyckel används eller snarare, har använts, får detta betydelse.

Vad som gäller i det enskilda fallet är kopplat till den policy som gäller för nyckeladministrationen. Policyn avgör vilken tilltro omvärlden kan tänkas vilja fästa vid en transaktion som signerats med en viss nyckel. Därför måste det framgå av certifikatet som skyddar användarens öppna nyckel, vilken policy som gäller

för just denna nyckel. Policyn omfattar i detta sammanhang inte bara om det är en hård eller mjuk nyckel, utan även i övrigt vilka administrativa krav som skall ha uppfyllts för att den skall kunna knytas till den part vilken nyckeln utfärdats för. Enligt nuvarande internationellt språkbruk ingår även i en policy information om kraven för viss "tjänsteklass".

17.2.5 Betrodda tredjepartstjänster

Behovet av betrodda tredjepartstjänster (Trusted Third Party, TTP) som stöd för de växande kraven på att kunna säkerställa äkthet och konfidentialitet i elektronisk information är uppenbart och många olika typer av sådan verksamhet växer fram i olika delar av världen.

De uppgifter som en TTP kan utföra är många och varierande, t.ex.:

- Certifieringsorgan (Certification Authority) för öppen nyckelcertifikat
- Certifieringsorgan för provning och utvärdering av systemimplementationer och produkter
- Incidenthanteringsorgan såsom t.ex. CERT (Computer Emergency Response Team)
- Elektroniska notariatstjänster (tidsstämpling, oavvislighet)
- Nyckeldeponering för återskapande av data vid förlust (data recovery)

De implementationer av TTP:er som finns har vuxit fram oberoende av och isolerade från varandra. I det globala perspektivet finns det emellertid behov av att etablera kontakter mellan olika TTP:er som erbjuder en rad olika tjänster under olika typer av lagstiftning.

En TTP kan erbjuda ett antal tjänster, var och en tillhandahållen av oberoende organisationer på kommersiell basis. En TTP-struktur kan vara modulärt uppbyggd och ha gränssytor som tillåter en flexibel konfiguration av systemet med hänsyn till de behov som finns hos olika roller och organisationer.

Användningen av TTP:er är beroende av det grundläggande kravet att TTP äger användarnas förtroende att utföra vissa funktioner. Dessutom kan en TTP också gå i god för trovärdigheten hos en annan användare genom att garantera dennes identitet. Det har den fördelen med sig att förtroende mellan olika objekt inom en TTP:s domän kan upprättas utan att objekten behöver göra bilaterala överenskommelser.

Bland annat har man inom ETSI (European Telecommunications Standards Institute) utarbetat ett dokument med tekniska krav för TTP-tjänster, Requirements for Trusted Third Party Services, som kan få viss betydelse för utvecklingen på området inom Europa.

I den svenska hållningen till kryptering skall det enligt utredningsgruppens uppfattning inte ingå några krav på obligatorisk deponering av krypteringsnycklar. Frågan om behovet av nyckeldeponering är upp till varje enskild verksamhet att bedöma.

Verifiering av certifikat och digitala signaturer skall skiljas från frågan om deponering av privata (lagrings)nycklar. Sådan deponering som innebär att man lämnar ifrån sig sin privata (lagrings)nyckel till någon annan skall vara frivillig och ske med syftet att kunna trygga återskapandet av lagrad information i en situation då det inte är möjligt att använda originalet.

Inom Europa pågår arbete med att finna tekniska lösningar för att kunna skapa signaturnycklar som inte går att använda som konfidentialitetsnycklar. Syftet med detta är att avdramatisera frågan om användning av kryptering då det anses att användning för att skapa digitala signaturer ur politisk synvinkel är mindre kontroversiell än användning för att skapa konfidentialitet.

Rätten till skydd av autenticitet, (data)integritet och mot intrång bör vara absolut. Samtidigt har rättsväsendet och samhället intresse av att rätten till konfidentialitet och anonymitet bör vara möjlig att häva vid misstanke om grov brottslighet.

17.2.6 Infrastruktur för nyckelhantering

En utbredd användning av asymmetriska kryptosystem kräver stöd i en infrastruktur för nyckelhantering, också kallad Public Key Infrastructure, eller kort och gott PKI. Problemet i ett asymmetriskt system med certifikat och öppna nycklar är att det är omöjligt att vara säker på att en viss persons öppna nyckel i själva verket inte är en förfalskning. Det är certifikatet som intygar bindningen mellan nyckel och individ. (Se bilaga 17 för en definition av certifikat).

Förtroendekedjor (chain of trust)

Lösningen på problemet är att placera nyckeln i ett certifikat som innehåller den öppna nyckeln plus en försäkran gjord genom nå-

gon annans digitala signatur. Denna "någon annan" kallas Certification Authority eller CA. Certifikatet flyttar trovärdigheten till den nya signaturen. Om den visar sig vara verifierbar och korrekt, så finns det större anledning att tro att den öppna nyckeln är äkta.

Om du inte heller litar på CA så måste du verifiera signaturen på CA:s digitala certifikat osv. Allt certifikaten gör är att flytta trovärdigheten uppåt i kedjan. Därigenom bildas en s.k. chain of trust. En stor utmaning i sammanhanget är just att utveckla den hierarki av förtroende som behövs för verifiering av certifikat.

I dagsläget kan de många tillämpningar som använder sig av certifikat endast hantera en nivå i en hierarki, t.ex. är detta fallet med webbläsare som kopplar mot en webbserver via SSL.

Förtroendenätverk (web of trust)

Hierarkier är inte den enda lösningen. Pretty Good Privacy (PGP), den spridda krypteringsprogramvaran för meddelandehantering, använder ett nätverk av signaturer för att garantera varje öppen nyckel. Den engelska termen för detta är "web of trust". Den öppna nyckeln signeras av dem som litar på att du är du, antingen genom att de känner dig, eller genom att du kan visa vem du är.

Användarens ansvar

Naturligtvis är frågan om förtroende ömsesidigt. Det ställer krav på användarna att de tar ansvar för att hantera nycklar korrekt och att de ser till att de vidtar alla nödvändiga åtgärder för att bibehålla den hemliga nyckeln hemlig. Det ansvarstagandet kommer förmodligen att vara det besvärligaste och svåraste att åstadkomma, eftersom majoriteten användare inte är särskilt medvetna om betydelsen av informationssäkerhet överhuvud taget.

Parametrar som påverkar förtroendekedjor

När man bygger en förtroendekedja måste man ta med i beräkningen:

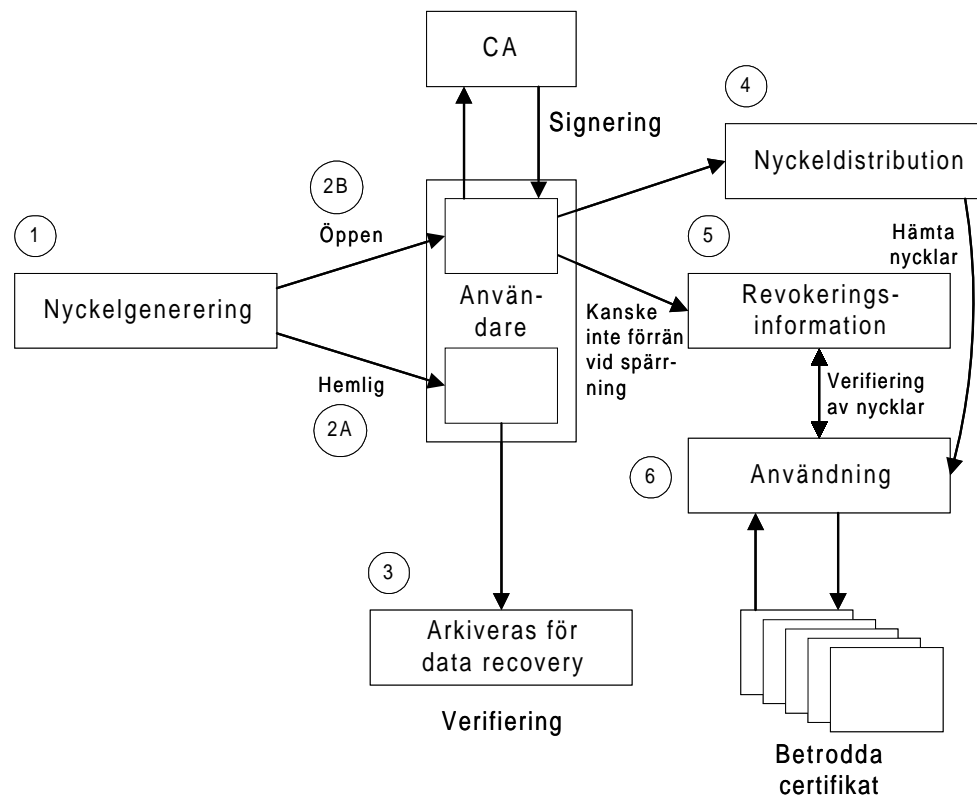
1. Hur nycklarna är lagrade och hanteras, efter vilka policier två inblandade nycklar har utgivits.
2. Hur hitta en kedja av verifierade certifikat mellan dessa två nycklar, genom att olika variabler i policyn ger en vikt för varje verifierat certifikat, som sammantaget avgör hur mycket du kan lita på kedjan i sin helhet.

Parametrar vars vikt bestäms av policyn är hur mycket förtroende som ligger i varje steg, antalet steg, hur nyckeln är lagrad och hur mycket man litar på något, exempelvis en CA.

Policyn bestäms av vilken tillämpning det gäller. Den skall publiceras och i vissa fall också kunna påverkas, accepteras eller förkastas av användarna.

Funktioner i en PKI

I bilden nedan återfinns en beskrivning av de funktioner som måste ingå i en infrastruktur för nyckelhantering (Public Key Infrastructure).



1. Nycklar som skapas (genereras) måste innehålla tillräckligt många bitar med ett standardiserat nyckelformat. Nycklar kan skapas av vem som helst. Nycklarna är initialt mycket sårbara, men genom att de signeras så erhåller de ett skydd.

Generering/signering bör alltså ske samlat (2B). I fallet PGP sker det genom "självsignering", den hemliga delen signerar den öppna delen, varefter man kan gå till en CA som intygar att den öppna nyckeln tillhör den person som man påstår sig vara. I fallet X.509 är det vanligare att CA såväl skapar som signerar nycklarna initialt. I fallet med aktiva kort som lagringsplats för nycklar blir distributionskedjan enklare om man låter en CA eller annan tredje part producera nycklarna åt användaren.

2. a) Den hemliga nyckeln måste lagras på ett säkert sätt, men den måste fortfarande kunna användas effektivt.
- 2 b) Den öppna nyckeln signeras av en CA, som har till ansvar

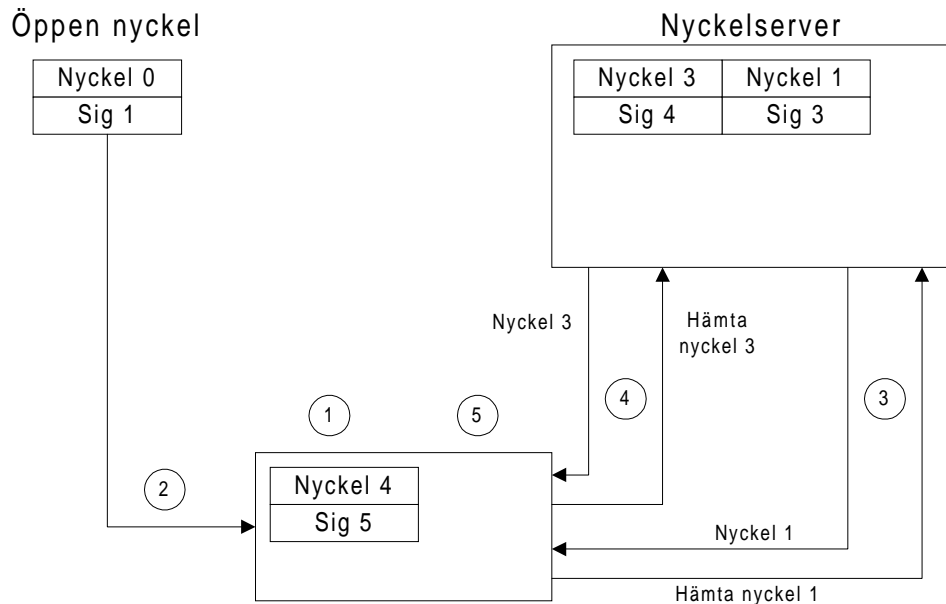
att intyga att den tillhör den som det påstås.

3. En kopia av den hemliga nyckeln kan arkiveras hos någon eller något som erbjuder den funktionen som en tjänst. Detta för att kunna återskapa klartext även om den egna privata nyckeln av någon anledning inte kan användas (glömt lösenord, någon har slutat sin anställning, filen där nyckeln lagras har kraschat etc).
4. Nyckeldistribution görs för att den öppna nyckeln måste göras tillgänglig för de som behöver använda den och för att kunna skapa förtroendekedjor (chain of trust) eller -nät (web of trust). Distributionen kan göras på en rad olika sätt, via kataloger, visitkort, personliga kontakter, tidningar etc.
5. Revokering är den viktigaste tjänst som användaren har till sitt förfogande för att verifiera att en nyckel fortfarande är korrekt och giltig. Nycklar kan behöva revokeras av olika anledningar t.ex. om ägaren förlorar kontrollen över nyckeln när ett aktivt kort tappas bort, eller om någon får sin dator stulen där nyckeln ligger lagrad. Då måste det finnas en möjlighet att ogiltigförklara sin hemliga nyckel, genom att revokera nyckelparet.

Revokeringsinformation (Certification Revocation List, CRL) ger svar på frågor om nycklars giltighet. Svaret måste man också kunna lita på, alltså måste också det kunna säkras. Svaret måste signeras med revokeringsserverns nyckel, som också måste kunna verifieras etc. Processen upprepas intill dess att man är förvissad om att informationen är korrekt. Det är den som utfärdar certifikat som också måste tillhandahålla revokeringsinformation. Här återstår en hel del att lösa. En är frågan hur användare kan finna rätt CRL. En annan fråga är att dessa revokeringslistor med tiden blir tämligen omfattande, kräver stort utrymme och riskerar att göra verifieringen långsammare.

6. Användning av nycklar/verifiering av certifikat (se nästa figur).

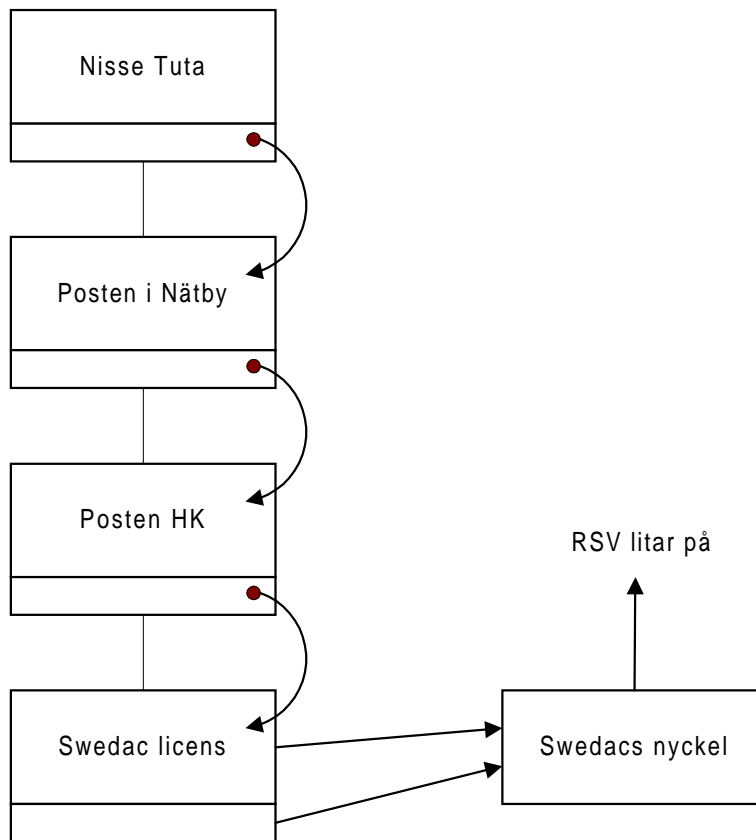
Användning av nycklar/Verifiering av certifikat



1. Förutsättningen är att användaren litar på nyckel 4 signerad av nyckel 5.
2. Användaren får nyckel 0 signerad med nyckel 1. Litar användaren på nyckel 0? Svar: Nej.
3. Användaren hämtar nyckel 1 (eftersom nyckel 0 var signerad med nyckel 1) Användaren får nyckel 1 signerad med nyckel 3. Litar användaren på nyckel 1. Svar: Nej.
4. Användaren hämtar nyckel 3 eftersom nyckel 1 signerats med nyckel 3. Användaren får nyckel 3 signerad med nyckel 4. Litar användaren på nyckel 3. Svar: Nej.
5. Nyckel 3 är signerad med nyckel 4. Användaren litar på nyckel 4, vilket gör att han också kan lita på nyckel 3, nyckel 1 och nyckel 0.

Förtroendekedja/PKI för PGP

Med hänsyn till att PGP används av många finns det behov av att erbjuda privatpersoner möjligheten att få sin PGP-nyckel signerad på ett enkelt sätt och i stor skala. Nedanstående modell utgör alltså ingen generell PKI-modell. Den beskriver bara ett sätt att realisera en PKI för PGP. Posten är i detta fall bara ett exempel, det kan lika väl vara en annan organisation med stor geografisk spridning t.ex. folkbiblioteken.



Nisse Tuta skapar och signerar initialt sina nycklar. Nycklarna tar han med sig till postkontoret i Nätby där han bor. Posten kollar Nisses identitet samt signerar Nisses nyckel med hjälp av posten i Nätbys certifikat. Posten i Nätbys certifikat är signerat av Posten HK. Posten HK har certifierats att vara CA i Sverige. Certifieringen kan till exempel innebära att Posten HK:s nyckel har signerats med Swedacs nyckel. När nu Nisse skall skicka ett signerat meddelande till RSV så kan RSV verifiera hela kedjan och därigenom lita på att Nisses nyckel är korrekt.

Användarna av PGP har behov av en PKI. Hur en sådan skall realiserats är en fråga som kräver ytterligare utredning anser utredningsgruppen.

Det bör finnas PGP-nyckelservrar centralt placerade. Behovet av tillgång till individers öppna certifikat ställer krav på en funktion som möjliggör detta. Det är dock i dagsläget för tidigt att säga något om hur dessa servrar skall implementeras och finansieras.

Initial nyckeldistribution

För att initiera en förtroendekedja måste man ha distribuerat en nyckel. Idag sker det, t.ex. inom SSL, på ett osäkert sätt. Det är oklart hur det skall göras, och det är en funktion som måste specificeras av den som bygger en PKI. Ett alternativ finns, nämligen att sprida nyckeln på ett osäkert sätt, men ge möjlighet för an-

vändaren att verifiera med användning av ett s.k. fingerprint eller en checksumma.

Hur mycket kan du lita på ett certifikat? Vilka garantier skapar de egentligen? De CA som finns måste kunna verka på kommersiella grunder. Det innebär att de tjänster de tillhandahåller måste balansera mellan trovärdighet och ekonomisk försvarbarhet.

Det är CA:s uppgift att distribuera sin öppna nyckel på ett säkert sätt till de användare som behöver kunna lita på den. Ett sätt är att när användaren får sin nyckel signerad av CA så erhåller användaren också CA:s öppna nyckel. Flera olika sätt att sprida den öppna nyckeln bör användas för att öka förtroendet; genom publicering i tidningar, radio, etc.

17.3 Nulägesbeskrivning

17.3.1 Standarder

I nedanstående tabell finns en förteckning över befintliga säkerhetsstandarder för användning på Internet. Tabellen omfattar en beskrivning av deras funktion, styrka, svaghet och geografisk spridning. Tabellen bygger på de fakta som gäller juni 1997.

Vad	Funktion	Styrka	Svaghet	Geografisk spridning
TLS/SSL, m X.509-cert främst för WWW	Verifierar server per session, kan också verifiera klienten Hierarkier skapas när nyckeln skapas.	Ger integritet och konfidentialitet av sessionen. SSL kan också rätt implementerat ge autentisering.	CA-certifikat i klienten overifierat	Spridd och mycket använd i WWW, dock med icke-hierarkisk X.509 PKI.
PGP PGP-MIME RFC 2015	Säker e-post, signering och kryptering PGP-MIME beskriver hur man stoppar in PGP-meddelanden i MIME Både text-skyddsformat och nyckelformat	Ger integritet, autentisering och konfidentialitet för e-post. Använder "web-of-trust" och inte nödvändigtvis hierarkiska nyckelstrukturer. Hierarkier skapas i efterhand genom signering	Individ-relaterat.	Spridd och mycket använt, men enbart genom icke-formaliserade kedjor av förtroende

Vad	Funktion	Styrka	Svaghet	Geografisk spridning
SSH	Använder RSA och symmetriska algoritmer för att ge autentisering, integritet och konfidentialitet vid inloggning, kopiering av filer m.m. Nycklar per användare eller per dator.	Mycket spritt och använt vad gäller telnet och ftp mot UNIX-datorer och liknande.	Standard för initial nyckeldistr saknas. Känslig för man in the middle-attacker. Nyckeldistribution manuell eller osäker Om det kommer andra fungerande nyckeldistributionsmetoder så kommer SSH sannolikt att användas av det.	Spridd och använd, trots problem med initial nyckeldistribution – antagligen p.g.a. dålig kunskap om bristerna.
Kerberos V.4 Kerberos V.5 Symmetrisk	autentisering av klienter och servrar. Använder symmetrisk kryptering och ett nyckeldistributionscenter (KDC). Används i huvudsak inom en organisation	Säker autentisering av server och klient vid telnet och ftp. Fungerar säkert även från osäker ändpunkt till skillnad från SSH som har problem med initial nyckeldistribution.	Kräver tredjepartsfunktion, som i sin tur kan bli känslig för attacker	Spridd i organisationer med stort behov av fjärrinloggning via telnet, t ex fjärrkonfiguration av nätnoder.
SEIS ID, X.509-cert	autentisering signering kryptering	Nyckellagring på kort garanterar att innehavaren inte kan duplicera sin privata nyckel	Förutsätter tillgång till kortläsare i alla situationer. Osäkert/oklart hur kommunikation med kortläsare sker.	Lokalt
S/MIME (PKCS#7) X.509	Beskriver hur man stoppar in PKCS#7-meddelande i MIME. Autentiserar användare per meddelande Signering och kryptering	Ger integritet, autentisering och konfidentialitet för e-post	Applikationerna ger inte stöd för hierarkier. Osäker utveckling	Begränsad spridning
IPSEC ISAKMP/Oakley alt manuellt	Implementerar säkerhetsfunktioner på IP-nivån. Hanterar all trafik mellan 2 IP-adresser på IP-nivån	Tunnling mellan olika brandväggar för LAN-LAN kommunikation	Standarden är inte klar	Experimentell
DNSSEC RFC2065	Säkerställer innehållet i DNS. Kan också användas för att distribuera krypteringsnycklar.	Ger genom domännamnshierarkin automatiskt en PKI för certifikat. Inte ifrågasatt.	Ännu inte testat i stor skala.	Ett fåtal implementationer finns. Experimentell

17.3.2 Olika certifikatstandarder

Ett certifikat är den informationsmängd som, signerad av en CA, skapar en bindning mellan exempelvis en person och en nyckel (ett nyckelpar). En mer detaljerad beskrivning av detta återfinns i bilaga 17.

I dagsläget finns det två dominerande certifikattyper, PGP-certifikat respektive X.509-certifikat. Båda varianterna skall kunna ingå i infrastrukturen. En användare skall ha möjlighet att skaffa såväl PGP- som X.509-certifikat från en CA.

17.3.3 X.509-certifikat vs PGP-certifikat

Ett problem med X.509-certifikat är att de innehåller olika information i olika implementationer. Det finns behov vid användning av X.509 att standardisera innehållet i ett certifikat. Särskilt viktigt är det att nyckelidentifieraren, (Distinguished name, DN), specificeras. Nyckelidentifieraren bör innehålla organisationsnummer för organisationer, personnummer för personer (eller annan unik identifierare för individer).

Arbete har initierats inom IETF med att standardisera nyckelinnehållet så att samma nyckel kan användas både i X.509 och PGP, dock med olika format. Separat arbete pågår vad gäller standardisering av nyckelidentitet för koppling till domännamn.

Tills dess att detta arbete är avslutat måste standardisering ske per tillämpning. Detta sker exempelvis inom SEIS. SEIS bör fortsättningsvis aktivt delta i arbetet inom dessa två områden, samt anpassa sitt eget arbete till den i framtiden fastslagna standarden, när den kommer.

17.3.4 DNS-Sec för nyckeldistribution

Utredningsgruppen konstaterar att SOF föreslår ett genomförande av DNS-Sec från den 15 november 1997. Det vore då också effektivt att dra nytta av DNS-Sec för att bygga en öppen-nyckel-infrastruktur (PKI) för servercertifikat för SSL.

Den som är innehavare av zonen .se blir därmed root-CA för denna hierarki och DNS kan här användas för nyckeldistribution och verifiering av nycklar. Hos zonen "." (punkt) kommer i sin tur .se-certifikatet att kunna verifieras. Det kan dröja innan det existerar någon nyckel och certifikat för ".", men genom att använda nyckeln för .se är vi inte heller beroende av detta.

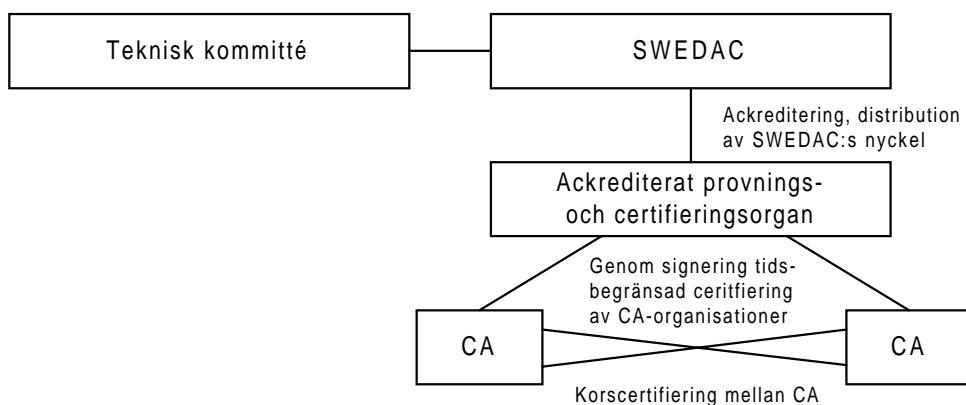
17.4 Ackreditering av CA

För att få till stånd en kontrollorganisation kring dem som vill erbjuda CA-tjänster på den svenska marknaden, föreslår utredningsgruppen att SWEDAC bör få i uppdrag att utreda om det med stöd av Lagen om teknisk kontroll kan skapas en ordning där SWEDAC bedömer och ackrediterar provnings- och certifieringsorgan med uppgift att prova och certifiera dessa CA.

Styrelsen för ackreditering och teknisk kontroll (SWEDAC) är central förvaltningsmyndighet för teknisk kontroll och mätteknik, och nationellt ackrediteringsorgan för ackreditering av laboratorier, certifierings- och kontrollorgan.

Certifieringsprocessen kan delas upp i fyra delar: Examinering, bedömning, certifiering och övervakning. Examineringen bör bestå av en bedömning av organisatoriska förhållanden, kompetens, ekonomi samt praktiska tester av tekniska implementationer. En certifieringsordning som endast omfattar dokumentgranskning accepteras inte. Efter genomförd certifiering har certifieringsorganet ansvar för att övervaka hur den certifierade CA:n uppfyller certifieringsvillkoren under certifikatets giltighetstid, som kan omfatta ett visst antal år.

SWEDAC tillkallar enligt sin instruktion tekniska kommittéer med uppgift att vara rådgivande i de tekniska frågor som SWEDAC bestämmer, och som faller inom myndighetens ram. Främst gäller det frågor som berör ackreditering och tillsyn av laboratorier, certifieringsorgan och kontrollorgan, utvecklingsprojekt, standardisering, investeringar, utbildning m.m. Det är i detta sammanhang viktigt att de personer som bemannar en teknisk kommitté för att vara rådgivande vid ackrediteringen av de organisationer som skall granska och certifiera CA sätts samman med såväl djup som bred kompetens inom juridik, säkerhet och om Internettekniken och dess villkor.



17.4.1 Korscertifiering mellan CA

För att slippa vandra genom hela förtroendekedjan är det lämpligt att utnyttja möjligheten med korscertifikat. Korscertifikat används vanligtvis när inte alltför många organisationer samverkar. Detta är en möjlighet att skapa genvägar vid verifieringen av certifikat. Normalt är sådana certifikat ömsesidiga, dvs organisationerna certifierar varandra. Det bygger på att parterna har förtroende för varandra (jag litar på dig, du litar på mig).

17.4.2 Rättsliga aspekter, pågående och tidigare arbeten

De för utredningsgruppen viktigaste rättsliga delarna bedöms vara att fastställa begrepp som omnämns i bilaga 17 under "Elektronisk dokumenthantering", i första hand begreppet digital signatur. Även internationellt är det den digitala signaturen som står i centrum för intresset. Resultatet av regeringskansliets referensgrupp i krypteringsfrågor förväntas styra prioriteringen inom det rättsliga området.

17.5 Hinder mot att tillgodose säkerhetsbehovet

17.5.1 Avsaknad av enhetliga standarder

Inom Internetsäkerhetsområdet finns det i dagsläget ett stort antal standarder som är under utveckling och oftast inte omsatts i någon större mängd tillämpningar. Det finns också ett stort antal konkurrerande standarder, dvs. standarder som är avsedda att lösa samma problem, på olika sätt, och som därmed inte är kompatibla. Utvecklingen kommer förhoppningsvis att gå i en riktning så att enighet kan uppnås inom några avgörande områden, men vi är inte där ännu.

Vad gäller exempelvis certifikatsstandarder så finns det i dagsläget två konkurrerande standarder, PGP och X.509. Båda an-

vänds men för olika tillämpningar. Användningen av dessa ökar stadigt i tillväxt, och det finns inget som tyder på att den ena eller andra kommer att gå segrande ur kampen. Det kan till och med vara så att ett alternativ uppstår som tar vara på fördelarna hos de båda andra. Ytterligare en möjlighet är att nyckelinnehållet kommer att vara ett och samma men formaten olika, dvs samma nyckel kan användas både i PGP och X.509-tillämpningar. Användningen av dessa standarder i tillämpningar på Internet diskuteras inom IETF.

17.5.2 Avsaknad av CA-hierarki, globalt resp nationellt

Utredningsgruppen föreslår att frågan om en modell för en generell infrastruktur för nyckelhantering belyses inom ramen för det uppdrag om bl.a. IT-säkerhetsstrategi som regeringen lagt på Statskontoret i september 1997.

En av de grundläggande komponenterna i användningen av öppen nyckel-system är tillskapandet av en Public Key Infrastructure (PKI). Utan en gemensam struktur för detta kommer Sverige att hamna i en situation likt den på 70-talet med isolerade system och tillämpningsspecifika lösningar som inte kan fungera tillsammans.

Om man i Sverige tänker genomföra ett allmänt införande av elektroniska ID-kort är en PKI nödvändig. Denna måste fungera för såväl handel, banktransaktioner och vid kontakt med myndigheter som vid behörighetskontroll.

För att kunna få fram ett regelverk på området måste redovisningen av rollerna TTP, CA, etc vara helt stringent.

17.5.3 Avsaknad av funktioner för verifiering av certifikat

Med funktioner för verifiering av certifikat avses att såväl certifikatsservrar som accessmetoder måste definieras, som klarar användning i stor skala. Exempel på accessprotokoll är LDAPv3 (Light Directory Access Protocol, version 3), eller HKP (Horowitz Key Protocol). Utan sådana funktioner som stöd för verifiering av certifikats äkthet eller giltighet har vi ingen fungerande infrastruktur.

17.5.4 Bristande stöd i klientprogramvaror

Det måste finnas programvaror som stödjer den lösning vi väljer i Sverige. En svensk lösning måste ha stöd i standardprogramvaror (utvecklade utanför specifika projekts ramar).

17.5.5 Exportrestriktioner

Ett trettiotal stater har genom att underteckna Wassenaar-arrangemanget kommit överens om att motverka spridningen av produkter som kan användas både för militära och civila ändamål, s.k. dual use-produkter. Krypteringsprodukter hör till denna kategori. Syftet är att förhindra, eller åtminstone försvåra, att stater som stödjer terrorism eller där terrorism eller annan allvarlig brottslighet, t.ex. narkotikabrott förekommer, skall få tillgång till sådan teknik.

Sverige deltar i detta samarbete och inom EU regleras handeln mellan EU:s medlemsstater och med tredje land. Det medel som används för kontroll av exporten bygger på ett system med licensgivning. Licenser kan beviljas för export av dual use-produkter efter prövning av ansökan om sådan licens från den som vill exportera.

Programvara för kryptering är undantagen från licenskravet om det är allmänt tillgänglig för allmänheten genom att den säljs via detaljist över disk, via postorder eller telefonförsäljning. Den skall också vara konstruerad så att användaren själv kan installera programvaran utan väsentlig medverkan av försäljaren. Detta är innebörden i den s.k. General Software Note (GSN). Mer om vad som gäller för dessa frågor står att finna i SFS 1994:2060, Förordning om strategiska produkter.

En begränsning av användningen av kryptering hämmar införandet av krypteringsteknik på Internet av gällande exportrestriktioner. Sverige bör undersöka möjligheterna att lätta på dessa restriktioner och verka för att andra gör likadant, åtminstone mellan EU:s medlemsstater. Med hänsyn till svenska företags intressen av att kunna importera produkter från andra länder som undertecknat Wassenaar-arrangemanget kan emellertid inte Sverige ensidigt avskaffa exportrestriktionerna. Ett ensidigt avskaffande skulle kunna rubba andra länders förtroende för Sverige och försvåra import av högteknologi. Detta är en politisk fråga som är föremål för diskussioner inom regeringskansliet.

17.5.6 Licensieringsproblem

Många tillämpningar som använder krypteringsalgoritmer använder sig i dag av RSA-algoritmen. Den algoritmen är patent-skyddad och programvaror som skall använda RSA måste erhålla licens från patentinnehavaren, RSA Data Incorporated. Patentskyddet för RSA upphör 2003.

Inom IETF har man på senare tid uppmanat användningen av algoritmen Diffie-Hellman/El Gamal vid utveckling av nya programvaror, en algoritm vars patentskydd gick ut den 6 september 1997.

Utredningsgruppen noterar detta och rekommenderar för nya tillämpningar användning av DH/El Gamal.

Stöd för RSA bör emellertid finnas i programvaror även i fortsättningen för att kunna acceptera information krypterad med RSA, dvs. man måste kunna ta emot information med RSA och DH/El Gamal, medan det är tillräckligt att kunna skicka enbart med DH/El Gamal.

Utredningsgruppen anser emellertid inte att det finns anledning att bromsa existerande arbete på området inom exempelvis Bankföreningen, SEIS, Postgirot, universitetsvärlden m.fl. Vi måste acceptera att fram till dess att en gemensam lösning finns är det enda tillgängliga alternativet att utveckla tillämpningsspecifika lösningar.

18 Utbildning och kompetensförsörjning

Statskontoret föreslår att regeringen snarast låter göra en detaljerad kartläggning över vilka utbildningsområden som skall vara prioriterade på kort sikt inom högskoleväsendet rörande teknisk kompetens för uppbyggnad av stora IP-nät, för att så snabbt som möjligt fylla upp bristerna på kompetent personal.

Intresset för IT och Internet, från såväl offentlig sektor som näringsliv, har medfört att det råder stor brist på kompetent personal. Länsarbetsnämndens prognoser fram till och med våren 1998 visar att efterfrågan på professionell arbetskraft kommer att öka inom samtliga datayrken i Stockholm, och allt talar för att situationen är densamma över hela landet. Samtidigt råder det redan idag stor brist på kvalificerad arbetskraft.

Behovet av kompetens finns i allt från stöd i upphandlingar till att i den löpande verksamheten kunna underhålla nätverk med datorer och programvaror.

Avsaknaden av eller ofullständiga kunskaper om IP-tekniken är ett av de allvarigare hoten mot den tekniska infrastrukturen. Svårigheten att hitta kompetent personal går ut över expansionen av Internet och har allvarliga konsekvenser bl.a. för kvaliteten på den service som tillhandahålls av operatörerna. Bristen på kompetenta nätverksbyggare gör att Sverige eventuellt inte lyckas bygga den infrastruktur som det informationssamhälle vi planerar för så väl behöver. För kommuner som satsar i egna nätlösningar är detta en allvarlig fråga. Offentlig sektor har också svårt att konkurrera med näringslivets eller konsultbranschens löner.

I dagsläget finns bara en utbildning i Sverige i att bygga stora nät. Utbildningen genomförs på KTH, och endast ett mycket begränsat antal personer i Sverige besitter de kunskaper som krävs för att kunna ge sådan utbildning.

Den stora bristen på kompetens drabbar data- och telekommunikationsföretagen särskilt hårt. Dessa företag behöver alla rekrytera mycket eftersom verksamheten expanderar snabbt, dessutom är rekryteringsbehovet kompetensmässigt i stort sett identiskt. Detta gör företagen mycket beroende av nyckelpersonal.

Att helt undvika beroendet av nyckelpersonal kan vara svårt i en situation där den snabba teknikutvecklingen, det växande antalet

aktörer och expansionen i anslutningar till Internet ofta kräver en allt större specialisering inom området.

Goda kunskaper hos alla aktörer, ett utbrett säkerhetsmedvetande och motivation i arbetet är av allra största betydelse för att minska sårbarheten hos den svenska delen av Internet. Det är känt att en stor del av alla händelser som förorsakar störningar i olika verksamheter har samband med bristande kunskaper, slarv eller slentrianmässig hantering. Sådana brister kan leda till direkta störningar i form av avbrott i driften etc. De kan också medföra att svagheter uppstår i säkerhetssystemet som gör att detta inte fungerar vid en störning, t.ex. i det enklaste av fall att man inte vet hur utrustningen för brandbekämpning fungerar.

Utbildning är aldrig ett engångsarbete. Det ligger i verksamhetsansvaret att fortlöpande kontrollera att kunskapsnivån är tillfredsställande.

Ett effektivt sätt att lösa problemet på lång sikt är att statsmakterna målmedvetet satsar på kvalificerad utbildning. Regeringen har beslutat att inrätta 60 000 nya högskoleplatser till år 2000, med tyngdpunkt på teknik och naturvetenskap. Utbildningen måste emellertid vara relevant för behoven. Vi täcker inte upp bristen på kvalificerad nätverkskompetens genom att ge ut datorkörkort och lära alla att använda kalkyl- och ordbehandlingsprogram.

Ett annat problem vad gäller utbildning är att det råder stor brist på behöriga lärare inom området. En undersökning som gjorts av Computer Sweden våren 1997 visar att två tredjedelar av landets högskolor har problem med att rekrytera lärare inom data/IT-området. Den stora efterfrågan på IT-kompetens har trissat upp lönerna så att högskolorna inte kan konkurrera med näringslivet. Detta är en situation vi kommer att få leva med under en tid. Allt eftersom fler människor utbildas inom området kommer också utbudet av utbildad personal att öka, och bristen förhoppningsvis att balanseras.

19 Accessnät och tillgång till information

Statskontoret anser att för bredbandsaccess till hushållen skall användas en infrastruktur som fullt ut bygger på den som används för övriga Internet, dvs. TCP/IP-arkitekturen. På detta sätt utnyttjas en och samma kommunikationsarkitektur mellan alla änds-system.

Statskontoret anser att användaren skall ha möjlighet att välja olika operatörer och tjänster och alltid erhålla goda prestanda till olika typer av databaser och informations-serverrar.

Syftet med detta avsnitt är att beskriva dels den utveckling som påbörjats för att erhålla accessförbindelser (bredbandsaccess) med överföringshastigheter som har större kapacitet än vad som tidigare har kunnat erhållas, dels den förändrade placeringen av vissa typer av informationsserverrar som nu kan förutses.

Med bredband avses här överföringshastigheter högre än 2 Mbit/s.

19.1 Bakgrund

Det fasta telefonnätet består av växlar (telefonstationer) och ett transmissionsnät. Det senare delas in i ett accessnät för anslutning av de enskilda kunderna och ett transportnät för överföring av trafiken mellan telestationerna.

Varje enskild kund är ansluten till en lokalstation via accessnätet. Samtliga lokalstationer inom ett visst geografiskt område är i sin tur anslutna till en gemensam förmedlingsstation, som genom transportnätet står i förbindelse med övriga förmedlingsstationer.

I accessnätet är varje enskild förbindelse avdelad för en specifik kund, medan kapaciteten i transportnätet är en gemensam resurs som delas av samtliga som är anslutna till nätet.

Transportnätet består till övervägande delen av fiberoptiska kablar, medan accessnätet i dag till större delen består av koppar-kabel. Dock förekommer även radiobaserade system och i ökad utsträckning används också fiberoptisk kabel i accessnätet.

19.2 Nätstrukturen närmast användaren förändras

När det gäller bredbandsaccess, som riktar sig mot hushåll, talar

man i dag om ett antal olika tekniker för att åstadkomma sådan access. Exempel är kabel-TV och den på kopparkablar baserade s.k. ADSL-tekniken (Asymmetric Digital Subscriber Line) och den ur ADSL kommande utvecklingen mot högre hastigheter. (För beskrivning av access via ADSL (xDSL) se bilaga 18 och för kabel-TV se bilaga 19.)

En annan fråga, som har samband med bredbandsaccess, är var (dvs. relativt användarna) servrar med "tung" information skall placeras i nätet. Operatörer och de leverantörer som står för "innehållet" har börjat placera servrar för webb-tjänster och andra tjänster liksom för video tjänster, "TV över Internet", på centrala punkter i nätet för att förbättra kvalitet och svarstider. Detta görs för att kunna få god kapacitet och svarstider till de egna användarna. Med olika programvarubaserade lösningar speglar man innehållet eller lagrar temporärt kopior av ofta efterfrågade webbsidor.

Samtidigt kommer ett allt större behov av att kunna sända mycket information även *från* användarna, exempelvis vid s.k. samarbetsystem med videokonferenssystem och delade dokument. Den senare tjänsten som också kan användas för distansundervisning ställer direkt krav på många-till-många kommunikation. Detta finns i dag som experimentell "tjänst" i form av den s.k. MBone-tekniken (Multicast Backbone).

19.3 Bredbandsaccess till hushåll

Statskontoret anser att man för bredbandsaccess till hushållen skall använda en infrastruktur som fullt ut stödjer den kommunikationsarkitektur som används i övrigt för Internet, dvs. TCP/IP-arkitekturen. På detta sätt utnyttjas en och samma kommunikationsarkitektur mellan alla änds-system.

19.4 Tillgång till information

Utgående från att TCP/IP-arkitekturen till fullo används även för accessförbindelsen anser Statskontoret att användaren skall ha möjlighet att välja olika operatörer och tjänster och då alltid erhålla goda prestanda till olika typer av databaser och andra informationsserver. Detta skall åstadkommas genom att den operatör som tillhandahåller informationstjänster till kunder i sitt eget nät skall vara skyldig att på begäran med samma prestanda ansluta andra operatörer antingen via knutpunkten eller bilateralt.

20 Telefoni över Internet

Statskontoret föreslår att införandet av en ny nummerserie för portabla nummer i Sverige utreds av DRS (expertgruppen för Domännamnsregler i Sverige) och att DNS-databaser utnyttjas för lagring av dessa nummer.

Statskontoret rekommenderar att DNS utnyttjas för att underlätta samtrafiken mellan telefoni över Internet och telefontätet.

I direktiven för uppdraget anges under rubriken "Samtrafik på applikationsnivå" att "Statskontoret skall dokumentera de fall där samtrafik är möjlig mellan applikationer, som använder eller kan förväntas använda Internetteknologi och existerande traditionella kommunikationssystem".

Telefoni över Internet behandlas även i bilaga 20. I bilagan beskrivs den principiella skillnaden mellan kretskopplade nät (telefontätet) och paketförmedlande nät (Internet), vidare beskrivs användning av Internet för fax och video samt vilka förutsättningar det finns att förbättra Internettelefone. Bilagan avslutas med en beskrivning av utvecklingstrender för Internettelefone.

I avsnitt 14 beskrivs DRS.

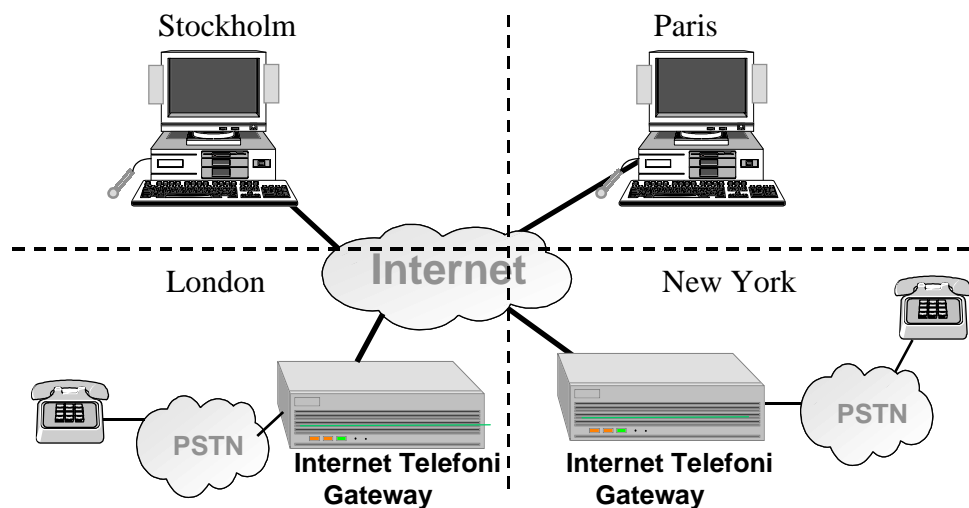
20.1 Bakgrund

Telefoni över Internet är en ung och snabbt växande marknad där de första programvarorna släpptes i början av 1995 av bl.a. VocalTec. Sedan 1995 har ett tiotal företag etablerat sig med programvara för telefoni över Internet (Voice over IP). Senaste trenden för dessa programvaror är att inkludera stöd för videokonferens. Möjligheten till "multimedial" kommunikation är en drivande faktor i utvecklingen av telefoni över Internet.

När telefoni över Internet startade var målgruppen främst entusiaster som ville komplettera ett utbyte av e-post med gratis telefoni. Förutsättningen var att både sändare och mottagare hade en persondator med ljudkort, högtalare och mikrofon samt att de visste hur de skall hitta (adressera) varandra. Kvaliteten på samtalet var urusel och liknade som bäst en primitiv kommunikationsradios kvalitet. Kvaliteten på samtal över Internet är i dag oftast bättre, men fortfarande inte i klass med ett vanligt telefonsamtal.

Utvecklingen går mot att den uppringda parten använder en vanlig telefon. I dessa fall kan det vanliga telefonnumret användas och samtliga telefonanvändare kan vara mottagare av samtalet. Internet utnyttjas som bärare av telefoni, den sista delen av transporten står det lokala telefonbolaget för. Detta kräver ett avtal med en tjänsteleverantör som tillhandahåller en brygga (gateway) mellan det publika telefonnätet och Internet.

En kompletterande utveckling kan vara att de nya terminalerna som behövs för att terminera bredbandsaccess till användare innehåller den konverterare som krävs mellan vanligt telefonnät och paketförmedlande nät.



Figur 20-1

Figur 20-1 visar hur Internet kan användas för telefonsamtal över Internet. Alla användare kan tala med alla oavsett utrustning. Användarna i New York och London använder en gateway som konverterar talet till Internettrafik så de kan tala med PC-användarna. Om personer i London och New York skall tala med varandra sker konverteringen två gånger.

20.2 Varför telefoni över Internet?

Ekonomi är i dag den främsta orsaken till att utnyttja Internet för telefoni. Såväl företag som privatpersoner betalar en fast anslutningsavgift till Internet, och debiteras inte för det faktiska utnyttjandet. Då de således har en låg rörlig kostnad för utnyttjandet av Internet är fjärrsamtal och internationella samtal över Internet mycket billigare än de som rings via det allmänna telefonnätet. Ett internationellt samtal på 10 minuter över Internet kostar 1-2 kr med Telias Internettjänst, om Telias telefonnät används kostar samma samtal 20-100 kr (maj 1997). Reduktionen av samtalskostnaden på internationella samtal är således i dag

den stora vinsten. För lokala och regionala samtal är vinsten inte lika påtaglig.

Kostnaden för internationella samtal kan antas falla under de närmaste åren varvid den ekonomiska fördelen med telefoni över Internet minskar eller kanske till och med elimineras. Troligen har då såväl kvalitet som tjänsteutbud för Internettelefoni utvecklats så långt att den ändå är attraktiv för många kunder. Det gäller framför allt de som vill komplettera taltrafik med video eller samtidig överföring av data. En intressant tillämpning av telefoni över ett IP-nät är också möjligheten att från t.ex. ett hotellrum ansluta datorn direkt till den egna organisationens telefonsystem och få tillgång till samma telefonitjänster som på kontoret hemma.

Vissa uppskattar produktionskostnaden för en samtalsminut mellan Sverige och USA till under 50 öre vilket ger utrymme för traditionell telefoni att justera gällande priser. Vid en viss nivå försvinner dock lönsamheten. Traditionell telefoni kommer emellertid inte att ersättas helt av telefoni över Internet under en betydande tidsperiod.

20.3 Problemen med telefoni över Internet

Den ekonomiska besparing som görs vid samtal över Internet måste ställas mot den - ibland avsevärt - sämre kvaliteten på talet, samt de stora kraven på utrustning.

20.3.1 Samtalskvalitet

Internet är i dag inte byggt för samtalstrafik. Vid hög belastning fördröjs datapaketet ibland flera sekunder - om de alls kommer fram. Detta kan hanteras vid överföring av datafiler, men kan bli förödande för telefontrafik. En fördröjning på 0,25 sek uppfattas av örat, 0,4 sek ger en känsla av kommunikationsradio och 1 sekunds fördröjning omöjliggör för de flesta ett samtal.

I dag kan TCP/IP-arkitekturen inte erbjuda garanterad bandbredd, den funktionen förväntas ligga i ändsystemen och anpassa sig till nätets prestanda. I takt med att Internet byggs ut i de centrala delarna kommer det att finnas möjlighet att begära viss prestanda i gränsytan mot användaren, t.ex. för att erhålla en förbindelse med konstant genomströmning av datapaket. I dag varierar kvaliteten med tiden, liksom avsändarens och mottagarens placering i nätet.

20.3.2 Terminal

Om persondator används som terminal för Internettelefone krävs att den förutom en bra anslutning till Internet (minst 28 kbit/s) också är utrustad med ett bra ljudkort som tillåter s.k. full duplex (båda kan prata samtidigt) samt högtalare och mikrofon.

Ska man använda sin vanliga telefon måste man ha ett abonnemang hos en operatör som länkar över telefontrafiken till Internet. Alternativt är en personlig gateway ansluten mellan den vanliga telefonen och den fasta anslutningen till Internet.

20.3.3 Adressering och portabla nummer

Ett annat problem med Internettelefone är adresseringen i de fall mottagarens terminal är en dator ansluten till Internet. En Internetadress (exempelvis 204.212.128.233) är ju inte lika lätthanterlig och begriplig som ett telefonnummer. Dessutom tilldelas ofta användaren en Internetadress (IP-adress) dynamiskt för varje session. Det finns sålunda i dag ingen etablerad metod för att lokalisera en specifik person på Internet.

I de fall då Internet endast används som bärare av telefontrafiken men mottagaren (den uppringda) använder en vanlig telefon uppstår inte problemet med adressering, det vanliga telefonnumret används.

Användning av DNS även för telefoni

För att primärt erbjuda faxtrafik över Internet har man redan i dag infört E.164-nummerserien (dvs. vanliga telefonnummer) i DNS-databaser. Denna lösning skalar, vilket betyder att det är möjligt att använda DNS-databaser även för att anordna samtrafik mellan Internetbaserad och traditionell telefontrafik på ett för användaren automatiskt sätt.

DNS med sina distribuerade databaser har kapacitet att agera nummeruppslagning för dagens samlade telefontrafik i Sverige, både vad det gäller volym och driftsäkerhet. Statskontoret rekommenderar att denna möjlighet utnyttjas även för telefoni.

Portabla nummer

De i dag existerande telefonnumren i Sverige kan ses som fysiska ändpunktsidentifikatorer av telefonjack.

Statskontoret föreslår att införandet av en ny nummerserie för portabla nummer i Sverige utreds av DRS (expertgruppen för Domännamnsregler i Sverige). Nummerserien skall inte vara knuten till vare sig operatör eller transportnät. Syftet med portabla nummer är att erhålla ett generellt sätt för elektronisk adressering,

dvs en nummerserie som även kan användas för andra ändamål än telefoni, exempelvis personliga e-postadresser.

I de fall DNS-databaser används för portabla nummer kan den plats där förbindelsen skall termineras väljas dynamiskt. Detta kan ske över godtyckligt nät och för godtycklig operatör.

21 År 2000-problemet

Allt eftersom Internets popularitet har ökat har fler och fler organisationer börjat använda Internet som ett viktigt arbetsredskap. Detta betyder att också allt fler oroats över om övergången till år 2000 kommer att vålla problem.

Inom IETF har därför bildats en arbetsgrupp med uppgift att undersöka hur Internet påverkas vid övergången till 2000-talet. Arbetsgruppen har inventerat hur alla viktiga Internetprotokoll och dess mest populära tillämpningar påverkas. Endast sådan programvara och sådana protokoll som har direkt samband med Internet har beaktats.

Arbetsgruppens arbetsresultat kommer att publiceras som en RFC med innehållet:

- beskrivning av år 2000-problemen och när de kommer att inträffa
- sammanfattning av möjliga lösningar
- inventering av år 2000-problemet i de mest populära Internetprotokollen och deras mest populära tillämpningar
- föreslagna lösningar av problemen vilka upptäckts under inventeringen.

Arbetsgruppen startade sitt arbete i februari 1997. Ett förslag till en RFC, som så småningom skall bli en informerande RFC, har publicerats. Information om arbetsgruppen och länk till RFC-förslaget finns på Internet på adressen <http://www.ietf.org/html.charters/2000-charter.html>.

2000-säker produkt

Statskontoret, IT-kommissionen, Industriförbundet och IT-Företagen har tillsammans tagit fram en definition för vad som utmärker sekelskiftessäkra dataprodukter. Syftena härmed är två:

1. att ge köparen av produkter en möjlighet att kontrollera att dessa klarar sekelskiftet
2. att ge leverantören en möjlighet att på eget initiativ och på eget ansvar deklarerar att produkterna klarar övergången vid sekelskiftet.

Med sekelskiftessäker menas att produkten, när den används såväl före som skäligen tid efter sekelskiftet enligt produkt-dokumentationen, kan med bibehållen funktionalitet lagras,

bearbeta, lämna och ta emot datum- och tidsangivelser för såväl 1900-talet som 2000-talet.

Det innebär:

- att sekelskiftet inte skall orsaka driftstörning för produkten
- att produkten hanterar år 2000 som skottår.

En förutsättning är att produkten får, för produkten, korrekta datum- och tidsangivelser i kontakten med andra produkter. Uppgift om att produkten är sekelskiftessäker bör framgå av produktspecifikation. Avtal mellan kund och leverantör reglerar hanteringen av fel och brister.