Inför en svensk policy för

SÄKER ELEKTRONISK KOMMUNIKATION

Referat från ett seminarium anordnat av IT-kommissionen, Närings- och handelsdepartementet och SEIS den 11 december 1996

IT-kommissionens rapport 6/97

KOMMISSIONEN

REGERINGSKANSLIET
Närings- och handelsdepartementet

SEIS
Secured Electronic Information in Society

Inför en svensk policy för

SÄKER ELEKTRONISK KOMMUNIKATION

Referat från ett seminarium anordnat av IT-kommissionen, Närings- och handelsdepartementet och SEIS den 11 december 1996

IT-kommissionens rapport 6/97

REGERINGSKANSLIET
Närings- och handelsdepartementet

SEIS
Secured Electronic Information in Society

Statens offentliga utredningar
1997:73
Kommunikationsdepartementet

Inför en svensk policy om SÄKER ELEKTRONISK KOMMUNIKATION

Referat från ett seminarium anordnat av IT-kommissionen, Närings- och handelsdepartementet och SEIS den 11 december 1996

IT-kommissionens rapport 6/97

Delrapport av IT-kommissionen
Stockholm 1997

SOU och Ds kan köpas från Fritzes kundtjänst. För remissutsändningar av SOU och Ds svarar Fritzes, Offentliga Publikationer, på uppdrag av Regeringskansliets förvaltningsavdelning.

Beställningsadress: Fritzes kundtjänst
106 47 Stockholm
Orderfax: 08-690 91 91
Ordertel: 08-690 91 90

Svara på remiss. Hur och Varför. Statsrådsberedningen, 1993.
– En liten broschyr som underlättar arbetet för den som skall svara på remiss.

Broschyren kan beställas hos:
Regeringskansliets förvaltningsavdelning
Distributionscentralen
103 33 Stockholm
Fax: 08–405 10 10
Telefon: 08–405 10 25

Graphic Systems AB, Göteborg 1997

ISBN 91-38-20606-4
ISSN 0375-250X

IT-kommissionen, Närings- och handelsdepartementet och föreningen för Säkrad Elektronisk information i Samhället (SEIS) anordnade i december 1996 ett seminarium med rubriken "*Inför en svensk policy för säker elektronisk kommunikation*". Syfte med seminariet var att presentera aktuella problemställningar och att ge tillfälle till ett meningsutbyte om dessa.

De olika anförandena under dagen spelades in på ljudband som sedan renskrivits. Respektive talare har givits möjligheter att redigera sina inlägg. En arbetsgrupp bestående av Kjell Skoglund, IT-kommissionen, och Jöran Wester, SEIS, har därefter sammanställt denna rapport.

Krypteringstekniken bidrar till att kommunikation över nätverk kan göras mer säker. En mer allmän användning av sådan teknik berör många olika samhällsintressen som belyses av denna rapport. Det kan röra enskildas integritetsskydd, näringslivets behov av säker kommunikation för företagskänslig information men också rättsväsendets möjligheter att beivra brott. Som framgår av rapporten kan de olika intressena stå i motsatsförhållande till varandra.

Frågan om en svensk policy för säker elektronisk kommunikation utreds för närvarande av regeringens särskilde utredare ambassadör Magnus Faxén. Med denna rapport vill vi ge ett bidrag till en debatt om säker elektronisk kommunikation. Synpunkter i anledning av denna rapport kan med fördel framföras till arbetsgruppen. Adresser återfinns på omslagets baksida.

Peter Nygårds Statssekreterare Närings- och handelsdepartementet	Ann-Marie Nilsson Kanslichef IT-kommissionen	Håkan Jansson Ordförande SEIS

SAMMANFATTNING

Denna redovisning har ställts samman av arbetsgruppen.

Ämnet är angeläget och ökar hela tiden i betydelse. Den springande punkten gäller hur säker är elektronisk kommunikation? Kan man vara säker på dokumentets ursprung och dessutom med stor säkerhet skydda innehållet? För att kunna göra rimliga avvägningar mellan olika intressen har regeringen lagt ut ett uppdrag att ta fram en svensk policy och att delta i arbetet inom OECD. Konferensen är ett bidrag för att belysa meningsutbyte mellan olika aktörer.

Vi bör befrämja framtagandet av defacto-standarder inom områden som stödjer elektronisk kommunikation. Likaså skapa en standard kring smarta kort som vi vill se i användning som bas för elektronisk identifiering och för att kunna signera och skydda dokument.

Personlig integritet och företagsintegritet måste balanseras emot samhällets skyddsbehov. En svensk lösning måste anpassas till vad man gör i andra länder. Ett nyckeldepositionssystem skall vara av global karaktär.

Exportkontrollen är en förutsättning för det förtroende som Sverige och svensk industri måste bygga upp för att även i fortsättningen få tillgång till högteknologi.

Om inte förtroendet för ett nyckeldeponeringssystem är fullständigt kommer potentialen i elektronisk kommunikation troligen inte att realiseras.

Frågan är hur man uppnår en balans som möjliggör brottsbekämpning samtidigt som förtroendet för systemet är så högt att vinsterna kan hämtas hem av samhället. Ur internationellt perspektiv synes system för nyckeldeponering ofrånkomliga. Vissa anser att den tekniska utvecklingen sprungit ifrån möjligheterna att i praktiken kunna upprätthålla ett system med nyckeldeponering - anden är redan ur flaskan.

USA lägger sig inte i sina medborgares fria användning av teknik men vill till varje pris skydda sig så att inte omvärlden kommer åt deras högteknologi.

Algoritmen i ett krypteringssystem är i ett bra system känd, det är individparametern, nyckeln, som skapar säkerheten.

Kryptoanvändningen är idag i Sverige omfattande. Mest känt är autentisering i betalsystem.

Kryptering är den enda teknik som kan framställa motsvarigheten till namnteckning och slutna kuvert för elektroniska meddelanden. Problemet är att samma teknik används för namnteckning och kuvert.

Depositionskravet kommer att lägga icke önskvärda begränsningar på tekniken.

Naturligtvis är vi i många lägen beroende av amerikanarna, men i många andra lägen spelar det ingen som helst roll vad de gör. I praktiken har vi fullständig tillgång till all den krypteringsteknik de försöker belägga med exportförbud.

Krypteringskontroll innebär att man måste förbjuda de algoritmer som finns och ersätta dem med nya fullständigt kontrollerade algoritmer.

Det finns ingen teknisk lösning på ett nyckeldeponeringssystem som går att genomföra i praktiken.

Fri konkurrens förutsätter att konkurrenter kan hemlighålla sina kunskaper och avsikter från varandra. Handelshinder och andra regelverk som begränsar överföring bör inte få förekomma. Mycket av de stora företagens hemligaste trafik är till och från andra länder. Mindre företag är omedvetna om hur dåligt skydd deras budskap har.

Vår regering och andra i Europa lägger sig platt på marken för de amerikanska intressen som kräver att endast lättknäckta kryptonycklar från USA får användas.

Möjligt att uppamma ett förtroende för en svensk myndighet som deponeringsinstans men oacceptabelt att främmande länder har tillgång till våra företags allra hemligaste information.

Har man inte tänkt på säkerheten när man bygger upp skyddssystem så kostar säkerheten ännu mer pengar om den skall implementeras i efterhand.

Fri kryptering är i USA en konstitutionell fråga och blir i Sverige en grundlagsfråga om man vill begränsa eller förbjuda den.

Att manipulera digital representation är inte ens med säkerhet straffbart.

Internationella handelskammaren gjorde 1994 ett Position Statement. Kravet från företagen att kunna hantera sina egna nycklar är mycket starkt.

Sverige har mycket god kompetens för standardiseringsarbetet på krypteringsområdet.

Hemlig teleavlyssning och hemlig teleövervakning är mycket viktiga redskap för att bekämpa framför allt grov narkotikabrottslighet. Om i en framtid tvångsmedlem på teleområdet blir verkningslösa på grund av utbredd användning av svårforcerade krypton måste vi se till att de brottsförebyggande myndigheterna får tillgång till information i klartext.

Det är lika viktigt att så tidigt som möjligt kunna avföra folk från misstankar som att få information som styrker brottsmisstankar. Krypterade förbindelser försvårar eller kan t.o.m. omöjliggöra polisens möjligheter. Polisen vill behålla de tvångsmedelsmetoder som redan finns, men som kan förlora verkan i IT-miljön. Deponering av nycklar är ett sätt. Straffansvar när det gäller vägran att utlämna nycklar ett annat.

Banker är IT. Kryptering är en av de komponenter banker använder för att bygga upp skydd och den används för säker identifiering på avstånd, säker lagring och bearbetning samt säker överföring av information.

Inte säkert att rättssäkerheten gynnas av en reglering.

Det finns ingen känd eller logisk anledning att reglera kryptering i Sverige.

Krypteringspolitiken är en förtroendefråga. Ny produktionsteknik höjer säkerhetskraven oerhört mycket. Skillnaden mellan det som kan hända i Internet och det som kan hända i det gamla manuella systemet har inte analyserats.

Utan tillgång till samma typ av säkerhetshöjande teknologi eller system som finns i USA är det risk att vi inte kan driva de nya produktionssystemen i Sverige. Krypteringsteknik är en viktig konkurrensfaktor om svenska tjänsteföretagen skall kunna arbeta från en svensk bas.

Självklart att ha tillgång till den teknik som krävs för upprätthållande av trovärdig rättssäkerhet i IT-samhället. Individen är maktlös att föra sin talan i egen sak.

Elektronisk handel fordrar minst samma förtroende mellan individer och handelspartners som dagens procedurer.

Kontroll och övervakning skall inte tillåtas inkräkta på den normale individens verksamhet. För det finns det andra lösningar än krypteringsreglering.

Ambition med den svenska exportkontrollen är att inte lägga större bördor på svensk industri än vad som är nödvändigt. Om vi har en bra exportkontroll så har våra svenska företag fördelar av detta genom att de får tillgång till teknologi och i stor utsträckning även marknader.

USA lägger inga restriktioner på att sälja krypteringsprodukter som enbart kan användas för integritetsskydd av data, digital signatur eller identifiering/autenticering av användare. Restriktionerna finns för kryptering av nycklar avsedda för att kryptera information.

Försäljning av krypteringsprodukter släpps fri av USA om leverantörerna kan visa upp en plan för att införa "key recovery (KR)". I framtiden kommer det därvid inte att finnas restriktioner på nyckellängder och algoritmer. De amerikanska myndigheterna kommer att genomföra dessa regler trots tveksamhet och motstånd både från IT-branschen och rättsföreträdare. Leverantörerna har accepterat detta och bildat den så kallade "KR-alliansen". Merparten av leverantörerna är med i denna allians.

Australien har tagit fram ett standardokument för en "Public Key infrastructure". Frankrike är det enda land där kryptering är förbjuden utan licens. Nederländerna försökte införa licenstvång 1994. I USA förs en livlig debatt och mycket information kommer ut. Svårt att förutsäga var det landar. Mycket svårt att finna lösningar som passar för hela EU-samarbetet. Direkt Internetkontroll har införts i Nederländerna, Singapore och Tyskland. Förslag till kontroll finns i bl.a. Storbritanninen, USA och vissa islamska länder.

INNEHÅLLSFÖRTECKNING

INLEDNING

Peter Nygårds, statssekreterare, Närings- och handelsdepartementet

Jag vill börja med att hälsa er alla välkomna till denna konferens. Personligen är jag positivt överraskad att konferensen väckt ett så stort intresse och att vi har så många deltagare. Ämnet är angeläget och ökar hela tiden i betydelse. Elektronisk kommunikation är idag redan omfattande och nya möjligheter yppas hela tiden. Allt fler användare från alla möjliga delar av samhället kommer in på arenan.

Från närings- och handelspolitisk utgångspunkt är elektronisk kommunikation mycket viktig på olika sätt. Som en del av ett snabbt och effektivt informationssystem skapar elektronisk kommunikation förutsättningar för en bra utveckling av näringsliv, av handelspolitiska relationer, av kontakter mellan olika aktörer i samhället, vilket i sig är en förutsättning för utveckling och tillväxt. Elektronisk kommunikation kan få stor betydelse för hur affärstransaktioner inom näringslivet organiseras och därigenom kan den få konsekvenser även för hur olika verksamheter organiseras.

Den springande punkten är hur säker elektronisk kommunikation är. Om man kan vara säker på dokumentets ursprung, dvs. att avsändaren är den som han eller hon utger sig för och att dokumentet inte har förändrats av någon utomstående så skapas nya förutsättningar t.ex. för att sluta bindande avtal. Kan man dessutom med stor säkerhet skydda innehållet i ett dokument skapar det naturligtvis ytterligare mycket omfattande användningsmöjligheter för elektronisk kommunikation.

När en säker elektronisk kommunikation är möjlig skulle mycket av det som idag sker inom organisationer eller i sammanhang där människor med portföljer möts, för att uttrycka sig poetiskt, kunna äga rum på elektronisk väg istället. Det skulle innebära en stor förändring för organisatio-

ner och deras effektivitet. Det skulle påverka problemet med länder med verksamheter som ligger avsides marknader. Det skulle förkorta ledtider, kommunikationsmöjligheterna och det skulle kunna ha samma rättsliga betydelse som vid personliga möten. Det är alldeles uppenbart att det här skulle öka effektiviteten i näringsverksamheten och i handeln. Det skulle också kunna minska möjligheterna för brottslig verksamhet t.ex. genom att innehållet i anbud, konstruktionslösningar eller vad det nu kan vara för någonting, inte kan avläsas av utomstående, exempelvis konkurrerande företag.

Den här tekniken är möjlig idag och den förekommer också naturligtvis i ökande omfattning. Som med det mesta är det här inte så enkelt som man gärna vill tro. Den teknologi som idag är tongivande inom området är också skyddsvärd ur säkerhetspolitisk synvinkel och den är också föremål för exportkontroll. USA:s dominans inom området är stor. Vi är i hög grad beroende av den snabba utvecklingen. Andra länder utvecklar också sitt förhållningssätt inom området. Frankrike har en lagstiftning som rör säker elektronisk kommunikation. Många utländska företag undviker enligt uppgift elektronisk kommunikation med sina dotterbolag eller affärspartners i Frankrike. Det är viktigt att förstå varför, så att en reglering av området inte får samma konsekvenser för Sverige.

Någon slags reglering kommer vi sannolikt behöva eftersom det finns ett samhällsintresse av att kunna komma åt data om det skulle vara nödvändigt när det gäller t.ex. brottsbekämpning. Medaljen har som vanligt två sidor.

För att kunna göra rimliga avvägningar mellan olika intressen har regeringen givit i uppdrag åt ambassadör Magnus Faxén att ta fram en svensk policy på området och att delta i arbetet inom OECD med detta. Till Magnus Faxéns arbete har knutits en referensgrupp med representanter för de olika departement som berörs av den här frågan och det är i det här sammanhanget som vi skall se dagens konferens. Det här är ett besvärligt om-

råde. Vi behöver alla bidrag som vi kan få och vi är inte klara med någon policy. Den här konferensen vill jag därför se som en arena för meningsutbyte mellan olika aktörer och som en sådan mycket angelägen i det här policyarbetet.

Vi är tre inbjudare till den här konferensen: IT-kommissionen, den ideella föreningen för Säkrad Elektronisk information i Samhället (SEIS) och Närings- och handelsdepartementet. Vi gör det här gemensamt för att frågan har ett stort allmänt intresse och för att vi behöver få in ett brett underlag för den vidare diskussion om en svensk policy för kryptering som skall leda fram till konkreta beslut.

Jag har ett självklart särskilt intresse av de närings- och handelspolitiska aspekterna av en säker kommunikation, men det är också lika självklart att ett regelsystem måste balansera mellan alla relevanta intressen i samhället. Det finns internationella krav och internationella förhållningssätt som vi måste anpassa oss till, det finns polisiära krav och förväntningar på ett system, det finns affärsmässiga och det finns integritetsskyddsaspekten för att nämna några. Det gäller alltså att hitta en balans där de olika intressena får bli rimligt tillgodosedda i det som senare blir en svensk policy.

Med de här orden vill jag åter igen hälsa er hjärtligt välkomna och jag hoppas att det här skall bli en givande dag, inte bara för er utan också för de som sedan skall ta vid och försöka få fram en svensk policy. Välkomna.

Håkan Jansson, ordförande i SEIS

Föreningen SEIS har varit verksam i snart två år. Föreningen har ca 50 medlemmar, vilka utgör ett gott tvärsnitt av Sverige. Syftet är att SEIS skall befrämja framtagandet av defacto-standarder inom områden som stödjer elektronisk kommunikation. Detta arbete bedrivs utefter ett antal huvudlinjer, bl.a. att skapa en standard kring smart-card som vi vill se i användning som bas för elektronisk identifiering, för att kunna signera och rättsskydda dokument. Syftet är även att kunna skydda överförda uppgifter, att öppna och tillhandahålla information på ett säkert sätt för att ur ett globalt perspektiv bedriva handel och verksamhet.

Från exportindustrins synpunkt är det väsentligt att skynda på processen med att klarlägga under vilka förutsättningar vi kan bedriva handel, men också hur vi kan rationalisera. Det gäller inte bara vår interna verksamhet eftersom exportindustrin idag i allt större utsträckning samverkar med underleverantörer och kunder. Det är väsentligt, inte endast ur SEIS perspektiv, att skapa en svensk uppfattning när det gäller kryptering, hantering av tullfrågor vid elektronisk handel, IPR[1], patenträttigheter samt ett flertal andra frågor.

Seminariet den 11 december syftar till att få fram synpunkter som kan ligga till grund för framtagandet av en policy så att Sverige aktivt kan bidra och påverka den internationella debatt som pågår.

---

[1] Intellectual Property Rights

MOTSTRIDIGA INTRESSEN VID UTVECKLINGEN AV EN NATIONELL POLICY

Magnus Faxén, ambassadör och särskild utredare

Vi har nu hört både statssekreteraren Nygårds och Håkan Jansson beskriva de positiva förtecknen i den här diskussionen som vi skall ha idag. Mitt uppdrag är kanske inte att formulera en färdig policy, mitt uppdrag är snarare att rekommendera regeringen en viss policy och ytterst är det naturligtvis regeringen som skall ta ställning. Uppdraget består i att försöka koordinera tänkandet på det här området i Regeringskansliet, det vill säga i de departement i regeringen som är berörda av krypteringsfrågan. Därför finns det en referensgrupp som jag samråder med och som består av företrädare för förutom Utrikesdepartementet och Justitiedepartementet, även Försvarsdepartementet, Kommunikationsdepartementet, Finansdepartementet och Närings- och handelsdepartementet. Vi träffas regelbundet och hittills har huvudsakligen våra kontakter handlat om att diskutera hur vi skall ställa oss i de diskussioner som har pågått inom OECD och i någon mån i de diskussioner på samma tema som faktiskt också pågår inom EU. Vi kommer naturligtvis så småningom allt djupare in i hur en nationell svensk position skall se ut i de här frågorna, men vi är långt ifrån framme vid detta. Det vill jag gärna ha sagt från början, det finns för närvarande om vi ser till vårt eget land inget regelverk på det här området. Kryptering har hittills varit ett privilegium för underrättelsetjänsten och den yrkeskår som jag tillhör numera nämligen diplomatin. Där har man ju använt sig av kryptering sedan lång tid tillbaka.

Underrättelsetjänstens utveckling på det här området är långt kommen och vi har knutit till oss en expert på just krypteringsfrågan ifrån försvaret. I övrigt arbetar med mig dagligen Göran Axelsson ifrån Statskontoret som har sysslat i flera år med de här frågorna.

Vilka problem är det som man ställs inför? Ja, det är naturligtvis frågan om att söka en balans mellan olika intressen. De intressen det rör sig om är i första hand integritetsfrågan - personlig integritet, företagsintegritet och företagsskydd - balanserat emot samhällets skyddsbehov. Samhället har skyddsbehov på ett par områden, t.ex. den polisiära som nämndes här. Det gäller att naturligtvis inte helt försätta sig i den situationen att man inte kan bekämpa grov brottslighet. Man har också behov av att skydda sig mot terrorism och vi har gudskelov hittills förskonats från sådan i någon större utsträckning. I de länder vi har haft kontakt med under det här arbetet, framför allt i Storbritannien, USA och Frankrike är man ganska plågad utav detta och i USA har man tydliga indikationer på att terrordåd har planerats med hjälp av kryptering. Även britterna har antytt att sådant förekommer inom deras område.

Det är en dyster framtidsbild naturligtvis och hur skall man hantera den frågan? Ja, det har vi bett polis och justitiedepartement här hos oss att fundera över. Några lösningar har vi inte men det är möjligt att vi får höra något ifrån polisens sida här under dagen. Det rör sig alltså om polisens rätt att, efter beslut i domstol eller av åklagare, få tillträde till lagrade data eller rätt att "avlyssna" pågående krypterad trafik vid misstanke om grov brottslighet.

En svensk lösning måste anpassas till vad man gör i andra länder eftersom en stor del av trafiken går över gränserna. Viktigt är då att se vilka tendenser som växer fram. Den amerikanska administrationen har i dagarna utfärdat en förordning som skall träda i kraft inom kort, som liberaliserar exporten utav utrustning och programvara för kryptering. Denna liberalisering består i att man kommer att ge generell licens för export av avancerad teknologi på det här området men den gäller under vissa villkor. Ett villkor är att den gäller i två år under förutsättning att de företag som levererar utrustning eller programvara kan visa på att utrustning respektive programvaran är så konstruerad att den är anpassad till ett

nyckeldepositionssystem. Detta nyckeldepositionssystem skall vara av global karaktär, det skall ha en global struktur. Hur det skall se ut det kan inte jag svara på men ett faktum är att detta beslut är fattat och det kommer att ha betydelse för hur övriga länder kommer att agera. Det gäller naturligtvis även Sverige.

Som ni vet så har Sverige exportkontroll på det här området, en konsekvens av de förhållanden som rådde i Europa och i världen under det kalla kriget. Exportkontrollen finns fortfarande och Sverige har gjort vissa åtaganden som vi måste leva upp till. Det är fullt möjligt att en ändrad amerikansk policy på området också kommer att leda till vissa justeringar av den svenska exportkontrollen, men hur den kommer att se ut det vågar jag inte ha någon mening om.

I övrigt kan man peka på tendenser som är rådande i övrigt. Frankrike har redan antagit en lag om hanteringen av kryptering. Utgångspunkten i Frankrike var att all kommunikation på ett hemligt språk i varje fall var förbjuden i Frankrike. Följaktligen kallar den franska regeringen det beslut man har tagit för en liberalisering. Liberaliseringen innebär dock att man skall ha licens för att få skicka meddelanden krypterade. Man får licens under förutsättning att man deponerar en nyckel till de krypterade meddelandena hos en nyckeldepositör som är licensierad utav den franska staten. Det finns ingen annan nation som har gått så långt som Frankrike och jag tror inte någon annan kommer att göra det heller, men det kommer naturligtvis att skapa vissa problem i det internationella umgänget.

Britterna har en annan approach till det här problemet även om den i vissa avseenden liknar den som Frankrike har. Britterna kommer att driva en lösning som innebär nyckeldeposition. Till skillnad från den franska, som hittills ändå bara talar om nyckeldeposition i Frankrike, så kan britterna tänka sig en lösning som innebär att man deponerar nycklar i de två länder som är berörda av en kommunikation. Man kan även tänka sig så kallade splitkeys, det vill säga att nycklarna kan placeras inte bara i två

depositionskontor utan i flera. Britterna kan också tänka sig att depositören inte nödvändigtvis behöver vara ett statligt kontor utan det kan vara ett kontor som får certifiering utav staten. Den lösning som britterna nu har tagit fram och som de har jobbat med under ett par års tid, den håller man nu på att lansera och driver kampanj för inom Europeiska Unionen och hoppas på att få stöd utav övriga EU-medlemmar.

De här tendenserna är de som är nu tydligast markerade och frågan är naturligtvis vad som kommer ut av det här i lite längre perspektiv. Jag har velat redovisa dem för att ni skall vara klara över under diskussionens gång idag att det här är frågor som vi naturligtvis inte ensamma råder över utan att vi är i hög grad beroende av inte minst den amerikanska industrins produkter på det här området.

När det gäller exportkontrollen bara några ord. Den är ju som sagt tillkommen under tuffare tider än de vi lever i just nu men den finns där och man skall räkna med att den kommer att finnas kvar. Bland annat av det skälet att den är en förutsättning för det förtroende som Sverige och svensk industri måste bygga upp för att även i fortsättningen få tillgång till högteknologi.

Christer Marking, departementsråd, Närings- och handelsdepartementet

Några balanspunkter vid utformningen av en policy för kryptering

Dagens situation är ganska komplex med flera intressen som står emot varandra och ett internationellt sammanhang som påverkar handlingsfriheten i Sverige. Urvalet av talare på konferensen har gjorts för att belysa detta och för att förtydliga vissa frågeställningar.

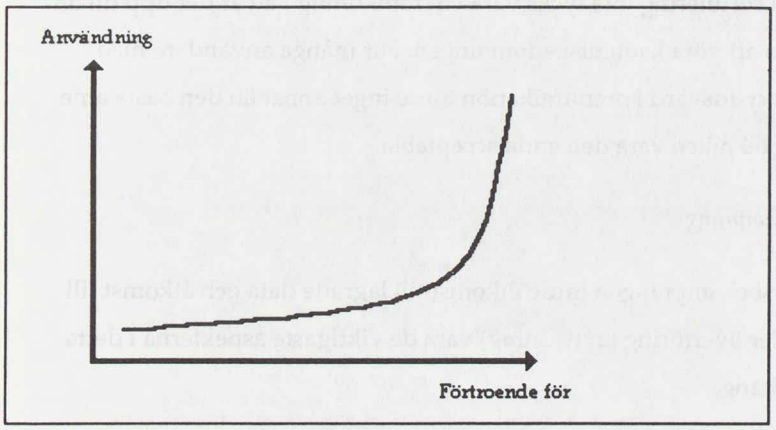
Elektronisk kommunikation har stor betydelse för alla som vill flytta information från en punkt till en annan. Det kan vara t.ex. konstruktionsritningar, personuppgifter av medicinsk art, kontouppgifter men det kan också handla om t.ex. att sluta avtal. Förutsättningen för att elektronisk kommunikation skall få den betydelse som många väntar sig är att kommunikationen är säker, dvs. att man kan veta säkert vem som är avsändare, att man kan veta om innehållet i det som sänts har förändrats och att innehållet kan skyddas mot otillbörlig åtkomst. Mycket talar samtidigt för att ett system för nyckeldeponering kommer att vara nödvändigt. Om inte förtroende för detta system är fullständigt kommer potentialen i elektronisk kommunikation troligen inte att realiseras.

Förtroende och transaktionskostnader

Den springande punkten är hur de som vill använda elektronisk kommunikation uppfattar säkerheten i kommunikationen. Om säkerhetsnivån uppfattas som hög har aktörerna förtroende för systemet och då kommer sannolikt användningen av elektronisk kommunikation vara hög i framtiden. Om förtroendet är lågt så kommer de berörda aktörer välja andra vägar för sin kommunikation.

Ur näringspolitisk synvinkel är det angeläget att modern kommunikationsteknik används. Det sänker företagens transaktionskostnad vilket in-

nebär att resurser frigörs för andra angelägna ändamål. Därför är det bra om förtroendet för de system som vi bygger upp är så stort bland berörda aktörer att potentiella vinster av elektronisk kommunikation kan realiseras. I figur 1 illustreras schematiskt hur användningen av elektronisk kommunikation kan variera med förtroende för säkerheten i systemet.



Figur 1. Användning som funktion av förtroendet för systemet

Vad är det som påverkar förtroendet för säkerheten? Två aspekter verkar självklara. Den ena rör kvaliteten i det använda kryptot och den andra rör tillgången till mina krypteringsnycklar.

Kvalitet

För lekmän är det svårt att bedöma kvaliteten på den krypteringsteknik som finns tillgänglig på marknaden. Många av dem kan tycka att "tillräckligt bra krypto" räcker för dem. Tiden och kostnaden för att knäcka ett sådant krypto kan vara tillräckligt hög för motivera risken att använda ett "second best" krypto, t.ex. om det som ska skyddas har kort livslängd eller relativt lågt värde. Vad användare vanligtvis inte vet är om någon obehörig har en bakdörr till kryptot. Förtroendet för krypto kan kanske i bland vara betydligt större än vad som är befogat. Detta kan i sin tur skapa förutsättningar för brottslighet och ekonomiska förluster hos t.ex. företag.

Ibland höjs röster för att få fram en certifiering av "god" krypto, kanske från ett statligt organ. Certifieringen kan emellertid aldrig bli bättre än kunskapen hos de experter som gör certifieringen. Varje certifiering innebär därför en kvalitetsstämpel på experterna. Det är naturligtvis orimligt att staten genom certifiering skulle annonsera sin egen kryptokompetens. Eftersom certifiering inte tycks vara en framkomlig väg är det upp till användarna att göra kvalitetsbedömningen. För många användare med mycket skyddsvärd kommunikation torde inget annat än den bästa amerikanska tekniken vara den enda acceptabla.

Brottsbekämpning

För brottsbekämpningen torde åtkomst till lagrade data och åtkomst till data under överföring (avlyssning) vara de viktigaste aspekterna i detta sammanhang.

I samband med t.ex. husrannsakan, måste polisen kunna komma åt sådant som kan underlätta deras arbete inom det mandat som polisen har. Polisen kan t.ex. behöva komma åt krypterade data på en hårddisk. Redan ett beslut om husrannsakan innebär att den som utsätts för den inte har rätt att undanhålla information. Det praktiska problemet uppstår när vederbörande vägrar att lämna ut nyckeln eller förstör den. Då måste polisens resurser räcka för att knäcka kryptot.

Funnes det en regel som kräver nyckeldeponering för att få använda krypto så skulle möjligen den tekniska höjden på "illegala" produkter normalt sett ligga på en lägre nivå, vilket i sin tur skulle underlätta för polisen.

Vid avlyssning behöver polisen ha tillgång till nycklar för att förstå vad som sänds. För detta krävs en generell nyckeldeponering, dvs. att alla som använder kryptering har deponerat nycklar som gör det möjligt för polisen att komma åt innehållet i det som sänds. Användningen av "illegala"

system skulle avslöja sig själva samtidigt som vi kan anta att de systemen inte har samma tekniska höjd som de "legala".

Om ett system utan nyckeldeponering används skulle förtroendet för systemets säkerhet vara hög, användningen omfattande och det skulle vara svårt att komma åt skyddsvärda data för brottslingar. Samtidigt skulle den avancerade brottsliga verksamheten vara lika väl skyddad.

I huvudsak gäller resonemanget även för terroristbekämpning på det internationella planet.

Exportkontroll

I vårt nuvarande system får vi inte föra ut vissa högteknologiska produkter utan tillstånd. Sverige deltar i internationella exportkontrollarrangemang, vilka säkerställer att t.ex. Sveriges näringsliv får tillgång till högteknologiska produkter i Sverige. Avsteg från de åtaganden som Sverige gjort internationellt kan få negativa konsekvenser för användningen av högteknologi i vårt land.

Personlig integritet

När allt fler aspekter av våra liv blir åtkomliga elektroniskt, dvs. lättillgängligare för allt fler, ökar också intresset för att vi skall kunna freda oss från intrång i vår privata sfär. I den mån som krypteringsteknik används är det självklart av stor betydelse att förtroendet för systemet kan upprätthållas. Den enskilde individen har inte samma möjligheter att välja kommunikationssätt som t.ex. ett företag har. Därför blir samhällets ansvar stort för att bygga sådana system som garanterar säkerhet och som kan skapa förtroende.

Den enskilde anställde kommer i framtiden att använda krypterad information i större utsträckning än i dag. Internt i varje organisation måste tillgången till organisationens information säkerställas. Om en anställd

dör behöver organisationen komma åt vederbörandes filer. De enskilda anställdas integritet på arbetsplatsen behöver genomlysas mer noggrant än hittills.

Balanspunkter

Med en ökad användning av säker elektronisk kommunikation blir den ekonomiska samfärdseln mer robust mot brottslig verksamhet (förfalskningar, industrispionage, otillbörlig åtkomst till medicinska journaler etc). Detta innebär sänkta kostnader i samhället genom lägre kostnader för brott.

Samtidigt minskar transaktionskostnaderna i det ekonomiska livet, t.ex. för näringslivet och för den offentliga förvaltningen (mindre resande, avtal över nätet, elektroniska betalningar etc).

Polisens brottsbekämpning försvåras om polisen inte får tillgång till nycklar för att dekryptera meddelanden (avlyssning) och lagrade data. Den besvärligaste punkten här är avlyssningen. Den förutsätter att polisen i praktiken har tillgång till nycklar då transaktionen äger rum. Det förutsätter deponering av nycklar.

Deponering av nycklar minskar förtroendet för säkerheten i den elektroniska kommunikationen. Det leder i sin tur till en minskad användning av elektronisk kommunikation enligt fig. 1. Det höjer transaktionskostnaderna i ekonomin, ökar potentiellt kostnaderna för brott enligt ovan samtidigt som polisens traditionella spaningsmetoder upprätthåller sin betydelse.

De samhälleliga kostnaderna och intäkterna av alternativen är inte klarlagda. Den viktigaste policyfrågan är hur en balans skall uppnås så att brottsbekämpning kan möjliggöras samtidigt som förtroendet för systemet är så högt att vinsterna av säker elektronisk kommunikation kan hämtas hem i samhället i sin helhet.

I det internationella perspektiv syns system för nyckeldeposition vara ofrånkomliga, både med hänsyn till exportkontrollarrangemang och med hänsyn till det nu pågående policyarbetet internationellt. Även här gäller det att finna system som kan skapa förutsättningar för största möjliga förtroende.

Är anden ur flaskan?

Många anser att utvecklingen har gått för långt för att det skall vara meningsfullt att utforma policies på området. Alltför många använder redan krypto som är tillräckligt bra för sitt ändamål. Tillgången till krypto på marknaden är redan god. Det finns redan nu möjligheter att utforma system så att krypterad kommunikation kan ske mellan USA och Europa med system som utvecklats i respektive land. Vissa anser att den tekniska utvecklingen sprungit ifrån möjligheterna att i praktiken kunna upprätthålla ett system med nyckeldeponering - ständigt nya nycklar används.

TEKNISKA MÖJLIGHETER OCH PROBLEM I SAMBAND MED KRYPTERING - EN ÖVERSIKT OCH DEMONSTRATION

Viiveke Fåk, Linköpings tekniska högskola, Linköpings universitet

De fakta jag valt att prata om bygger ytterst på att det vi skall tala om är krypteringspolitik, alltså säkringspolitik för elektronisk informationsöverföring.

Det finns idag olika införda system och olika förslag internationellt. Vi kan notera att man både pratar om och använder sådan kontroll som omfattar den interna användningen av kryptering och sådan som reglerar export av kryptering. Till exempel Frankrike har en lag som reglerar den interna användningen av kryptering inom landet. Man kan också ha enbart en exportkontroll, där det uppenbara exemplet är USA, som inte lägger sig i sina fria medborgares fria användning av teknik, men som däremot till varje pris vill skydda så att omvärlden inte kommer åt deras högteknologi och därför har lagt på exportkontroller.

Oberoende av om man talar om den interna användningen och/eller export, så kan man skilja på total kontroll, tillstånd per användning eller tillämpning och förbud mot "stark" kryptering, dvs. man kan tala om kontroll i meningen att svag kryptering - sådant som vi tror att vi som är starka och duktiga trots allt kan komma åt och komma igenom - det tillåter vi, men en stark kryptering - det tillåter vi inte. USA är just nu ett exempel på att man tillåter export av kryptering som är så svag att man kan knäcka den, men man har starkare kontroller för annan kryptering.

Nu hörde vi alldeles nyss att de har funderat länge på och kommer i januari att lätta på det här. Men lättandet innebär att man också tar in en annan typ av politik, nämligen krav på nyckeldeposition, som vi nyss hörde. Nyckeldeposition innebär att myndigheterna struntar i hur stark eller

svag krypteringen är. "Se till så vi har tillgång till nyckeln, så har vi därmed löst problemet", säger man.

Sedan finns naturligtvis möjligheten att säga att "Nej men kryptering, det reglerar vi inte , det är fri användning, hurså". Vi kan notera att till exempel internt inom Sverige är det ju så vi har det idag. Vi har exportkontroll men vi har ingen reglering av den interna krypteringen.

Det kan också noteras, som har framhållits ett par gånger här idag, att vi har ett klart behov av kryptering. Vi går mer och mer mot att kommunikation, även i formella, juridiskt viktiga och giltiga sammanhang inte går via papper utan går via elektroniska meddelanden. Så vi har således ett mycket klart behov av en motsvarighet till namnteckning på papper. Det kan noteras att det här är ett bevisvärdeskrav, så ytterst har det att göra med både polisarbete och juridik. Det innebär också att det är ett rättssäkerhetskrav. Det finns vissa system, som man kan använda idag, som jag inte vill använda. Jag säger högt och tydligt till alla i min omgivning att "Det här använder jag inte", därför att jag vet att om jag ger mig med i det laget och drabbas av ett oriktigt krav, så kan jag inte inför en domstol bevisa om det är jag eller motparten som ljuger. Jag deklarerar i sådana fall att det där systemet är för dåligt. Det vill inte jag använda. Men de används idag, och vi skall vara medvetna om det.

Låt oss glömma krypteringen ett tag. Det allra enklaste exemplet är ju postorderbeställning utan namnteckning, vilket faktiskt är vad man mycket sysslar med över nätet. Om då någon faktiskt försöker juridiskt driva igenom ett omstritt krav och säger "Du har beställt det här, var god betala", vem ljuger då? Vi har ingen rättssäkerhet när folk går med på att använda sådana system. Vi har ett krav även i elektroniska sammanhang att ha en namnteckning. Vi har också ett behov till motsvarighet till slutna kuvert. Det kommer ni att höra mer om innan lunch. Ni kommer att höra om behovet från den personliga integritetens sida, ni kommer att höra om behovet ifrån näringslivet, ni kommer att få höra finanssektorns krav på

det här med namnteckning, och deras behov av sekretess kommer vi också att få belyst. Det är faktiskt så att det är ett polisiärt intresse i vissa sammanhang att ha det här skyddet, det skall vi inte glömma. Polisen har inte bara behov av att titta på andras data, de har behov av att det finns skydd också. Det här skall inte jag gå in på, utan jag vill bara nämna att vi kommer att få höra mer om det.

Kryptering är den enda teknik, som kan ge oss en motsvarighet till namnteckning och slutna kuvert vid elektroniska meddelanden. Det är alltså ohjälpligt. Det är den enda teknik vi känner idag och har något som helst hopp om att upptäcka. Problemet här är att vi har samma teknik för namnteckning och kuvert. Vi kan inte diskutera de här punkterna var för sig.

Det är så att för varje tillämpning behövs dels en beräkningsbeskrivning, en algoritm, och dels en individbestämd parameter, en nyckel. "Individbestämd" betyder inte att den måste vara unik för varje individ. Den kan till exempel vara unik för varje tillämpning eller den kan vara unik för en grupp individer, men den är inte allmängiltig och känd. Däremot säger man att vare sig man själv har publicerat algoritmen eller inte så är det vansinnigt i alla praktiska användningssammanhang att tro att kryptoalgoritmen är sekretessbelagd på något sätt. (Det finns folk som på 80-talet försökte prångla ut kryptosystem och sade att "det är hundra procent säkert". När kryptologer sade att "Jag har köpt din produkt, analyserat den och knäckt den" fick de svaret "Jamen, då har du väl tittat på algoritmen..."). Algoritmen räknas i bra system som känd, och det är individparametern, nyckeln, som är säkerhet.

Namnteckning motsvaras av att en individs i det här fallet helt unika nyckel (det måste vara en unik nyckel) används i en autentiseringsalgoritm på meddelandet. Normalt, i vanliga pappersvärlden, binds innehållet i meddelandet till ett papper och till samma fysiska stycke papper binder vi namnteckningen. Vi kan inte binda innehållet i ett elektroniskt medde-

lande till någonting fysiskt. Det finns i själva verket ett otal massa kopior samtidigt av meddelandet när det går runt i ett datasystem. Vi måste alltså binda namnteckningen till själva innehållet, och det kan vi bara göra med en algoritm, dvs. kryptering.

Kuvert är samma sak. Vi kan inte skydda meddelandet fysiskt när det går över halva jordklotet på satellitlänkar och allt möjligt annat. Vi måste räkna med att det kan bli avlyssnat. Hur hindrar vi att någon tillgodogör sig innehållet, ser till att innehållet i sig är dolt och att innehållet i sig är opåverkat? Jo, genom kryptering.

Sedan är det särskilt en sak som jag vill betona här. Ibland hör man att man skulle kunna tänka sig att tillåta namnteckningar, men förbjuda slutna kuvert . Det går inte. För vanliga medelsvenssons som får en algoritm laddad ner i sin PC så kan någonting sådant fungera. Medelsvensson kommer aldrig att kunna lista ut vad han har fått för någonting och kommer inte att kunna använda det på fel sätt. Men får till exempel någon av de cirka femtusen per år, som vi utbildar på de tekniska högskolorna, tillgång till systemet, så är det en bagatell för dem att ta den autentiseringsalgoritm, som de har fått av banken för att kunna göra sina bankärenden hemma, och använda den för hemlig kryptering. Känner man till lite grann om tekniken så kan man göra det. Vill man lära sig mer så kan man ta till exempel den nuvarande "bibeln" i det här sammanhanget "Applied Cryptography" av Bruce Schneier och läsa den. Den finns tillgänglig i alla bättre bokhandlar. Det är således inte svårare än så. Vi kan inte räkna med att man kan ha enbart autentiseringsalgoritmer och lägga något särskilt skydd för sekretessalgoritmer. Det funkar inte tekniskt.

Algoritmerna ja! Deras tillgänglighet diskuteras ju också ibland. Man säger till exempel "Vi kan inte ha något säkert fungerande krypteringsförbud, för algoritmer är så allmänt tillgängliga". Det måste vi onekligen slå fast som sant. Å andra sidan kan vi notera att vi vet väl också var man kan få tag på uppgifter om tekniken för hembränning, om man inte visste det

förut och lärt sig i kemin, och att göra en hembränningsapparat är verkligen inget märkvärdigt. Men vi har ändå ett hembränningsförbud, fast vi vet att vi inte hundra procent kan genomdriva det.

Man skall komma ihåg att det här med att krypto är allmänt tillgängligt, det är bra att veta, så man inte går och inbillar sig något annat. Men vi har inte påstått att vi med ett förbud har totalt hindrat användandet. Vi har bara straffbelagt och därmed förhoppningsvis minskat användandet, det måste vi ha klart för oss. Vi kan å andra sidan också då notera att det finns en mycket stark skillnad mellan hembränning och krypto.

Det finns inget som helst samhällsintresse av att folk bränner hemma. Det finns däremot ett starkt samhällsintresse av att folk dricker mindre, att det inte är för billigt och lättillgängligt med sprit. (Det finns dock ett individintresse ibland att spara sina egna kostnader genom att bränna hemma och få billig sprit och det finns ett klart intresse hos vissa individer, som har en ren sjukdom, att få fri tillgång till sprit.)

Med krypto är det en annan sak. Här måste vi komma ihåg att det finns ett mycket starkt samhällsintresse att krypto används. Krypto är det enda vi kan ha för att säkra elektronisk kommunikation och elektronisk kommunikation är vad alla säger behövs idag för effektiviteten. Så bara är det.

Utifrån detta föreslår somliga att vi tillåter "tillräckligt svaga algoritmer". Då skall vi till en början med notera att en algoritm som är svag skall vi inte alls använda. Det man ofta använder uttrycket "tillräckligt svaga algoritmer" för, det är att använda tillräckligt små och svaga nycklar. Algoritmerna är bra i sig, men nycklarna begränsar man, så man vet precis vilken säkerhet man har. Detta är alltså vad USA försökte med i sin nu gällande exportrestriktion. Där finns det angivet att det är fri export av krypton med nycklar under fyrtio bitars storlek. Vilket fick till följd att bland annat en doktorand vid just vår tekniska högskola på skoj, när datorerna inte var så upptagna på sommaren, knäckte ett sådant krypto, därför att

nyckeln var för liten och det visste han. Det var mycket ute i tidningarna för drygt ett år sedan. Den som fick den största äran var hans kollega i Frankrike, som gjorde samma sak bara för att se vem som kom först. Fransmannen kom två timmar före och fick nästan all publicitet, vilken svensken var mycket glad för. Han hade inte alls någon lust att figurera i några tidningar.

Det vi måste komma ihåg, det är att detta krypto ansågs vara tillräckligt starkt för finansiella intressen men så svagt att till exempel USA:s statsintressen var skyddade. Och en doktorand, som tycker det här är kul och har lite datorer till hands, knäcker det. Det är den situationen vi är i, där det är en sådan här flytande gräns. Vi vet ju alla att utvecklingen på maskinvarusidan och programvarusidan går mycket snabbt framåt inom datorer. Om vi säger att idag är femtiosex bitar lagom för en nyckel, så måste vi komma ihåg att den nyckeln är för svag om fem år. Och den gräns vi sätter då är för svag om ytterligare fem år, så vi måste i så fall ha en lagstiftning, där vi beslutar om årets säkra nyckellängd! Då skall vi också komma ihåg att det, som nationen har råd med i regelbunden brottsbekämpning eller liknande, det har en stor maffia råd med i form av systematiskt industrispionage och liknande. För det finns ingen gräns som vi kan sätta där legala intressen är tillgodosedda och där illegala intressen hindras. Den gränsen finns rent tekniskt inte.

Sedan har vi det här med nyckelhanteringen. Nyckelhantering är den stora stötestenen i praktiken idag. Algoritmer kan vara problem, men om man inte får importera från USA och är verkligt angelägen, så programmerar man väl det själv. Ta den här boken som jag nämnde, Bruce Schneiers "Applied Cryptography"! Det är nästan så man känner sig matt, hur man kan besluta någonting så som skett med den. Vem som helst får exportera text från USA, komplett med färdig maskinskriven kod som vem som helst kan knacka in på sin dator. I den amerikanska bokversionen finns sådan kod för algoritmer dessutom med på diskett, så jag slipper sit-

ta och knacka på tangentbordet själv, men den disketten får inte exporteras från USA, eftersom den är "utrustning" och inte "text".

Så det här med att få tag på starka algoritmer är inget problem. Problemet är att sätta upp systemet så att nyckelhanteringen fungerar säkert. Nyckelhanteringen är bland annat någonting som SEIS sysslar med, dvs. att försöka få fram bra teknik för dagligt användande av nycklar. Nyckeldeposition förutsätter att nyckeln förutom hos användaren i någon form av säkert förvaringsställe också finns på andra ställen. Det är ganska uppenbart att all extra kopiering av nycklar och all extra transport av nycklar är en risk. Fråga vilken bankmänniska som helst vad de tycker om uttalanden som "Ja, bankvalvsnyckel får ni ha men dessutom skall ni deponera en extra bankvalvsnyckel någonstans, det vill säga ni måste göra en kopia, ni måste transportera den och ni måste ha rutiner för när den får hämtas ut och när den inte får hämtas ut". Vi skall inte överdriva riskerna med deposition, men vi skall heller inte blunda för att de ökar.

Arbetsnycklar är också ett problem, därför att det normala i ett datorsystem är att den personliga och/eller gruppnyckel som jag talade om nyss, den används inte för själva krypteringen, när jag skyddar för sekretess. Jag använder en enda nyckel upprepade gånger för namnteckning, men jag kan och skall av kryptotekniska skäl inte använda samma nyckel hela tiden för sekretesskryptering. Den nyckel jag använder för sekretesskryptering skall bytas ofta av tekniska säkerhetsskäl. Om detta skall kunna ske rent praktiskt, kan det inte komma springande med en kurir mellan bankerna för varje gång vi skall skicka en transaktion, utan vi använder en redan existerande nyckel för att skicka nya nycklar. Det här är alltså ett tekniskt nödvändigt förfarande.

Problemet är att för att nyckeldeposition skall fungera, så måste vi ha lagstiftat om ett system av den typ som fanns då man försökte få fram en defactostandard i USA som kallas "Clipper Chip". Det innehåller en algoritm, som somliga förväxlar med själva chippet, men grundidén med

Clipper Chip var att man skulle ha en tillräckligt bra algoritm och ett system där det fanns en fast individnyckel per chip. Denna nyckel användes för all ytterligare nyckeltransport över nätet. Alla meddelanden inleddes med den nyckel, som man tänkte använda för meddelandet, krypterad med individnyckeln. Då är avlyssning meningsfull, därför att när jag än går in och avlyssnar ett helt meddelande, så har jag all information jag behöver för att kunna dekryptera det, genom att jag har meddelandet och jag får det individuella chippets egen nyckel från depositionsstället.

Men det här är inte vare sig den enda tänkbara eller det alltid rekommendabla sättet att hantera det här med transaktionsnycklar. I vissa fall är det till och med olämpligt. Framför allt kräver det att om jag skall använda det här sättet, så måste jag byta chip och därmed deponera nyckel rätt ofta. Alternativet att banken till exempel en gång för alla deponerar en nyckel och använder den i tio år till alla sina kommunikationer, det är tekniskt förkastligt. Det man skulle tänka sig idealiskt, det är att man kan byta säg en gång i veckan eller en gång per dag, och sedan använda den nycklen för att kryptera transaktionsnycklarna. Men hur går det då med depositionen? Depositionskravet kommer alltså att lägga icke önskvärda begränsningar på tekniken.

Så dagsläget är alltså att kryptoanvändningen idag i Sverige är mycket omfattande och en av de mest spridda och mest kända användningarna är just för autentisering i betalsystem. Vi skall också komma ihåg att det här är en tjugo år gammal användning. Ibland får man intrycket att nu på nittiotalet har vi börjat med civil kryptering. Men kryptering har funnits i allmän användning ute i samhället i tjugo år utanför till exempel militära och polisiära kretsar, som har använt det längre.

Vi kan också notera att idag används det många helsvenska algoritmer förutom de amerikanska. I internationella sammanhang krävs det gemensamma algoritmer. Då kan man fråga sig om de svenska verkligen kan hävda sig på marknaden. Men det intressanta i sammanhanget, det är att

för att exportera en algoritm, så behöver man ytterst inte exportera någonting som är exportkontrollerbart. Ytterst behöver man till slut bara transportera en människa med bra minne, och förbjud det om ni kan!

För att komplicera bilden ytterligare är dagsläget så att det inte bara handlar om USA-beroende, och när vi klarat det så har vi klarat allting. Vi använder idag helsvenska system, vi använder idag svenska system som baseras på amerikanska delar, och vi använder idag helamerikanska system.

Tekniskt finns det alltså vissa saker inom dagens diskussioner och förslag kring kryptopolitik som bara inte är möjliga. Tekniskt finns det andra saker som i högsta grad är gångbara och möjliga, men man skall då fundera på hur man begränsar tekniken. Det finns ytterligare saker, som är i allra högsta grad möjliga både tekniskt och politiskt vad gäller kryptopolitik. Det är det jag ha velat belysa lite här. Men det allra viktigaste tror jag kommer att upprepas gång på gång under den här dagen. Det är alltså att krypto är idag en teknisk nödvändighet, om vi skall ha det elektroniska informationssamhället. Vi kan således inte diskutera om vi skall ha civil användning av kryptering utan att samtidigt diskutera om vi skall ha informationssamhället. Det enda vi egentligen kan diskutera, det är hur vi handskas med den kryptering vi måste ha.

Håkan Persson, AU-System

Tillgång på krypteringsteknik i världen

I bland blir det lätt i sådana här ämnen lite för mycket teknik och lite för lite politik. I det här fallet tycker jag ibland att det har varit lite för lite teknik och lite för mycket politik. Jag tänkte spinna an lite till det som Viiveke Fåk pratade om och försöka visa lite praktiskt hur det kan se ut när man krypterar.

Jag tänkte börja med att bara kort prata om tillgången på krypteringsteknik i världen. Precis som Viiveke Fåk säger är vi naturligtvis i många lägen väldigt beroende av vad amerikanarna gör på krypteringsområdet, men i många lägen spelar det ingen som helst roll vad de gör. I det här fallet har vi faktiskt fullständig tillgång till all den krypteringsteknik som de försöker exportera eller göra exportförbud av.

Kryptering är lätt

Man kan börja med att fastslå att kryptering faktiskt i grunden är relativt lätt. Bara för att ta ett litet enkelt exempel.

EN HEMLIG TEXT +
72 675007 7633 =
LP NLRLIN ÄKÅW -
72 675007 7633 =
EN HEMLIG TEXT

Vi har en hemlig text och sedan adderar vi till ett tal. I det här fallet råkar det vara då mitt telefonnummer till jobbet som jag lägger till. Jag förflyttar bokstäverna enligt Caesars gamla princip, vilket innebär att jag förflyttar bokstäverna så många steg som talet anger. E plus 7 blir t.ex. L. Genom att

på detta enkla sätt förskjuta bokstäverna olika långt får jag sedan en krypterad text.

Om jag sedan gör samma operation baklänges så kommer texten tillbaka. Detta fungerar faktiskt alldeles strålande och mer komplicerat än så här behöver det oftast inte vara. Det som är problemet med den här typen av algoritmer och det var Viiveke Fåk inne på, det är nyckelhanteringen. Kan jag skydda nyckeln genom att jag i det här fallet kommer överens med mottagaren om vad nyckeln är, så behöver inte ett krypto vara mer kompplicerat än så här. Man behöver inte springa till amerikanarna och be om en massa algoritmer. Det här kan vem som helst klara av.

Det är lätt att få tag på färdiga krypton

Dessutom så är det väldigt lätt att få tag på färdiga kryptolösningar. Jag gick ut och sökte på Internet med en sökmotor som heter Archie. Den är visserligen inte på något sätt är heltäckande. För att finnas med i Archie till skillnad från till exempel AltaVista så måste man anmäla och säga: här har jag ett bibliotek eller här har jag en programvara som jag gärna vill göra tillgänglig. Jag sökte på ett rätt välkänt DES-bibliotek som heter Libdes. Jag fick nittioåtta träffar worldwide. Jag stegar igenom lite snabbt och tittar på vad jag hittade.

Archie Query Results

Found: 98 Hit(s)

(23) sunsite.doc.ic.ac.uk
23 /Mirrors/ftp.netbsd.org/pub/NetBSD/NetBSD-current/src/domestic/lib drwxr-xr-x 1024 00:00:00 18 Jan 1996 GMT libdes

(72) ftp.ntua.gr
72 /pub/crypt/mirrors/idea.sec.dsi.unimi.it drwxr-xr-x 512 03:41:00 22 Jul 1996 GMT libdes

(76) ftp.iij.ad.jp
76 /NetNews/comp.sources.misc/volume29 -rw-r--r-- 23204 00:00:00 23 Mar 1992 GMT libdes

(78) ftp.sogang.ac.kr
78 /.5/FreeBSD/FreeBSD-current/src/secure/lib drwxr-xr-x 512 13:04:00 29 Sep 1996 GMT libdes

(88) ftp.irisa.fr
88 /News/comp.sources.misc/volume40 drwxr-xr-x 512 01:00:00 25 Nov 1993 GMT libdes

Bildtext: Tillgänglighet på DES-bibliotek via sökmotorn Archie

Där har vi England till exempel som vi kan hämta DES-algoritmer från. England som skall vara ett föregångsland när det gäller att hemlighålla krypton för sina medborgare och andras medborgare. Vi fortsätter och ser att från Grekland och Japan kan vi hämta DES-algoritmer om vi vill göra det. Kroatien, varför inte hämta en DES-algoritm från Kroatien om vi behöver implementera kryptering i vårt system. Det fungerar lika bra som det som inte USA exporterar. Här hittar vi också en fransk Internetserver. Jag kan alltså idag gå ut på Internet och ladda ner DES-algoritmer från franska Internetserver.

Jag sökte också på PGP som är betydligt bättre än DES. 174 träffar fick jag då.

Tillgänglighet på PGP

Archie Query Results

Found: 174 Hit(s)

Det är således inte mer komplicerat än så här att gå och hämta programvara om inte jag vill knåpa ihop mitt lilla krypto själv. Konsekvensen av krypteringskontroll är också att man måste förbjuda de algoritmer som finns. Om algoritmen är allmänt tillgänglig- om man till exempel bestämmer att "nu skall ni lämna in DES-nycklarna så får ni fortsätta använda DES"- då kan de som vill kryptera visserligen lämna in DES-nycklarna men de kan kryptera först en gång med en hemlig nyckel som de har och sedan krypterar med den godkända nyckeln. Så rasslar det iväg och då

blir det ju fullkomligt omöjligt för de som sitter och avlyssnar även om de då får tillgång till den deponerade nyckeln.

Skall man komma åt det här problemet måste man förbjuda alla befintliga algoritmer och bokstavligen slå ihjäl alla Internetservrar som har de här grejerna. Sedan måste man ut med nya algoritmer som är fullständigt kontrollerade.

Det är också väldigt viktigt att komma ihåg och det var det Viiveke Fåk talade om. Vi måste inte få tillgång till algoritmerna från ursprungslandet för att kunna kommunicera med det landet. Jag kan till exempel idag utveckla en algoritm i Sverige och kommunicera med ett annat land och med ett annat företag i det landet som också har utvecklat algoritmer på sin sida. Vi kanske har läst samma bok eller vi har gjort någonting annat som gör att vi har samma lösning på båda sidor.

I det här fallet så har vi på AU-system implementerat en algoritm eller ett kommunikationsprotokoll som heter SSL och är det dominerande säkerhetssprotokoll när det gäller Internetkommunikation. Man har från amerikansk sida förbjudit export av de algoritmerna som ingår i SSL när nycklarna överstiger fyrtio bitar. 128 bitar använder man internt i USA men 128 bitar är det alltså förbjudet att exportera från USA.

Kryteringsalgoritmer måste inte exporteras från USA

Ja, vad gör vi då? Jo, vi kodar naturligtvis algoritmerna själva här och så stoppar vi in dem i vårt kommunikationsprotokoll. Här ser ni en inspelning av en krypteringssessionen som jag har spelat in när jag kopplat upp mig mot en server i USA. Servern är naturligtvis fullständigt godkänd där den står i USA.

```
961205 151422 client:c7 Send 50 bytes  Klienten skickar sitt första data

    0000  16030000 2d010000  29030032 a6d8be37    - ) 2  7

    0010  868333ec eeebfc6f  485fe5e1 7500564d   †3  oH_  u VM
```

```
0020 f37ae822 82ec8f25 d4a84e00 00020004   z ",  :% N
0030 0100
961205 151423 client:c7 Receive 1315 bytes  Servern svarar
0000 16030005 1e020000 46030032 a6da57e5        F 2 W
0010 a57ead0f 6ee6305b f441fea9 73c77a67   ~ n 0[ A s zg
0020 aa132f6f 44392d68 90cdff20 3a94624f   /oD9-h□  :"bO
0030 7c10e706 6526d70d 5d858d81 167ba442   |  e& ] □ { B
0040 4a8a114d 3fa1a60c 45d3812e 0004000b   J M?  E □.
0050 0004cc00 04c90002 96308202 92308201          0, 0,
0060 ff020502 7a0006f0 300d0609 2a864886      z  0  *†H†
0070 f70d0101 02050030 5f310b30 09060355        0_1 0  U
0080 04061302 55533120 301e0603 55040a13      US1 0  U
0090 17525341 20446174 61205365 63757269   RSA Data Securi
00a0 74792c20 496e632e 312e302c 06035504   ty, Inc.1.0,  U
00b0 0b132553 65637572 65205365 72766572   %Secure Server
00c0 20436572 74696669 63617469 6f6e2041   Certification A
00d0 7574686f 72697479 301e170d 39363035   uthority0  9605
00e0 32393030 30303030 5a170d39 36313132   29000000Z  96112
00f0 39323335 3935395a 3081c531 0b300906   9235959Z0□ 1 0
0100 03550406 13025553 31133011 06035504   U   US1 0  U
0110 08130a43 616c6966 6f726e69 61311630      California1 0
0120 14060355 0407130d 4d6f756e 7461696e      U   Mountain
0130 20566965 77312c30 2a060355 040a1323      View1,0*  U  #
0140 4e657473 63617065 20436f6d 6d756e69   Netscape Communi
0150 63617469 6f6e7320 436f7270 6f726174   cations Corporat
0160 696f6e31 1d301b06 0355040b 13145353   ion1 0  U   SS
0170 4c207633 2e302054 65737420 53657276   L v3.0 Test Serv
0180 6572311a 30180603 55040313 1173736c   er1 0  U   ssl
0190 332e6e65 74736361 70652e63 6f6d3120   3.netscape.com1
```

```
01a0 301e0609 2a864886 f70d0109 01161174  0 *†H†  t
```

Bildtext:128 bitars SSL-kommunikation mot Netscape i USA

Det första är ett handskakningsmeddelande. Sedan kommer ett svar från servern och ni ser att servern svarade att den står hos Netscape. Det är en testserver som dessutom är avsedd för att företag skall kunna testa sina egna SSL-implementeringar. Det är alltså inget misstag att den står där. Det finns dessutom tusentals andra servrar, speciellt bankservrar av den här kalibern som står och körs i USA.

Bildtext: Fortsättning 128 bitars SSL-kommunikation mot Netscape i USA

```
961205 151424 client:c7  Receive 61 bytes  Sista svaret innan krypting
    0000  16030000 38ef12ca  6acd3985 4d32199e    8  j 9 M2
    0010  7c56e02c 4326bd41  515fc2b4 0b2942b4   |V ,C& AQ_  )B
    0020  d14b6585 543d409c  9d9fb114 4df56d48   Ke T=@   M mH
    0030  3ba9f6b4 a696311c  c92215c5 41      ;  1 " A
961205 151424 client:c7  SSL END OK
961205 151424 client:c7  Receive 174 bytes
    0000  47455420 2f204854  54502f31 2e300d0a  GET / HTTP/1.0
    0010  436f6e6e 65637469  6f6e3a20 4b656570  Connection: Keep
    0020  2d416c69 76650d0a  55736572 2d416765  -Alive  User-Age
    0030  6e743a20 4d6f7a69  6c6c612f 332e3031  nt: Mozilla/3.01
    0040  20285769 6e4e543b  2049290d 0a507261   (WinNT; I) Pra
    0050  676d613a 206e6f2d  63616368 650d0a48  gma: no-cache  H
    0060  6f73743a 2066676e  0d0a4163 63657074  ost: fgn  Accept
    0070  3a20696d 6167652f  6769662c 20696d61  : image/gif, ima
    0080  67652f78 2d786269  746d6170 2c20696d  ge/x-xbitmap, im
    0090  6167652f 6a706567  2c20696d 6167652f  age/jpeg, image/
    00a0  706a7065 672c202a  2f2a0d0a 0d0a      pjpeg, */*
961205 151425 client:c7  Receive 223 bytes
```

```
0000  17030000 da71d017  75ef7976 cfa48392     q u yv
0010  b088978d 5ee70836  04c2f832 94c4b8f8     ^ 6  2"
0020  3661c493 5f5647c1  d398af31 20f86cc6  6a  _VG  1 l
0030  2e96d90a d49f03c5  81cdced8 1f5225dd  .     R%
0040  9006f4cc 14ac896a  6750459b 7b7de3d8     jgPE {}
0050  54d26896 32dcf165  14e83476 6f75e6f3  T h 2  e  4vou
0060  f2504690 3f25a975  e297cc34 9afe87cb  PF?% u  4š
0070  585c3830 84cad8c9  2fef97db 4435a943  X\80„  /  D5 C
0080  df11045e 590a7f91  b1c966fc 99ff0a94     ^Y     f™  "
0090  1dc93ede 62809c3c  a8bc4376 f9b02703     > b  <  Cv  '
00a0  382c2faa feb50019  e4d8e14e 3fe86b10  8,/       N? k
00b0  26ba3fe2 4985bba0  747a0290 2414ad6b  & ? I  tz $  k
00c0  65b4c26f a7648571  e5e74d9d 4d21b2d9  e  o d q  M M!
00d0  d8386488 c42b3ebe  3501a1db dc96c5     8d  +> 5
```

Där det står "SSL END OK" slutar handskakningen. Sedan övergår hela kommunikationen till att vara 128 bitars icke exporterbar kryptering. Klienten skickar/hämtar sidan. Det översätts sedan till krypterad text. Så ser det alltså ut när det går ut på linan. Sedan kommer svaret från servern och när svaret avkodas så ser det ut så här:

SSL v3.0 Test Server

This server supports both version 3.0 and version 2.0 of the Secure Sockets Layer protocol.
If you have any questions or comments you can contact tomw@netscape.com.
The SSL v3.0 Specification dated March 1996, may be viewed online.
It is also available as PostScript® in a single compressed tar file .
If you wish to participate in the public discussion of the SSL Protocol, you can subscribe to the ssl-talk mailing list by sending mail to
ssl-talk-request@netscape.com.
® PostScript is a registered trademark of Adobe Systems Incorporated.

En intressant sak i sammanhanget är också, vilket sällan nämns i samband med den här nya exportlättnaden från USA, att man samtidigt har slagit

fast att kryptering kommer att vara helt fri i USA. Amerikanarna kommer ha en konstitutionell rätt att - åtminstone inom Clinton-administrationens närmaste fyra år - kryptera hur de vill, med vilka algoritmer de vill och med vilka nyckellängder de vill. Det innebär att den här typen av servrar kommer att stå i USA. Vi kommer att kunna kommunicera med dem och vi kommer att ha ett behov av att kommunicera med dem.

Det intressanta med det här kommunikationsprotokollet, som kommer att bli fastställd Internetstandard inom kort, är att jag i samband med ovanstående kommunikation inte hade någon egen nyckel. Om jag som svensk blir utsatt för ett nyckeldeponeringssystem så har jag helt enkelt ingen nyckel att deponera. Det är nämligen serverns nyckel som styr uppkopplingen. Eftersom amerikanarna får använda det här fritt och inte har deponerat sina nycklar och jag har inga nycklar som jag kan deponera, så är detta ett system som man måste totalförbjuda för svenskar att använda. Eftersom det måste te sig som helt orealistiskt att förbjuda svenskar att kommunicera på ett säkert sätt i internationella sammanhang så kommer man helt enkelt inte att komma åt den krypterade kommunikationen. Det finns alltså ingen teknisk lösning på ett nyckeldeponeringssystem som praktiskt går att genomföra.

NÄRINGSLIVETS INTRESSEN OCH FRÅGESTÄLLNINGAR

Gustaf Richert, Sveriges Industriförbund

Stat och näringsliv har intresse av en väl fungerande marknadsekonomi som karaktäriseras av fri konkurrens. En sådan förutsätter att konkurrenter kan hemlighålla sina kunskaper och sina avsikter för varandra. De som i största grad har intresse av att detta fungerar väl är företagens kunder.

Information representerar allt större värden i jämförelse med de materiella tillgångarna. En snabbt ökande del av företagens - och statens - verksamhet består också av att flöda information. Låt oss kalla detta att sända och ta emot budskap. Konkurrenskraften beror i mycket hög grad på att detta fungerar effektivt.

Eftersom inte alla budskap behöver hemlighållas, kan vi människor och företagen i många fall acceptera en mindre säker men billigare överföringsmetod. Men i vissa fall, de kanske viktigaste, är kravet på säkerhet och hemlighållande absolut.

Det kan gälla förhandlingar om företagsköp, det kan gälla mycket stora anbud, det kan gälla betalningar, det kan gälla samkörning av olika moduler i produktutveckling tillsammans med leverantörer och partners, det kan gälla kundregister i samtrafik med dotterbolag utomlands. Och så vidare. Listan kan bli hur lång som helst. Olika företag och olika branscher har olika arbetssätt och förutsättningar. Läkemedelsföretagen vill kunna kommunicera snabbt och säkert med tillståndsmyndigheter i olika länder.

Observera att jag enbart talar om skydd av information vid överföring. Frågan om lagrad information är en annan och kanske mindre kontrover-

siell fråga som bör behandlas helt separat även om tekniken är likartad. Där duger existerande regler ganska långt har man sagt mig.

Jag talar heller inte annat än indirekt om skapande av elektroniska signaturer.

Företag av alla de slag kräver när de sänder viktiga budskap att budskapen kommer fram oförvanskade och kompletta, att de når rätt adressat och att de inte når några andra. Tänk efter: det är samma krav vi ställer som privatpersoner.

Kraven ställer vi på de system och operatörer som vi anlitar för att förmedla våra budskap. Och som skall styras av någon slags lagstiftning.

Inför dagens konferens har jag ringt runt till ett knippe företag. Då framtonar ett budskap mycket tydligt och ungefär likadant från alla håll; vår regering och andra i Europa verkar lägga sig platt på marken för de amerikanska intressen som krävt att endast lättknäckta kryptonycklar från USA skall få användas. Oavsett den konkreta innebörden upplevs detta med stor besvikelse.

Ett företag som vill sända ett budskap måste kunna få veta exakt vilket skyddsnät som ligger runt budskapet.

Varje företag och människa måste ha rätt att använda den säkerhets- och trygghetsnivå som han eller hon vill välja/betala för beroende på vad slags budskap som skall överföras.

Det har ju alltid varit möjligt att resa till varandra för att mellan glas och vägg utbyta hemligheter. Men det är dyrt och långsamt. Och numera är det så att den som inte utnyttjar IT/tele kommer på efterkälken.

Varje företag måste ha rätt att själv rå över sin krypteringsnyckel och (exempelvis) över hur många bitar han skall ha i nyckeln. Skall någon utomstående komma åt nyckeln skall det vara lika svårt som nu när domstol

beslutar om avlyssning skall tillåtas. Förutsättningarna för detta måste regleras i lag.

Vad jag nu sagt leder till följande självklara slutsats: handelshinder och andra regelverk som begränsar överföring och användning av krypteringsteknik bör inte få förekomma. Begränsningar medför också att alltför många inte fullt utnyttjar den nya informations- och teletekniken och därför inte är så effektiva som de skulle kunna varit.

Detta hindrar inte att ett visst mått av internationell standardisering bör främjas. Således bör krav på utrustning och metoder för kryptering kunna standardiseras så att en god marknad för sådant etableras.

Det är svårt att tänka sig en instans där krypteringsnyckel skall deponeras och som också har företagens fulla förtroende. Det närmaste man kan komma är kanske säkerhetsföretag av typ Securitas och deras kolleger.

Mycket av de stora företagens hemligaste trafik är till och från andra länder. Det är således alldeles olämpligt att lägga upp ett system av statliga myndigheter som deponeringsinstanser. Visserligen är det ju möjligt att uppamma ett förtroende för en svensk myndighet. Men det känns helt oacceptabelt att veta att främmande länders myndigheter har tillgång till våra företags allra hemligaste.

Överhuvudtaget så tenderar utvecklingen av IT, av tele och av de stora företagen att gradvis minska betydelsen av nationalstaterna. Vem har sagt att svenska större företag skulle uppleva som det mest lämpade att en deponeringsinstans vore svensk? Varför i så fall inte en global? Som FN håller i !? Nej! Det är säkert bäst att inte ha någon deponeringsinstans alls! Skall en deponeringsinstans finnas skall det vara frivilligt att använda den.

Småföretagen då?

Alla möjliga olika organisationer (vi med! och staten!) kämpar för att få de mindre företagen att i större utsträckning ta till sig och använda IT och tele som ett verktyg för högre konkurrenskraft. Småföretagen är i många fall svåra att övertyga att de har så mycket att vinna. De som lyckas bäst med att övertyga dem är ofta de företag som är deras kunder.

För det mesta är nog de mindre företagen omedvetna om hur dåligt skydd deras budskap har.

Skall vi sluta att främja IT-användning där? Skall vi i Sverige slå ifrån oss de möjligheter till ökad konkurrenskraft som IT och tele erbjuder genom att begränsa möjligheterna till skydd för vår och företagens verksamhet?!!

Utan bra kryptoskydd kommer säkerligen mycket av företagens kommunikation att ske med relativt ineffektiva metoder. Det kan mycket väl vara så att kostnaden för samhället av att göra industrispionage "lätt och lagligt" är avsevärt större än vinsten av att lättare komma åt brottslingar och busar hur legitimt detta och andra behov än må vara.

Det är näringslivsargument som bör råda i första hand om det nu är tillväxt vi vill ha. Det är bra att Näringsdepartementet, som exempelvis med dagens konferens, tar aktivt i de här frågorna. Justitiedepartementets eventuella önskan att hjälpa polisväsendet på traven får på rimligt sätt komma i andra hand.

Vi vill, från näringslivet, gärna delta mer direkt i det fortsatta utformandet av svensk kryptopolicy.

Inom näringslivet arbetas det med de här frågorna i olika konstellationer. Bl.a. har ICC i Stockholm en grupp som bearbetar säkerhetsfrågorna. ICC internationellt har tagit fram ett Position Paper i kryptofrågan. Det är redan ett par år gammalt men det beskriver på ett bra sätt företagens allmänna åsikter ännu idag.

Med den här korta inledningen har jag redovisat grunden för näringslivets synpunkter i kryptofrågorna genom att på ett brett sätt beskriva företagens behov av säkerhet för sina informationsflöden.

Stefan Bernhard, Lagerlöf & Leman Advokatbyrå

Frågan är om kryptering egentligen har så stor betydelse. Det går ju att skicka meddelanden och dessa kommer fram och man får meddelanden tillbaka. Är det så farligt egentligen?

Den situation som man möter internationellt just nu gäller just frågan om att kunna få tillgång till annans information. Det är inte för inte som FOA annonserar efter en hacker för att bättre kunna skydda sina egna informationstillgångar från alla de försök till påhälsning som FOA har just nu. Banker och stora företag - inte minst i USA - använder så kallade brandväggar för att skilja ut de behöriga och obehöriga från varandra. Men med jämna mellanrum rapporteras det om att sådana brandväggar har knäckts av någon hacker. En verkställande direktör i ett bolag i Kalifornien fick sin privata fil tömd.

Problemet är att man ogärna vill prata om säkerhet vare sig man är bank, försäkringsbolag eller industriföretag. Om någon kommer igenom brandväggen anses det vara en brist men det är också ett tecken på att man har otillräcklig säkerhet. Har man otillräcklig säkerhet är det negativt och kan resa frågor om skadeståndsskyldighet. Man vill alltså inte gå ut offentligt med sådana här saker, lika lite som man vill gå ut med intern svindel och liknande i pressen. Sedan kostar säkerhet pengar. Har man inte tänkt på säkerhet när man bygger upp skyddssystem så kostar säkerheten ännu mer pengar om den skall implementeras i efterhand. Det finns med andra ord förhållandevis lite information offentligen tillgänglig. Men inom de grupper som ägnar sig åt säkerhetsfrågorna finns det ganska påtaglig information. Det är dessutom rätt skrämmande information över omfattningen av den informationssammanställning som sker över världen. Att till exempel använda sig av Internet utan kryptering bör man bara göra om de meddelanden man sänder eller mottar lika gärna kan skrivas på ett vykort. Det förekommer alltså avlyssning i ganska ordentlig omfattning. I

Tyskland finns till och med en halvoffentlig debatt där en del hävdar att underrättelsetjänsten skulle sälja information som samlas in på underrättelsetjänstens vägnar till tyska företag. Motsidan i debatten hävdar att det bör man inte göra. Redan att debatten förekommer visar med styrka att det här är viktiga frågor, minst sagt.

De problem man står inför är mångfacetterad. Det finns lagstiftning som reglerar affärsverksamhet och det finns olika typer av lagstiftning som skall beaktas för den verksamhet som man bedriver runt om på jorden. Vi har i Sverige vår egen utgångspunkt - den svenska lagstiftningen. När man skall diskutera kryptering uppkommer i princip en konstitutionell fråga, nämligen om man kan begränsa möjligheterna för en svensk person eller ett svenskt företag att använda sig av IT-tekniken, att använda kryptering för sina kommunikationer. Den här frågan är likadan som i USA. En begränsning av möjligheten att kryptera fritt är i USA en konstitutionell fråga och i Sverige blir det en grundlagsfråga om man vill begränsa eller förbjuda. Jag tror det är oerhört viktigt inför ett policybeslut om kryptering att staten bestämmer sig för att deklarera att i Sverige skall det fortsättningsvis vara möjligt att kryptera fritt.

Den andra frågan är ännu mer mångfacetterad. Vi har mycket lagstiftning i Sverige och många av problemen är ganska likartade, såväl för de offentliga organen som för de privata organen. Det finns behov av sekretess i sjukhusvård, för patienter, läkare m. fl. Det finns liknande behov av sekretess för präster, för advokater, för revisorer, och det finns en mängd förhållanden inskrivna i lagstiftningen där sekretess råder och där skydd för privata kommunikationer gäller.

I all kommunikation som rör dessa förhållanden måste man ha tillgång till kryptering.

Det finns en stor skiljelinje mellan det privata och det offentliga. Offentlighetsprincipen gäller för den offentliga sektorns verksamhet. Offentlighets-

principen gäller inte i det privata (även om den ibland kan gälla i vissa företag). För den privata sektorn finns emellertid också inom lagstiftningen om företagshemligheter möjlighet och rätt att skydda sina tillgångar.

Det finns olika grader av sekretess. Den mest absoluta sekretessen bryts bara vid väldigt allvarliga situationer, den sekretess som gäller för präster och advokater. Skall advokater kunna fortsätta att betjäna sina klienter så måste man utnyttja kryptering om man skall kunna iaktta sin sekretesskyldighet. Vi skall heller inte glömma bort banksekretessen.

Det torde vara rätt stor enighet om att i lag påbjudna sekretessbestämmelser skall kunna tillgodoses även inom ramen för en ny teknisk värld. Frågan är bara: hur gör man då?

I den digitala världen finns inga original. En handling är inte en handling utan informationen måste knytas ihop och kopplas till en utställare med vissa metoder (t.ex. kryptering). Ett meddelande är inget traditionellt meddelande. Om man via Internet loggar in på någon "site" och lägger ned t.ex. programvara därifrån, så vet man egentligen bara att det där är en "bitsträng" som träffar minnet (hårddisken). Man vet inte med säkerhet varifrån "bitsträngen" kommer. Man vet inte med säkerhet om den motsvarar vad man tror att man har köpt. Man vet inte om man har importerat virus. Man vet egentligen ingenting alls. Därför måste vi ha metoder som gör att man kan säkerställa vem man pratar med och att innehållet verkligen kommer från rätt källa och motsvarar vad man förväntar sig. Just frågorna om säkerhet i ursprunget och säkerhet så att ingenting har hänt under överföringen är typfall som man använder krypteringsteknik för.

I dagens värld är det bara att öppna tidningen så ser man nya konstellationer, nya metoder, nya produkter när det gäller elektronisk handel, när det gäller betalsystem etc. Jag har mycket svårt att förstå att staten inte har ett mycket starkt intresse av att se till att det finns ett rimligt regelverk

som säkerställer t.ex. utnyttjande av digitala betalningsmetoder.

I dagens pappersvärld har vi sedelpress, Tumba Sedeltryckeri, vi har särskild kvalitet på sedelpappret, vi stoppar in silvertrådar och liknande. Varje sedelenhet är numrerad och dessutom har man applicerat påskrifter på de här sedlarna. Det är bra att veta att det är svårt att göra pappers-pengar. Men vi har också en struktur runt detta. Vi har en lagstiftning där man vid falskmynteri får ut polisen väldigt fort. Det är inte fallet när det gäller digitala frågor. Man får ut polisen väldigt fort för att försöka spåra upp falska sedlar och spåra upp förövarna. Dessutom har vi en lagstiftning som gör att det kostar rätt mycket i straffskala att förfalska en sedel. Att manipulera en digital representation är inte ens med säkerhet straffbart. Jag tycker det är häpnadsväckande att datastraffrättsutredningens betänkande från 1992 ännu inte föranlett någon åtgärd i detta avseende. Man måste lägga en grund för att kunna bygga ett system som är tillförlitligt. Nu kan det tyckas egendomligt att företrädare för näringslivet ropar på lagstiftning. Å andra sidan tror jag det är nödvändigt att göra just dessa saker. Ett av problemen är väl kommunikationen mellan olika departement men framför allt förståelse för tekniken.

Man måste inse att om man övergår till digital teknik tappar man möjligheten att kontrollera innehållet. Det går ganska enkelt att ändra historien. Man kan bara tänka sig vad som händer i marknadsekonomin med de krav vi har på transaktioner och bevisbarhet. Varenda transaktion i ett företag skall omsättas i en verifikation. Denna skall attesteras av någon. Dagligen förekommer miljarder transaktioner. Alla dessa verifikationer buntas sedan ihop och landar slutligen i en resultat- och balansräkning för respektive företag. Resultat- och balansräkningen för ett företag är sådant som påverkar kursrörelserna på aktiebörsen. Man handlar med aktier med de här siffrorna som underlag. Man måste med andra ord ha en tillförlitlighet, en säkerhet i detta system om vi skall behålla systemet som grund. Det är detta som jurister kallar för omsättningssäkerhet. Vare sig man gör

ekonomiska transaktioner som privatperson eller företag är ett rimligt regelverk som kan verkställas nödvändigt för att åstadkomma säkerhet i omsättningen. Kryptering är - i vart fall så här långt - en metod som kan utnyttjas för detta ändamål.

När det gäller krypteringsfrågorna är det också så att IT-världen gör gränser fullständigt meningslösa. Jag är säker på att Ni tidigare idag har hört om detta. Det innebär att staterna måste enas om metoderna om man skall få en tillförlitlig internationell hantering. Från svensk utgångspunkt, och när det gäller svensk krypteringspolitik borde man definitivt klargöra att det inte skall ske några inskränkningar i möjligheterna att kryptera vid kommunikation inom Sverige. Det här är ju lätt att säga men spelar liksom ingen roll. Kommunikationen sker ju lika lätt utomlands som i Sverige. Därför måste man försöka tillskapa metoder som gör att det går att använda sig av välkända krypteringsmetoder för utlandskommunikationen.

Det råder internationellt sett relativt stor enighet när det gäller digitala signaturer och den typen av integritetskontroll. Här är man internationellt sett beredd att släppa till krypteringsmetoder för att säkerställa signaturer och identitet. Detta är emellertid en ganska ny företeelse. Insikten om att man annars har väldigt stora svårigheter har börjat sprida sig. När det gäller innehållet i meddelanden är man emellertid mycket mer känslig och det finns många länder som har ambitioner att verkligen komma åt information och använda sig av den. För företag och för enskilda borde det vara lika svårt att acceptera att tvingas använda någon annans krypteringsnyckel. Detta gäller inte minst i internationella sammanhang, där man inte vet om det finns bakvägar inbyggda.

ICC, Internationella Handelskammaren, gjorde 1994 ett Position Statement, som också ligger till grund för näringslivets internationella hantering av krypteringsfrågan. I detta Position Statement är kravet på att kunna hantera sina egna nycklar väldigt starkt från företagens sida. Med säkerhet kan man förutse att det kommer att finnas behov av företag eller

andra som under tillräckliga garantier kan tillhandahålla nyckelservice eller säkerhetsservice åt mindre företag. Men detta måste ske under klara premisser och ansvar om att om nyckeln försvinner ut av någon anledning så finns det ett mycket starkt ansvar. Man måste också kunna ha vad som kallas "audit trail" för att säkerställa hur nyckeln behandlats. Alla organisationer - under arbetsnamnet TTP - bör vara starkt skilda från staten och förutsättningarna för att driva TTP-verksamhet bör vara objektivt fastslagna i lag. Likaväl som värdet på pengar idag är en fråga om förtroendet för valutan så är förutsättningarna för att utnyttja krypteringstekniken en fråga om förtroende hos användaren. Om användaren inte har förtroende för att konfidentialiteten kan upprätthållas kommer man inte att använda tekniken i den omfattningen som det finns möjlighet att göra. Jag vill bara ta ett exempel. Man talar idag om att tekniken inom mycket kort tid kommer att tillåta videokonferenser i stor skala. Det är sannolikt att det kommer att påverka resandet. Det är också klart att om man sitter och diskuterar sin patentansökan med ett patentombud i USA och ett annat i Hong Kong så vill man vara säker på att man slipper bli föremål för andras sniffande på de kunskaperna. En annan praktisk stiuation är rättegångar. Vill man ha vittnesförhör inom stängda dörrar kan man inte utnyttja en videokonferens i stället för att flyga folk från halva jorden till sådana rättegångar. Man kan alltså inte utnyttja tekniken.

En annan viktig fråga när det gäller krypteringsteknik och metoder är också att de algoritmer som skall ligga till grund för krypteringen bör vara öppna och utsättas för en internationell öppen prövning så att var och en kan övertygas om att just dessa algoritmer är säkra, tillräckligt bra. En sådan öppen prövning är ett viktigt led i att få fram standards som är internationellt accepterade. Hemliga algoritmer kan innehålla möjligheter till så kallade "back doors" eller annat. I det flöde av produkter som kommer från USA finns t.ex. i Windows en usel krypteringsfunktion. Windows exportversion tillåter inte längre nyckellängd än de amerikanska exportföreskrifterna medger. Den amerikanska versionen av Windows har mycket

bättre nyckel, en bättre modul för hantering. Man måste också tänka på att om man använder sig av amerikanska programvaror, finns det från amerikansk sida en vilja att så att säga gå längre och kräva att man inte får byta ut krypteringsmodulen. Om man gör det får man inte använda systemet. Man kan med andra ord inte stoppa in någon annan krypteringsmodul utan att överträda regler. Det är faktiskt en ren förhandlingsfråga internationellt sett om man skall acceptera exportregler som direkt missgynnar svenska företag. Ambitionen från svensk sida bör vara klar annars kommer man snart strategiskt sett att ha importerat så många system att man egentligen sitter fast och förhindrar utvecklingen av svenska produkter som är mycket bra även internationellt sett.

På längre sikt finns det all anledning att överväga vilken linje man skall driva från svensk sida i det här avseendet. Vi har emellertid ännu inte sett någon publikation eller någon framställning där man diskuterar de här sakerna öppet. Det är en brist. Nu pågår ett stort informationssamlande för policyutformningen. Det är en framgång att de olika departementen nu samverkar inom näringsdepartementets ram. Men man skulle gärna vilja se ett utflöde av det här samverkande informationsinhämtandet och en verklig diskussion kring vilken politik som är rimlig i för samhället och näringslivet så viktiga frågor som det här rör sig om. Det är också viktigt när man fastställer standard att det inte tar för lång tid att fastställa dessa. Standardiseringsarbetet pågår i olika fora. Här bör Sverige delta. Min erfarenhet är att Sverige har mycket god kompetens för det på krypteringsområdet. Även om vi i Sverige bestämmer oss för att ha en fri kryptering i Sverige, är det som Gustaf Richert sade, att en stor del av informationsutbytet kommer att ske över gränser. En sak är de regler vi internt bestämmer skall gälla i Sverige, en annan sak är de regler som man inom OECD kommer att vilja implementera så småningom. En tredje fråga och den kanske viktigaste just nu är väl exportkontrollen, som är en högst politiskt känslig fråga. Den säkerhetsnivå som exportkontrollföreskrifterna tillåter är väsentligt lägre än den nivå man diskuterar för svenskt internt vid-

kommande. Även på den här punkten är man från näringslivets sida intresserat. Jag tycker knappt att man har fått tillräcklig möjlighet att diskutera Sveriges ställningstagande och Sveriges roll när det gäller exportfrågorna. Även om det är en känslig fråga tycker jag att man borde kunna lätta på förlåten en hel del.

POLISIÄRA INTRESSEN OCH FRÅGESTÄLLNINGAR

Lena Moore, departementsråd, Justitiedepartementet

Jag är chef för justitiedepartementets processrättsenhet. Jag har tänkt att ta upp krypteringsfrågan från min horisont, alltså några av de frågeställningar som aktualiseras när kryptering ställs i relation till polisens och åklagarnas behov och möjligheter av att kunna utreda brott.

De frågor som faller inom processrättens ram i detta sammanhang är framförallt möjligheten för polis och åklagare att använda olika straffprocessuella tvångsmedel och då särskilt tvångsmedlen på teleområdet. Dessa är hemlig teleavlyssning och hemlig teleövervakning men kryptering har också betydelse vid beslag och husrannsakan. Även s.k. hemlig teknisk avlyssning - buggning - är av intresse i sammanhanget.

Hemlig teleavlyssning, eller telefonavlyssning som det hette förr, innebär att i princip alla telemeddelanden alltså även fax och datorkommunikation, kan avlyssnas i hemlighet. För att sådan avlyssning skall få ske krävs att någon är skäligen misstänkt för ett brott som har ett minimistraff på två års fängelse. Det krävs att åtgärden är av synnerlig vikt för brottsutredningen och det är domstol som beslutar om avlyssning ska få ske.

Hemlig teleövervakning innebär att andra uppgifter än själva innehållet i ett meddelande hämtas in. Det kan t.ex. röra sig om att ta reda på varifrån ett visst telefonsamtal rings, till vem vederbörande ringer, hur länge samtalet pågår etc. På samma sätt som för hemlig teleavlyssning kan åtgärden även ta sikte på fax, e-mail etc. Hemlig teleövervakning får användas vid förundersökning i brottmål när minimistraff för brottet är fängelse i sex månader och för narkotikabrott med enbart fängelse i straffskalan. I övrigt gäller motsvarande regler som för hemlig teleavlyssning.

Det är självklart att hemlig teleavlyssning och hemlig teleövervakning är mycket viktiga redskap när det gäller att bekämpa framförallt den grova narkotikabrottsligheten. Detta framhålls också av riksdagen varje år när regeringen redovisar hur dessa tvångsmedel använts under föregående år.

Regeringen har nyligen överlämnat en skrivelse till riksdagen där det lämnas en redogörelse för hur hemlig teleavlyssning och hemlig teleövervakning enligt rättegångsbalken använts under år 1995. Av skrivelsen framgår att förra året användes dessa tvångsmedel i 460 fall. De allra flesta brottsutredningarna avsåg just grova narkotikabrott men teleavlyssning och teleövervakning användes också i förundersökningar som gällde t.ex. mord och försök till mord, grovt rån, människorov m.m. Åtgärderna hade enligt redovisningen betydelse för brottsutredningen i drygt 50 procent av fallen.

Jag vill påpeka att redovisningen inte omfattar den hemliga teleavlyssning och teleövervakning som SÄPO använder enligt särskilda bestämmelser; de siffrorna är inte offentliga.

Den tekniska utvecklingen på teleområdet och den förändrade telemarknaden har relativt nyligen satt spår i lagstiftningen. Ändringar i rättegångsbalken och i telelagen har gjorts för att se till att vi i största möjliga utsträckning skall kunna bibehålla hemlig teleavlyssning och hemlig teleövervakning som effektiva tvångsmedel. I de lagstiftningsärendena var det bl.a. den GSM-baserade mobiltelefonin som stod i centrum. Resultatet blev bl.a. att teleoperatörerna numera är skyldiga att se till att deras telesystem är utformade och uppbyggda på ett sådant sätt att hemlig teleavlyssning och hemlig teleövervakning kan verkställas. I propositionen framhålls att meddelandet skall levereras till polisen i klartext om det är teleoperatören själv som tillhandahåller ett krypteringssystem, och har möjlighet att dekryptera meddelandet. Däremot togs i propositionen inte ställning till frågan vad som skall gälla betäffande kryptering i övriga fall, dvs. när det är någon annan än teleoperatören som tillhandahåller krypte-

ringsprogrammet. Det sägs i propositionen att frågorna är komplicerade och måste lösas i samförstånd med andra länder i vår omvärld.

Under lagstifningsarbetet framfördes den åsikten att detta att det finns lätthanterliga krypteringsprogram skulle innebära att tvångsmedlen på teleområdet i en framtid inte kommer att vara lika verkningsfulla som de en gång varit. I propositionen framhöll regeringen att man inte hade för avsikt att mer eller mindre ge upp tvångsmedlen på teleområdet. Men man konstaterade samtidigt att det finns skäl att följa utvecklingen på teleområdet och, bl.a. med hänsyn till teknikutvecklingen, överväga behovet av avlyssning i klartextmomentet, dvs. buggning.

Regeringen har nu också tillsatt en utredning för att utreda olika frågor om hemlig teleavlyssning, bl.a. *buggning*. Buggning är ju som ni alla vet inte tillåtet idag och polisen har alltså inga lagliga möjligheter att bugga. I direktiven till utredningen (Dir 1996:64) sägs att utredaren förutsättningslöst skall utreda frågan om användning av buggning som polisiär arbetsmetod. Jag vill framhålla att det är en förutsättningslös utredning; utredaren måste svara ja på tre frågor innan han går vidare och undersöker vad slags regler som krävs: 1) finns det behov av buggning? 2) är buggning en effektiv metod? 3) finns det utrymme för buggning om man väger in intresset av ett starkt skydd för den personliga integriteten?

Behovet av buggning skall belysas mot bakgrund av möjligheterna att inhämta motsvarande information på något annat sätt, t.ex. genom hemlig teleavlyssning och hemlig teleövervakning.

I direktiven ställs frågan om möjligheterna till informationsinsamling genom dessa tvångsmedel har försämrats de senaste åren. Även så kallade motmedel mot buggning skall belysas av utredningen. Dessa formuleringar tar bl.a. sikte på vilken inverkan förekomsten av kryptering kan ha på hemlig teleavlyssning och hemlig teleövervakning. Utredningen skall avsluta sitt arbete före den 1 mars 1998.

När det gäller *husrannsakan och beslag* är en av de situationer som är av intresse när man talar om kryptering den när polisen bereder sig tillträde till en bostad eller ett kontor för att komma åt uppgifter som finns i en dator och finner att informationen i datorn är krypterad.

Frågan om beslag och husrannsakan i IT-miljö är aktuella på Justitiedepartementet. Frågorna är komplicerade och vi är ännu inte helt övertygade om bl.a. vilken lagteknisk lösning som man bör välja. Det känns extra angeläget att på detta område ha en reglering som, så långt som det nu är möjligt, kan stå sig över tiden. Tyvärr har arbetet med detta fördröjts men frågorna är prioriterade. Jag vill nämna att vi här inte fokuserar på kryptering; det handlar istället om att anpassa våra regler om husrannsakan och beslag till dagens samhälle.

Det krävs väl inte någon större fantasi för att inse vilken betydelse det skulle få för brottsutredningar om polisen inte kan tillgodogöra sig information i t.ex. en dator på grund av att informationen är krypterad. Kryptering är således en viktig faktor att väga in när det gäller vår ambition att bibehålla effektiva straffprocessuella tvångsmedel. Med de utgångspunkter som jag som chef för Justitiedepartementets processrättsenhet har att beakta är min inställning till de olika problemen tämligen given. Skulle det visa sig i en framtid att tvångsmedlen på teleområdet blir verkningslösa på grund av en utbredd användning av svårforcerade krypton måste vi se till att de brottsutredande myndigheterna får tillgång till informationen i klartext. Detsamma gäller när information som finns t.ex. i en dator och inhämtas via husrannsakan och beslag.

Jag är samtidigt medveten om de problem som en sådan ordning kan innebära. Jag vet att en lösning med nyckeldeposition är kontroversiell. Men som jag har förstått det finns det i dagsläget ingen som förmått att presentera ett alternativ till ett system med deponering av nycklar. Inte heller i det relativt omfattande internationella arbete som pågår på området har det mig veterligen förts fram några andra lösningar. Alternativet skulle då

vara att ge upp tvångsmedlen med de konsekvenser som det innebär, inte bara för möjligheten att utreda grova brott och förhindra t.ex. terroristdåd, utan också för den nationella säkerheten. Ett sådant resultat är knappast godtagbart.

Det jag nu har sagt innebär inte att jag tycker att krypteringsfrågan helt och hållet skall kretsa kring brottsutredningar och polisens behov av information. Tvärtom. Jag är medveten om de enorma fördelar som en säker elektronisk kommunikation har. Jag är också medveten om att det finns starka polisiära intressen som talar mot att krypterad information skall kunna göras tillgänglig i klartext för annan än mottagaren. Det finns också andra områden som Justitiedepartementet ansvarar för, t.ex. upphovsrätten och skyddet för ADB-baserade personuppgifter, där det finns ett starkt intresse av en säker kryptering.

Justitiedepartementet har därför inga problem med att inse vikten av att försöka tillgodose det intresse som finns t.ex. inom näringslivet. Samtidigt är det min förhoppning att näringslivets företrädare på motsvarande sätt inser vikten av att kunna bekämpa t.ex. terrorism och den grova narkotikahandeln. Om vi startar där - med ett sådant ömsesidigt erkännande som utgångspunkt - bör man kunna finna rimliga avvägningar och på ett konstruktivt sätt kunna arbeta fram en bra svensk krypteringspolicy.

Bengt Angerfelt, Rikspolisstyrelsen[2]

A. Ur nationell brottsbekämpningssynvinkel

- Samhällsutvecklingen

Det är viktigt att ett samhälle som i så hög grad tillämpar den nya tekniken måste kunna ta hand om hot och risker på ett acceptabelt sätt. *Det ligger givetvis i allas intresse att skapa förutsättningar för robusta IT-system som är motståndskraftiga mot kriminella angrepp.*

Polisen ställs allt oftare inför det faktum att man behöver eftersöka spår och bevis i IT-system. Det rör sig inte bara om IT-relaterade brott utan snart sagt varje kriminalpolisutredning kommer i kontakt med IT. Vid många typer av brott, t.ex. narkotika- och ekobrott, administrerar man ofta den brottsliga verksamheten med IT-stöd i olika former.

- Brottsprevention

Traditionellt bedrivs brottsförebyggande åtgärder av oss alla bl.a. genom försegling av försändelser, inlåsning av pengar, värdefulla dokument och föremål samt genom information och utbildning. När det gäller framtida *brottspreventiva* åtgärder krävs komplement till traditionella åtgärder. Kryptering kan bidra till att förhindra brott som begås via kommunikationsnäten. Exempelvis försvåra intrång i IT-system eller säkerställa ekonomiska transaktioner så att de inte förvanskas eller genereras av obehöriga. Även när det gäller skydd av den personliga integriteten kan kryptering utgöra ett bra hjälpmedel. Allt större informationsvolymer bärs omkring på datamedia, t.ex. i bärbara datorer, vilket kan utgöra en stor risk för allvarliga informationsläckor vid en ev. förlust av datamediat.

Observera att de synpunkter jag här framför inte är något av myndigheten och rikspolischefen officiellt ställningstagande utan synpunkter lämnade av ett antal, inom polisväsendet, berörda befattningshavare

Även här kan kryptering utgöra ett bra hjälpmedel för att förhindra att obehöriga tar del av informationen.

- Brottsutredande verksamhet

Inom polisens brottsuppdagande och utredande verksamhet utnyttjas en rad metoder som t.ex.:

- Spaning med hjälp av olika metoder
- Husrannsakan
- Hemlig teleövervakning och avlyssning
- Kriminalteknik som t.ex. fingeravtrycks-, DNA-, dokument- och handstilsundersökningar

Hur skall man utnyttja dessa metoder då traditionella skriftliga handlingar och meddelanden försvinner och då pengar och värdehandlingar digitaliseras?

Framtidens spanare måste troligen även spana på "nätet". Bevis- och spårsökning måste göras i IT-miljö. Elektroniska dokuments äkthet måste bedömas med hjälp av nycklar och krypteringsmetoder. Ev. måste även metodernas tillförlitlighet bedömas innan yttrande om äkthet och utställarangivelse kan formuleras.

När det gäller spanings- och avlyssningsverksamheten uppstår det problem då kriminella (eller misstänkta) utnyttjar kryptering. Det gäller bl.a. vid utnyttjandet av tvångsmedlen "hemlig teleavlyssning" och "husrannsakan".

I samband med hemlig teleavlyssning är det lika viktigt att så tidigt som möjligt kunna avföra folk från misstankar som att få information som styrker brottsmisstankar. Krypterade förbindelser försvårar eller kan t.o.m. omöjliggöra polisens möjligheter i dessa fall, vilket inte är acceptabelt.

Detta gäller också hanteringen av beslagtagna datamedia innehållande krypterad information.

- Gemensamt intresse.

Det är inte så, som så ofta framställs, att rättsväsendet och näringslivet har helt olika intressen.

För rättsväsendet är det viktigt att brott kan förhindras men man måste också ha möjlighet att utreda brott.

För näringslivet är det givetvis viktigt att kunna skydda sina intressen men det är också viktigt för näringslivet att det finns ett fungerande rättsväsende.

- Dagsläget

I brottsutredningarna har vi redan stött på problemet med kryptering, om dock i begränsad omfattning. I huvudsak har det varit i samband med husrannsakan och beslag. Det har hitintills inte berett oss några större problem eftersom de krypteringsmetoder som utnyttjats har varit möjliga att forcera. Att det varit på det viset beror troligen på att många utnyttjar programvaror från USA och att dessa är underkastade deras exportrestriktioner och därför inte haft tillräckligt starka algoritmer eller tillräckligt lång nyckellängd. Vi har dock konfronterats med andra krypteringssystem, som numera kan hämtas från "nätet", och som har en nivå som förr bara var åtkomlig för försvars-, säkerhets- och underrättelsetjänster.

- Framtidsutsikter

Polisväsendets brottsutredande verksamhet ställs inför delvis nya förutsättningar:

- Brott kan begås via telenätet utan att gärningsmannen lämnat bostaden.
- Traditionella skriftliga handlingar och pengar ersätts av digitala dokument/pengar.
- Klartext och information skyddad av svaga krypteringsmetoder ersätts av information krypterad med starka krypteringsmetoder. Detta gäller både under överföring (kommunikation) och vid lagring (på datamedia).

- Meningsfullt utnyttjande av vissa tvångsmedel försvåras.

- Ställningstagande.

För rättsväsendets brottsbekämpande verksamhet är det av största vikt att finna en lösning som gör det möjligt att tvångsmedlen "hemlig teleavlyssning", "husrannsakan" och "beslag" kan utnyttjas med avsett resultat även då kryptering utnyttjas.

Observeras bör att det handlar om att bibehålla de tvångsmedelsmetoder som redan finns, men som kan förlora verkan i IT-miljön, under samma förutsättning som tillstånd.

Det är därför önskvärt med någon form av reglering av hur kryptering skall få ske.

Vilken form man skall välja bör utredas närmare. Deponering av algoritm och nycklar är ett sätt. Straffansvar när det gäller vägran att utlämna nycklar, i likhet med straffansvar vid avsaknad av bokföring (bokförings-brott) hos bokföringsskyldig är ett annat, och det finns säkert fler. Det är givetvis viktigt att finna en lösning som står sig även internationellt så att svenska företag och intressen inte hamnar i en sämre konkurrenssituation.

Tvångsmedlet "hemlig teleavlyssning" får endast utnyttjas i fråga om vissa grova brott. En ev. lösning med straffansvar för vägran att utlämna nycklar kan, om nyckeln endast förvaras hos den som är föremålet för avlyssningen, givetvis inte utnyttjas i detta fall. Någon annan form av reglering av kryptering kan bidra till att minska gruppen som måste bearbetas/analyseras för att avlyssningen skall få avsedd verkan.

B. Ur nationella säkerhetsintressens synvinkel

I princip samma frågeställningar och problem som redan beskrivits. Samma lagstiftning styr tvångsmedelsutnyttjandet även i detta fall.

Huvudproblemen ligger i att särskilja relevant information ur en stor mängd krypterad information. När det gäller utformningen av ev. ny eller förändrad lagstiftning måste man beakta den kryptering som avser totalförsvarssekretess och för vilken speciella regler gäller vad avser behörighet, utrustning och nyckelhantering.

C. *Internationellt polisiärt samarbete.*

- Interpol

När det gäller Interpols europaregion så har frågan just väckts i den arbetsgrupp som arbetar med IT-relaterad brottslighet. Bland de frågor vi arbetar med ingår bl.a. förslag på utredningsmetoder. I samband med detta har flera länder rapporterat att man ibland påträffar krypterad information som behöver dekrypteras och tills vidare har vi bara föreslagit att utredaren skall kontakta expertis inom området. I gruppen uttrycks dock oro för en spridning av de starka krypteringsmetoder som nu finns tillgängliga och vad ett ökat nyttjande bland brottsmisstänkta kan komma att innebära.

- Europol

Enligt tillfrågade svenska representanter inom Europol i Stockholm och Haag har frågan inte diskuterats.

- EU

Svensk polis har en representant med i arbetet, inom tredje pelaren, med teleavlyssningsfrågan. De frågor som behandlas där rör teleoperatörernas roll i samband med utnyttjandet av tvångsmedlet avlyssning. Man har ej tagit upp krypteringsproblematiken vad avser kryptering utanför teleoperatörernas roll, dvs. då användarna av teletjänster själva utnyttjar kryptering innan det skickas ut på nätet.

FINANSEKTORNS INTRESSEN OCH FRÅGESTÄLLNINGAR

Hans Peterson, Östgötabanken tillika ordförande i Bankernas IT-säkerhetsgrupp

Rubriken på detta seminarium är " Inför en svensk policy för säker elektronisk kommunikation" . Vi har hittills pratat väldigt mycket om kryptering, som ju används i många fler sammanhang än kommunikation." Inför" kan man om man vill utläsa som en uppmaning: " Inför en policy!" Men skall vi införa en policy eller inte? Jag är ärligt talat inte så säker på att det är helt nödvändigt eller ens bra. Men vad är då banker i det här sammanhanget, och vad har banker och IT med varandra att göra?

Bankerna har tidigt varit igång med att använda datorer, datakommunikation och liknande. Såvitt jag vet var Kreditbanken den första bank som datoriserades i Sverige. De skaffade sig en så kallad automatisk räknemaskin 1958. Jag vet att vi i Östgöta Enskilda Bank började med vår databehandling 1959, då vi köpte en väldigt stor dator - den hade ett primärminne på hela åtta K, vilket var mycket stort på den tiden. Själv har jag inte hållit på riktigt lika länge med IT. Jag skrev mina första kodrader 1973.

"Banksystemet" - banker *är* IT

- **Betalningar**
  - inom och utom Sverige via svenska och internationella system
  - olika valutor och metoder
- **Placering och finansiering**
  - in- och utlåning av olika slag
  - med hjälp av konton, värdepapper eller andra värden
  - hantering av säkerheter, både in och ut
- **Trading**
  - värdepapper, valutor, derivat etc
  - ett flertal marknadsplatser och system
  - aktörer inom och utom bankvärlden

Till skillnad från i andra företag kan man säga att i banken är det IT som är företaget. I vilket annat företag som helst har de en produktionsprocess, de gör lastbilar eller klädhängarekrokar eller skruvar eller vad de håller på med för någonting. De har en produktionsapparat, de har leverantörer,

det kommer in material som bearbetas, och produkterna lagerhålls och säljs så småningom.

När det gäller banker sker allt detta i princip inne i våra datorer. Istället för att skugga verksamheten i ekonomisystem så utgör ekonomisystemet verksamheten - det vill säga svarvarna, maskinerna, transportapparaten, råvaran, produkterna är IT i bank. Där finns en stor skillnad mot annan slags verksamhet.

Vad är det då vi gör? Ja, traditionellt sett har banker tre uppgifter.

Det ena är att flytta värden i rummet, det brukar vi kalla för betalningsförmedling. Det innebär att vi flyttar pengar eller värden i olika steg, mellan konton, mellan företag, inom och utom Sverige, via svenska och internationella system. Vi använder oss av girosystem, kontosystem, clearingsystem med mera. Vi använder olika valutor, vi använder olika metoder, de är både IT-baserade och fysiska, vi flyttar pappersdokument och datafiler. Allt mer och mer blir IT i det här sammanhanget.

Den andra produktgruppen är när vi flyttar värden i tiden, det vill säga du kan disponera din framtida inkomst redan idag (låna) eller du kan lägga undan din inkomst för att disponera den i framtiden (spara eller placera). Det finns olika tekniker för det. Man kan spara på konton eller låna på konton. Man kan spara i värdepapper eller låna genom att ge ut värdepapper. Den som lånar måste lämna en säkerhet, den som lånar ut vill ha en säkerhet. Ibland litar man på banken och sparar utan att begära säkerheter, ibland kräver man att få en pant, särskilt när man placerar mycket pengar.

Det tredje arbetsområdet för banker är att konvertera värden mellan olika sorter. Vi växlar D-mark mot dollar, mot pund, mot svenska kronor, i framtiden mot euro, vad det nu blir för någonting. Vi mäklar affärer med värdepapper av olika slag, inte bara med enskilda värdepapper utan också

med derivat (optioner, terminer etc). Det här sker över ett stort antal marknadsplatser. De två största marknadsplatserna för värdepapper i Sverige är OM och Börsen, men det finns andra marknadsplatser också, både inom och utom Sverige. Svenska banker agerar på i stort sett alla större börser runt om i världen. Aktörerna på dessa marknadsplatser finns både inom och utom bankvärlden. På den svenska penningmarknaden, till exempel, är flera av de riktigt stora aktörerna inte banker utan transnationella företag.

Ett banksystem ger en ganska så komplex bild och här krävs naturligtvis säkerhet från väldigt många olika utgångspunkter.

Varför kryptering i bank?

- *Lagkrav*: Skydda kundernas - och bankens - värden och information
- *Lagkrav*: Skydda kunders och anställdas integritet
- *Lagkrav*: Bevara banksekretess
- Eget intresse: Bevara företagshemligheter

Kryptering är en av de komponenter banker använder för att bygga upp skydd. Det finns ett antal motiv till dessa olika skydd. I en del fall är det så att vi är skyldiga enligt lag att utföra ett skydd.

- Vi är skyldiga att skydda insättarnas värden, bankens egna värden och insättarnas information. Det framgår av bankrörelselagen. En bank har en enda skyldighet här i världen till skillnad från andra företag och det är att ta emot inlåning. Vi är inte skyldiga att göra något annat. Om någon kommer till oss och vill sätta in sina pengar så måste vi ta emot dem, och det är grunden för bankens oktroj, dvs. tillståndet att bedriva bankverksamhet. Oktroj får vi om vi på ett säkert sätt kan visa att vi kan skydda insättarnas medel.

• Vi är också enligt till exempel datalagen skyldiga att ta hänsyn till personlig integritet. Det framgår också av bankrörelselagen och av annan lagstiftning.

• Vi har också enligt bankrörelselagen ett sekretesskrav på oss. Vi har i Sverige världens äldsta banksekretesslagstiftning. Den är formellt sett väldigt stark, reellt sett är den inte fullt lika stark, men som den är skriven så är den vår starkaste sekretessbestämmelse i Sverige.

• Slutligen har vi ett eget intresse av att bevara företagshemligheter. Där kan vi säga att vi har lagens stöd, men inte lagens krav, genom till exempel lagen om företagshemligheter, genom de kollektivavtal som vi har och genom de möjligheter kollektivavtalslagen ger att tillämpa de här avtalen.

Kryptering är ett utomordentligt verktyg för att bygga goda skydd för dessa olika intressen.

Beredskap inför kris och krig

- Kris/krig ökar kravet på skydd
- Beredskapen kräver, enligt bl a ÖCB:
  - robusta system och rutiner
  - förberedda för kris/krig redan i fred
  - ev. alternativ planerade och testade
- Tillfredsställande kryptering måste därför finnas redan i fred om den behövs i krig!

Samhället har intresse av att betalningsväsendet - det finansiella systemet - alltid fungerar. Det innebär förutom normalläget - fred - också kris- och krigssituationer. Skulle det bli kris eller krig behöver vi kunna skydda transaktioner, värden etc i större utsträckning än normalt.

Tyvärr är det svårt att upprätthålla den skyddsnivå vi har i fredstid om det skulle hetta till, så samtidigt som kraven ökar så kommer vår förmåga att uppfylla dem att minska. ÖCB och andra säger till oss att vi måste ha så robusta system och rutiner att funktionen upprätthålls även om det är

kris och även väldigt långt in i en krigssituation. Alternativ skall vara planerade, och de skall också vara testade.

Det betyder att om vi har behov av till exempel kryptering som skyddsmetod i en krigssituation måste vi faktiskt ha den installerad och fungerande redan i fred. Det här gäller inte bara banker. Det gäller alla K-företag, alla myndigheter och ett stort antal andra aktörer på andra marknader också.

Vad används kryptering till?

- Säker identifiering - på avstånd
- Säker lagring och bearbetning av information
- Säker överföring av information

Enklare fråga: När använder banker *inte* kryptering?

Banker använder kryptering i många olika sammanhang. Vi har i källaren ett antal hårdvaruburkar som står och tickar för olika ändamål, vi har diverse program installerade, och man kan säga att kryptering används i princip i tre olika situationer i vår del av världen.

- Det första området är relativt nytt, det är någonting som kanske kommer i praktiken under 1997 om allt går som det skall. Det handlar om elektroniskt ID-kort, och vi hoppas att därmed kunna identifiera människor på avstånd på ett säkert sätt. Att identifiera människor över disk, speciellt om vi känner dem, är inte särskilt krångligt, men när någon sitter vid sin dator någonstans i världen och vill göra saker på sitt bankkonto måste vi vara säkra på att den vi har att göra med är den person som har rätt att disponera kontot, och att säkerställa det är inte så enkelt. Tekniken som vi anser oss behöva bygger på kryptering.

- Vi använder naturligtvis också kryptering i samband med lagring och bearbetning av information för att säkerställa ett antal saker som jag kommer till senare.

- Det som vi kanske har pratat om mest idag, men som kanske inte är den tyngsta biten ur svårighetssynpunkt, det är överföring, dvs. när vi skickar data mellan datorer.

Det är kanske enklare att fundera över när vi inte använder kryptering, för det är antagligen i betydligt färre fall än när vi gör det.

Säker identifiering - på avstånd

- Kräver stark, asymmetrisk kryptering
- Användaren skall vara bunden till ett unikt nyckelpar - på ett säkert sätt
- Ingen annan skall kunna använda hemligheten - någonsin
- Den öppna nyckeln skall kunna kontrolleras på ett säkert sätt

För att kunna identifiera någon krävs det att man har användaren - den man vill identifiera - säkert bunden till något unikt. I det här sammanhanget använder vi den hemliga delen av ett nyckelpar som vi låser in på ett sådant sätt att det bara är användaren själv som rimligen har möjlighet att komma åt den. För att kunna göra den här identifieringen på ett säkert sätt krävs att man använder en mycket stark asymmetrisk krypteringsteknik.

Identifiering på detta sätt kan man använda sig av i många olika sammanhang, exempelvis för att identifiera sig för ett system, för att signera ett elektroniskt dokument eller liknande.

Det som är väldigt viktigt i sammanhanget är att ingen annan person någonsin skall kunna använda sig av den hemliga nyckeln för något annat ändamål. Den enda som skall kunna använda den är den som vi avser att

identifiera, alltså den som hemligheten är utlämnad till. Finns den tillgänglig hos någon annan är det inte fråga om säker identifiering längre.

Det är naturligtvis viktigt att den öppna, icke hemliga nyckelhalvan går att kontrollera på ett säkert sätt av den som vill verifiera identiteten. Då använder vi också kryptografiska metoder för att säkerställa att den öppna informationen inte har förändrats när vi tar del av den för att verifiera en identitet.

Säker lagring och bearbetning

- Endast behöriga skall kunna läsa, tillföra eller ändra information
- Obehöriga skall inte på något sätt kunna läsa, tillföra eller ändra information
- Information skall vara aktuell, korrekt och fullständig nog för ändamålet

Det är inte bara för att gömma hemligheter utan också för att säkerställa sådant som är öppet som vi använder oss av kryptering. Detta är de traditionella sårbarhetsbegreppen i lite annorlunda tappning:

- De som är behöriga skall kunna göra vad som helst utan några särskilda svårigheter.
- De som är obehöriga skall inte kunna göra någonting, hur de än anstränger sig.

Därmed har vi kontroll över att det bara är behöriga som har möjlighet att läsa, ändra eller tillföra information. Vi har också därmed en grund för att uppnå någon slags informationskvalitet, det vill säga:

- Den information vi har är inte för gammal, den är riktig i någon mening och den är så fullständig att den kan användas till det ändamål som den är framtagen för.

Detta är klassiskt, och för att kunna säkerställa dessa egenskaper finns olika nivåer av kontroll- och styrsystem. Men framför allt spelar kryptering en stor roll för att stänga obehöriga ute och förhindra ändringar som vi inte är intresserade av.

Säker överföring

- Informationens egenskaper skall inte röjas eller ändras under transport
- Information skall alltid komma fram
  - i tid
  - till rätt plats
- Ingen oönskad information skall kunna tillföras via överföringen

Det tredje området är säker överföring.

- Den som inte har rätt att få del av informationens innehåll och egenskaper skall inte kunna få del av dessa, vilket kanske låter självklart.

- Informationen skall alltid komma fram i tid och till rätt plats. Där har vi ingen hjälp av kryptering, snarare tvärtom - kryptering kan ställa till det rejält i de här sammanhangen, om man är oskicklig.

- Men den tredje punkten, där har naturligtvis kryptografiska metoder stor betydelse för att säkerställa att den information som kommer fram är precis den som avsändaren avsåg att skicka eller att den information som vi hämtar är precis den vi avsåg att hämta.

Dagsläget för kryptering

- Kryptering är fri, än så länge - inom Sverige
- Exportrestriktioner försvårar tillgång till krypteringsteknik - men det lättar efter hand
- Olika länder har olika policy
- Svenska banker kan inte skydda sina hemligheter effektivt - utanför Sverige
- "Key Escrow" diskuteras som lösning - ja, på vad, egentligen?

Att bankerna har stort behov av kryptering tror jag är tämligen klart för de flesta, och vi har väl fått det bekräftat genom den diskussion som har varit tidigare idag att dagsläget ser ut på det här sättet.

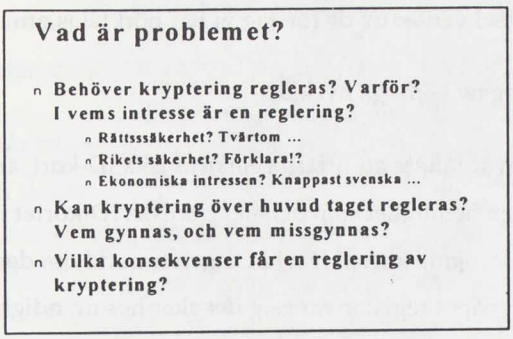
- Krypteringen är fri, än så länge, inom Sverige.

- Vi har problem med exportrestriktioner, det vill säga vi får inte alltid tag på den teknik som vi vill ha på det där enkla sättet att vi köper en produkt, utan vi måste sitta och hacka själva om vi vill ha den. Vi tror att det lättar efter hand. Den aviserade « lindringen« av de amerikanska exportrestriktionerna, om det nu är det, kan medföra möjligheter att få tag på lite bättre produkter. Frågan är om det är värt priset, det vet vi väl inte.

- Vi kan konstatera att olika länder har olika policy. Det är intressant att se hur amerikanerna har så total frihet hos sig själva, medan de försöker lägga locket på hos alla andra. Det är rätt festligt egentligen.

- Vi tycker nog att vi som svenska banker kan skydda oss ganska så bra - inom Sverige. Vi kan lägga på i stort sett de skyddsåtgärder vi vill, även om vi kanske inte har de bästa metoderna, men de av oss banker som har mycket verksamhet utomlands har klara problem när det gäller att skydda sin verksamhet, sina egna intressen och sina kunder just utomlands. Vi kan inte uppnå riktigt samma skyddsnivåer, inte överallt i alla fall.

- Det som har dykt upp i diskussioner på senare tid det är att man skall kunna lagra undan hemliga nycklar i särskilda förvaringsinstitut, och det ser man som en lösning. Det är intressant att det är en lösning, men på vad? Jag inser inte problemet, trots vad jag har hört hittills idag. Och det beror kanske på att jag inte förstår, det erkänner jag villigt.



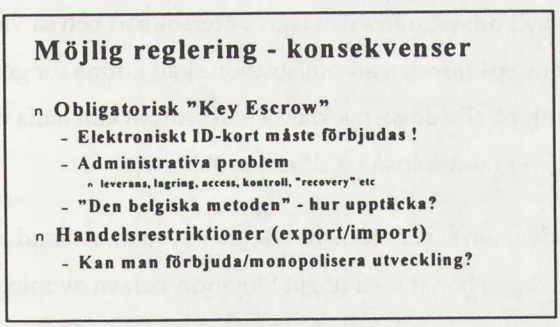
När vi har diskuterat det här i bankerna har vi frågat oss varför det behöver krypteringsregleras över huvud taget. Det finns ett antal synpunkter, vi har hört några av dem nu, men i vems intressen är de?

- Vi är inte säkra på att rättssäkerheten gynnas av reglering. Blir det så att vi skall lagra undan hemliga nycklar utanför vår egen kontroll kan det faktiskt bli så att rättssäkerheten urholkas, och det är inte så kul.

- När det gäller frågeställningar kring rikets säkerhet så kanske vi inte skall förstå dem ens, men någon form av begriplig förklaring bör vara intressant att presentera.

- De ekonomiska intressen man kan skydda med hjälp av en reglering är inte de svenska, möjligen de amerikanska.

Det kan som synes vara lite svårt för oss banker att förstå, att det verkligen skall vara så viktigt att vi genomför en reglering, speciellt om den innebär restriktioner för användning av stark kryptering.



Vad ser vi då för konsekvenser av de förslag vi har hört talas om.

Det ena är deponering av hemliga nycklar.

Det som vi inser, som är tänkta att utfärda elektroniska ID-kort, är att om vi måste deponera den hemlighet som det elektroniska ID-kortet innehåller kan vi lika gärna förbjuda kortet. Det har ingen framtid om den hemligheten skall lagras i något register vare sig det sker hos myndighet eller i en kommersiell tjänst. Ingen bank i Sverige kommer att utfärda eller acceptera elektroniska ID-kort om utfärdaren eller kunden måste lagra denna typ av hemligheter någonstans. Produkten är helt enkelt stendöd.

Vi får ett antal administrativa problem. Jag kan ge lite storleksordning på det hela om ni vill. Östgöta Enskilda Bank är en ganska liten bank och vi har ett datanät med femtio noder, ett litet datornät. Vi skyddar trafiken mellan noderna, och vi använder den teknik som Viiveke Fåk beskrev att med hjälp av asymmetrisk kryptering kryptera symmetriska nyckelpar som med oregelbundna intervall förs över till noderna för att användas vid kryptering av trafiken mellan två noder fram till nästa bytestidpunkt. För att kunna läsa meddelandet måste man ha tillgång till den nyckel som användes vid själva överföringen. Vi har byggt upp vår teknik på ett sådant sätt att vi byter minst 29 400 nycklar varje dygn i vårt lilla nät. Om de skall lagras med rätt tidsstämplingar så blir bara vår lilla bank ett stort problem. Om man då tar en bank med cirka fyrahundra kontor så kommer de under samma förutsättningar att byta knappt två miljoner nycklar varje dag som skall tidsstämplas och lagras återsökbart och så vidare. Jag funderar lite grann på hur den administration skall kunna fungera som kan hålla ordning på alla dessa nycklar och dessutom kan hålla dem hemliga. Jag har ingen praktisk lösning på det problemet.

Det finns ju länder som säger att de har det här systemet, bland annat Frankrike har nyligen börjat med något liknande, och en av mina kolleger har frågat en belgisk kollega hur de hanterar situationen. De har ju stora

flöden av information mellan Belgien och Frankrike, och den här killen sade ungefär så här:

- Ja, man får en nyckel av oss en gång i månaden ungefär, men vi byter ju oftare, och skulle de komma på oss så kommer vi att be om ursäkt.

Handelsrestriktioner är något som USA försöker tillämpa, och frågan är ju egentligen vad det leder till. Är man den starkare parten så kan man ju på samma sätt som med höga tullmurar möjligen nå någon form av ekonomisk fördel av det på kort tid, men vi i Sverige har ju alltid kämpat för frihandel, och egentligen leder ju handelsrestriktioner till att man försöker monopolisera utvecklingen - eller egentligen förbjuda utveckling i andra länder. Frågan är vad det kan vara värt. Jag återkommer till det där med handelsrestriktioner om ett par minuter.

Möjlig reglering - konsekvenser

- **Förbud mot "stark" kryptering**
  - **Elektroniskt ID-kort måste förbjudas !**
  - **Hur upptäcker man överträdelse?**
- **Förbud mot gränsöverskridande kryptering**
  - **Transnationella företag?**
  - **Affärsresor, turism?**
  - **Internet?**
  - **Radio, TV, upphovsrätt?**

Man kan också tänka sig att man förbjuder stark kryptering. I enlighet med vad jag sade tidigare kan man i så fall glömma det här med elektroniskt ID-kort. Den intressantaste frågan är kanske hur man upptäcker om någon bryter mot förbudet genom att exempelvis kryptera först och sedan kryptera igen. En annan variant som också har diskuterats är att man skulle tillåta stark kryptering inom Sverige men om man går över gränser förbjuder man. Men det hjälper inte våra transnationella företag typ ASEA, Ericsson, SAAB, Volvo och allt vad de heter. Vi får problem i samband med affärsresor och turism. Redan idag vet jag inte om jag skulle våga ta med mig min PC utomlands när jag åker någonstans just med tanke

på att jag kan trampa i något klaver när det gäller vad den innehåller. Internet är ett annat område som är svårt att överskåda. Jag kan inte vara säker på att informationen inte slinker iväg någonstans där den inte får vara krypterad.

Vi kommer också in på de frågor som vi nätt och jämnt har berört här, som har att göra med satellitkommunikation, massmedia, upphovsrättsskydd och sådana saker. Om man förbjuder kryptering så innebär det också att man inte heller kan skydda upphovsrätten i multimedia- och IT-världarna.

Det enda vettiga?

- Fri användning av kryptering i Sverige
- Inga (egna) svenska exportrestriktioner
- Domstol kan i särskilda fall kräva klartext från den som krypterat - som idag
- Kommersiell "Key Escrow" i Sverige kan erbjudas transnationella företag som alternativ till lagring utomlands (kräver avtal med länder som har lagringskrav)

Efter att ha diskuterat från den ganska enkla utgångspunkt som vi har i bankerna, låt oss skylla på vår dåliga kunskap i det här sammanhanget, så har vi kommit fram till att detta antagligen är den enda vettiga policyn - om man nu skall ha en policy.

• Det finns ingen känd och logisk anledning att reglera krypteringen i Sverige. De polisiära skäl som skymtat i debatten har två sidor - för och emot fri och stark kryptering - och detta gäller även de rent kriminalpolitiska skälen. Man kan dessutom undra varför inte den svenska polisen tror sig klara av det som den amerikanska polisen tvingas klara av i en situation där möjligheterna att få tag i stark kryptering är betydligt enklare och där dessutom problemen antagligen är betydligt större.

• Vi tycker inte att man skall ha några egna svenska exportrestriktioner. Observera, köper jag en produkt så är det klart jag får acceptera villkoren vid försäljningen. Köper jag en amerikansk produkt och de säger du får inte använda längre nycklar än fyrtio tecken, då använder jag inte längre nycklar än fyrtio tecken. Men det betyder inte att min policy skall vara att jag inte får använda nycklar längre än fyrtio tecken vid kryptering överhuvudtaget, det är en helt annan fråga.

• Idag har vi ett regelverk kring domstolars rätt att kräva klartext i olika sammanhang. Jag inser att det finns problem med vissa typer av spaning. Samtidigt inser jag att det finns resurser för att hantera det här i samhället, och det här är ju ett regelverk som finns redan idag.

• Vi har länder som kommer att ha andra policys: Frankrike, Ryssland, möjligen Storbritannien, troligen inte Danmark. (Danmark förresten, de skulle ha ett medborgarkort som ni kanske vet. De skall inte det längre på grund av det internationella motståndet mot stark kryptering.) De länder som då anser att man skall lagra nycklar någonstans kan man ju komma överens med om att vi får lagra nycklarna i Sverige istället. Då kan man bygga upp kommersiella tjänster i Sverige som kan tillhandahålla nyckeldeponeringstjänster på frivillig basis för de företag som har behov av det för att kunna fungera i andra länder. Men att som sagt vi skulle göra något sådant obligatoriskt i Sverige är det väldigt svårt att förstå de bärande motiven för, i varje fall för oss från bankerna.

Göran Ernmark, Posten AB

Posten kan skriva under på det mesta av Bankföreningens synpunkter, som Hans Peterson nyss presenterat, när det gäller den bankmässiga delen av vår verksamhet. Möjligen har Postgirot ännu så länge inte fullt så stora problem, som den samlade bankverksamheten i Sverige har, men vi är på väg mot det hållet allihop. Jag tänker därför hoppa över dessa aspekter och istället vidga perspektivet och prata om tjänsteföretagens situation i det här sammanhanget. Vi har tidigare idag hört en hel del ur industriföretagens perspektiv.

Dagens ämne, krypteringsteknik, handlar från tjänsteföretagens horisont väldigt mycket om *förtroende.*

Förtroende och tilltro till att våra nya elektroniska system uppfyller kraven på funktion och säkerhet. Det här är inte i första hand tekniska krav utan det är frågan om de värderingar, de uppfattningar som våra kunder, våra konsumenter och användare har om de här systemen. De kan vara sanna, de kan vara falska: det spelar inte så stor roll. I tjänstesammanhang är det ju vad kunderna tycker som betyder något, inte hur produkten faktiskt ser ut, till skillnad från en fysisk produkt. Den kan man ju undersöka och på något sätt objektivt konstatera kvaliteten eller egenskaperna i.

Förtroendefrågan blir för mig väldigt viktig i en situation när vi står inför att byta system eller byta produktionsteknik. Vi har väldigt många system igång som konsumenterna och kunderna litar på därför att de har funnits under lång tid, och de har utvecklats under väldigt lång tid. Ta brevsystemet som exempel eller Postgirot. Om man går in och gör en analys av olika moment där utifrån de krav vi idag ställer på säkerhet i *nya* system kan vi konstatera att de kanske inte uppfyller de krav som vi i dag skulle ställa, men folk är vana vid dem, folk litar på dem, de har visat sig fungera

i praktiken under lång tid. Alltså är de säkra i någon bemärkelse. När vi nu går över i en ny produktionssituation och skall använda elektroniska medier för att göra samma sak, då höjer vi säkerhetskraven oerhört mycket och det är det som jag då kallar för förtroende.

Man kan ta något litet exempel för att belysa detta t ex från bankvärlden. Vi har vant oss vid kortbetalningar, de har fungerat på ett visst sätt i början med pappersnotor, sedan har vi successivt gått över till elektroniska system för att samla in transaktionerna. När vi går över till Internet konstaterar man väldigt snabbt - det är för osäkert, det går inte. Frågan är i praktiken, hur stor är skillnaden mellan det som kan hända i Internetsystemet och det som kan hända i det gamla manuella systemet? Det har vi inte analyserat så särskilt mycket, men konsumenterna har väldigt snabbt bibringats den uppfattningen att Internetbetalningar via korttransaktioner, där är tekniken just nu för dålig. Vi är på väg och fixa det också just genom att höja den tekniska säkerhetsnivån väldigt kraftigt.

Vad är Postens roll i det här sammanhanget? Ja, vi är på väg från manuella system och pappersbundna system in i elektroniskt baserade system. Vi kan t.ex. ta elektronisk handel som ett närliggande intresse, det är den som driver väldigt mycket av den här diskussionen och utvecklingen just nu. (Principbild visad men ej medtagen i detta referat). Elektronisk handel består av en hel kedja av system som skall fungera tillsammans för att vi skall få ett elektroniskt handelssystem. Det innehåller väldigt många och olika transaktioner, man blir nästan förbluffad när man ser hur mycket transaktioner som ingår i totalsystemet. Jag tänker inte gå igenom bilden utan det är bara en illustration av hur många delfunktioner och moment som ingår. Hur många hundra transaktioner innehåller det här innan det är färdigt? Det här ser ju väldigt komplicerat ut när vi ritar upp det på det här sättet. I det gamla manuella systemet har vi fått det att fungera utan

alla dessa säkerhetssystem därför att det är uppbyggt under lång tid och på något sätt så har vi tilltro till det system vi har.

Nu skall vi alltså ersätta det gamla systemet med ett elektroniskt system (bild visad men inte medtagen i detta referat) och då är vi tillbaka till de frågor som flera andra har pratat om idag: enkla frågor egentligen som är självklara i det gamla. Pratar man med någon i telefon så skapar man en relation och rösten är en tillräcklig identifikation i många fall för att man skall förstå vem det är och så vidare. Nu byter vi personlig identifikation mot olika elektroniska moment och system för säker identifikation som vi måste ordna.

Förtroendefrågan, jag kommer tillbaka till den hela tiden, är alltså oerhört viktig när vi skall gå över till och bygga upp den här typen av system. Om vi inte får dem som skall använda systemet att lita på att vi som tjänsteleverantör kan tillhandahålla ett tillräckligt bra och säkert system, då kommer man inte att gå in och använda det. Eftersom det är tjänster vi pratar om, är det ju inte hur det tekniskt ser ut och hur vi skulle kunna bevisa saker och ting som har betydelse, utan det är hur man uppfattar saker och ting.

Därmed kommer jag in på dagens huvudfråga, hur kan man skapa eller förstöra det här förtroendet? Om vi i Sverige utvecklar en marknad och bygger upp system som vi tycker är bra, ligger det nära till hands att någon annan vill ta sig in på svenska marknaden med andra system. Risken finns att dessa då kan hävdas vara bättre, till exempel genom längre nyckellängd i krypteringen eller vad det nu kan vara för någonting. Då är det väldigt lätt att misstänkliggöra det svenska systemet eller Postens system eller vems det nu är för att på det sättet skapa sig en tjänstemöjlighet. Vi som är tjänsteleverantörer på det här området ser ju framför oss att det finns intressanta affärer som kan göras genom att driva sådana här system

och hantera transaktioner och därigenom få ytterligare affärer. Om vi har rätt i den tron så är det klart att det är intressant för andra att spela på den här marknaden och om vi då inte har tillgång till samma typ av säkerhetshöjande teknologi eller system, som finns till exempel i USA, då finns en stor risk att vi inte kan driva systemen i Sverige. Det kommer kanske amerikanska leverantörer som sätter upp sina drifttjänster i USA, kommunikationen är ju enkel. Man kan tekniskt sett köra sådana här system t. ex. från USA lika väl som från Sverige. Genom att lägga servern i USA och utföra funktionerna där, kan man använda den bättre teknik som av legala skäl eventuellt bara kommer att finnas där. Då kan jag se framför mig ett stort handelsproblem om vi hamnar på t. ex. en annan säkerhetsnivå än de stora konkurrentländerna i det här sammanhanget. Ur vår synpunkt sett är det alltså viktigt att vi kan driva och marknadsföra system på en svensk bas och att vi inte tvingas driva dem från någon slags utländsk bas. Kan vi inte det vet jag inte riktigt hur vår konkurrenskraft ser ut i framtiden.

Sammanfattningsvis: Vi ser tillgång till krypteringsteknik och krypteringsmöjligheter som en viktig konkurrensfaktor i framtiden. Det är naturligtvis inte tekniken i sig som är viktig utan möjligheten att påverka kundernas förtroende och utöva handelshinder från dem som sitter på tekniken. Lösningen på det problem vi diskuterar här idag är en balansgång mellan olika intressen. Vårt bidrag till diskussionen, utöver vårt instämmande i vad andra sagt, är att det måste tas stor hänsyn till de svenska tjänsteföretagens möjligheter att i framtiden kunna konkurrera från en svensk bas. Tillgången till krypteringsteknik får inte tillåtas vara en väsentligt avgörande faktor.

INDIVIDENS INTEGRITETSSKYDD

Louise Yngström, Institutionen för Data- och systemvetenskap, Stockholms universitet

Individens krav på rättsäkert integritetsskydd i samband med kryptering.

Anledningen till att jag överhuvudtaget kom in på IT-säkerhetsområdet var just frågeställningar kring den personliga integriteten i IT-samhället. Jag, som många andra yrkesverksamma inom ADB-området, såg framför mig IT-samhällets möjligheter för alla - inte bara för företagen utan också för individerna - att få ett framtidsorienterat och intressant samhälle med stora utvecklingspotentialer. Men jag såg också de hot som skulle komma framöver. Därför engagerade jag mig i forskning, och framförallt i undervisning, om IT-säkerhet vid min institution.

Det är ett par saker som frapperar mig när jag lyssnar till diskussioner om krypteringsrestriktioner - jag förstår uppenbarligen inte vilket problem man avser att lösa: Vi hör dagligen om samhällets förhoppningar att IT skall bringa Sverige välstånd och komparativa fördelar; vi läser det i tidningar, vi hör det i radio&TV och vi hör det av politiker. Samtidigt vet vi också att vi inte klarar IT-samhället utan kryptering. Och därför förstår jag inte vilka frågor som avses att lösas i diskussionerna om krypteringsrestriktioner. För mig och många andra, såväl näringsidkare, offentliganställda som ordinarie medborgare, förefaller diskussionerna inte föras utifrån rationella argument.

Vilka skulle de rationella grunderna för enskilda individer vara i IT- samhället? Det torde vara sådana enkla företeelser som rättssäkerhet; att vi skall ha samma rättssäkerhet i IT-samhället som i det konventionella samhället både vad avser samröre med andra enskilda personer och företag, som med myndigheter. När jag säger "samma" rättsäkerhet, innebär det inte att det sker på samma sätt i IT-samhället som i det konventionella

samhället. Andra föredragshållare har tidigare visat hur det gick till igår och hur det går till idag. Det har också presenterats som konventionell teknik och framtidens teknik. Men eftersom framtiden redan är här, tycker jag att det är en fullständig självklarhet att vi skall ha tillgång till den tekniken som krävs för upprätthållande av trovärdig rättssäkerhet i IT-samhället.

Det svåraste i att tala för individens krav är förmodligen individens maktlöshet att föra sin talan i denna sak. Näringsliv och myndigheter har både pengar, kunskaper och makt att framställa sina krav. Båda kan dessutom lägga stor tyngd bakom sina krav: näringslivet skall leverera arbetstillfällen och inbringa skattepengar, och myndigheterna skall spara och effektivisera sina verksamheter. Andra berättigade krav kommer från t.ex. Polisen, vars uppgift är att bevara samhället - och till en rimlig kostnad.

Det föreligger inte några skilda krav när det gäller tillgång till trovärdig och säker teknik för rättssäkerhetsändamål mellan individer och näringsliv. Troligen föreligger det inte heller några skilda krav i detta avseende mellan individer och merparten av myndigheterna - Polisen och några andra undantagna. Däremot föreligger det en maktlöshet i att få individers krav framställda, jämfört med övriga nämnda. Jag har inte sett någon politiker - det gängse sättet i moderna demokratier att framställa individers krav - som på egen hand tagit upp denna fråga.

Enskilda individer kan utöva sin makt som konsumenter på marknaden. Jag kan t.ex. byta bank om jag finner att min bank inte sköter mina pengar på ett säkert sätt. Men jag kan inte byta land, om jag finner att mitt land inte sköter mina personliga uppgifter på ett säkert sätt.

Eftersom jag inte kan finna att det finns några motstridiga krav på rättssäkerhet i IT-samhället mellan civila myndigheter, näringsliv och individer, misstänker jag att man inte ställer rätt frågor i sammanhanget.

När det gäller användning av teknik, hör man ofta att sakfrågorna är alldeles för svåra för icke specialister att ta ställning till. Det kan vara ett av skälen till att man inte vågar ta en debatt om individens krav på rättssäkerhet i IT-samhället. Men det går att framställa sakfrågorna så att de kan förstås av lekmän. Problemet blir då att "vanligt folk" gärna uppfattar det som Grönköpingsanda - och det är det kanske? Följande exemplifierar detta förhållande:

> *Den danska facktidskriften DataSikkerhedsBladet använde i november 1996 fingeravtryck som en liknelse för krypteringsnycklar i en artikel som återgav ett "lagförslag". Förslaget gällde förbud mot bruk av handskar: eftersom man inte lämnar några fingeravtryck efter sig som bevis var man varit när man använder handskar, har detta gett problem för Polisen i olika utredningar. Det går att få dispens från handskförbudet, enligt förslaget, om man först lämnar in sina fingeravtryck hos myndigheterna. (Det finns, som bekant, länder där kryptering är förbjudet om inte krypteringsnycklarna inlämnats i förväg till myndigheterna.)*

Med anledning av DataSikkerhedsBladets artikel skrev DN 961205 att den påminde om Grönköpings Veckoblads förslag om att kräva att brottsplatser skall vara väl upplysta för att stävja den tilltagande ljusskyggheten.

Ytterligare ett internationellt exempel på att försöka framställa sakfrågan på ett, för tekniskt okunniga personer, förestående sätt, var en bild i en australiensisk dagstidning våren 1993, i samband med den internationella krypteringsdebatten Clipper Chip. Vid den tiden pågick likaledes internationella påtryckningar från USA att acceptera användning av ett krypteringssystem, där krypteringsnycklar efter lagenliga procedurer kunde hämtas i register och användas för avlyssning. Kryptering med andra former än s.k. Clipper Chip teknik skulle göras olagligt. På bilden ser man en patrullerande polis, som kommer in på polisstationen medförande två vardagligt klädda manspersoner, båda iförda handfängsel. Texten lyder "We found these two persons having a private conversation".

"Vanligt folk" tar sig säkert för pannan och undrar om de har förstått sakfrågorna i krypteringsdebatten. "Så dumt kan det väl ändå inte vara?".

Jo, sakfrågorna i både DataSikkerhedsBladet och i den australiensiska dagstidningen är både rätt uppfattade och korrekt beskrivna. Enskilda individer som privatmänniskor och professionella utövare skall inte tillåtas använda krypteringsfunktionalitet med mer än att orginalnycklar kan återfinnas på annan plats än hos den rättmätige ägaren. På detta vis, hävdar nationalstater världen över, att de skulle främjar och skyddar sina medborgares intressen. Givetvis protesterar näringslivsintressen världen över, medan enskilda individer inte har funnit några kanaler att framföra sina åsikter via. Deras representanter tiger och representanter för civila myndigheter likaså. Alla vet - men ingen vågar säga - att IT-samhällets kejsare är naken.

Om jag ändå skulle drista mig till att försöka föreslå konstruktiva förslag till hantering av problem med krypteringsrestriktioner skulle det vara följande:

Elektronisk handel, såväl nationell som internationell, fordrar tillgång till och utnyttjande av sådan krypteringsfunktionalitet vilken upprätthåller minst samma förtroende mellan individer och handelspartner som dagens procedurer. Det innebär bl.a. att nycklar för autenticering, signering och dekryptering som regel inte kan tillåtas vara utelämnade till olika nationella, statskontrollerade nyckeldeponeringscentraler.

Likaledes måste uppgifter som insamlas, lagras, bearbetas och distribueras av andra än dess rättmätige ägare (dvs. individer i roller som t.ex. medborgare, patienter, skattebetalare, arbetstagare, ägare, kunder etc.), kunna skyddas på minst lika trovärdiga och reviderbara sätt som idag.

Personlig konfidentialitet och anonymitet måste kunna beaktas i IT-samhället.

Procedurer avsedda för kontroll och övervakning av kriminella grupper eller individer skall inte tillåtas inkräkta på den normala individens eller näringsidkarens verksamhet, ej heller tas som ursäkt för krav på sänkt skydd för individuell-, näringslivs-, statlig-, landstings- eller kommunal verksamhet.

Det finns anledning att skilja mellan krypteringsfunktionalitet krävd för kommunikation och krypteringsfunktionalitet krävd för lagring/arkiv. För den senare står det klart att rekonstruktion av nycklar behöver ske, och då på helt annat sätt än för kommunikation.

Sammanfattningsvis anser jag att det krävs

- fri tillgång till och användning av stark kryptering,
- mininala restriktioner avseende export av krypteringsfunktionalitet för säker identifiering, digital signatur och övrig krypteringsfunktionalitet som krävs i ett trovärdigt IT-samhälle,
- att funktioner för nyckelrekonstruktioner i huvudsak skall beslutas med hänsyn till verksamhetskrav snarare än regleras med hänsyn till nationella eller internationella övervaknings- och informationskrav,
- att man söker andra lösningar än krypteringsreglering för kontroll och övervakning av kriminell verksamhet,
- internationell harmonisering och standardisering av krypteringsfunktionalitet.

EXPORTKONTROLL

Magnus Faxén, ambassadör och särskild utredare

Jag tänkte börja med att sätta in frågan om exportkontroll i dess vidare sammanhang och konstatera att under de senaste sex åren så har det internationella samarbetet på exportkontrollområdet intensifieras vad det gäller just högteknologiprodukter som kan användas för både civila och militära ändamål. Sverige deltar nu i alla existerande exportkontroll-arrangemang för produkter och teknologier som kan användas för utveckling av så kallade massförstörelsevapen det vill säga; kärnvapen, kemiska vapen, biologiska vapen och missiler. Regimerna, som de kallas de olika kontrollorganen, har sammanlagt ett trettiotal länder som medlemmar.

Exportkontrollen på "dual use"-området, det vill säga det område som gäller både militära och civila användningar, har en annan karaktär än krigsmaterielkontrollen. Krigsmaterielen är kontrollerad på grundval av ett generellt exportförbud medan handeln med "dual use"-produkter är en handel som i princip är fri, det vill säga frihandel, men känsliga produkter är underkastade en kontroll. Kontrollen är viktig ur säkerhetspolitisk synvinkel. För utförsel av högteknologi och kanske i synnerhet av massförstörelseteknologi som riskerar att missbrukas i ett militärt destabiliserande syfte kan vara allvarligare än ren vapenexport.

Exportkontrollregimerna har medlemmar från som jag sade ett trettiotal länder, främst från den industrialiserade delen av världen. Även inom EU så finns ett särskilt samarbete på "dual use"-området. Medlemsskapet i regimerna medför i och för sig inga juridiska åtaganden men däremot förpliktelser av politisk karaktär. Samarbetet inom regimerna har lett till en ökad internationell samsyn. Vi har en svensk lagstiftning som bekant på

det här området och inom EU finns en förordning som reglerar utförseln av "dual use"-produkter och "dual use"-teknologi.

Den regim som kontrollerar utförseln av produkter och teknologi som kan komma till användning vid tillverkning av kärnvapen kallas för Nuclear Suppliers Group - NSG brukar det stå i tidningarna - och den har funnits ända sedan sjuttiotalet. Den har aktiverats under senare år när det stod klart att Irak var nära att skaffa sig kärnvapen.

Sedan finns det en grupp som kallas för Australiengruppen och den daterar sig sedan 1985. Den var också föranledd av irakiska åtgärder, det var efter det att irakierna hade anfallit kurder med kemiska vapen. Gruppens uppgift är följdaktligen att förhindra utvecklingen av kemiska och biologiska stridsmedel.

Dessutom finns det sedan 1987 en regim som kontrollerar export av produkter och teknologi som kan användas av bärare för massförstörelsevapen, den så kallade Missilteknologikontrollregimen - MTCR. Om ni stöter på det i tidningarna så vet ni vad det handlar om. Sverige har för övrigt haft ordförandeskapet i det arrangemanget under 1995.

Det senaste tillskottet inom exportkontrollregimerna är det så kallade Wassenararrangemanget, Wassenaar från den förort till Haag där man kom överens om att sätta upp detta arrangemang. Där har för närvarande Sverige ordförandeskapet, det är krigsmaterielinspektören Staffan Sohlman som handhar detta ordförandeskap.

Jag skall bara säga några ord till slut om hur kryptofrågorna hanteras eller rättare sagt syftet med kontrollen utav avancerad kryptering. Man kan definiera målen på följande sätt. Det första målet gäller att hindra att terrorgrupper får tillgång till avancerad kryptologi och det andra är att försvåra för organiserad brottslighet att få tillgång till denna kryptologi. Ett tredje mål är att en seriös exportkontroll måste ses som en förtroendeska-

pande åtgärd, det nämnde jag om i morse. Det kan vara avgörande för svensk industris möjligheter att komma över avancerad teknologi att vi har en seriös exportkontroll. Ett sista mål är att svenskägda, seriösa företag skall ha tillgång till avancerad kryptologi.

Egon Svensson, Inspektionen för strategiska produkter (ISP)

Det är den här samlingen av länder som sitter runt bordet i vad som blev COCOM:s uppföljare The Wassernaar Arrangement (WA).

MEDLEMMAR I WASSENAAR ARRANGEMANGET

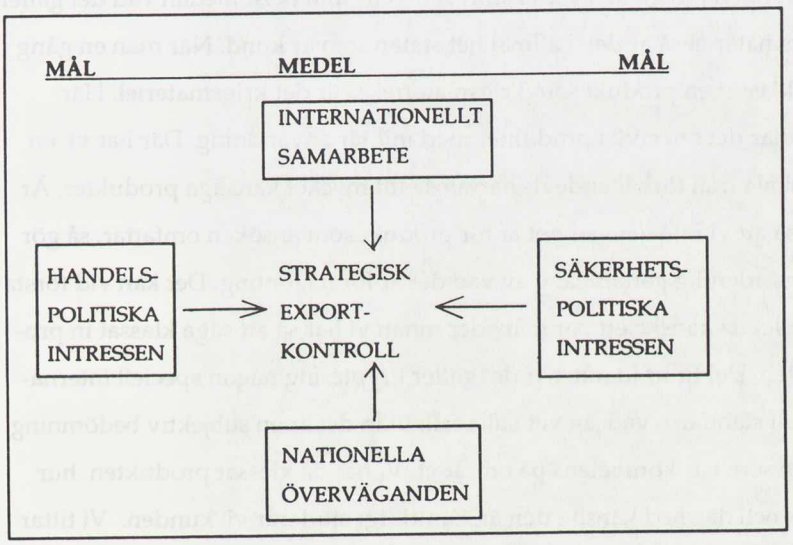
Argentina, Australien, Austria, Beligium, Bulgaria, Canada, Czech Republic, Denemark, Finland, France, Germany, Greece, Republic of Hungary, Ireland, Italy, Japan, Republic of Korea, Luxembourg, Netherlands, New Zeeland, Norway, Poland, Portugal, Romania, Russian Federation, Slovak Republic, Spain, Sweden, Switzerland ,Turkey, Ukraine, United Kingdom and United States

Jag kan som kuriosa berätta att det kändes lite konstigt när Ryssland kom och satte sig vid det f. d. COCOM-bordet, men å andra sidan kändes det nog väl så konstigt för dem. Jag vill gärna nämna att de ryska kollegorna snabbt satte sig in i materialet och var mycket konstruktiva i förhandlingsarbetet. Vi hade kommit överens om att tillämpa den sista versionen av COCOM-listan i övergångsskedet tills förhandlingarna var klara. När vi då kom till förhandlingarna vad gäller kryptering så kan man väl säga att det gruffades lite grann runt bordet, men det rådde dock ingen större tvekan om att kryptering skulle vara med i den lista som trädde i kraft i EU den femtonde november och i Sverige den tjugosjunde december 1996.

Det är dessutom så, att kryptering hör till de områden som vi har kommit överens om att ha en viss transparens inom, dvs. att vi skall på aggregerad nivå redovisa flödet utav krypteringsutrustningar i världen inför varann. Dock med en reservation från några mindre länder att, om det är så att redovisningen avslöjar enskilda företags affärer så förbehåller de sig rätten att inte rapportera detta, för att inte avslöja kundnätet för företaget i fråga.

Var finns då kompetensen på kryptering? Den är inte så spridd som man tror. Det är relativt lätt att lära sig en krypteringsalgoritm och att skaffa sig en uppfattning om hur den rent matematiskt är uppbyggt. Detta finns det läroböcker om, men all den kunskap som är runt omkring som att kunna hantera nycklar, få det att fungera mot andra delar av världen via telenät, osv. är en kompetens som det inte är så många som har. Det är alltså långt ifrån alla som har systemkompetensen. Som jag ser det finns systemkompetens på det här området i USA, Kanada, England, Tyskland, Sverige, Frankrike, Holland, Schweiz och, jag gissar, Ryssland. Vad gäller Ryssland har jag dålig kunskap om deras kompetens, men vad gäller de andra länderna så vet jag att de kan.

Det här är en bild över det kraftfält som ISP befinner sig i. Vi har de



internationella överenskommelserna i botten. Vi har säkerhetspolitiska intressen och det är väldigt lätt att få de flesta att ställa upp på att vi inte skall sprida teknologi som kan då användas militärt och skapa instabilitet i någon del av världen. Här finns också handelspolitiska intressen som att svenska företag får tillgång teknologi och marknader. Vi har internatio-

nellt samarbete där vi kommer överens om vad som skall kontrolleras samtidigt som vi har nationella överväganden om hur detta skall hanteras. Detta är inte en så enkel sits, därför att vi måste göra överväganden om vad svensk industri får exportera utan att veta hur andra länder hanterar samma fråga.

Vi får då och då påpekanden om hur enkelt det är att få tillstånd där och där. Vi har naturligtvis ambitionen att inte lägga större bördor på svensk industri än vad nödvändigt samtidigt som vi har ambitionen att helt och fullt leva upp till våra internationella åtaganden.

Låt mig gå tillbaka till det nationella övervägandet. Hur går det då till hos oss på ISP? Ett företag ansöker om att få exportera något till en kund i något land. Det här är ibland svårare än när det gäller krigsmateriel därför att kunden i fråga kan vara i stort sett vem som helst medan vad det gäller krigsmateriel så är det i allmänhet staten som är kund. När man en gång har klassat en produkt som krigsmateriel så är det krigsmateriel. Här handlar det om civila produkter med militär användning. Där har vi en gråskala från förhållandevis harmlösa till mycket känsliga produkter. Är det så att vi inte vet vad det är för produkt som ansökan omfattar, så gör vi en ordentlig genomgång av vad det är för någonting. Det kan vid första tillfället ta kanske ett par månader innan vi har så att säga klassat in produkten. Det finns ju inte när det gäller kryptering någon speciell internationell standard, vad jag vet i alla fall, utan det är en subjektiv bedömning av de som har kompetens på området. Vi har då klassat produkten, hur stark och därmed känslig den är. Samtidigt studerar vi kunden. Vi tittar då på landet som sådant. Vad är det för land? Är landet med i WA . I vilken bransch är kunden? Hur etablerad är den? Är den känd för oss tidigare? Är vi säkra på att uppgiven användning stämmer? Efter att ha samlat in all tänkbar relevant information så gör vi ett övervägande och beslut fattas. Nästa gång som företaget kommer med en ansökan så vet vi vad det är för produkt och vad den har för egenskaper och då räcker det att tit-

ta på kunden denna gång. Då går naturligtvis handläggningen betydligt snabbare.

Ungefär så där går det till och det finns de som upplever oss som hinder och en administrativ börda men Sverige har valt denna säkerhetspolitiska väg. Jag är dessutom övertygad om att om vi har en bra exportkontroll så har våra svenska företag bara fördelar av detta genom att de får tillgång till teknologi och i stor utsträckningar även marknader på grund av detta.

MARKNADEN FÖR KRYPTERINGSTEKNIK

Leif Jonsson, IBM Svenska AB

Amerikanska exportrestriktioner för krypteringsprodukter

IBM och andra amerikanska IT-företag har under många år varit underkastade restriktioner vad gäller försäljning av krypteringsprodukter ("export") utanför USA. Kring dessa regler florerar ett antal myter, varför det är väsentligt att börja med att klargöra vad de innebär och inte innebär.

Restriktionerna gäller enbart sekretesskryptering, dvs. användning av krypteringsteknik för att hemlighålla information. Inga hinder finns således att sälja produkter som enbart kan användas för integritetsskydd av data, digital signatur eller identifiering/autenticering av användare. Hit hör också produkter som enbart kan kryptera PIN-koder i samband med plastkortshantering. Vad gäller nyckelhantering gäller normalt samma regler som för målfunktionen, dvs. kryptering av nycklar avsedda för PIN-kryptering eller digital signatur är OK, medan restriktioner finns för kryptering av nycklar avsedda för nyckelkryptering.

Vissa skillnader finns mellan importländer. Inga restriktioner finns således för export till Kanada, och ett litet antal utomeuropeiska länder har i stället extra hårda restriktioner.

Skillnader finns också mellan olika kundkategorier. För försäljning till banker och USA-ägda företag i Sverige har vi inte haft några problem - i allt väsentligt samma regler som för amerikanska kunder har gällt. Nyligen har dock distinktioner införts även här. För andra svenska kunder har vi vid ett antal tillfällen blivit nekade licens att sälja till t.ex. svenska exportföretag, som blir allt angelägnare om att kunna skydda sina stora nät-

verk från insyn, och därför behöver få krypteringsprodukter levererade över hela världen.

Tekniska faktorer som algoritm, nyckellängd etc spelar också roll. Situationen är här extremt komplex och ingen publicerad dokumentation av reglerna existerar.

Under årens lopp har möjligheten att i någon mening inskränka möjligheten att sekretesskryptera information varit föremål för en het debatt framför allt i USA men också i Europa. Anförda skäl för restriktioner har främst varit:

- Nationell säkerhet. Myndigheter vill med ett minimum av problem kunna avlyssna tele- och radiotrafik i underrättelsesyfte.
- Brottsbekämpning. Man vill hindra organiserad brottslighet från att använda kryptering för att skydda sig mot avlyssning från rättsvårdande myndigheter.

Amerikanska myndigheter lade för några år sedan fram förslag om det s.k. clipperchipet, som skulle möjliggjort avlyssning av bl.a. krypterad telefontrafik. Våren 1996 kom man med en framstöt om nyckeldeposition, ("key escrow"). Båda dessa förslag möttes med kraftiga protester och en inflammerad debatt. Ett väsentligt skäl till detta, som jag skall återkomma till, är att man börjat i fel ände, med en teknik för att hantera problematiken utan att grundligt utreda de juridiska aspekterna, som i debatten uppfattades som öppna.

Den 1 oktober 1996 offentliggjordes i ett uttalande från Vita Huset att nya exportregler skulle gälla från nyår 1997. Innebörden av dessa är på kort sikt främst att export av krypteringsprodukter med nycklar om max 56 bits släpps fri till alla kunder i "normala" länder inklusive Sverige. Förut var gränsen 40 bits och det innebär alltså att avsevärt starkare krypteringsprodukter än tidigare kommer att vara tillgängliga för alla kunder.

Emellertid har villkor för detta pålagts leverantörerna. De måste visa i en plan att de kommer att implementera någonting som kallas "key recovery" (KR) i sina produkter inom de närmaste två åren. Denna plan kommer sedan att återgranskas av myndigheterna varje halvår. Om två år kommer man sedan att kräva att KR-teknik finns med i alla produkter, med nyckellängder över 40 bits, som exporteras. Å andra sidan kommer man då inte att lägga några restriktioner på nyckellängder och algoritmer. Man avser också att stimulera användning av KR-produkter i USA, bl.a. genom att kräva tekniken vid federal upphandling.

Vad är då KR? Det påminner något om den numera diskrediterade "key escrow"-tekniken (KE), men det finns väsentliga skillnader. Med KE menade man traditionellt att man deponerar en nyckel eller möjligen en del av en nyckel hos en depåhållare så att denna kan utkrävas av myndighet i laga ordning.

KR å andra sidan, innebär förenklat att information om en sessions- eller arkivnyckel krypteras i en "header" till den med sessions/arkivnyckeln krypterade informationen. Headern krypteras med publika asymmetriska nycklar tillhöriga en eller flera "key recovery service providers" (KRSP). Om en sessions/arkivnyckel behöver återvinnas kan då en behörig person be KRSP att kryptera upp sin del av "headern". Ur den samlade informationen från samtliga KRSP plus ytterligare information i "headern" kan sedan nyckeln återvinnas (eventuellt kan man låta en rest om t.ex. 40 bits återstå för att ytterligare avskräcka från missbruk). KRSP har således ingenting deponerat hos sig, utan är endast aktiv i samband med nyckelåtervinning då man med sin privata asymmetriska nyckel krypterar upp en överlämnad "header". Den ovan nämnda "behöriga personen" kan tänkas vara användaren själv, hans arbetsgivare (i vika fall nyckeln antas ha gått förlorad så att viktig information ej kan återvinnas) eller en behörig myndighet.

Allt tyder f.n. på att de amerikanska myndigheterna kommer att genomföra dessa regler trots tveksamhet och motstånd både från IT-branschen och rättssäkerhetsförespråkare. IBM och ett antal andra IT-företag har därför bestämt sig för att gilla läget och anpassa sig till situationen. I detta syfte har den s.k. KR-alliansen bildats (av Apple, Atalla, Bull, DEC, HP, IBM, NCR, RSA, SUN, TIS och UPS vartill kommer ytterligare 30 medlemmar som anslutit sig senare) för att ta fram regler och standards för KR i syfte att säkra interoperabilitet mellan produkter från olika leverantörer. Det handlar då inte bara om de enkla, specialiserade säkerhetsprodukter som hittills har marknadsförts. Krypteringsfunktioner kommer i framtiden att byggas in i alla typer av programvara - i ordbehandlare, e-postprogram, grupparbetsprogram etc. Programtyper som används av i stort sett alla användare kommer att vara försedda med krypteringsfunktioner.

Som jag nyss antydde, räcker det här inte med att bara efterfråga, utveckla och publicera teknik för hantering av krypteringsrestriktioner. Vi kommer då raskt att få samma typ av debatt som tidigare, med resultat att utvecklingen stoppas och vi behåller den rådande, otillfredsställande situationen .

Av detta skäl har IBM lagt fram ett "position paper" , "The Need for a Global Cryptographic Policy Framework" med förslag till riktlinjer för ett internationellt juridiskt regelverk för KR. Dokumentet är riktat främst till ansvariga myndigheter i de aktuella länderna, alltså inte bara i USA utan även i Sverige.

Låt mig snabbt sammanfatta de viktigast punkterna i detta dokument (som finns publicerat i sin helhet på *http://www.ibm.com/ security / html/ pp_global.html).*

- Myndigheterna bör stöda ett system för KR utan begränsningar av nyckellängder. Viktigt är här att KR kommer att vara attraktivt även för större företag och andra användare som är angelägna att säkra tillgång-

en till sin information även om den i stor utsträckning är krypterad. Fall där krypteringsnycklar avsiktligt eller av misstag förstörs kommer att förekomma i framtiden och risker förknippade härmed måste minimeras.

- Myndigheterna i de länder som producerar och exporterar krypteringsprodukter bör snarast ena sig om ett globalt regelverk för KR. Detta är nödvändigt för att tekniskt och juridiskt säkra interoperabilitet i alla avseenden.

- Myndigheterna bör ej begränsa legal, inhemsk användning av kryptering. Sådana restriktioner finns idag endast i ett fåtal länder. Den inhemska infrastrukturen i vissa branscher kräver kryptering och vi ser i dag ingen anledning till skärpningar på denna punkt.

- Myndigheter bör tillåta interoperabilitet mellan system som tillämpar KR och sådana (se föregående punkt) som ej gör det. Vissa användare kommer ej att acceptera KR, men har ändå legitima behov att kommunicera med andra användare som gör det.

- Myndigheterna bör ej begränsa nyckellängder vid export av KR-produkter. KR ger myndigheterna tillgång till informationen oberoende av nyckellängd, varför begränsning är överflödig.

- KRSPs bör ej överregleras. Auktorisationskriteria bör begränsas till

1. snabb service till myndighet som presenterar en legitim begäran om information,
2. starka revisionsmekanismer för uppföljning av KRSPs aktiviteter,
3. förmåga att tillfredsställa konfidentialitet (viktigt för polisundersökningar) för alla önskemål om KR-information (vilket är speciellt viktigt om en organisation har sin egen KRSP, vilket bör vara rimligt för t.ex. större företag).

En bra metod att undvika överreglering kan vara att överlåta auktorisationen till standardiseringsorgan, som kan auktorisera på i princip samma sätt som man t.ex. certifierar för ISO9000.

- KR-information bör vara tillgänglig enbart under avtal mellan KRSP och kund eller till myndighet genom lagreglerad process (t.ex. domstolsbeslut). Utan garantier för detta kan användarna aldrig få förtroende för ett KR-system.

- Internationellt utbyte av KR-information får endast ske mellan myndigheter i länderna, dvs. en myndighet i ett land kan ej ställa krav direkt på en KRSP i ett annat land. Staterna bör ömsesidigt godkänna varandras KRSP. Det senare innebär att en kund kan välja en KRSP i ett annat land om han hyser misstro till det egna landets myndigheter, vilket innebär en god säkerhetsventil mot missbruk av KR.

- Myndigheter bör acceptera export av KR-produkter när dessa stöder KR via acceptabla KRSP.

- Myndigheterna bör internationellt överenskomma om acceptans av KR-metoder som kräver KR-information från mer än en KRSP. Detta delade ansvar ökar väsentligt användarens säkerhet.

- Myndigheterna bör vidtaga åtgärder som stöder utveckling av KR-produkter, t.ex. lagstiftning, modifiering av upphandlingspolicies och omedelbar exportlicentiering av KR-produkter i vissa fall.

Dessa punkter kan representera ett rimligt juridiskt-politiskt ramverk för internationell reglering av krypteringsanvändning och utgöra en tänkbar kompromiss mellan ett antal motstridiga intressen hos krypteringsanvändare, rättsäkerhetsförespråkare, IT-branschen, rättsvårdande myndigheter och säkerhetsorgan. Som jag tidigare nämnde är det med frågeställningar som dessa som en internationell diskussion måste börja - inte med tekniken.

EN INTERNATIONELL UTBLICK

Göran Axelsson, Statskontoret

I den internationella översikten ska jag tala om tre saker. Först går jag in på krypteringsfrågorna och vad som händer med krypteringen i några olika länder och några olika sammanhang. Sedan tar jag upp utvecklingen vad det gäller digitala signaturer som är ett annat spår och som utvecklas på lite olika sätt. Slutligen kommer jag in på frågan om kontroll av Internet, Internets användning och innehåll som är kopplat till de tidigare ämnena som jag tar upp, framför allt nu när Internet får en mycket större betydelse än det har haft under de gångna åren.

1. *Kryptering*

1.1 Exportkontroll

- 31 länder deltar i Wassenaar Arrangement och tillämpar exportkontroll
- EU-länderna tillämpar exportkontroll för intern handel av krypto

31 länder deltar i Wassenaar-arrangement och har således implementerat exportkontroll. EU-länderna, som Magnus Faxén sade, tillämpar också exportkontroll även för handel mellan sig när det gäller kryptoprodukter. Det är med andra ord exportkontroll mellan Sverige och Finland och Sverige och Danmark.

1.2 Australien

- ökade krav på att lämna ut nyckel vid husrannsakan

I Australien har det förts diskussioner om hur långt man bör gå när det gäller att lösa problemen med en kraftigt ökad kryptering. En av de tankarna som man speciellt har lyft fram i den diskussionen är krav på att lämna ut nyckel vid husrannsakan. Den typen av krav skulle öka kraftigt. Det skulle vara ett mycket signifikant brott om man hävdar att man har

glömt sin nyckel eller slarvat bort den. Man har också i Australien tagit fram ett standarddokument för hur en Public Key Infrastructure kan se ut.

1.3 Danmark

- IT-säkerhetsrådet: fri kryptering
- staten ska tills vidare inte ge ut något medborgarkort för offentlig service
- krypto-policy-process pågår i regeringskansliet, ingen antydan om resultatet
- IT-säkerhetsrådet fortsätter kampanj för fri kryptering

I Danmark har det varit lite fram och tillbaka, kan man säga. IT-säkerhetsrådet gick ut i somras med ett pressmeddelande och ett förslag om att det skall vara fri kryptering och ingen nyckeldeponering i Danmark. Under hösten har staten bestämt sig för att tills vidare inte ge ut något medborgarkort för offentlig service utan försöka finna andra lösningar. I detta pressmeddelande säger man att det beror på att man har problem med standarden och med tekniska lösningar i sammanhanget. Det pågår en kryptopolicy-process i danska regeringskansliet där man försöker komma fram till en lösning som den danska regeringen blir överens om. Det pågår en viss lobby-verksamhet från IT-säkerhetsrådet för fri kryptering.

1.4 Frankrike

- enda land i EU där kryptering är förbjuden, utan licens
- lag 18 juni 96 om TTP, nyckeldeponering, utlämnande av nycklar (liberalisering)
- avser att använda Royal Holloway-konceptet för TTP:er

Frankrike är det enda land i EU där kryptering kräver licens och som Magnus Faxén var inne på. Lagen beslöts den 18 juni 1996 och handlar om Trusted Third Party, dvs. om nyckeldeponering, utlämnande av nycklar. I Frankrike är detta en liberalisering. Det krävs dock ett särskilt beslut från regeringen innan lagen träder i kraft och man tror att lagen träder i kraft någon gång i början av 1997. Man tänker använda sig av en arkitektur som är utvecklad på ett universitet i London (Royal Holloway) för TTP-ernas verksamhet.

1.5 Kanada

- fri tillgång till kryptolösningar från USA

Kanada har till skillnad från andra länder fri tillgång till kryptolösningar från USA. Det finns ett avtal mellan de två staterna om fri export.

1.6 Nederländerna

- försökte införa licenstvång för kryptering 1994
- intresse att använda TTP enligt Royal Holloway-konceptet

Nederländerna försökte införa licens för kryptering 1994. Förslaget publicerades och det lyckades inte att få enighet i regeringen om detta. Nederländerna är också intresseerat av att använda Royal Holloway för TTP-er.

1.7 Tyskland

- Interministerial Task Force on Crypto Politics för att ta fram krypto-policy, svårt att balansera frihet/reglering
- intresse att använda TTP enligt Royal Holloway-konceptet

I Tyskland finns på samma sätt som i Sverige en referensgrupp i regeringskansliet som kallas på engelska Ministerial task force on crypto politics. Gruppen arbetar på att få fram en kryptopolicy och har såvitt jag känner till inte ännu lyckats med detta. Man är också intresserad av att använda Royal Holloway-konceptet för TTP-lösningar.

1.8 UK

- föreslås förbli fritt att kryptera
- inte fritt att sälja TTP-tjänster?
- lag om licensiering av TTP förbereds, och kan träda i kraft slutet 1997
- man vill att TTP ska arbeta enligt Royal Holloway-konceptet
- staten avses själv använda TTP enligt Royal Holloway-konceptet

Det finns inte särskilt mycket publicerat om Storbritanniens krypto-policy. Det är svårt att sia om vad som kan komma att hända. I dagsläget är det fritt att kryptera. Man har lanserat ett förslag som bygger på att det skall fortsätta att vara fritt att kryptera men inte fritt att sälja TTP-tjänster efter-

som TTP-tjänsterna skall grundas på lag. En lag kan träda i kraft i slutet av 1997 har det sagts. Man föreslår att TTP-erna skall baseras på Royal Holloway-konceptet. Staten har avsett att för egen del använda TTP:er enligt Royal Holloway för den statliga administrationen.

1.9 USA

- öppen debatt, rik tillgång till information
- effektivt utbyggd exportkontroll för bl.a. teknologi, kontroll av köparna
- mer långtgående kontroll av krypto-lösningar
- massmarknadslösningar: USA/Kanada (fri nyckellängd) vs övriga länder (40 bitars nyckellängd = fritt att exportera)
- många key escrow/keyrecovery förslag under senare år:
Clipper I, Clipper II, Clipper III, Clipper III.1, Clipper III.1.1
- förslag 1 oktober (principbeslut 15 nov, detaljbeslut kommer senare av Dep of Commerce):
- fritt att exportera 56 bitars DES 1997 om leverantör inom 2 år säljer "godkänd" TTP-lösning
- fri nyckellängd i TTP-lösningen
- möjlighet för "in-house TP"
- "key recovery-alliansen" (ca 35 företag) har lanserat gemensamt key recovery-koncept
- stark kritik i nov/dec från MicroSoft och Business Software Association mot implementering av 1 okt-förslaget
- USA har utsett en "crypto-ambassador"

USA har det talats mycket om. Ett skäl att det är så många punkter på min lista är faktiskt att det finns i USA en mycket öppen debatt. Det är rik tillgång till information. Mycket information finns på Internet och därför är det lätt att ställa samman ett antal punkter.

Vi har ju talat om den amerikanska utvecklingen redan. Jag skall bara peka på att en viktig ingrediens i den amerikanska kryptopolitiken är att man har exportkontroll för teknologi och man har kontroll av köparna. Det är väl genomfört på en lång rad olika produktområden och det tillämpas således även på kryptoområdet. Vi har redan talat om nyckellösningar, om förslagen om Key-recovery och om det förslaget den 1 oktober 1996, samt om IBM-alliansens lansering. Det har även på senare tid kommit en mycket stark kritik mot amerikanska regeringen från näringslivet

om hur kryptopolitiken implementeras. Det är svårt att säga var det landar. Tanken är att det skall börja genomföras i januari 1997.

1.10 Krav på "tillstånd" för att få kryptera inom landet

- Frankrike
- Indien
- Israel
- Ryssland
- Saudi Arabia
- Sydkorea
- några islam-stater
- m fl

Krav på tillstånd för att få kryptera inne i landet finns i några länder. Sådan information kan man ganska lätt hämta på Internet.

1.11 Standardiseringsorgan

ETSI

- rapport med krav på TTP-tjänster (hösten 1996)

Ett standardiseringsorgan som arbetar med dessa frågor är exempelvis ETSI (European Telecommunication Standard Institute) där europeiska länders experter deltar. Det finns ett utkast till rapport från hösten 1996 med specifikationer på TTP-tjänster.

1.12 EU

- 3 pelare berörs
  - pelare 1: har inte lagt förslag i INFOSEC-programmet, förslag om e-handel förbereds
  - pelare 2: dual-use regler finns
  - pelare 3: regler för polissamarbete finns

Inom EU är det ett speciellt problem att det är tre stycken pelare enligt EU-fördraget som berörs av kryptopolicyn.

Den första pelaren handlar om den inre marknaden. Där finns för närvarande inga förslag i samband med Infosec-programmet. Man förbereder förslag om electronic commerce som skall komma under våren 1997. Det tas fram av tre stycken general-direktorat (DG III, XIII, XV). Det finns inga indikationer idag på när det skulle kunna komma något förslag i samband med Infosec-programmet. Ett sådant förslag har vi väntat i ett par års tid.

Pelare två handlar om utrikeshandel och försvarssamarbete. Där finns dual-use-reglerna som Magnus Faxèn och Egon Svensson har talat om.

Pelare tre handlar om det polisiära samarbetet. Där finns också en del regler.

Beslutsmekanismerna i de tre pelarna skiljer sig åt. I pelare ett är det kommissionen som har, så att säga, monopol att lägga förslag till ministerrådet som sedan beslutas då på sedvanligt sätt. I pelare två och pelare tre är det ministerrådsarbetsgrupper som gör arbetet och kommissionen har lite eller inget att säga till om. Min tolkning av detta är att det är mycket svårt att finna lösningar som passar för hela EU-samarbetet. Det är förmodligen ett viktigt skäl varför så lite har hänt inom pelare ett.

1.13 OECD

- utarbetar riktlinjer för krypto-policy

OECD har vi talat om. Man arbetar med riktlinjer för kryptopolicy och EU. Jag skall kommentera OECD lite ytterligare. I OECD-gruppen för krypto-policy sitter, kan man säga representanter för "de tre pelarna i EU". De tre pelarnas intressen finns med i OECD-arbetet. Detta är unikt i arbetet med krypto-policy. Tanken är att förslaget från gruppen i OECD ska komma innan detta årets slut. Förlaget ska sedan gå vidare till andra grupper inom OECD och dokumenten blir offentligt när OECDs ministerråd framöver har godkänt detta. Det kanske kan komma ett sådant godkännande under 1997.

2. *Digitala Signaturer*

2.1 Utah (USA)

• första lagen om digitala signaturer, ca 10 delstater har/förbereder liknande lagar.

Arbetet med digitala signaturer började i delstaten Utah i USA som är det första landet, som jag har sett, där man har en lag om digitala signaturer som är i drift. Ytterligare ett antal delstater i USA har kommit igång med liknande lagstiftningsarbete eller redan genomfört detta.

2.2 Australien

• standarddokument för Public Key Infrastructure (PKI) och digitala signaturer finns

2.3 USA

• PKI system lanseras nu för federal användning

2.4 Kanada

• digitala signaturer i statlig verksamhet

2.5 Danmark

• lag om digitala signaturer förbereds, till Folketinget i januari 1997?

2.6 Tyskland

• lag om digitala signaturer förbereds, beslutas sommaren 1997 (?)

Det är viktigt i sammanhanget att det är två länder i Europa som ligger långt framme, Danmark och Tyskland. Det är svårt att säga vilket av de här två som kommer att ha en lag genomförd först. Förmodligen blir det ett ganska dött lopp, fram mot sommaren 1997 i båda fallen.

2.7 EU

- studier om digitala signaturer igångsatta (okt 96)

Inom EU har inledande studier om digitala signaturer satts igång.

3. *Kontroll av Internet*

- Internet har blivit viktigare
- sårbart för angrepp
- i dagsläget bestämmer användarna innehållet i databaserna
- G7 anser att Internet ger fördelar för terrorism - utarbetar åtgärdsplan
- begynnande innehållskontroll i Singapore, NL, Ty, UK, US, Kina, islamstater, m fl.
- EU-rekommendation om "illegal and harmful content on the Internet" godkändes 28 nov 1996 (gäller även Sverige)

Internet har blivit viktigare genom att det används i allt flera sammanhang. Vi märker till exempel i den svenska statliga förvaltningen att Internet har blivit något av en livlina för väldigt mycket kommunikation. Det är sårbart för angrepp, det har man sett många exempel på. Rykten säger att Information Rosenbad var delvis förstörd igår ett tag. Det var någon som hade kommentarer om hur Göran Persson agerade. Jag har sett liknande exempel från USA där olika webar har varit förstörda under några timmar.

Användarna bestämmer innehållet på Internet. På senare tid har kommit olika intressen som har uppmärksammats, till exempel G7/P8-länderna i somras som uppger att Internet ger stora fördelar för terrorismverksamheten. G7/P8 har lanserat principer och förslag som nu vidarebearbetas. EU har i november månad tagit en rekommendation där också Sverige är med på området "Illegal and harmful content on the Internet". Man föreslår olika form av självreglerande åtgärder men de går i så att säga en reglerande riktning.

Mera direkt innehållskontroll på Internet finns i Nederländerna, Singapore, Tyskland. Det finns förslag från Storbritannien, USA har kontroll lik-

som några islamstater med flera. Förteckningen av länder växer över tiden.

Rapporter

IT-kommissionens arbetsprogram, SOU 1995:68
Delbetänkande om kommissionens övervägande och prioriteringar samt arbetsprogram. 34 sidor. Kan beställas hos Fritzes kundtjänst. Fax: 08-690 91 91. Telefon: 08-690 91 90

Kommunikation utan gränser - rapport från IT-kommissionen, juni 1995
Skriften är ett sammandrag av kommissionens arbetsprogram. 15 sidor. Kan beställas hos IT-kommissionen.

Communication Without Frontiers - report by the Swedish IT-Commission, june 1995
Engelsk översättning av sammandraget. 15 sidor. Kan beställas från IT-kommissionen

Så kan Sverige utveckla en framgångsrik programvaruindustri inför 2000-talet
Rapport 1/96. 25 sidor.

IT-mått. Hur kan IT-användning beskrivas?
Av Nils-Göran Olve & Carl-Johan Westin, CEPRO AB.
Rapport 2/96. 65sidor.

När det regnar manna från himlen, har den fattige ingen sked. Om IT och handikapp.
Rapport 3/96. 32 sidor.

Kvinnor och IT
Rapport 4/96. 41 sidor.

Rättsinformation och IT - Svårigheternas advokater eller möjligheternas ambassadörer?
Rapport 5/96. 60 sidor.

ERROR, När IT inte fungerar - en rapport om IT och dess användbarhet
Av Per Gustafsson på uppdrag av IT-kommissionen.
Rapport 6/96. 50 sidor.

IT-kommissionens hearing om infrastrukturen för information och kommunikation.
Dokumentation från IT-kommissionens hearing den 5-6 juni 1996.
Rapport 7/96. 127 sidor.

Affärsnyttan med Internet
Sammanfattning av det seminarium som anordnades av IT-kommissionen, Swebizz och Sveriges Tekniska Attachéer den 4 juni 1996. Rapport 8/96. Rapporten är publicerad på IT-kommissionens hemsida <http://www.itkommissionen.se>.

IT-problem inför 2000-skiftet, SOU 1997:12
Referat och slutsatser från en hearing anordnad av IT-kommissionen den 18 december 1996. Rapport 1/97. Kan beställas hos Fritzes kundtjänst. Fax: 08-690 91 91. Telefon: 08-690 91 90.

Digital demokra@ti, SOU 1997:23
Ett seminarium om Teknik, demokrati och delaktighet den 8 november 1996 anordnat av Folkomröstningsutredningen, IT-kommissionen och Kommunikationsforskningsberedningen. Rapport 2/97. Kan beställas hos Fritzes kundtjänst. Fax: 08-690 91 91. Telefon: 08-690 91 90.

Kristallkulan - 13 röster om framtiden, SOU 1997:31
Rapport 3/97. Kan beställas hos Fritzes kundtjänst. Fax: 08-690 91 91. Telefon: 08-690 91 90.

IT och miljö - en samling goda exempel, SOU 1996: 178
Rapport 4/97. Kan beställas hos Fritzes kundtjänst. Fax: 08-690 91 91. Telefon: 08-690 91 90.

Sverige inför epokskiftet, SOU 1997:63
Rapport 5/97. Kan beställas hos Fritzes kundtjänst. Fax: 08- 690 91 91. Telefon: 08- 690 91 90.

Rapporter utgivna på uppdrag eller i samarbete med IT-kommissionen

Data om IT i Sverige
Statitsitisk sammanställning om IT gjord av Statistiska Centralbyrån på uppdrag av IT-kommissionen. Kan beställas från SCB Förlag, 701 89 Örebro. Fax: 019-17 69 32. Telefon: 019-17 68 00.

Datorvanor 1995
Undersökning av svenska folkets datorvanor utförd av Statistiska Centralbyrån på uppdrag av IT-kommissionen. 102 sidor.
Kan beställas från SCB Förlag, 701 89 Örebro. Fax: 019-17 69 32.
Telefon: 019-17 68 00.

IT världen runt - Nationella initiativ
Undersökning av Sveriges Tekniska Attachéer på uppdrag av IT-kommissionen och Näringsdepartementet. Kan beställas från STATT, Box 5282, 102 46 Stockholm

IT världen runt - Regionala initiativ
Undersökning av Sveriges Tekniska Attachéer på uppdrag av IT-kommissionen och Näringsdepartementet. Stencil.

IT världen runt - Statligt stöd till mjukvaruindustrin
Undersökning av Sveriges Tekniska Attachéer på uppdrag av IT-kommissionen och Näringsdepartementet. Stencil.

Europeiska Unionen - IT, telekommunikation och nya medier
En kartläggning och analys gjord av Statskontoret på uppdrag av IT-kommissionen. 111 sidor.

Statens offentliga utredningar 1997

Kronologisk förteckning

1. Den nya gymnasieskolan – steg för steg U.
2. Inkomstskattelag, del I-III. Fi.
3. Fastighetsdataregister. Ju.
4. Förbättrad miljöinformation. M.
5. Aktivt lönebidrag. Ett effektivare stöd för arbetshandikappade. A.
6. Länsstyrelsernas roll i trafik- och fordonsfrågor. K.
7. Byråkratin i backspegeln. Femtio år av förändring på sex förvaltningsområden. Fi.
8. Röster om barns och ungdomars psykiska hälsa. S.
9. Flexibel förvaltning. Förändring och verksamhetsanpassning av statsförvaltningens struktur. Fi.
10. Ansvaret för valutapolitiken. Fi.
11. Skatter, miljö och sysselsättning. Fi.
12. IT-problem inför 2000-skiftet. Referat och slutsatser från en hearing anordnad av IT-kommissionen den 18 december. IT-kommissionens rapport 1/97. K.
13. Regionpolitik för hela Sverige. N.
14. IT i kulturens tjänst. Ku.
15. Det svåra samspelet. Resultatstyrningens framväxt och problematik. Fi.
16. Att utveckla industriforskningsinstituten. N.
17. Skatter, tjänster och sysselsättning. + Bilagor. Fi.
18. Granskning av granskning. Den statliga revisionen i Sverige och Danmark. Fi.
19. Bättre information om konsumentpriser. In.
20. Konkurrenslagen 1993-1996. N.
21. Växa i lärande. Förslag till läroplan för barn och unga 6-16 år. U.
22. Aktiebolagets kapital. Ju.
23. Digital demokr@ti. Ett seminarium om Teknik, demokrati och delaktighet den 8 november 1996 anordnat av Folkomröstningsutredningen, IT-kommissionen och Kommunikationsforskningsberedningen. IT-kommissionens rapport 2/97. K.
24. Välfärd i verkligheten – Pengar räcker inte. S.
25. Svensk mat – på EU-fat. Jo.
26. EU:s jordbrukspolitik och den globala livsmedelsförsörjningen. Jo.
27. Kontroll Reavinst Värdepapper. Fi.
28. I demokratins tjänst. Statstjänstemannens roll och vårt offentliga etos. Fi.
29. Barnpornografifrågan. Innehavskriminalisering m.m. Ju.
30. Europa och staten. Europeiseringens betydelse för svensk statsförvaltning. Fi.
31. Kristallkulan – tretton röster om framtiden. IT-kommissionens rapport 3/97. K.
32. Följdlagstiftning till miljöbalken. M.
33. Att lära över gränser. En studie av OECD:s förvaltningspolitiska samarbete. Fi.
34. Övervakning av miljön. M.
35. Ny kurs i trafikpolitiken + bilagor. K.
36. Bekämpande av penningtvätt. Fi.
37. Ett tekniskt forskningsinstitut i Göteborg. U.
38. Myndighet eller marknad. Statsförvaltningens olika verksamhetsformer. Fi.
39. Integritet Offentlighet Informationsteknik. Ju.
40. Unga och arbete. In.
41. Staten och trossamfunden
    Rättslig reglering
    – Grundlag
    – Lag om trossamfund
    – Lag om Svenska kyrkan. Ku.
42. Staten och trossamfunden
    Begravningsverksamheten. Ku.
43. Staten och trossamfunden
    Den kulturhistoriskt värdefulla kyrkliga egendomen och de kyrkliga arkiven. Ku.
44. Staten och trossamfunden
    Svenska kyrkans personal. Ku.
45. Staten och trossamfunden
    Stöd, skatter och finansiering. Ku.
46. Staten och trossamfunden
    Statlig medverkan vid avgiftsbetalning. Ku.
47. Staten och trossamfunden
    Den kyrkliga egendomen. Ku.
48. Arbetsgivarpolitik i staten.
    För kompetens och resultat. Fi.
49. Grundlagsskydd för nya medier. Ju.
50. Alternativa utvecklingsvägar för EU:s gemensamma jordbrukspolitik. Jo.
51. Brister i omsorg
    – en fråga om bemötande av äldre. S.
52. Omsorg med kunskap och inlevelse
    – en fråga om bemötande av äldre. S.
53. Avskaffa reklamskatten! Fi.
54. Ministern och makten.
    Hur fungerar ministerstyre i praktiken? Fi.
55. Staten och trossamfunden. Sammanfattningarna av förslagen från de statliga utredningarna. Ku.
56. Folket som rådgivare och beslutsfattare. + Bilaga 1 och 2. Ju.
57. I medborgarnas tjänst.
    En samlad förvaltningspolitik för staten. Fi.
58. Personaluthyrning. A.
59. Svenskhemmet Voksenåsens förvaltningsform. Ku.
60. Betal-TV inom Sveriges Television. Ku.

Statens offentliga utredningar 1997

Kronologisk förteckning

61. Att växa bland betong och kojor.
Ett delbetänkande om barns och ungdomars uppväxtvillkor i storstädernas utsatta områden från Storstadskommittén. S.
62. Rosor av betong.
En antologi till delbetänkandet Att växa bland betong och kojor från Storstadskommittén. S.
63. Sverige inför epokskiftet.
IT-kommissionens rapport 5/97. K.
64. Samhall. En arbetsmarknadspolitisk åtgärd
+ Bilagedel. A
65. Polisens register. Ju.
66. Statsskuldspolitiken. Fi.
67. Återkallelse av uppehållstillstånd. UD.
68. Grannlands-TV i kabelnät. Ku.
69. Besparingar i stort och smått. U.
70. Totalförsvaret och frivilligorganisationerna – uppdrag, stöd och ersättning. Fö.
71. Politik för unga.
+ 2 st bilagor. In.
72. En lag om socialförsäkringar. S.
73. Inför en svensk policy om säker elektronisk kommunikation. Referat från ett seminarium anordnat av IT-kommissionen, Närings- och handelsdepartementet och SEIS den 11 december 1996. IT-kommissionens rapport 6/97. K.

Statens offentliga utredningar 1997

Systematisk förteckning

Justitiedepartementet

Fastighetsdataregister. [3]
Aktiebolagets kapital. [22]
Barnpornografifrågan.
Innehavskriminalisering m.m. [29]
Integritet Offentlighet Informationsteknik. [39]
Grundlagsskydd för nya medier. [49]
Folket som rådgivare och beslutsfattare.
+ Bilaga 1 och 2. [56]
Polisens register. [65]

Utrikesdepartementet

Återkallelse av uppehållstillstånd. [67]

Försvarsdepartementet

Totalförsvaret och frivilligorganisationerna
– uppdrag, stöd och ersättning. [70]

Socialdepartementet

Röster om barns och ungdomars psykiska hälsa. [8]
Välfärd i verkligheten – Pengar räcker inte. [24]
Brister i omsorg
– en fråga om bemötande av äldre. [51]
Omsorg med kunskap och inlevelse
– en fråga om bemötande av äldre. [52]
Att växa bland betong och kojor.
Ett delbetänkande om barns och ungdomars uppväxtvillkor i storstädernas utsatta områden från Storstadskommittén. [61]
Rosor av betong.
En antologi till delbetänkandet Att växa bland betong och kojor från Storstadskommittén. [62]
En lag om socialförsäkringar. [72]

Kommunikationsdepartementet

Länsstyrelsernas roll i trafik- och fordonsfrågor. [6]
IT-problem inför 2000-skiftet. Referat och slutsatser från en hearing anordnad av IT-kommissionen den 18 december. IT-kommissionens rapport 1/97. [12]
Digital demokr@ti. Ett seminarium om Teknik, demokrati och delaktighet den 8 november 1996 anordnat av Folkomröstningsutredningen, IT-kommissionen och Kommunikationsforskningsberedningen. IT-kommissionens rapport 2/97. [23]
Kristallkulan – tretton röster om framtiden.
IT-kommissionens rapport 3/97. [31]
Ny kurs i trafikpolitiken + bilagor. [35]
Sverige inför epokskiftet.
IT-kommissionens rapport 5/97. [63]
Inför en svensk policy om säker elektronisk kommunikation. Referat från ett seminarium anordnat av IT-kommissionen, Närings- och handelsdepartementet och SEIS den 11 december 1996.
IT-kommissionens rapport 6/97. [73]

Finansdepartementet

Inkomstskattelag, del I-III. [2]
Byråkratin i backspegeln. Femtio år av förändring på sex förvaltningsområden. [7]
Flexibel förvaltning. Förändring och verksamhetsanpassning av statsförvaltningens struktur. [9]
Ansvaret för valutapolitiken. [10]
Skatter, miljö och sysselsättning. [11]
Det svåra samspelet. Resultatstyrningens framväxt och problematik. [15]
Skatter, tjänster och sysselsättning.
+ Bilagor. [17]
Granskning av granskning.
Den statliga revisionen i Sverige och Danmark. [18]
Kontroll Reavinst Värdepapper. [27]
I demokratins tjänst. Statstjänstemannens roll och vårt offentliga etos. [28]
Europa och staten. Europeiseringens betydelse för svensk statsförvaltning. [30]
Att lära över gränser. En studie av OECD:s förvaltningspolitiska samarbete. [33]
Bekämpande av penningtvätt. [36]
Myndighet eller marknad.
Statsförvaltningens olika verksamhetsformer. [38]
Arbetsgivarpolitik i staten.
För kompetens och resultat. [48]
Avskaffa reklamskatten! [53]
Ministern och makten.
Hur fungerar ministerstyre i praktiken? [54]
I medborgarnas tjänst.
En samlad förvaltningspolitik för staten. [57]
Statsskuldspolitiken. [66]

Utbildningsdepartementet

Den nya gymnasieskolan – steg för steg. [1]
Växa i lärande. Förslag till läroplan för barn och unga 6-16 år. [21]
Ett tekniskt forskningsinstitut i Göteborg. [37]
Besparingar i stort och smått. [69]

Statens offentliga utredningar 1997

Systematisk förteckning