Regeringens skrivelse 1998/99:116

Om kryptografi

Skr. 1998/99:116

Regeringen överlämnar denna skrivelse till riksdagen.

Stockholm den 6 maj 1999

Göran Persson

Leif Pagrotsky
(Utrikesdepartementet)

Skrivelsens huvudsakliga innehåll

I skrivelsen redovisar regeringen sin uppfattning när det gäller vissa aspekter på användning av kryptografi vid överföring och lagring av information i elektronisk form samt när det gäller export av kryptoprodukter.

Regeringens ståndpunkt innebär i huvudsak följande.

För närvarande föreligger det inte skäl att begränsa användningen av kryptoteknik i Sverige. Alla skall ha rätt att själva välja sådan teknik.

Import av kryptoteknik skall förbli fri.

Det finns fortsatta säkerhetspolitiska skäl att förhindra spridning av kryptoteknik till olämpliga mottagare i vissa andra länder.

Skulle utvecklingen motivera skärpta regler kommer regeringen att överväga lämpliga åtgärder för att skapa möjligheter till laglig åtkomst i klartext av krypterad information för brottsbekämpande och kontrollerande myndigheter.

Sveriges politik bör präglas av flexibilitet och lyhördhet i syfte att kunna möta en ökad efterfrågan på säker kryptoteknik, förändringar i andra länders politik och den fortsatta tekniska utvecklingen på området.

Innehållsförteckning

1 Ärendet och dess beredning

För att kartlägga användningen av kryptoteknik och ta fram ett underlag för Sveriges politik på området inrättades i början av 1996 en referensgrupp inom Regeringskansliet.

I uppdraget har också ingått att samordna svenskt deltagande i internationella överläggningar och att förhandla om internationella riktlinjer för krypterad kommunikation.

Referensgruppen presenterade i oktober 1997 rapporten ”Kryptopolitik – möjliga svenska handlingslinjer”. Rapporten har offentliggjorts och synpunkter på den har kommit in från berörda intressenter. Yttrandena finns tillgängliga i Regeringskansliet (Doss. HP 24). Referensgruppen har härefter fortsatt sitt arbete i syfte att ta fram ett underlag för en svensk ståndpunkt när det gäller användningen av kryptoteknik. Resultatet av detta arbete har legat till grund för den skrivelse som regeringen nu förelägger riksdagen.

Arbetet med att följa utvecklingen på området och ta ställning till vilka åtgärder denna kan motivera fortsätter. Regeringen avser att låta detta ske i delvis andra former än hittills, i syfte att fördjupa dialogen med företrädare för olika användare och andra berörda.

2 Utgångspunkter

2.1 Bakgrund

Den snabba tekniska utvecklingen underlättar en dynamisk framväxt av nationell och global elektronisk handel och elektronisk kommunikation. Detta leder i sin tur till en omfattande potential för tillväxt och effektivitet. Denna potential kan emellertid realiseras fullt ut först om myndigheter, företag och enskilda kan vara säkra på att den information som de utbyter och lagrar är oåtkomlig för obehöriga.

Användning av kryptografi tillmötesgår krav på säkerhet i överföring av meddelanden och på skydd av lagrad information. Handlingars och signaturers äkthet kan också säkerställas med sådan teknik. I bilaga 1 återfinns en förklaring av tekniska termer som används i skrivelsen. Bilaga 2 innehåller en kortfattad beskrivning av kryptografi.

Den tekniska utvecklingen har gjort det möjligt för såväl myndigheter och företag som enskilda personer att använda kryptoteknik vid hantering av känslig information. Samtidigt finns det både nationellt och internationellt ett behov av att kunna förhindra missbruk av sådan teknik.

Användningsområdena för kryptoteknik har utvidgats under de senaste åren från att tidigare främst ha använts inom försvaret och utrikesförvaltningen. Kryptoteknik är klassificerad som en strategisk produkt omfattad av exportkontroll, eftersom det fortfarande finns viktiga säkerhetspolitiska aspekter på den tekniken.

De aspekter som bör beaktas vid utformningen av en politik för kryptografi är:

- trovärdighet hos dokument i elektronisk form som avser att ersätta dokument i skriftlig form,
- trovärdighet hos elektroniska signaturer och skydd för konfidentialitet vid användning av elektronisk kommunikation samt vid lagring av information,
- brottsbekämpning, kontroll eller tillsyn (exempelvis åklagar-, polis- samt skatte- och tullmyndigheter),
- exportkontroll för att förhindra spridning till olämpliga mottagare i vissa länder.

Gällande svenska regler för användning av kryptoteknik kan sammanfattas på följande sätt.

- Det är fritt att importera, tillverka och använda denna teknik.
- Ansökningar om tillstånd till utförsel av kryptoprodukter skall prövas av Inspektionen för strategiska produkter (ISP).
- De rättsvårdande myndigheterna har möjlighet att tvångsvis – genom t.ex. husrannsakan – få tillgång till användares kryptonycklar. En användare av kryptering som misstänks för brott kan emellertid inte tvingas att aktivt medverka i en brottsutredning genom att t.ex. lämna ut sin privata konfidentialitetsnyckel.

I en skrivelse till riksdagen om elektronisk handel (skr. 1997/98:190) har regeringen redovisat olika frågor som berörs av den snabba utvecklingen av elektronisk handel. Regeringen har där uttalat att utvecklingen bör drivas av marknadens aktörer och att regleringar bör tillgripas endast när branschstandarder och avtal inte är tillräckliga. I skrivelsen betonas att ett övergripande intresse från statsmakternas sida i fråga om såväl kryptografi som digitala signaturer är att tillit skapas till kommunikationssystemen.

I regeringens proposition om statlig förvaltning i medborgarnas tjänst (prop. 1997/98:135) sägs att statliga myndigheter bör använda säker överföring av dokument och meddelanden i öppna kommunikationsnät. Regeringen aviserar att ett för myndigheterna gemensamt regelverk för säker kommunikation i statsförvaltningen kommer att utarbetas.

I propositionen Förändrad omvärld - omdanat försvar (prop. 1998/99:74) säger regeringen att den avser att pröva förutsättningarna för att inrätta en särskild funktion för att motverka attacker mot informationssystem, liksom om det finns skäl att utvidga ansvarsområdet beträffande signalskyddstjänsten (skydd av kommunikationer) i enlighet med förslaget från Regeringskansliets arbetsgrupp om informationskrigföring. Arbetsgruppens förslag skulle innebära att Försvarsmaktens ansvarsområde vidgas till att även omfatta civila totalförsvarsviktiga informationssystem. För att ge underlag för ett eventuellt införande av en IT-kontrollfunktion för statsförvaltningen, kommer regeringen att uppdra åt Försvarsmakten att genomföra en försöksverksamhet inom försvarssektorn under år 2000.

Departementspromemorian Digitala signaturer – en teknisk och juridisk översikt (Ds 1998:14) innehåller underlag som legat till grund för svenska ståndpunkter i EU rörande digitala och elektroniska signaturer. I fortsättningen används genomgående begreppet ”elektroniska signaturer” eftersom EU kommer att använda det i kommande reglering.

Kryptografi används i avkodningsutrustning för kodade sändningar av TV- och ljudradioprogram. Detta regleras i lagen (1993:1367) om förbud beträffande viss avkodningsutrustning.

2.2 Användning av kryptoteknik

Elektroniska informationstjänster i samhället

Regeringen har tidigare bl.a. i skrivelsen om elektronisk handel (skr. 1997/98:190) givit uttryck för uppfattningen att informationstekniken skall utnyttjas för att skapa tillväxt och sysselsättning samt ge bättre service. Därmed ökas Sveriges konkurrenskraft och medborgarnas välfärd. För företagen medför informationstekniken ökad effektivitet och förbättrade möjligheter att tillgodose kunders behov. Den innebär helt nya möjligheter och förutsättningar för de ekonomiska aktiviteterna i samhället och för samhällets organisation, där geografiska avstånd inte behöver ses som svåröverkomliga hinder för att etablera och driva verksamhet och bereda människor goda livsbetingelser. Regeringen anser att det är av stor vikt att ta vara på dessa möjligheter.

Den tekniska utvecklingen medger att elektroniska meddelanden och dokument kan innehålla text, bild, ljud och andra data. Telefoni och datakommunikation växer samman. Gamla nät- och systemgränser suddas ut. Internet är det tydligaste exemplet på detta, och illustrerar även att gränserna mellan massmedia och interaktiv databehandling håller på att försvinna. Nya tillämpningar växer fram där t.ex. skyddet av upphovsrätt skärper kraven på informationssäkerhet och användning av kryptografi.

De elektroniska tjänsterna skapar nya samarbetsformer mellan organisationer i Sverige eller utomlands, samt ger ökade möjligheter till arbete på distans.

Svenska IT-företag ligger långt framme när det gäller tekniska innovationer. Även inom programvarubranschen hävdar sig svenska företag väl i internationell konkurrens.

Den svenska användningen av den nya informationstekniken och av kommunikationstjänster är omfattande. Enligt Sifo använde ca 48 procent av den svenska befolkningen i åldern 12–79 år (dvs. 3,4 milj. personer) Internet i mars 1999. Även när det gäller nya tjänster har spridningen gått relativt långt. Exempelvis har ca 700 000 kunder egen anslutning till banktjänster på Internet. Under 1999 förutspås 1,3 milj. personer komma att handla på Internet.

Den offentliga förvaltningen använder sig i stor utsträckning av informationsteknik vid sina kontakter med medborgare och företag. En viktig ambition i förvaltningspolitiken är att introducera en omfattande elektronisk självservice, med användning av Internet-teknik. Den

utrustning som hushåll och företag skaffar sig för användning av Internet skall även kunna användas för elektronisk kommunikation med kommunala och statliga myndigheter. Det ger bättre service till lägre kostnad och frigör resurser som kan användas där personlig kontakt alltjämt erfordras.

Informationssäkerhet och kryptografi

Under slutet av 1980-talet började användningen av öppna kommunikationsnät att ta fart. Det främsta exemplet idag är Internet som bl.a. utmärks av att inte ha en tydlig nätägare med ansvar för hela nätets säkerhet. I stället består Internet av en mängd hopkopplade nät med skilda nätägare.

Numera förbinder dessa öppna nät verksamheter inom samhällets olika sektorer och möjliggör nya arbetsformer och allianser. Myndigheter, företag och enskilda kommer i ökad utsträckning att utnyttja de öppna kommunikationsnäten för allt flera tjänster. Ett problem är emellertid att användare måste vidta särskilda åtgärder för att skydda sin kommunikation på öppna nät. Detta skapar behov av informationssäkerhetsåtgärder, främst kryptografi. Kryptografin erbjuder även andra möjligheter och kan exempelvis användas för att försvåra eller förhindra att en avsändare förnekar att ett meddelande har skickats. Det senare är viktigt om elektroniska funktioner skall kunna ersätta pappersdokument, skrivna kvitton eller andra bevishandlingar.

Grundläggande säkerhetskrav, som kan uppfyllas av kryptografi och ge förtroende för kommunikationstjänster är:

- att säkerställa identiteten hos avsändare och mottagare av dokument eller meddelande,
- att skydda dokument eller meddelande mot förvanskning,
- att skydda dokument eller meddelande från obehörig insyn,
- att en sändare inte kan förneka sina dokument eller meddelanden.

Även när information lagras i datorer kan kryptografi användas som skydd mot insyn och förvanskning av informationen, t.ex. om en dator blir stulen, eller om en obehörig bereder sig tillträde till ett kontor och försöker få tillgång till data som är lagrade på datorns hårddisk eller på disketter.

Kryptografi är också ett medel att skydda den personliga integriteten, t.ex. vid överföring av känsliga personuppgifter.

Förutsättningar i form av infrastruktur och tillgång till kryptografi börjar nu växa fram i Sverige. För att säkerställa identitet och skydda dokument mot förvanskning krävs elektroniska signaturer. Sådana kan vid elektronisk kommunikation bl.a. ersätta traditionella underskrifter och ge en högre grad av säkerhet både när det gäller identifieringen och innehållet jämfört med en egenhändig underskrift. Både elektroniska signaturer och konfidentialitet skapas med hjälp av kryptoalgoritmer och kryptonycklar. Kryptoalgoritmerna bör vara starka och beprövade samt internationellt accepterade.

Sambandet mellan kryptonycklarna och en bestämd person eller organisation intygas i så kallade certifikat. Särskilda organ tillhandahåller tjänster för hantering av certifikat och kryptonycklar, främst inom tre huvudområden: identifiering, signaturer och konfidentialitet.

För att kryptonycklar, certifikat och elektroniska signaturer skall kunna få en omfattande användning måste dock vissa problem lösas. En fråga gäller vilken rättslig status elektroniska signaturer skall ha i förhållande till sedvanliga underskrifter. Vidare kan näringsrättsliga regler behövas för de särskilda organens verksamhet. Användare måste ha möjlighet att bli informerade om vilka regler som gäller.

När dessa organ finns på plats i Sverige och erbjuder sina tjänster väntas allt flera börja använda kryptografi för säker kommunikation, men också för att skydda lagrad information.

Det växande antalet datorer på arbetsplatser och i hemmen samt spridningen av Internet kommer att leda till större efterfrågan på kryptoteknik för elektroniska signaturer och för konfidentialitet.

Svensk kryptografi har sedan länge ett grundmurat anseende. Den första svenska kryptomaskinen konstruerades så tidigt som år 1786. Svensken Boris Hagelins kryptomaskiner var under 1940-talet världens mest sålda. Även idag hävdar sig svenska kryptoprodukter väl i internationell konkurrens.

Vissa gemensamma insatser i näringslivet

I Sverige görs i näringslivet olika gemensamma insatser för att främja utveckling och användning av kryptografi samt för att stimulera företag att utveckla och marknadsföra kryptoprodukter och kryptotjänster. Några exempel lämnas här.

SEIS (Säkrad Elektronisk Information i Samhället) är en ideell svensk förening med ett 50-tal medlemmar. Föreningens syfte är att för medlemmarnas räkning förvalta, utveckla och skapa acceptans för den elektroniska lösning för identifikation, signering och konfidentialitet som föreningen tagit fram. Föreningen har även till uppgift att bevaka och påverka utvecklingen inom sitt verksamhetsområde så att alla användare skall kunna kommunicera elektroniskt på ett tryggt och säkert sätt.

Sveriges Industriförbund har identifierat elektroniska affärer som en av de viktigaste globala näringslivsfrågorna de kommande åren. Förbundet anser att en förutsättning för att elektroniska affärer skall få den tillväxt som många förväntar sig är att säkerhetsfrågorna kan lösas varvid tillgången till starka kryptoprodukter är en avgörande faktor.

För att stimulera och driva på utvecklingen av elektroniska affärer i Sverige har Industriförbundet tillsammans med Företagarnas Riksorganisation, Landstingsförbundet, Statskontoret, Svensk Handel, Svenska Bankföreningen, Svenska IT-företagens Organisation, Exportrådet samt Svenska Kommunförbundet bildat föreningen Gemenskapen för elektroniska affärer, GEA. En av de viktigaste uppgifterna för GEA är att arbeta för en ökad säkerhet vid elektroniska affärer.

Svenska Bankföreningen bevakar IT-säkerhetsområdet, genom Bankernas Säkerhetskommitté och dess undergrupp IT-säkerhetsgruppen. Bl. a. bevakas hotbildsförändring, teknisk utveckling och standardisering.

Svenska Nationalkommittén för den Internationella Handelskammaren (ICC) har en IT-säkerhetsgrupp som är starkt engagerad i kryptografifrågorna. ICC verkar för enhetliga internationella regler och har bl.a. tillsammans med andra industri- och användargrupper i ”The Alliance for Global Business” formulerat en ”Global Action Plan”.

Dataföreningen i Sverige med ca 28 000 medlemmar i Sverige, verksamma på IT-området, har en särskild intressegrupp, SIG Security, som bedriver utvecklingsarbete och tar initiativ till utbyte av erfarenheter på området IT-säkerhet och kryptografi.

IT-Företagen, en branschförening inom Industriförbundet bestående av över 600 IT-företag verksamma inom hårdvaru-, mjukvaru- och Internetområdena, har en arbetsgrupp för säkra elektroniska affärer. Gruppen består av flera säkerhetsorienterade IT-företag tillsammans med tjänste- och systemleverantörer. Dessa företag tillverkar säkerhetsprodukter, erbjuder tjänster som certifikatutgivning eller erbjuder systemlösningar där kryptografi ingår i komponenter eller där kryptografi används i den interna företagskommunikationen, t.ex. mellan enheter lokaliserade i olika delar av världen.

Föreningen Svensk Programvaruindustri är en branschförening i Svensk Industriförening med ca 70 programvaruföretag som medlemmar. Flera utvecklar kryptoteknik och kryptosystem. Ännu fler bygger in sådana säkerhetslösningar i sina produkter och programvaror.

2.3 Brottsbekämpning m.m.

Det är ett viktigt samhällsintresse att användarna själva skyddar sin informationsbehandling och kommunikation och därmed förhindrar eller försvårar brottslig verksamhet. Att använda kryptografi är ur denna synvinkel en önskvärd åtgärd. Kryptoteknik kan dock användas även i syfte att dölja brottslighet. För att förhindra och utreda brott som utförs med stöd av denna teknik, är det nödvändigt att brottsbekämpande myndigheter får effektiva redskap till sitt förfogande.

De brottsbekämpande myndigheterna har behov av att få tillgång till lagrad information hos misstänkta samt kunna ta del av information som inhämtats genom avlyssning. Om informationen är krypterad måste den kunna dekrypteras av de brottsbekämpande myndigheterna.

De grundläggande bestämmelserna om husrannsakan och beslag vid utredning av brott finns i rättegångsbalken. En husrannsakan får bl.a. ske i syfte att söka efter föremål som är underkastat beslag eller för att på annat sätt utröna omständigheter som kan ha betydelse för utredningen av ett brott. Ett föremål som skäligen kan antas ha betydelse för utredningen av ett brott får tas i beslag. Några särskilda regler som avser IT-miljön finns inte, men regelsystemet är för närvarande föremål för en översyn inom Justitiedepartementet.

Regler om hemlig teleavlyssning m.m. finns i rättegångsbalken. Hemlig teleavlyssning innebär att alla slags telemeddelanden, också datakommunikation kan avlyssnas i hemlighet. För att sådan avlyssning skall få ske enligt rättegångsbalken krävs bl.a. att någon är misstänkt för ett brott som har ett minimistraff på två års fängelse eller att misstanken avser ett förbrott till ett sådant brott. Det krävs att åtgärden är av synnerlig vikt för brottsutredningen. Det är domstol som beslutar om avlyssning skall få ske. En teleoperatör är i princip skyldig att tillhandahålla en av operatören själv krypterad signal i klartext.

Hemlig teleavlyssning är ett viktigt hjälpmedel för att utreda och avslöja brott. Misstänkta som blivit föremål för hemlig teleavlyssning har hittills inte i någon påtaglig utsträckning utnyttjat möjligheten att använda sig av kryptering. Den hemliga teleavlyssningen har därför fungerat i stort sett som avsett. Om kommunikationsnät i ökad utsträckning utnyttjas för brottslig verksamhet och tillgången till effektiv kryptoteknik underlättas, kan det förutses att de brottsbekämpande myndigheterna kommer att möta allvarliga hinder om det inte finns möjlighet att få tillgång i klartext till krypterad kommunikation eller lagrad information.

Av regeringens skrivelse till riksdagen i oktober 1998 om hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning vid förundersökning i brottmål under år 1997 (skr. 1998/99:21) framgår att domstol under samma år, när det gäller förundersökning avseende grova narkotikabrott, har meddelat tillstånd att i hemlighet *avlyssna* kommunikation till eller från telefonapparater eller andra teleanläggningar som har innehafts eller använts av 281 misstänkta personer. Under åren 1988–1996 har antalet fall legat mellan 210 och 333. När det gäller andra grova brott där det enligt rättegångsbalken är tillåtet att använda hemlig teleavlyssning har detta skett i 58 fall under år 1997. Under åren 1988–1996 har antalet fall legat mellan 13 och 91. Det har år 1997 gällt förundersökningar huvudsakligen rörande mord eller försök, förberedelse och stämpling till detta brott, grovt rån eller medhjälp, försök och förberedelse till detta brott, människorov, mordbrand, grovt koppleri och grov penningförfalskning.

Avlyssningen har haft betydelse för förundersökningen i fråga om den misstänkte i 41,5 procent av fallen år 1997. Under åren 1988–1996 har antalet fall där åtgärden haft betydelse för förundersökningen legat mellan 44 och 56 procent.

Under år 1997 lämnades tillstånd i 165 fall till hemlig *teleövervakning*. Av dessa avsåg 115 fall narkotikabrott. Övervakningen hade betydelse för förundersökningen beträffande den misstänkte i 36 procent av fallen.

Skattemyndigheter och andra myndigheter behöver också tillgång till lagrad information för att kunna utöva kontroll och tillsyn. Om informationen är krypterad måste den först omvandlas till klartext.

Enskilda är skyldiga att medverka i skatteutredningar, men självklart kan ett skattesystem inte fungera enbart på uppgifter som den skattskyldige lämnar frivilligt. Skattemyndigheten måste kunna använda sig av olika former av tvångsåtgärder för att säkerställa skattesystemets funktion. Om den skattskyldige inte fullgör sina skyldigheter får skattemyndigheten förelägga vite. Om det finns anledning att anta att den

skattskyldige har begått brott så får dock den skattskyldige inte föreläggas att medverka i utredningen av en fråga som har samband med den gärning som brottsmisstanken avser. Skattemyndigheten kan vidare göra revision för att granska näringsidkares bokföring m.m. Vid revision skall den skattskyldige tillhandahålla de handlingar och lämna de upplysningar som behövs för revisionen. Skattemyndigheten kan också under vissa förutsättningar tillgripa tvångsåtgärder för att kunna genomföra en revision, bl.a. får ADB-material omhändertas.

Det kan i detta sammanhang nämnas att det enligt bokföringslagen inte är tillåtet att göra bokföringsmaterial oläsligt. Bokföringsmaterialet skall alltid kunna tas fram i läsbar form, och det får således inte vara krypterat vid presentationen.

2.4 Skydd av samhällsfunktioner

För att skydda Sveriges säkerhet och oberoende samt ge underlag för regeringens bedömning av den allmänna utrikes- och säkerhetspolitiska utvecklingen bedriver försvaret signalspaning i syfte att upptäcka verksamhet riktad mot vårt land. Svensk signalspaning är enbart riktad mot utlandet och har därför inte behov av att den inhemska användningen av kryptografi regleras.

Signalspaningens möjligheter att förvarna om olika slags hot beror bl.a. på om man genom exportkontroll lyckas förhindra spridning av avancerad kryptoteknik till oönskade användare. En vidgad internationell användning av avancerad kryptoteknik riskerar att försvåra eller omöjliggöra för signalspaningen att dekryptera signaler och redovisa meddelanden i klartext.

Om kryptosystem som används i totalförsvaret eller utrikesförvaltningen är behäftade med svagheter och främmande makt får tillgång till känslig information, kan konsekvenserna bli förödande i en krigssituation. Om instruktioner inför en regeringsförhandling blir kända av motparten kan det påverka förhandlingsresultatet. Information kan läcka ut under lång tid, eftersom den som har lyckats forcera ett system kan hålla detta hemligt.

Kryptosystem som används inom utrikesförvaltningen och totalförsvaret granskas och godkänns av TSA (Totalförsvarets signalskyddssamordning) innan de tas i bruk. TSA utför också inspektioner för att kontrollera att systemen handhas på ett riktigt sätt. TSA har möjlighet att ge råd till verksamheter i Sverige utanför totalförsvaret, såväl inom den offentliga som den privata sektorn.

Den praktiska hanteringen av driftsatta kryptosystem är vital för att de skall ge avsett skydd. Den i avsnitt 2.1 föreslagna IT-kontrollfunktionen för statsförvaltningen kan enligt arbetsgruppen om informationskrigföring ha TSA som en lämplig bas.

Svaga system kan leda till problem, även då de används av myndigheter som inte tillhör totalförsvaret. Ett dataintrång kan ske i syfte att störa samhällsfunktioner såsom utbetalningar av pensioner eller försäkringar och för att förorsaka problem av olika slag. Den som lyckas tränga in i

centrala datasystem kan slå ut viktiga infrastrukturer som järnvägstrafik, flygledning och elförsörjning.

Det är även ett nationellt intresse att näringslivet genom säkra kryptosystem skyddar sig mot kvalificerad brottslighet och industrispionage. Företagen är beroende av korrekta och snabba informationer och tillförlitliga tekniska system. När valutahandel och finansiella system störs och viktiga företagshemligheter kan inhämtas av utländska konkurrenter, får detta konsekvenser för hela samhället.

2.5 Exportkontroll

Exportkontroll av vissa strategiska produkter, dvs. produkter som kan användas för både civila och militära ändamål, avser att förhindra att känsliga produkter och teknik exporteras till sådana mottagare som kan antas använda dem för att framställa massförstörelsevapen eller för annat fredshotande syfte.

I stället för strategiska produkter används ibland uttrycket varor med dubbla användningsområden eller dual use-produkter. Kryptoteknik är en sådan högteknologisk produkt, som kan störa svenska säkerhetsintressen.

Exportkontrollen av strategiska produkter har en annan karaktär än kontrollen av krigsmateriel. För handel med krigsmateriel gäller ett generellt förbud mot utförsel utan särskilt tillstånd. För strategiska produkter gäller däremot presumtionen att export skall tillåtas.

33 länder (flertalet OECD-länder samt bl.a. Ryssland, Ukraina och Argentina) ingår i det år 1996 etablerade Wassenaar-arrangemanget som samarbetar om exportkontroll av krigsmateriel och produkter med dubbla användningsområden, däribland kryptoprodukter.

Inom EU har rådet med stöd av artikel 113 i EG-fördraget beslutat förordning (EG) nr 3381/94 av den 19 december 1994 om upprättandet av en gemenskapsordning för kontroll av export av varor med dubbla användningsområden. Förordningen innebär i huvudsak att tillstånd krävs för export (dvs. utförsel ut ur EU) av sådana varor som finns förtecknade i bilaga I till rådets beslut 94/942/GUSP av den 19 december 1994. För produkter upptagna i bilagorna IV och V till samma beslut krävs tillstånd för utförsel till annat EU-land, dvs. för dessa produkter gäller f.n. inte frihandel inom EU.

Den svenska exportkontrollen av strategiska produkter styrs av EU:s regelverk på området. I Sverige har rådsförordningen och rådets beslut kompletterats genom lagen (1998:397) om strategiska produkter och genom förordningen (1998:400) om strategiska produkter.

Ansvaret för tillämpningen av den svenska exportkontrollen ligger hos Inspektionen för strategiska produkter (ISP). I kryptofrågor samråder ISP med totalförsvarets experter. Om man önskar exportera en kryptoprodukt av viss beskaffenhet från Sverige skall en skriftlig ansökan lämnas till ISP. För kryptoteknik kan man ansöka om två slags tillstånd, globalt och individuellt. Globalt tillstånd gäller för en produkt under en viss tid och till ett visst antal länder medan individuellt tillstånd gäller för en speciell utförsel.

3 Vissa internationella frågor

3.1 Samarbetet inom EU

Frågor om kryptografi behandlas i Europeiska unionens tre pelare (den inre marknaden, säkerhetspolitik och rättsligt samarbete). Åtgärder inom en pelare påverkar förutsättningarna för och behoven av åtgärder i de båda andra.

När det gäller kryptografi verkar Sverige för att en nödvändig samordning kommer till stånd. Den s.k. SOGIS-kommittén (Seniors Officials Group on Information Systems Security) på IT-säkerhetsområdet, har sedan år 1992 rådets uppgift att verka för samarbete och samordning.

Elektroniska signaturer

Kommissionen lade den 13 maj 1998 fram ett förslag om en gemensam ram för elektroniska signaturer, KOM (1998) 297 slutlig. Direktivförslaget syftar till att främja användandet av elektroniska signaturer på den inre marknaden, och därmed stödja utvecklingen av elektronisk handel. Detta skall ske genom en rättslig ram för användning av elektroniska signaturer och genom att signaturerna erkänns rättsligt.

I direktivförslaget finns regler om certifikat och elektroniska signaturer. ”Kvalificerade certifikat” och ”avancerade elektroniska signaturer” förses med speciella villkor och regler som anger skyldigheter och rättigheter som innehavarna åtnjuter.

Direktivförslaget innehåller också regler om marknadstillträde för certifieringsinstanser, som i direktivförslaget benämns Certification Service Providers (CSP), dvs. sådana instanser som tillhandahåller signaturtjänster. Reglerna innebär att medlemsstaterna inte får göra tillhandahållandet av signaturtjänster beroende av tillstånd i förväg. Frivilliga ackrediteringssystem är dock tillåtna, vilket innebär ett system för bedömning av överensstämmelse med uppställda krav. Medlemsstaterna skall se till det finns lämplig tillsyn av verksamhet för signaturtjänster. Medlemsstaterna får dock ställa ytterligare krav på användningen av elektroniska signaturer i den offentliga sektorn.

En elektronisk signatur, som uppfyller vissa krav, skall anses likvärdig med en handskriven underskrift. Detta gäller dock endast på de områden där medlemsstaterna har bestämt sig för att acceptera användningen av elektroniska signaturer. Direktivförslaget innehåller även regler om skadeståndsansvar för certifieringsinstanser som tillhandahåller signaturtjänster och utfärdar kvalificerade certifikat.

Rådet antog en gemensam ståndpunkt avseende direktivförslaget i april 1999. Efter det att Europaparlamentet har behandlat rådets gemensamma ståndpunkt kan rådet slutligt ta ställning till förslaget.

Kommissionen har den 15 maj 1998 lagt fram ett förslag (KOM (1998) 257 slutlig) till en ny förordning för kontroll av export av varor och teknik med dubbla användningsområden. I förslaget uppger kommissionen att den nuvarande ordningen inte fungerar på ett tillfredsställande sätt. Det har inte upprättats en fullt trovärdig kontrollordning på gemenskaps-nivå för export till tredje land. Kommissionen anser också att den nuvarande ordningen måste förenklas vad gäller handeln inom EU.

EG-domstolen har i två domar, meddelade i oktober 1995, fastställt att gemenskapen har exklusiv behörighet i fråga om exportkontroll av varor med dubbla användningsområden. Enligt domstolen omfattas bestämmelser om restriktioner för exporten till tredje land av varor med dubbla användningsområden av artikel 113 i EG-fördraget.

Kommissionens förslag till ny förordning inbegriper även kontroll av tekniköverföring via elektroniska medier, telefax och telefon. Förslaget likställer fysisk överföring av teknik med överföring av teknik med hjälp av elektroniska media, fax och telefon. Enligt nu gällande ordning är kontrollen begränsad till att endast gälla fysisk överföring, t.ex. då en ritning skickas med post. Om ritningen i stället skickas som fax eller e-post finns det ingen kontroll av överföringen. Förslaget innebär att en lucka i lagstiftningen på gemenskapsnivå täpps till.

För området kryptografi skulle detta förslag påverka skyldigheten att söka licens för att exportera kryptoprodukter via elektroniska media till destinationer utanför EU.

Ett annat förslag av betydelse för kryptografin är att licens för att få föra ut en kryptoprodukt till ett annat EU-land ersätts med ett anmälningsförfarande i efterhand. Detta förslag skulle kunna medföra att företag i EU kan få hela den inre marknaden som sin hemmamarknad. En sådan hemmamarknad blir storleksmässigt likvärdig med den amerikanska hemmamarknaden för kryptoprodukter.

Kommissionens förslag bereds i en ad hoc-grupp i rådet. Ett ställningstagande väntas under år 1999. När detta har skett behöver det svenska regelverket ses över och anpassas till den nya förordningen.

Brottsbekämpning

Inom EU:s tredje pelare har diskussioner inletts i rådet under våren 1998 om brottsbekämpande myndigheters befogenheter i samband med brottslingars användning av kryptering.

Ministerrådet har den 28 maj 1998 godkänt vissa slutsatser om kryptering och brottsbekämpning. Rådet noterade att brottsbekämpande myndigheter är oroade av att den allmänna tillgången till kryptotjänster för konfidentialitet allvarligt kan påverka kampen mot grov brottslighet och terrorism om det inte finns möjlighet, när så är nödvändigt och lämpligt, att från fall till fall skaffa sig laglig tillgång till privata konfidentialitetsnycklar. Rådet har därför enats om att noga bevaka i vilken utsträckning grova brottslingar och terrorister använder sig av kryptoteknik.

En av flera möjliga metoder, som kunde tillgodose brottsbekämpningens intressen, skulle enligt rådets uppfattning kunna vara främjandet

av tjänster för konfidentialitet, med innebörd att en dekrypteringsnyckel eller annan information deponeras hos en tredjepart. Brottsbekämpande organ kan även komma att kräva laglig tillgång till dekrypteringsnycklar i de fall där det är nödvändigt att dekryptera material som har beslagtagits. Rådet medger att en rad åtgärder, inbegripet lagstiftning, kan komma att krävas för att skydda medborgarna mot grov brottslighet och terrorism. Alla sådana åtgärder måste emellertid vara väl avvägda och övriga viktiga intressen måste beaktas. De måste framför allt fullt ut beakta eventuella menliga återverkningar samt behovet av skydd för medborgerliga fri- och rättigheter och vikten av att garantera den inre marknadens funktion så att den elektroniska handeln kan utvecklas på bästa sätt. Eventuella åtgärder för att möjliggöra tillgång till dekrypteringsnycklar måste därför även innefatta starka säkerhetsgarantier.

Enligt rådets uppfattning är det viktigt att det skapas en allmän förståelse för de brottsbekämpande organens behov i de fall kryptotjänster används i konfidentialitetssyfte.

Rådet har därför enats om att utarbeta en resolution om kryptografi och brottsbekämpning som komplement till det arbete som pågår på annat håll inom rådet. I resolutionen kommer medlemsstaterna att uppmanas att ta hänsyn till brottsbekämpningens behov vid utarbetandet av sina nationella strategier.

3.2 Wassenaar-arrangemanget och nya EU-regler

Under år 1998 har en översyn skett av varulistorna för den exportkontroll som Wassenaar-arrangemanget fastställer. Dessa varulistor används vid tillämpningen av EG-förordningen om kontroll av export av varor med dubbla användningsområden.

Den nya varulistan för informationssäkerhet, som länderna enades om den 3 december 1998, är uppbyggd så att det tydligt anges vilken utförsel av kryptoprodukter som skall kontrolleras och därmed också vad som inte är under kontroll. En avsikt är att personer och företag som önskar exportera kryptoprodukter skall kunna få en tydlig vägledning. En annan avsikt är att länderna skall kunna kontrollera exporten på ett likartat sätt. Reglerna skall inte vara svåra att tolka. Ett exportföretag skall varken diskrimineras eller gynnas av det egna landet, jämfört med företag i andra länder. De nya reglerna innebär att en stor del av den nuvarande användningen av kryptografi i världen är fri från kontroll. Endast kryptoprodukter med en nyckellängd som överstiger 56 bitar för symmetriska kryptosystem eller överstiger 512 bitar för asymmetriska kryptosystem är föremål för exportkontroll. Dessa begränsningar skall ses över senast år 2000.

I listan anges också några väsentliga undantag från kontroll. Kryptoprodukter som den enskilde användaren för med sig till utlandet för eget bruk är t.ex. undantagna från exportkontrollen.

En särskild not om kryptografi (som innefattar både programvara och hårdvara) har tillkommit, som undantar s.k. massmarknadsprodukter från kontroll. Noten gäller sådana produkter som säljs utan restriktioner över

disk, via postorder, elektroniskt eller via telefon. Användaren skall inte kunna ändra den kryptografiska funktionen och han skall själv kunna installera programvaran utan väsentlig medverkan av försäljaren. Vidare gäller för symmetriska kryptosystem att de inte skall kunna skapa nycklar som överstiger 64 bitar. På begäran skall också leverantören kunna visa upp teknisk information om kryptoprodukten för berörd myndighet i det egna landet. 64-bitarsgränsen i kryptografinoten gäller fram till den 3 december 2000. Om inte deltagarna i Wassenaar-arrangemanget då har kommit överens om de fortsatta reglerna faller denna begränsning bort.

Även fortsättningsvis gäller bestämmelsen att kryptoprogramvaror, som är allmänt tillgängliga (”in the public domain”) skall vara undantagna från exportkontroll. Med ”allmänt tillgänglig” avses att en programvara har gjorts allmänt tillgänglig utan restriktioner för dess vidare spridning. Regeringen anser att programvaror som var ”allmänt tillgängliga” vid reglernas ikraftträdande skall undantas från exportkontroll. Om någon utan tillstånd senare har gjort kryptoprogramvaror tillgängliga i strid mot gällande bestämmelser, bör däremot utförseln fortsatt kontrolleras.

Rådet har genom beslut den 9 mars 1999 (1999/193/GUSP) ändrat bilagorna till den nuvarande EG-förordningen om kontroll av export av varor med dubbla användningsområden i enlighet med överenskommelsen den 3 december 1998 i Wassenaar-arrangemanget. Ändringen, som trädde i kraft den 19 april 1999, innebär bl.a. att massmarknadsprodukter, oavsett styrka, både hårdvara och mjukvara, omfattas av den inre marknadens fria rörlighet.

Som nämnts har kommissionen lagt fram ett förslag till en ny förordning om upprättande av en gemenskapsordning för kontroll av export av varor och teknik med dubbla användningsområden, vari föreslås att all kryptoteknik skall kunna säljas på den inre marknaden på för leverantören ungefär samma villkor som på den egna hemmamarknaden. Det är viktigt i samband med denna liberalisering att alla EU-länder har en likartad tillämpning av kontrollen vid vidareexport av kryptoprodukter till tredje land utanför unionen. I detta syfte har kommissionen föreslagit ett konsultationsförfarande mellan myndigheterna i produktens ursprungsland och i exportlandet samt ett stärkt informationsutbyte.

3.3 OECD

Organisationen för ekonomiskt samarbete och utveckling (OECD) har i mars 1997 antagit riktlinjer för kryptografi (OECD/GD(97)204); se bilaga 3). Riktlinjerna har påverkat flera länders och organisationers arbete med att utforma en politik på kryptografiområdet.

USA och Storbritannien har, tillsammans med några andra länder, tagit initiativ till att vid sidan av OECD utforma mera konkreta åtgärder som ett led i att få fram en global infrastruktur för användning av kryptografi. Avsikten är att användare i olika länder skall kunna kommunicera med varandra även då deras kommunikation är signerad och krypterad. Sverige deltar i dessa diskussioner.

Efter den ministerkonferens om elektronisk handel som genomfördes i Ottawa i oktober 1998 har OECD inlett planeringen av ett internationellt möte om förutsättningar och möjligheter att få till stånd regler och lösningar för säker identifiering av handelsparter. Mötet planeras komma att genomföras i juni 1999 i USA av OECD tillsammans med näringslivsorganisationer, EU samt medlemsländer i Asia Pacific Economic Cooperation.

3.4 Europarådet

I Europarådets ”Recommendation No. R (95) 13 concerning problems of criminal procedural law connected with information technology” sägs bl.a. att åtgärder bör övervägas i syfte att vid brottsundersökningar minimera de negativa effekterna av användning av kryptografi, så att den legitima användningen av kryptografi inte påverkas mer än vad som är oundgängligen nödvändigt. Rekommendationen anger dock inte vilka åtgärder som bör genomföras.

Europarådet har inlett ett arbete om ”Crime in cyberspace” som tar sin utgångspunkt i rekommendation R (89) 9 om datorrelaterad brottslighet och i den ovan nämnda rekommendation R (95) 13. Det nya arbetet syftar till att arbeta fram en konvention.

3.5 Utvecklingen i andra länder

I flera länder pågår för närvarande arbete med att utforma en kryptopolitik. Diskussionerna har i huvudsak gällt frågan om hur man skall kunna tillgodose både användarnas och de rättsvårdande myndigheternas behov och huruvida man skall bygga upp en infrastruktur för nyckeladministration där s.k. tillförlitliga tredje parter (TTP:er) tillhandahåller säkerhetstjänster till användare, bl.a. hantering av kryptonycklar. En lösning som diskuterats är att privata konfidentialitetsnycklar skall deponeras hos en tillförlitlig tredje part. Förvaring av privata konfidentialitetsnycklar bedömer emellertid många som kontroversiell, eftersom den som får tillgång till en sådan nyckel kan dekryptera vissa meddelanden.

I de länder där nyckeldeponering övervägts har en huvudfråga varit om den bör vara frivillig eller obligatorisk. Frankrike hade tidigare ett obligatoriskt system som var kopplat till tillståndskrav för att få importera och använda kryptografi i landet. I januari 1999 beslöt den franska regeringen att liberalisera import och användning samt gå över till ett frivilligt system. I USA har administrationen för några år sedan lanserat tekniska system som möjliggör obligatorisk nyckeldeponering. På senare år har politiken emellertid inriktats på att främja frivilliga system.

Andra länder där man verkar för att främja eller etablera frivillig nyckeldeponering är Australien, Kanada, Nederländerna, Storbritannien och Tyskland, men det finns olikheter mellan de lösningar som övervägs.

I Danmark, där regeringen har låtit utreda frågan om nyckeldeponering, har föreslagits att regeringen skall nöja sig med att avvakta utvecklingen.

I flera länder, där man diskuterar hur frivilliga system skall utformas övervägs bl.a. följande:

- om de instanser/organ som svarar för deponering och återskapande måste vara tredjepartsinstanser,
- om större organisationer får ha egna interna instanser,
- om tredjeparts- och interna instanser själva får välja om de vill bli auktoriserade eller om detta skall vara obligatoriskt,
- om staten eller någon annan organisation på marknaden skall auktorisera tredjeparts- och interna instanser,
- om auktoriserade tredjeparts- eller interna instanser kan ålägga användaren att deponera sin privata konfidentialitetsnyckel hos instansen eller om detta är frivilligt för användaren.

Ett antal länder har krav på tillstånd för import eller användning av kryptoteknik eller har villkorat användningen till vissa av staten godkända procedurer eller produkter för att användare skall få kryptera inom landet.

Exempel på länder med reglering av användning eller införsel av kryptoteknik är Israel (användning/import), Kina inkl. Hongkong (import), Lettland (import), Polen (import), Ryssland (användning/import), Singapore (användning/import), Spanien (användning), Sydkorea (import) och Ungern (import).

4 Regeringens överväganden och slutsatser

Regeringens bedömning: För närvarande föreligger det inte skäl att begränsa användningen av kryptoteknik i Sverige. Alla skall ha rätt att själva välja sådan teknik.

Import av kryptoteknik skall förbli fri.

Det finns fortsatta säkerhetspolitiska skäl att förhindra spridning av kryptoteknik till olämpliga mottagare i vissa andra länder.

Skulle utvecklingen motivera skärpta regler kommer regeringen att överväga lämpliga åtgärder för att skapa möjligheter till laglig åtkomst i klartext av krypterad information för brottsbekämpande och kontrollerande myndigheter.

Sveriges politik bör präglas av flexibilitet och lyhördhet i syfte att kunna möta en ökad efterfrågan på säker kryptoteknik, förändringar i andra länders politik och den fortsatta tekniska utvecklingen på området.

Skälen för regeringens bedömning

Bakgrund

Det kan konstateras att ett flertal olika synsätt kommer fram i diskussionen om användningen av kryptoteknik.

- Användare (en myndighet, ett företag, en enskild) betonar friheten att kryptera information och skydda den mot obehörig insyn eller mot brottslig verksamhet och vill i det avseendet inte utsättas för några inskränkningar. Användare har samtidigt, liksom samhället i övrigt, intresse av att polisen har förmåga att i sin brottsbekämpande verksamhet kunna dekryptera meddelanden för spaning och bevissäkring.
- Användare vill ha ett starkt skydd av den information som skickas eller lagras i krypterad form. Han vill också kunna rädda sådan information om hans privata konfidentialitetsnyckel skulle förkomma och vill då kunna få tillgång till en kopia av nyckeln. Rättsvårdande myndigheter måste få använda tvångsmedel för att få laglig tillgång till sådana privata nycklar.
- Användare vill, vid eventuell deponering av sin privata konfidentialitetsnyckel, att den förvaras på ett säkert och förtroendefullt sätt. Om denna nyckel måste deponeras utanför användarens kontroll minskar förtroendet. Användaren kan då föredra ett annat sätt för förmedling av meddelanden än datakommunikation, t.ex. kurirpost eller en personlig resa.
- Rättsvårdande myndigheter har intresse av att användare skyddar sig med starka kryptosystem för att försvåra eller förhindra brottslig verksamhet. Samtidigt kan en fri tillgång till kryptoteknik för att

skydda data och meddelanden leda till att viss brottsbekämpning försvåras eller förhindras.

- Staten, som ansvarar för rikets säkerhet och skyddar samhället mot terrorism och annan brottslighet, har klassificerat kryptoteknik som en teknik med både civil och militär användning, vars utförsel ur landet bör kontrolleras. Andra anser att export av kryptoteknik inte behöver kontrolleras.

Elektronisk handel m.m.

Elektronisk handel och annan elektronisk kommunikation har under de senaste åren vuxit fram som betydelsefulla användningsområden för den moderna informationstekniken. Det medför nya affärsmöjligheter och nya arbetssätt som ger tillväxt och sysselsättning. Samtidigt ställs stora krav på säkerhet i överföring av meddelanden och dokument samt på säker identifiering av användarna. Detta kan åstadkommas med stöd av kryptografi. Det finns således ett allmänt intresse av att användarna får tillgång till starka kryptosystem och att det finns förutsättningar för bruk av elektroniska signaturer och för skydd av konfidentialitet. Regeringens bedömning är att en bred användning av kryptografi ökar tilliten till kommunikationssystemen. Risken för missbruk av kryptografi är inte heller av sådant slag att det för närvarande föreligger skäl att begränsa användningen. Alla skall ha rätt att själva välja kryptoteknik och importen av kryptoteknik skall förbli fri.

Som tidigare nämnts, se avsnitt 2.2, används elektroniska signaturer för att säkerställa identitet och skydda dokument mot förvanskning. En central fråga vid utformandet av svenska regler för elektroniska signaturer är hur hanteringen av certifikat och kryptonycklar skall utformas. En s.k. certifieringsinstans är det organ som tillhandahåller signaturtjänster. Organet utställer och signerar certifikat som anger vem som är innehavare av den öppna signaturnyckeln. Certifieringsinstansens roll är alltså avgörande för tilliten till elektroniska signaturer. Vissa grundläggande krav behöver därför ställas på sådana instansers inre organisation samt på de certifikat och nycklar som de utfärdar.

Användarna har ett behov av säkra elektroniska signaturer och tillgång till en öppen marknad för signaturtjänster. Hur ett system för tillsyn och kontroll av signaturtjänster kommer att se ut i Sverige måste ses mot bakgrund av de regler som det kommande EG-direktivet om elektroniska signaturer uppställer. Utgångspunkten är att medlemsstaterna inte får införa obligatoriska tillståndsvillkor för signaturverksamhet. Däremot finns möjlighet att utforma frivilliga ackrediteringssystem. Staten kommer att kunna fungera som förebild i sitt eget användande av signaturtjänster.

Inom regeringskansliet har arbete påbörjats med att skyndsamt ta fram handlingsmöjligheter och förslag till en framtida struktur och organisation av signaturtjänster. Detta arbete kommer att bedrivas i nära samarbete med myndigheter, näringsliv och intresseorganisationer på området.

Kryptografi är ett viktigt hjälpmedel för att förhindra eller försvåra brottslig verksamhet. Användare som skyddar sin information med stöd av kryptografi bidrar till att förebygga brott.

Kryptoteknik kan dock även användas i brottsligt syfte. Brottsbekämpande myndigheter har därför ett behov av att vid tvångsmedelsanvändning, t.ex. husrannsakan och beslag, få tillgång till krypterad information i klartext, samt vid hemlig teleavlyssning få tillgång till privata konfidentialitetsnycklar, utan den misstänktes vetskap, för att kunna dekryptera meddelanden. Kontroll- eller tillsynsmyndigheter har likaså behov av att vid revision och annan kontroll eller tillsyn få tillgång i klartext till lagrad och krypterad information.

De nuvarande reglerna om tvångsmedel skulle erbjuda brottsbekämpande och kontrollerande myndigheter vissa möjligheter att från särskilda organ som tillhandahåller tjänster för hantering av certifikat och kryptonycklar få tillgång till t.ex. privata konfidentialitetsnycklar som deponerats eller annan information som finns om det särskilda organets kunder. Husrannsakan, vittnesförhör eller liknande åtgärder kan också användas för att åstadkomma detta. Sådan tvångsmedelsanvändning sker med stöd av lag och i kontrollerade former. Det är angeläget att den teknik som används i ett särskilt fall inte utgör hinder för sådan legal åtkomst. Kryptonycklar avsedda för elektroniska signaturer bör inte användas för att också skydda konfidentialitet, eftersom en privat signaturnyckel inte bör deponeras. I stället bör separata signaturnycklar och konfidentialitetsnycklar användas.

Brottsbekämpande och andra utredande myndigheters möjligheter till laglig åtkomst i klartext till krypterad information måste säkerställas. För att möjliggöra detta kan, förutom erforderliga inhemska åtgärder, initiativ behöva tas på det internationella planet. Skulle utvecklingen motivera skärpta regler kommer regeringen att överväga lämpliga åtgärder för att skapa möjligheter till laglig åtkomst i klartext av krypterad information för brottsbekämpande och kontrollerande myndigheter.

Regeringen anser härutöver att Sverige bör aktivt medverka i utvecklingen av EU-gemensamma regler och andra internationella överenskommelser på detta område.

Exportkontroll

Enligt regeringens bedömning finns det fortsatta säkerhetspolitiska skäl att förhindra spridning av kryptoteknik till olämpliga mottagare i vissa andra länder. Den svenska inställningen till kontrollen av spridning av kryptoteknik till utlandet (exportkontroll) bör ta hänsyn till att Sverige gynnas av frihandel och global elektronisk kommunikation. Samtidigt är Sverige för sin nationella säkerhet beroende av ett internationellt samarbete där exportkontrollen utgör en del.

- Exportkontrollen av kryptoprodukter fortsätter i enlighet med EU:s regler och Sveriges förpliktelser i Wassenaar-arrangemanget (WA). Sverige verkar bl.a. för att skapa en enhetlig och icke-diskriminerande tillämpning av reglerna i de länder som samarbetar inom WA och inom EU, så att svenska företag inte får en konkurrensnackdel.
- Med nuvarande regler för exportkontroll gynnas företag i länder med en stor hemmamarknad. Sverige välkomnar därför att kommissionen föreslagit att kryptoprodukter skall omfattas av den inre marknadens fria rörlighet.
- Det är viktigt att exportkontrollen successivt liberaliseras och koncentreras på sådana känsliga kryptoprodukter där kontrollintresset väger över frihandelsintresset.
- Regelverken bör uttryckligen likställa fysisk utförsel av kryptoprogram med att göra dem tillgängliga via datanät. Spridningen på nät har redan i dag nått betydande omfattning och därmed har förutsättningarna för den nuvarande exportkontrollpolitiken förändrats.

Den offentliga sektorn

Den offentliga sektorn är liksom andra delar av samhället i behov av säker och tillförlitlig kryptoteknik. Här ingår att kunna bedöma vilka produkter och tekniker som bör utnyttjas. Detta ställer särskilda krav på god kunskap och goda bedömningar i myndigheternas upphandlingar och den rådgivning som de kan behöva i samband därmed.

Statliga myndigheter bör utnyttja nyckelhanteringssystem med inbyggda funktioner för nyckelåterskapande. För att främja detta torde interna organ för hantering av certifikat och kryptonycklar behöva inrättas. De statliga organen bör ha ett sådant regelverk att de kan tjäna som modell även för den privata marknaden. Arbete med sådan inriktning bedrivs i länder som Australien, Finland, Kanada, Storbritannien och USA.

I propositionen om Statlig förvaltning i medborgarnas tjänst informerade regeringen om att ett gemensamt regelverk för säker kommunikation i statsförvaltningen kommer att utarbetas.

Den fortsatta utvecklingen

Utvecklingen inom EU och i länder utanför unionen, bl.a. USA, är av betydelse för utformningen av en svensk politik för användningen av kryptografi. De senaste årens erfarenheter visar emellertid att utvecklingen är svårbedömd och att flera länders kryptopolitik förändrats, ibland snabbt och oväntat. Även tekniken och användningen förändras ständigt. Detta talar för att en svensk politik bör vara öppen för de krav som ställs. Beslut och åtgärder måste fortlöpande kunna omprövas.

Antalet datorer är stort och användningen av Internet är utbredd i Sverige. En betydande del av informationstjänsterna och försäljningen av programvara sker via datanät och allt bättre kryptoprogramvaror blir

tillgängliga på Internet. En kraftigt ökad användning av kryptografi är därför att vänta under de närmaste åren.

En viktig fråga i detta sammanhang är, i vilken omfattning kryptoteknik används för att dölja brottslig verksamhet. Datakunniga brottslingar kan redan i dag skaffa sig mycket kraftfulla kryptoredskap och använda dem utan möjligheter för de rättsvårdande myndigheterna att dekryptera meddelanden och dokument. Sverige, liksom andra länder i EU, följer denna utveckling. Skulle utvecklingen motivera detta kommer regeringen att överväga skärpta regler. Även detta talar för att en svensk politik bör utvecklas stegvis.

Man kan tänka sig olika handlingsvägar vid utformningen av en kryptopolitik. Ett alternativ är att förlita sig på marknadens egen utveckling och inte ta initiativ till att införa några regleringar. Om man vill betona statens roll så kan alternativet vara att skapa möjligheter att tillhandahålla signatur- och konfidentialitetstjänster i Sverige samt att erbjuda organ som tillhandahåller sådana tjänster en lämplig form av auktorisation. Regeringen önskar främja användningen av modern teknik i alla delar av samhället. Informationstekniken skapar möjligheter som måste tas tillvara. Regeringen är vidare angelägen att främja elektronisk handel och annan elektronisk service samt ett säkert utnyttjande av de elektroniska kommunikationsmöjligheterna. En bred användning av kryptoteknik kan gynna utvecklingen av den elektroniska handeln genom att tilliten till systemen ökar. Användningen av kryptoteknik bör därför underlättas och användarna skall själva ha rätt att välja vilken teknik som skall användas.

Vad gäller användningen av *signaturtjänster* förbereds i Regeringskansliet ett införande av det kommande EG-direktivet om en gemensam ram för elektroniska signaturer. Vad gäller frågan om *konfidentialitets-tjänster* bör det utredas om det finns skäl för staten att engagera sig i ett frivilligt auktorisationsförfarande av särskilda betrodda organ som vill tillhandahålla sådana tjänster.

Sveriges politik bör präglas av flexibilitet och lyhördhet i syfte att kunna möta en ökad efterfrågan på säker kryptoteknik, förändringar i andra länders politik och den fortsatta tekniska utvecklingen på området.

Bilaga 1: Terminologi

Ordförklaringarna i denna bilaga är i första hand hämtade från:

Terminologi för informationssäkerhet, Informationstekniska standardiseringen 1994. Rapport ITS 6, ISBN 91-630-2483-7.

OECD:s riktlinjer för politik för kryptografi (mars 1997), se bilaga 3.

asymmetriskt kryptosystem (eng. asymmetric crypto system)
kryptosystem där olika nycklar används för kryptering och dekryptering (ITS 6). Se även bilaga 2.

autenticering (eng. authentication)
1) kontroll av uppgiven identitet, t.ex. vid inloggning vid kommunikation mellan två system eller vid utväxling av meddelanden mellan användare
2) kontroll av att ett meddelande är äkta, i bemärkelsen att det inte förändrats sedan det lämnade avsändaren (användare, dator, kommunikationsnod, etc.).

Anm.: Autenticering (1) är synonymt med verifiering av identitet.

Autenticering (2) benämns ofta meddelandeautenticering (ITS 6).

certifieringsinstans (eng. Certification Authority, CA)
av flera användare betrodd instans som har till uppgift att skapa och utge nyckelcertifikat.

Anm.: Certifieringsinstansen kan även ha andra uppgifter, t.ex. att skapa nyckelpar (öppen/privat nyckel) för varje användare, att hålla och sprida spärrlista för indragna certifikat, etc. (ITS 6). Jfr TTP.

certifikat av öppen nyckel; nyckelcertifikat (eng.: [public key] certificate)
användarens öppna nyckel i ett asymmetriskt kryptosystem, vilken tillsammans med dennes namn och eventuell annan information signeras och utgives av en certifieringsinstans (ITS 6).

CSP (eng. Certification Service Provider)
en person eller ett företag som utfärdar certifikat eller tillhandahåller andra tjänster som har anknytning till elektroniska signaturer.

Anm.: I det kommande EG-direktivet om en gemensam ram för elektroniska signaturer införd benämning som motsvarar certifieringsinstans (se ovan). Etablerad svensk term saknas.

dekryptering (eng. decryption)
återskapande av klartexten, dvs. den omvända funktionen till kryptering.

digital signatur (eng. digital signature)
omvandling av ett meddelande (eller ett kondensat av detta) på ett sätt som endast avsändaren kan utföra och som tillåter mottagaren att kontrollera meddelandets äkthet, innehåll och avsändarens identitet.

Anm.: Digital signatur kan utföras på informationsobjekt i digital form med avsändarens privata nyckel i ett kryptosystem och kontrolleras med den öppna nyckeln (ITS 6). Se även bilaga 2.

elektronisk signatur (eng. electronic signature)
uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra elektroniska uppgifter och som används som autenticeringsmetod.

Anm.: Denna term används i stället för digital signatur (se ovan) i EG-direktivet om en gemensam ram för elektroniska signaturer.

integritet (eng. integrity)
oberörbarhet, helhet med förmåga att upprätthålla ett värde genom ett skydd mot oönskad förändring, påverkan eller insyn.

Anm.: I svensk debatt används termen oftast med hänsyftning till den personliga integriteten när information om personer hanteras i datorsystem. Observera att man i detta fall i engelskspråkiga länder använder termen ”privacy”. Om tveksamhet föreligger bör uttrycket förtydligas: personlig integritet, systemintegritet (ITS 6).

konfidentialitet (eng. confidentiality)
avsikten att innehållet i ett informationsobjekt (eller ibland även dess existens) inte får göras tillgängligt eller avslöjas för obehöriga (ITS 6).

Anm.: Eftersom begreppet inte är kopplat till sekretess i lagens mening, används i föreliggande skrivelse termen konfidentialitet. Sekretess kan dock förekomma som synonym i andra sammanhang.

kryptering (eng. encryption)
omvandling av klartext till kryptotext medelst kryptosystem och aktuell krypteringsnyckel i syfte att förhindra obehörig åtkomst av konfidentiell information (ITS 6).

kryptoalgoritm (eng. cryptographic algorithm)
uppsättning matematiska regler för kryptografiska omvandlingar (ITS 6). I bilaga 2 omnämns olika slags kryptoalgoritmer.

kryptografi (eng. cryptography)
det ämnesområde som innefattar principer, medel och metoder för att omvandla data i avsikt att dölja ett meddelandes informationsinnehåll, verifiera dess autenticitet, förhindra dess fördolda förändring samt förhindra att data förnekas och förhindra dess obehöriga användning (OECD).

kryptosystem (eng. crypto system)
utrustningar och/eller program med tillhörande instruktioner och hjälpmedel som används för kryptografiska tillämpningar (ITS 6, något modifierat).

nyckel (eng. key)
varierbar information som styr en kryptografisk process, t.ex. kryptering, dekryptering eller skapande eller verifiering av en elektronisk signatur. Se vidare bilaga 2.

nyckeldeponering (eng. key escrow)
säker förvaring av en kopia av en kryptonyckel för dekryptering hos någon annan än användaren.

Anm.: Vid nyckeldeponering lämnar den som använder ett kryptosystem frivilligt eller under tvång ifrån sig den privata nyckeln till en fristående instans. Efter domstolsbeslut kan polisen få tillgång till nyckeln eller få hjälp med dekryptering. Även användaren själv kan behöva få tillgång till nyckelkopian om han förlorat sin nyckel eller råkat göra den obrukbar. Jämför nyckelåterskapande.

nyckelhantering (eng. key management)
administration och tekniska metoder för alstring, förvaring, distribution, användning och förstöring samt eventuell certifiering av kryptonycklar på ett säkert sätt (ITS 6).

nyckelåterskapande (eng. key recovery)
i denna skrivelse åsyftar termen vilken som helst teknik för att erhålla en kryptonyckel för dekryptering från någon annan än användaren.

Anm.: Detta kan exempelvis ske genom att en deponerad nyckel hämtas eller att genom att nyckeln återskapas efter visst beräkningsarbete. I andra sammanhang syftar termen ibland endast på återskapande av en nyckel som i krypterad form åtföljer ett meddelande (eng. key encapsulation).

oavvislighet (eng. non-repudiation)
egenskap hos data som förvärvats genom kryptografiska metoder vilken förhindrar en fysisk eller juridisk person att neka till att ha utfört en särskild handling relaterad till data (exempelvis mekanismer som förhindrar förnekande av auktoritet [ursprung], mekanismer för bevis på skyldighet, avsikt eller åtagande eller för bevis på äganderätt) (OECD).

samverkansförmåga (eng. interoperability)
Se bilaga 3.

symmetriskt kryptosystem (eng. symmetric crypto system)
kryptosystem där samma nyckel används för kryptering och dekryptering (ITS 6). Se även bilaga 2.

tillförlitlig tredje part (eng. Trusted Third Party, TTP)
organisationsenhet som är betrodd av en grupp av (kommunicerande) användare med avseende på specificerade säkerhetsrelaterade tjänster (ITS 6).

Anm.: En TTP utför betrodda tjänster på områdena elektroniska signaturer och konfidentialitet, exempelvis skapande och deponering av nycklar. Eftersom en TTP även kan erbjuda certifikattjänster, används i

bilaga 2 TTP som en överordnad term, som bl.a. innefattar termerna certifieringsinstans och CSP. I större företag och myndigheter kan finnas en intern instans som ingår i organisationen.

Bilaga 2: Kortfattad beskrivning av kryptografi

1. Inledning

När man skickar ett viktigt meddelande, kan det skapa stor olägenhet om någon obehörig lyckas läsa det. Man kan vidta olika försiktighetsåtgärder beroende på hur viktigt meddelandet är. Ett brev kan rekommenderas eller skickas med kurir. För att den moderna informationsteknikens möjligheter att skicka meddelanden och lagra data skall kunna tas tillvara måste man kunna skicka viktiga meddelanden och lagra känslig information utan att någon obehörig kan ta del av innehållet.

Ett sätt att förhindra obehöriga att läsa ett meddelande är att förändra klartexten, så att endast den behörige kan läsa det. Man säger att man krypterar klartexten och får en så kallad kryptotext. En krypteringsalgoritm kan liknas vid ett recept på hur man skall förändra en klartext. Ett sådant recept kan ha många varianter. Om två personer skall kommunicera måste de komma överens om både algoritm och variant. Varianten håller man hemlig men inte nödvändigtvis algoritmen. I stället för att säga att man har olika varianter, så säger man att man har olika nycklar. Två personer som skall kommunicera måste alltså komma överens om vilken nyckel de skall använda. När en person vet både algoritm och nyckel, kan denne också omvandla kryptotext till klartext. Det kallas för att dekryptera kryptotexten.

En kryptotext kan forceras, dvs. läsas av någon annan än den tänkta mottagaren, bl.a. genom att olika nycklar prövas till dess att man finner den klartext som ursprungligen krypterades. Är antalet möjliga nycklar litet, hittas den rätta nyckeln snart och meddelandets innehåll är röjt.

Dekrypteras meddelandet manuellt kanske det räcker med några tusen nycklar för att det skall bli omöjligt att dekryptera det inom rimlig tid. I våra dagar används datorer för förmedling av information och för kryptering/dekryptering. Moderna datorer arbetar mycket snabbt och antalet nycklar måste därför vara nästan ofattbart stort. Den kanske mest kända algoritm som används i dag är Data Encryption Standard (DES) med ungefär 72 miljoner miljarder nycklar.

Det krävs mycket stor datorkapacitet för att metodiskt forcera DES-krypterade meddelanden. Enligt uppgift från USA har flera samlade attacker genomförts. I ett fall under 1998 användes en dator som var speciellt utformad för att forcera DES-krypterade meddelanden. Den visade sig behöva i genomsnitt nästan fem dygn för att forcera *ett* meddelande. I ett annat fall i januari 1999 användes samma dator tillsammans med 100.000 persondatorer i ett globalt nätverk på Internet. Detta system med datorer prövade hela 245 miljarder nycklar per sekund och behövde i genomsnitt 1,7 dygn för att forcera *ett* meddelande.

Istället för att ange antalet nycklar brukar man ange nyckellängden. Den enhet som nyckellängden anges i kallas för bitar. För varje tillkommande bit fördubblas antalet möjliga nycklar och därmed tiden för att pröva sig fram till rätt nyckel. Tio bitar betyder ungefär tusen nycklar, 20 bitar ca en

miljon. DES har 56 bitars nyckel. Exempel på andra algoritmer är triple-DES och IDEA med 112 resp. 128 bitars nyckel. Det hela framgår av följande tabell:

10 bitar	1 000
20 bitar	1 000 000
30 bitar	1 000 000 000
40 bitar	1 000 000 000 000
50 bitar	1 000 000 000 000 000
56 bitar	72 058 000 000 000 000
64 bitar	18 450 000 000 000 000 000
osv	

Enligt vad som sagts ovan kan en nyckel (56 bitar) som används för ett DES-krypterat meddelande hittas på mindre än två dygn. Att på motsvarande sätt hitta en 64-bitars nyckel skulle i genomsnitt ta ett år. Att med samma metod pröva alla nycklar i ett kryptosystem med 128 bitars nyckel skulle kräva en miljard gånger universums uppskattade ålder.

En kryptoalgoritms styrka beror emellertid inte enbart på nyckelns längd. Skulle en svaghet finnas i konstruktionen av algoritmen eller kryptosystemet skulle ett meddelande eventuellt kunna läsas av obehöriga på mycket kort tid.

Det finns två olika sorters kryptosystem, symmetriska och asymmetriska.

DES-algoritmen, liksom algoritmerna triple-DES och IDEA, används i symmetriska system. Sådan kännetecknas av att samma nyckel används både för att kryptera och för att dekryptera. Om två personer skall kommunicera med varandra måste de kunna utbyta nyckel med varandra utan att den röjs. I dagens kryptosystem skapas en unik DES-nyckel för varje kommunikationstillfälle. Se vidare avsnitt 3.

För ungefär tjugo år sedan konstruerades de asymmetriska kryptosystemen. Istället för identiska nycklar används nyckelpar, med en öppen och en privat nyckel. RSA-algoritmen är en av de mest kända av de algoritmer som används i asymmetriska kryptosystem. Den nyckellängd som väljs uppgår numera ofta till 1024 eller 2048 bitar. Observera att dessa nyckellängder inte är jämförbara med nyckellängder i symmetriska kryptosystem.

Ett nyckelpar kan användas för att:

- kryptera innehållet från klartext till kryptotext samt för att dekryptera innehållet från kryptotext till klartext. Vid kryptering av innehållet använder sändaren mottagarens öppna nyckel för att kryptera och mottagaren får sedan använda sin privata nyckel för att dekryptera innehållet. Även kryptonycklar kan översändas i krypterad form på detta sätt. Se vidare avsnitt 3.
- signera data och skapa en elektronisk signatur samt för att verifiera den elektroniska signaturen. Vid signering använder sändaren sin privata nyckel för att signera data och mottagaren använder sändarens öppna

nyckel för att verifiera sändarens elektroniska signatur. Se vidare avsnitt 2.

Om endast den öppna nyckeln är känd, är det inte möjligt att räkna ut och använda den privata nyckeln. När A skall skicka ett krypterat meddelande till B måste han, som nämnts, ha tillgång till B:s öppna nyckel. A krypterar nu meddelandet med nyckeln och skickar kryptotexten till B. Eftersom B håller sin privata nyckel hemlig, är han den ende som kan dekryptera och läsa meddelandet.

Nyckelhanteringen för asymmetriska system är enklare än för de symmetriska. Asymmetriska system kallas också för öppna eller publika system.

Vid användning av det asymmetriska systemet måste A kunna försäkra sig om att han verkligen får B:s öppna nyckel och inte den illvillige C:s. I avsnitt 3 behandlas detta. En möjlig lösning är att B:s öppna krypteringsnyckel tillhandahålls av en tillförlitlig tredje part (på engelska Trusted Third Party, TTP). Vill någon sända ett krypterat meddelande till B vänder han sig till TTP:n, som levererar nyckeln och i ett certifikat intygar att det verkligen är B:s nyckel. TTP:ns trovärdighet garanteras normalt genom en licens eller dylikt.

I avsnitt 2, 3 och 4 illustreras på ett mycket förenklat sätt hur ett öppet nyckelsystem kan fungera för sändare A och mottagare B samt deras relation till den tillförlitliga tredje parten, TTP.

I beskrivningen ingår att nycklarna kan certifieras av TTP:n, dvs. de öppna nycklarna kan presenteras på ett sådant sätt att det säkert framgår att en viss nyckel hör till en viss person (apparat, funktion, system etc.). Sådana certifierade nycklar kan därefter distribueras i elektronisk form och göras tillgängliga via öppna medier, t.ex. via öppna katalogsystem.

En TTP certifierar både användarens identitet och dennes öppna nyckel genom att åsätta sin egen elektroniska signatur.

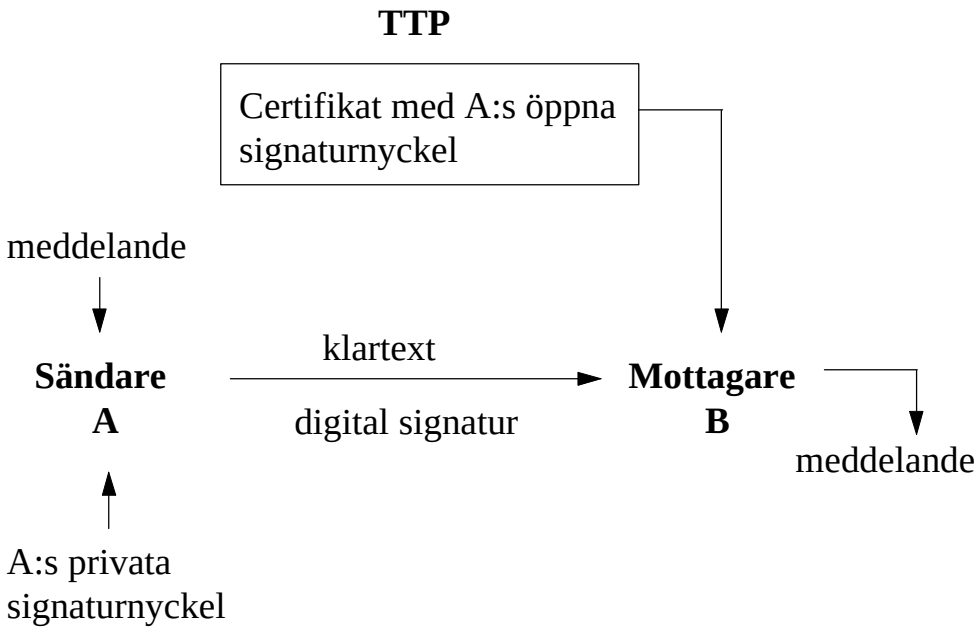
2. Elektroniska signaturer

Om A skickar ett meddelande till B, måste B kunna övertyga sig om att det verkligen är A som har skickat meddelandet och att inte någon har ändrat meddelandets innehåll. Öppna nyckelsystem kan användas för detta. A skaffar sig ett par signaturnycklar, dvs. en privat signaturnyckel (för signering) och en öppen signaturnyckel (för verifiering). Den privata signaturnyckeln behålls av A som en väl bevarad hemlighet. Den öppna signaturnyckeln kan certifieras av en tillförlitlig tredje part (TTP), som både A och B litar på. Denna s.k. certifieringsinstans går i god för att den öppna nyckeln verkligen tillhör A. I fortsättningen används genomgående det något bredare begreppet TTP.

När A skall skicka sitt meddelande så räknar A ut en kontrollsumma, grundat på innehållet i det meddelande som skall överföras. A omvandlar därpå kontrollsumman med sin privata signaturnyckel. Den så omvandlade kontrollsumman utgör den elektroniska signaturen för meddelandet. A skickar sedan den elektroniska signaturen tillsammans

med meddelandet till B. B använder sig nu av A:s öppna signaturnyckel (för verifiering), som t.ex. hämtas från ett katalogsystem. Eftersom den öppna nyckeln är certifierad av en TTP som B litar på är han säker på att han får rätt nyckel. B räknar med hjälp av klartexten ut kontrollsumman samt omvandlar tillbaka den från A erhållna elektroniska signaturen med hjälp av A:s öppna signaturnyckel och jämför resultaten. Stämmer de överens vet B att meddelandet kommer från A och att det ej har ändrats. A:s öppna och privata nycklar utgör ju ett unikt par. Har den ena nyckeln omvandlat kontrollsumman, så är det bara den andra nyckeln i paret och ingen annan nyckel som kan återskapa kontrollsumman. Kontrollsumman är dessutom beräknad så att minsta ändring i meddelandet ger ett tydligt utslag. Därmed har B verifierat A:s elektroniska signatur.

Anmärkning: För att B skall kunna verifiera A:s elektroniska signatur räcker det att A:s öppna signaturnyckel finns säkert åtkomlig. Om B önskar svara på A:s brev och signera svaret skaffar sig B ett par signaturnycklar och samma procedur användas åt andra hållet. Därvid kan alltså A verifiera B:s elektroniska signatur på svarsmeddelandet.



3. Konfidentialitet

Med konfidentialitet avses egenskapen att data och information inte är tillgängliga för eller kan läsas av obehörig.

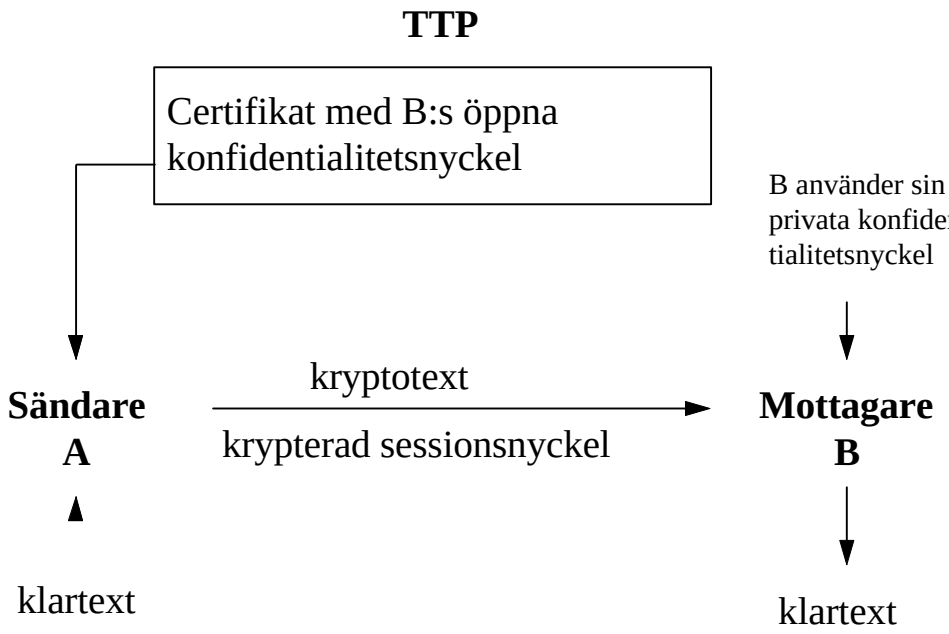
I avsnitt 2 introducerades begreppen symmetriskt och asymmetriskt kryptosystem. I detta avsnitt beskrivs hur de två slagen av system kan kombineras för att på ett smidigt sätt skapa konfidentialitet.

Även här skaffar sig A och B var sitt nyckelpar, s.k. konfidentialitets-nycklar. Varje sådant par består av en öppen (publik) nyckel för kryptering och en privat (hemlig) nyckel för dekryptering. A och B behåller sina privata konfidentialitetsnycklar och får sina öppna konfidentialitets-nycklar certifierade hos en TTP. När A skall skicka ett

meddelande till B, väljer A slumpvis en sessionsnyckel, dvs. en nyckel som används endast vid den överföring av meddelanden som skall ske i den aktuella "sessionen". Med hjälp av sessionsnyckeln och ett symmetriskt kryptosystem, t.ex. DES, krypterar A sin klartext. Anledningen till att man använder ett symmetriskt system för att kryptera klartexten är att ett sådant i regel är snabbare än ett asymmetriskt system vid kryptering av längre meddelanden.

A hämtar därefter B:s öppna konfidentialitetsnyckel från t.ex. ett öppet katalogsystem. Eftersom den öppna nyckeln är certifierad av en TTP som A litar på är han övertygad om att det verkligen är B:s nyckel som han får. Med hjälp av B:s öppna nyckel och det asymmetriska systemet krypteras sessionsnyckeln. Slutligen skickar A det krypterade meddelandet och den krypterade sessionsnyckeln till B.

B dekrypterar den krypterade sessionsnyckeln med hjälp av sin privata konfidentialitetsnyckel. Sedan dekrypterar B kryptotexten med sessionsnyckeln.

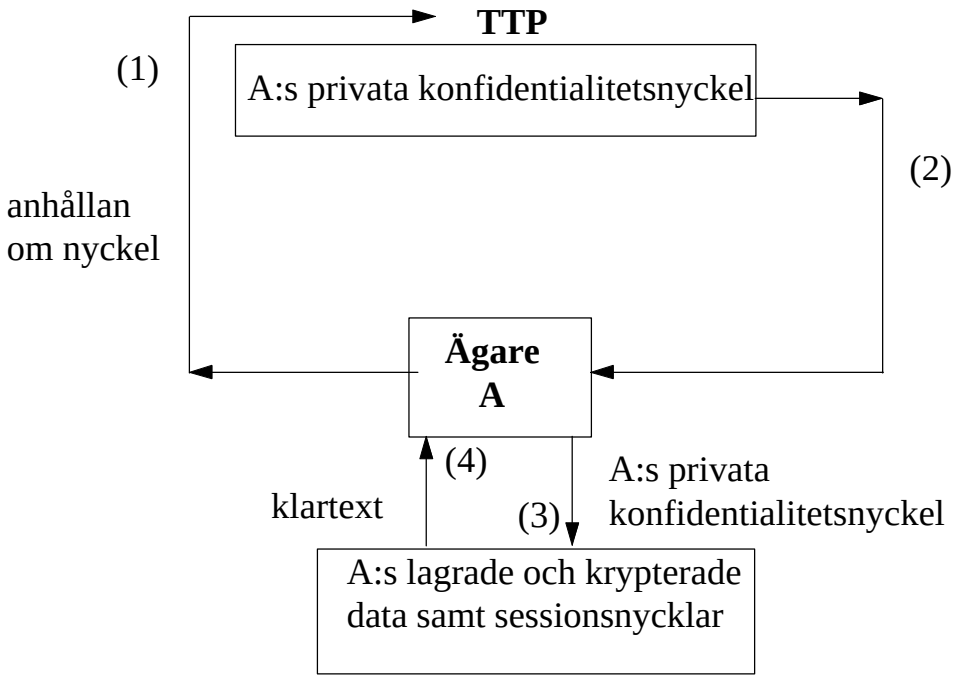


4. Lagring av data och förlorad nyckel

När en användare A önskar skydda sina lagrade data går han i princip tillväga på samma sätt som när han skickar ett skyddat meddelande. A väljer en sessionsnyckel med vilken han krypterar sin klartext. Därefter krypterar A sessionsnyckeln med sin öppna konfidentialitetsnyckel. Den krypterade sessionsnyckeln lagras tillsammans med kryptotexten. Om A skulle förlora sin privata konfidentialitetsnyckel, blir det omöjligt för honom att dekryptera sina kryptotexter. De kan inte återskapas i klartext. Ett sätt att gardera sig är att A deponerar sin privata konfidentialitetsnyckel hos en TTP.

Om A förlorar sin nyckel kan han gå tillväga som bilden nedan visar. I (1) begär A av sin TTP att få ut sin privata konfidentialitetsnyckel. TTP:n

granskar A:s identitet och lämnar i (2) ut nyckeln. I (3) och (4) återskapar A sina klartexter med hjälp av den från TTP:n hämtade nyckeln. A bör även spärra sitt certifikat för den öppna konfidentialitetsnyckeln hos TTP:n.



5. Användning av olika kryptonycklar

Sammanfattningsvis gäller följande beträffande nyckelhantering och certifikat.

- En användares egen *öppna* signaturnyckel bör finnas på användarens certifikat som erhålls av certifieringsinstansen. Den öppna nyckeln görs av användaren åtkomlig för övriga användare, t.ex. via öppna katalogsystem.
- En användares egen *öppna* konfidentialitetsnyckel bör finnas på användarens certifikat som erhålls av certifieringsinstansen. Den öppna nyckeln görs av användaren åtkomlig för övriga användare, t.ex. via öppna katalogsystem.
- En användares *privata* signaturnyckel skall inte göras tillgänglig för andra.
- Svårigheten ligger i att bedöma hur en användares *privata* konfidentialitetsnyckel skall hanteras och i vissa fall göras tillgänglig för andra. Här finns olika behov av deponering och återskapande av nyckeln:

  - användare behöver ha egen kopia av nyckeln ifall den kommer bort eller förstörs,

  - arbetsgivare kan vilja kontrollera vilken klartextinformation som anställda har,

- rättsvårdande myndigheter kan behöva ha tillgång till klartext eller nyckeln vid misstanke om grov brottslighet,

- rättighetsinnehavare i civilrättsmål (t.ex. vid arvstvister) kan behöva ha tillgång till klartext eller nyckeln.

6. Allmänt tillgängliga tjänster för att stödja användningen av elektroniska dokument och elektroniska signaturer

När många skall kunna kommunicera med varandra elektroniskt behövs unika och säkra adresser och elektroniska signaturer och skydd för innehållet i texten. Dagens användning av elektroniska tjänster på öppna nät (främst Internet) erbjuder begränsad säkerhet. I många länder och sammanhang är man överens om att det behövs nyckelhanteringssystem med unika, öppna nycklar för signaturer resp. för konfidentialitet samt certifikat som visar att nycklarna är korrekta.

Enligt en rapport från European Telecommunication Standard Institute, ETSI "Telecommunication Security, Trusted Third Parties (TTP), Requirements for TTP Services" (version 1.1.1, May 1997) väntas följande sju kategorier av tjänster komma att tillhandahållas av TTP:er.

1. Nyckelhanteringstjänster för symmetriska kryptosystem
1.1 Skapande av symmetriska nycklar
1.2 Distribution av symmetriska nycklar
1.3 Återkallande av symmetriska nycklar
1.4 Lagerhållning och åtkomst till symmetriska nycklar
1.5 Långtidsförvaring av symmetriska nycklar

2. Nyckelhanteringstjänster för asymmetriska kryptosystem
2.1 Skapande av nyckelpar med öppna/privata nycklar
2.2 Certifiering av öppna nycklar
2.3 Distribution av nyckelpar med öppna/privata nycklar
2.4 Återkallande av nyckelpar med öppna/privata nycklar
2.5 Lagerhållning och åtkomst av nyckelpar med öppna/privata nycklar
2.6 Långtidsförvaring av nyckelpar med öppna/privata nycklar

3. Tjänster för nyckeldeponering och nyckelåterskapande

4. Tjänster för identifikation och för att fastställa autenticitet
4.1 Identifikationstjänster med hjälp av datanät
4.2 Identifikationstjänster med hjälp av skriftlig korrespondens
4.3 Identifikationstjänster med hjälp av personlig inställelse

5. Tjänster för att stödja kontroll av åtkomst till system och data
5.1 Skapande av certifikat för åtkomstkontroll
5.2 Distribution av certifikat för åtkomstkontroll
5.3 Återkallande av certifikat för åtkomstkontroll
5.4 Långtidsförvaring av certifikat för åtkomstkontroll

6. Tjänster för att förhindra förnekande av att data skickats eller tagits emot
6.1 Tillhandahållande av bevishandlingar
6.2 Registrering av bevishandlingar
6.3 Verifiering av bevishandlingar
6.4 Tillhandahållande av information i samband med förlikning

7. Övriga tjänster
7.1 Tidsstämpling för åtgärder eller mottagande av handlingar
7.2 Loggning och revision
7.3 Kontrollerad utlämning av handlingar

De sju generella kategorierna klassificerar olika säkerhetstjänster som kan komma att erbjudas från TTP:er. Dessa tjänster kan användas i samband med bl.a. autenticering, signaturer eller konfidentialitet. Enskilda TTP:er kan erbjuda tjänster från en eller flera av de sju kategorierna.

Bilaga 3: OECD:s riktlinjer för politik för kryptografi

OECD:s råd rekommenderar att medlemsstaterna

1. inför nya eller anpassar nu gällande politiska riktlinjer, metoder, åtgärder, praxis och förfaranden för att avspegla och ta hänsyn till de principer för kryptografipolitik som anges i de riktlinjer som bifogas denna rekommendation (nedan kallade *riktlinjerna*) och utgör en integrerad del härav; härvid också beaktar rådets *rekommendation om riktlinjer för skydd av privatlivet och det gränsöverskridande flödet av personuppgifter* av den 23 september 1980 [C(80)58/FINAL] och rådets *rekommendation om riktlinjer avseende säkerheten i informationssystem* av den 26 och 27 november 1992 [C(92)188/FINAL]

2. samråder, samordnar sina åtgärder och samarbetar på det nationella och internationella planet i fråga om införande av riktlinjerna

3. rättar sig efter behovet att uppnå praktiska och funktionsdugliga lösningar för internationell kryptografipolitik genom att lägga riktlinjerna till grund för överenskommelser i särskilda frågor som rör internationell kryptografipolitik

4. ger spridning åt riktlinjerna inom hela den offentliga och privata sektorn för att höja medvetandet om frågor och politik som rör kryptografi

5. avlägsnar - eller avhåller sig från att i namn av kryptografipolitik införa - omotiverade hinder för internationell handel och utveckling av nätverk för information och kommunikation

6. klart anger och offentliggör alla nationella, statliga kontrollåtgärder med avseende på användning av kryptografi

7. granskar riktlinjerna minst vart femte år för att förbättra det internationella samarbetet i frågor som rör kryptografipolitik.

Riktlinjer för kryptografipolitik

I. Syften

Riktlinjernas syften är följande:

- att främja användning av kryptografi,

- att främja förtroendet för infrastruktur, nätverk och system för information och kommunikation samt för sättet att använda dem,

- att hjälpa till att trygga datasäkerheten och skydda den personliga integriteten i nationella och globala infrastrukturer, nätverk och system för information och kommunikation,

- att främja sådan användning av kryptografi utan att onödigtvis äventyra allmän säkerhet, rättsvård och nationell säkerhet,

- att höja medvetandet om nödvändigheten av att olika länders politik och lagstiftning för användande av kryptografi är förenliga med varandra, liksom om behovet av kryptografiska metoder som har förmåga att samverka, och är flyttbara och rörliga i nationella och globala informations- och kommunikationssystem,

- att hjälpa beslutsfattare inom den offentliga och privata sektorn med utveckling och införande av sammanhängande politik, metoder, åtgärder, praxis och förfaranden för effektiv användning av kryptografi på det nationella och internationella planet,

- att främja samarbete mellan den offentliga och privata sektorn när det gäller att utveckla och införa politik, metoder, åtgärder, praxis och förfaranden med avseende på nationell och internationell kryptografi,

- att underlätta internationell handel genom att främja kostnadseffektiva, flyttbara och rörliga kryptografiska system som har förmåga att samverka,

- att främja internationellt samarbete på regeringsnivå, näringslivsnivå, inom forskarvärlden och mellan standardiseringsorgan i syfte att åstadkomma koordinerad användning av kryptografiska metoder.

II. Omfattning

Dessa riktlinjer riktar sig i första hand till regeringar med avseende på rekommendationerna i dem, men de förväntas också bli lästa i vidare kretsar och följas inom både den privata och den offentliga sektorn.

Det erkänns att regeringar har särskilt och otvetydigt ansvar för skydd av information som kräver sekretess i nationens intresse; dessa riktlinjer är inte avsedda att tillämpas på sådana frågor.

III. Definitioner

I dessa riktlinjer avses med

autenticering: den funktion som fastställer giltigheten av den uppgivna identiteten för en användare, en anordning eller annan del av ett informations- och kommunikationssystem,

tillgänglighet: egenskapen att data, information samt informations- och kommunikationssystem är åtkomliga och användbara i rätt tid på det sätt som fordras,

konfidentialitet: egenskapen hos data och information att inte vara tillgängliga eller läsbara för obehöriga fysiska eller juridiska personer eller processer,

kryptografi: det ämnesområde som innefattar principer, medel och metoder för att omvandla data i avsikt att dölja ett meddelandes informationsinnehåll, verifiera dess autenticitet, förhindra dess fördolda förändring samt förhindra att data förnekas och förhindra dess obehöriga användning,

kryptografisk nyckel: en parameter som används för att med hjälp av en kryptografisk algoritm omvandla, validera, autenticera, kryptera eller dekryptera data,

kryptografiska metoder: kryptografisk teknik, d:o tjänster, system, produkter och nyckelhanteringssystem,

data: framställning av information på ett sätt som är lämpligt för kommunikation, tolkning, lagring eller behandling,

dekryptering: motsatt funktion till kryptering,

kryptering: omvandling av data genom användning av kryptografi för att framställa obegripliga data (krypterade data) för att säkerställa deras konfidentialitet,

integritet: egenskapen att data eller information inte obehörigen har ändrats eller förvanskats,

samverkansförmåga med avseende på kryptografiska metoder: den tekniska förmågan till samverkan mellan flera kryptografiska metoder,

nyckelhanteringssystem: system för att skapa, lagra, distribuera, ogiltigförklara, ta bort, arkivera, certifiera och använda kryptografiska nycklar,

nyckelinnehavare: en fysisk eller juridisk person som innehar eller har kontroll över kryptografiska nycklar; en nyckelinnehavare är inte nödvändigtvis densamme som en nyckelanvändare,

rättsvård: all rättstillämpning/utövning utan avseende på ämne,

laglig åtkomst: åtkomst för tredje part som är fysisk eller juridisk personer, inbegripet regeringar, till klartext eller kryptografiska nycklar, i enlighet med gällande lag,

rörlighet med avseende på kryptografiska metoder: den tekniska förmågan att fungera i flera länder eller informations- och kommunikationsmiljöer,

oavvislighet: egenskap hos data som förvärvats genom kryptografiska metoder vilken förhindrar en fysisk eller juridisk person att neka till att ha utfört en särskild handling relaterad till data (exempelvis mekanismer som förhindrar förnekande av auktoritet [ursprung], mekanismer för bevis på skyldighet, avsikt eller åtagande eller för bevis på äganderätt),

personuppgifter: information relaterad till en bestämd person som är eller kan bli identifierad,

klartext: begripliga data,

flyttbarhet för kryptografiska metoder: teknisk förmåga att anpassas till och fungera i flera system.

IV. Integration

Principerna i avsnitt V i denna bilaga, som var och en är inriktad på ett viktigt politikområde, är ömsesidigt beroende och skall tillämpas som en helhet för att skapa jämvikt mellan olika intressen. Ingen princip skall tillämpas isolerat från de övriga principerna.

V. Principer

1. Förtroende för kryptografiska metoder

Kryptografiska metoder bör vara tillförlitliga för att skapa förtroende för användning av informations- och kommunikationssystem.

Marknadskrafterna bör tjäna till att bygga upp förtroende för tillförlitliga system; även statliga regelverk, licensiering och användning av kryptografiska metoder kan befrämja användarnas förtroende. Bedömning av kryptografiska metoder, särskilt gentemot kriterier som accepterats av marknaden, kan också skapa förtroende från användarnas sida.

För att förstärka användarnas förtroende bör i avtal om användning av nyckelhanteringssystem anges vems lag som skall gälla för systemet.

2. Val av kryptografiska metoder

Användare bör ha rätt att fritt välja kryptografisk metod med iakttagande av gällande lagar.

Användare bör ha tillgång till den kryptografi som motsvarar deras behov så att de kan lita på informations- och kommunikationssystemens säkerhet liksom på konfidentialitet och integritet för data som befinner sig i dessa system. Fysiska och juridiska personer som äger, kontrollerar, har åtkomst till, använder eller lagrar data kan ha ansvar för att skydda dessa datas konfidentialitet och integritet och kan därför vara skyldiga att använda lämpliga kryptografiska metoder. Det kan förväntas att olika kryptografiska metoder kan behövas för att motsvara olika datasäkerhetskrav. Med iakttagande av gällande lagar bör användare av kryptografi fritt få bestämma vilken typ och nivå av datasäkerhet som behövs och välja och införa lämpliga kryptografiska metoder, inklusive det nyckelhanteringssystem som passar bäst för deras behov.

I syfte att värna ett bestämt allmänt intresse, som exempelvis skydd av personuppgifter eller elektronisk handel, har regeringar rätt att införa riktlinjer som kräver att kryptografiska metoder håller en tillfredsställande skyddsnivå.

Den statliga kontrollen över kryptografiska metoder bör inte vara strängare än vad som är nödvändigt för att uppfylla statens ansvar och bör respektera användarnas val i största möjliga utsträckning. Principen skall inte tolkas såsom innebärande att regeringar bör införa lagar som begränsar användarnas valfrihet.

3. Marknadsledd utveckling av kryptografiska metoder

De kryptografiska metoderna bör utvecklas för att motsvara enskilda personers, näringsidkares och myndigheters behov, efterfrågan och ansvar.

Utveckling och saluförande av kryptografiska metoder bör styras av marknadskrafterna i en öppen och konkurrensmässig miljö. Detta är det förhållningssätt som bäst tillgodoser att lösningarna håller jämna steg med den teknologiska utvecklingen, användarnas krav och uppkommande hot mot informations- och kommunikationssystemens säkerhet. Marknaden bör också vara ledande för utvecklingen av internationell teknisk standard, kriterier och protokoll relaterade till kryptografiska metoder. Regeringarna bör uppmuntra och samarbeta med näringslivet och forskarna när det gäller att utveckla kryptografiska metoder.

4. Standardisering av kryptografiska metoder

Teknisk standard, kriterier och protokoll för kryptografiska metoder bör utvecklas och införas på det nationella och internationella planet.

För att motsvara marknadens behov bör de internationellt erkända standardiseringsorganen, regeringarna, näringslivet och andra sakkunniga på området utbyta information och samarbeta för att utveckla och införa teknisk standard, kriterier och protokoll för kryptografiska metoder som kan samverka. Nationell standard för kryptografiska metoder bör, i den mån sådan förekommer, vara förenlig med internationell standard för att underlätta samverkan på global nivå samt flyttbarhet och rörlighet. Mekanismer för att bedöma överensstämmelse med sådan teknisk standard, kriterier och protokoll för samverkan, flyttbarhet och rörlighet för kryptografiska metoder bör utvecklas. I den utsträckning konformitetstester eller bedömning av standard förekommer, bör ett brett accepterande av dessa uppmuntras.

5. Skydd av personlig integritet och personuppgifter

Enskildas grundläggande rätt till personlig integritet, inklusive meddelandeskydd och skydd av personuppgifter, bör respekteras i nationell politik för användning av kryptografi och vid införande och användning av kryptografiska metoder.

Kryptografiska metoder kan vara ett värdefullt verktyg för skydd av den personliga integriteten, innefattande både konfidentialitet för data och kommunikation och skydd av enskildas identitet. Kryptografiska metoder erbjuder också nya möjligheter att minimera insamlingen av personuppgifter genom att de möjliggör säkra men anonyma betalningar, transaktioner och interaktioner. Samtidigt har kryptografiska metoder för att trygga dataintegriteten vid elektroniska transaktioner följdverkningar för den personliga integriteten. Dessa följdverkningar, som innefattar insamling av personuppgifter och skapande av system för personidentifiering, bör behandlas och klarläggas; där så är lämpligt bör skydd för den personliga integriteten införas.

OECD:s riktlinjer för skydd av den personliga integriteten och gränsöverskridande flöden av personuppgifter ger en allmän vägledning för insamling och hantering av personuppgifter och bör tillämpas i överensstämmelse med relevanta nationella lagar vid införande av kryptografiska metoder.

6. Laglig åtkomst

Nationell politik för användning av kryptografi får tillåta laglig åtkomst till klartext eller kryptografiska nycklar till krypterade data. Denna politik måste respektera de övriga principerna i dessa riktlinjer i största möjliga utsträckning.

Om regeringar överväger att tillämpa en politik för kryptografiska metoder som tillåter laglig åtkomst, bör de noga väga nyttan, inklusive nyttan för den allmänna säkerheten, rättsvården och den nationella säkerheten, liksom risken för missbruk, extrakostnaderna för stödjande infrastruktur, risken för tekniskt haveri samt andra kostnader. Denna princip bör inte förstås som att regeringar bör eller inte bör införa lagar som tillåter laglig åtkomst.

I de fall åtkomst till klartext eller kryptografiska nycklar till krypterade data begärs i ett lagligt förfarande, måste den fysiska eller juridiska person som begär åtkomst ha laglig rätt att inneha klartexten; åtkomna data får bara användas i lagliga syften. Det förfarande genom vilket den lagliga åtkomsten har uppnåtts bör registreras för att tillåta att röjandet av de kryptografiska nycklarna eller informationen kan prövas i enlighet med nationell lag. I de fall laglig åtkomst begärs och beviljas bör denna beviljas inom angivna tidsramar anpassade från fall till fall. Förutsättningarna för laglig åtkomst bör klart anges och tillkännages på ett sätt som är lättillgängligt för användare, nyckelinnehavare och för dem som saluför kryptografiska metoder.

Nyckelhanteringssystem skulle kunna utgöra grunden för en möjlig lösning som skulle kunna ge jämvikt mellan användarnas och de rättsvårdande myndigheternas intressen; denna teknik skulle också kunna användas för att rädda data i händelse av förkomna nycklar. Förfaranden för laglig åtkomst till kryptografiska nycklar måste ta hänsyn till skillnaden mellan nycklar som används för konfidentialitet och sådana som används enbart för andra ändamål. En kryptografisk nyckel som endast ger identitet eller integritet (till skillnad från en kryptografisk nyckel som certifierar endast identitet eller integritet) skall inte göras tillgänglig utan samtycke av den fysiska eller juridiska person som lagligen innehar nyckeln.

7. Ansvar

Det ansvar som åvilar fysiska och juridiska personer som saluför kryptografiska tjänster eller är innehavare av eller har åtkomst till kryptografiska nycklar skall klart anges, oavsett om ansvaret har tillkommit genom avtal eller enligt lag.

Det ansvar som åvilar en fysisk eller juridisk person, inklusive ett offentligt organ, som saluför kryptografiska tjänster eller är innehavare av eller har åtkomst till kryptografiska nycklar bör fastställas genom avtal eller, om så är lämpligt, i nationell lag eller genom internationella

överenskommelser. Användares ansvar för missbruk av egna nycklar bör också fastställas. Nyckelinnehavare bör inte vara ansvariga för att tillhandahålla kryptografiska nycklar eller klartext av krypterade data i överensstämmelse med laglig åtkomst. Den part som får laglig åtkomst bör vara ansvarig vid missbruk av kryptografiska nycklar eller klartext som mottagits.

8. Internationellt samarbete

Regeringar bör samarbeta för att samordna sin politik för användande av kryptografi. Som en del av denna strävan bör regeringar undanröja eller undvika att i namn av denna politik skapa oberättigade handelshinder.

För att främja ett brett internationellt accepterande av kryptografi och dra nytta av alla de möjligheter som de nationella och globala informations- och kommunikationssystemen erbjuder bör den politik för användande av kryptografi som antas av ett land så långt som möjligt koordineras med motsvarande politik i andra länder. I detta syfte bör föreliggande riktlinjer användas vid utformningen av nationell politik.

Nyckelhanteringssystem som utvecklas bör i lämplig utsträckning medge internationell användning av kryptografi.

Laglig åtkomst över nationsgränser kan åstadkommas genom samarbete och överenskommelser bilateralt och multilateralt.

Ingen regering bör hindra det fria flödet av krypterade data från att passera genom sitt jurisdiktionsområde endast med hänvisning till politiken för användning av kryptografi.

För att främja internationell handel bör regeringarna avhålla sig från att utveckla politik och praxis på kryptografins område som skapar oberättigade hinder för internationell elektronisk handel. Regeringarna bör undvika att skapa oberättigade hinder för internationell tillgång till kryptografiska metoder.

Utrikesdepartementet

Utdrag ur protokoll vid regeringssammanträde den 6 maj 1999

Närvarande: statsministern Persson, ordförande, och statsråden Hjelm-Wallén, Freivalds, Schori, Winberg, Ulvskog, Lindh, Sahlin, von Sydow, Klingvall, Pagrotsky, Östros, Messing, Engqvist, Rosengren, Larsson, Wärnersson, Lejon, Lövdén, Ringholm

Föredragande: statsrådet Pagrotsky

Regeringen beslutar skrivelsen 1998/99:116 Om kryptografi.