

Sammanfattning

I sina överväganden med anledning av regeringens skrivelse 1998/99:116 Om kryptografi och motion 1998/99:U16 (fp) framhåller utskottet att det delar regeringens uppfattning i fråga om användning av kryptografi vid överföring och lagring av information i elektronisk form samt när det gäller handel med kryptoprodukter.

Innebörden av ställningstagandet är att det för närvarande inte föreligger skäl att begränsa användningen av kryptoteknik i Sverige, utan att alla skall ha rätt att själva välja sådan teknik. Skulle utvecklingen motivera skärpta regler bör lämpliga åtgärder övervägas för att skapa möjligheter till laglig åtkomst i klartext av krypterad information för brottsbekämpande och kontrollerande myndigheter. Import av kryptoteknik skall förbli fri.

Utskottet noterar införandet av interimistiska amerikanska regler vad gäller export av kryptoprodukter och konstaterar att de svenska bestämmelserna alltså är lättare att tillämpa.

Utformningen av exportkontroll av kryptoprodukter innebär en svår avvägning mellan olika faktorer såsom säkerhetspolitiska överväganden, skyldigheten av att fullgöra internationellt överenskomna åtaganden samt tillgängligheten av teknik för försvaret och näringslivet. De civila nyttjarnas behov och näringspolitiska intressen är andra faktorer som måste beaktas.

Sverige deltar i det internationella arbetet med exportkontroll och kommer fortsättningsvis, enligt vad utskottet erfarit, att än mer verka för en friare handel med kryptoprodukter som ett led i utvecklingen av elektroniska tjänster men med hänsynstagande till att det kvarstår ett säkerhetspolitiskt betingat intresse av att försvåra åtkomsten av starka krypton för exempelvis sådana användare som är länkade till utveckling eller produktion av massförstörelsevapen. Vidare framhåller utskottet att Sverige, för att säkra egen tillgång till utländsk högteknologi, har ett behov av att upprätthålla samma kontrollnivå som viktigare leverantörsländer. Enligt utskottets mening innebär detta en lämplig avvägning. Utskottet vill framhålla att detta synsätt också bör vara vägledande för Sveriges insatser i samband med arbetet med den nya EG-rådsförordningen som är under utarbetande.

Själva tillämpningen av exportregleringen är i betydande utsträckning en nationell angelägenhet. Detta har utnyttjats av Sverige för att på olika sätt förenkla för företagen. Utskottet, som vid en föredragning av statsrådet

Pagrotsky erfarit att ytterligare arbete med denna inriktning pågår, understryker betydelsen härav.

1999/2000:UU7

Förhållandena beträffande exportkontroll av kryptoprodukter har i icke oväsentlig grad förändrats sedan skrivelsen underställdes riksdagen och motionerna väcktes. Enligt utskottets bedömning är därmed flertalet av de krav som motionsledes framförts redan tillgodosedda.

Utskottet delar regeringens uppfattning att 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.

Utskottet föreslår att regeringens skrivelse läggs till handlingarna. Samtliga motioner besvaras eller avstyrks.

Skrivelsen

Regeringen överlämnar skrivelse 1998/99:116 Om kryptografi till riksdagen.

Motionerna

Motion väckt med anledning av skrivelsen

1998/99:U16 av Eva Flyborg m.fl. (fp) vari yrkas

1. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om att inga svenska restriktioner i rätten att använda kryptering får finnas,

2. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om att civila produkter med kryptoinnehåll jämföras med andra civila produkter i exporthänseende,

3. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om ett initiativ till en översyn av IT-samhällets sårbarhet och framtågande av en plan för att minska riskerna med IT-användning,

4. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om fri import, export och användning av krypteringsprogram.

Motioner väckta under den allmänna motionstiden 1999/2000

1999/2000:U410 av Per Bill och Sten Tolgfors (m) vari yrkas

1. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om att Sverige i allt internationellt samarbete bör verka för fri handel med kryptoprodukter,

2. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om fasta och tydliga spelregler för de människor och företag som för sin kommunikation eller direkta verksamhet använder sig av eller tillverkar kryptoprodukter,

3. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om att det inte finns några skäl att begränsa användningen av kryptoteknik i Sverige,

4. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om ett avvisande av alla planer på obligatoriska system för deponeering av krypteringsnycklar, såväl nationellt som internationellt,

5. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om ett aktivt arbete för att starka civila krypteringsprodukter stryks från den varulista för exportkontroll som Wassenaararrangemanget fastställer,

6. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om en liberal tolkning av nu gällande Wassenaararrangemang,

7. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om en signal om att den nordamerikanska kryptopolitiken riskerar att bli ett rent handelshinder som gynnar amerikanska IT-företag på andra konkurrenters bekostnad.

1999/2000:T703 av Lennart Daléus m.fl. (c) vari yrkas

16. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om framtida reglering av kryptering inom landet,

17. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om tolkning av Wassenaararrangemanget och EG-rätten för att underlätta export av svenska krypteringsprodukter,

18. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om Sveriges agerande i fortsatta förhandlingar om kryptering inom ramen för Wassenaararrangemanget och inom EU.

1999/2000:T705 av Eva Flyborg m.fl. (fp) vari yrkas

8. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om borttagande av import- och exportrestriktioner på krypteringsprodukter.

1999/2000:T717 av Bo Lundgren m.fl. (m) vari yrkas

15. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om användning och export av kryptobaserade produkter,

16. att riksdagen hos regeringen begär förslag om avskaffande av restriktioner när det gäller export av kryptobaserade produkter i enlighet med vad som anförts i motionen.

Utskottet

Ärendets beredning

I betänkande 1999/2000:UU3 behandlade utskottet regeringens skrivelse 1998/99:116 jämte ett antal motioner väckta såväl med anledning av skrivelsen som under den allmänna motionstiden. Under kammarbehandlingen den 3 november 1999 yrkades att ärendet skulle återremitteras till utrikesutskottet för fortsatt beredning. Riksdagen beslutade samma dag i enlighet härmed. Det återremitterade ärendet omfattar samtliga de frågor som behandlades i betänkande 1999/2000:UU3.

Under den förnyade beredningen av ärendet har utskottet erhållit en förredragning av statsrådet Leif Pagrotsky samt även i övrigt inhämtat information om den internationella utvecklingen sedan hösten 1999.

1999/2000:UU7

Sammanfattning av skrivelsen

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.

Bakgrund

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.

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 häfter 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.

Som bakgrund till sina överväganden och slutsatser anför regeringen bl.a. följande.

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.

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 signalskyddstjäns-

ten (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 uppdraga åt Försvarsmakten att genomföra en försöksverksamhet inom försvarssektorn under år 2000.

Regeringens överväganden och slutsatser

Regeringens bedömning

Regeringen bedömer att det för närvarande inte finns skäl att begränsa användningen av kryptoteknik i Sverige utan att alla skall ha rätt att själva välja sådan teknik.

Import av kryptoteknik skall förbli fri.

Det finns fortsatta säkerhetspolitiska skäl för 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 utförelse 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 arbetsätt 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.

Elektroniska signaturer används 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 signatortjänster. 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 signatortjänster. Hur ett system för tillsyn och kontroll av signatortjänster 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 signatortjänster.

Inom Regeringskansliet har arbete påbörjats med att skyndsamt ta fram handlingsmöjligheter och förslag till en framtida struktur och organisation av signatortjänster. 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 behövas 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 aktivt bör 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.

Regeringen anser att följande åtgärder bör vidtas.

Exportkontrollen av kryptoprodukter fortsätter i enlighet med EU:s regler och Sveriges förpliktelser i Wassenaararrangemanget (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 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 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 till vara. 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 *konfidentialitetstjänster* 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.

Sammanfattning av motionerna

I motionerna 1998/99:U16 (fp) och 1999/2000:T705 (fp) yrkande 8 framhålls att praktiskt taget allt som i dag skickas på svenska datanät saknar skydd mot avlyssning. Folkpartiet betraktar detta som ett allvarligt och växande problem. Det enda verkningsfulla skyddet mot avlyssning är kryptering.

Motionärerna konstaterar att regeringen visserligen säger att alla även i fortsättningen skall ha rätt att fritt använda kryptering, men att detta påstående inte är reservationslöst. Motionärerna betraktar det som en självklarhet för ett demokratiskt IT-samhälle att användning, utveckling och spridning av kryptering skall vara tillåtet. Några svenska restriktioner i rätten att använda kryptering får därför inte finnas (motionerna 1998/99:U16 (fp) yrkande 1 och 1999/2000:T705 (fp) yrkande 8 [delvis]).

Inom en snar framtid kommer kryptering att krävas som en integrerad del i de flesta mjukvaruprodukter. Exportrestriktioner avseende kryptering kommer därför att drabba stora delar av den svenska programvaruindustrin. Mot-

ionärerna stödjer av FN sanktionerade handelsembargon men menar att civila produkter med kryptoinnehåll bör jämföras med andra civila produkter i exporthänseende och inte beläggas med exportrestriktioner då det gäller handel med länder som inte står under embargo (*1998/99:U16 (fp) yrkande 2*). Motionärerna efterlyser inte bara fri export utan också fri import och användning av krypteringsprogram (*motionerna 1998/99:U16 (fp) yrkande 4* och *1999/2000:T705 (fp) yrkande 8 [delvis]*).

I motion *1998/99:U16 (fp) yrkande 3* begärs en översyn av IT-samhällets sårbarhet och framtagande av en plan för att minska riskerna med IT-användningen.

I den enskilda motionen *1999/2000:U410 (m)* begärs i *yrkande 1* att Sverige i allt internationellt samarbete, främst med USA och andra demokratiska länder, bör verka för fri handel med kryptoprodukter.

I *yrkande 2* begärs vidare att regeringen anvisar fasta och tydliga spelregler för de människor och företag som för sin kommunikation eller direkta verksamhet använder sig av eller tillverkar kryptoprodukter. Därför bör riksdagen, enligt *yrkande 3*, slå fast att det inte finns några skäl för att begränsa användningen av kryptoteknik i Sverige. Varje sådan begränsning bidrar till att minska Sveriges möjligheter att bli ett framgångsrikt IT-land med alla de fördelar som människor och företag kan dra av en sådan utveckling. Riksdagen bör dessutom, enligt *yrkande 4*, slå fast att alla planer på obligatoriska system för deponering av dekrypteringsnycklar bör skrinläggas och att Sverige motsätter sig andra länders krav på sådan deponering.

All nyckeldeponering bör ske på frivillig basis och skötas av icke-statliga organ. En sådan ordning behöver inte nödvändigtvis innebära att möjligheten att i efterhand utkräva dekrypteringsnycklar vid misstanke om brott försvinner.

Enligt motionärerna bör Sverige i EU, WTO, Europarådet och i Wassenaar-arrangemanget aktivt arbeta för en liberal exportpolicy och en ökad frihandel med kryptobaserade produkter. För att åstadkomma detta bör Sverige verka för att starka civila krypteringsprodukter stryks från den varulista för den exportkontroll som Wassenaararrangemanget fastställer (*yrkande 5*). Fram till dess att ändringar av arrangemanget vunnit gehör bör Sverige, sägs det i motionens *yrkande 6*, tillämpa gällande bestämmelser så liberalt som möjligt.

Kryptopolitiken från nordamerikanskt håll, som tidigare har varit militärstrategiskt betingad, håller nu på att förändras. I *yrkande 7* krävs att Sverige "bör sända en signal" om att den nordamerikanska kryptopolitiken riskerar att bli ett rent handelshinder som gynnar amerikanska IT-företag på andra konkurrenters bekostnad.

I partimotion *1999/2000:T703 (c)* framhålls att Centerpartiet i huvudsak är tillfreds med den bedömning regeringen i dag gör i skrivelse 1998/99:116.

Partiet välkomnar att regeringen i skrivelsen konstaterar att kryptering för närvarande inte bör begränsas i Sverige, men det är, enligt motionärerna, inte tillräckligt. Eftersom skyddet för integritet och affärshemligheter kan antas spela en roll för företags etableringsbeslut och för investeringar i system för

elektronisk handel och informationsutbyte, borde det också, enligt *yrkande 16*, göras klart att Sverige inte heller har för avsikt att i framtiden reglera användningen av kryptering inom landet.

Regeringen bör, enligt *yrkande 17*, för svenska myndigheter göra klart att de skall tillämpa bestämmelserna inom Wassenaararrangemanget och inom EG-rätten så generöst som möjligt så att det inom ramen för gällande regelverk går att exportera svenska krypteringsprodukter så enkelt och fritt som möjligt.

Centerpartiet beklagar att riksdagen inte beretts möjlighet att diskutera den svenska ståndpunkten i de förhandlingar som förts inom ramen för Wassenaararrangemanget. Partiet menar (*yrkande 18*) att Sverige i fortsatta förhandlingar, inom EU likaväl som inom Wassenaararrangemanget, måste vara pådrivande för en nedmontering av de exportrestriktioner som i dag gäller för krypteringsprogram till ett absolut minimum.

I partimotion 1999/2000:T717 (m) hävdar moderaterna att den svenska exportkontrollen när det gäller mjukvara som innehåller krypto hindrar utvecklingen av elektronisk handel och missgynnar svenska exportföretag.

I internationella förhandlingar har regeringen, sägs det, verkat för en restriktiv syn på export av sådana program och även förespråkat s.k. nyckeldeponering, som i praktiken utgör ett hinder för laglydiga företag att exportera. Nyligen offentliggjordes att USA inom kort kommer att avskaffa tillståndsplikten för stora delar av kryptoexporten. Detta kommer ytterligare att försämra konkurrensmöjligheterna för svenska företag.

Riksdagen bör slå fast att det inte finns några skäl för att begränsa användningen av kryptoteknik i Sverige (*yrkande 15 [delvis]*). I stället bör regeringen driva en politik och lägga fast regler som uppmuntrar användning av stark och säker kryptering. Riksdagen bör dessutom slå fast att alla planer på obligatoriska system för deponering av dekrypteringsnycklar bör skrinläggas och att Sverige motsätter sig andra länders krav på sådan deponering. All nyckeldeponering bör därför ske på frivillig basis och skötas av icke-statliga organ. En sådan ordning behöver inte nödvändigtvis innebära att möjligheten att i efterhand utkräva dekrypteringsnycklar vid misstanke om brott försvinner.

Sverige bör sträva efter frihandel även för kryptobaserade produkter (*yrkande 15 [delvis]*) och i EU, WTO, Europarådet och inom Wassenaararrangemanget aktivt arbeta för en liberal exportpolicy och en ökad frihandel med kryptobaserade produkter. Sverige bör tillämpa gällande internationella regimer så liberalt som möjligt.

Den nuvarande exportkontrollen bör (*yrkande 16*) till större delen avskaffas. Enda undantagen från frihandelslinjen bör gälla militära höggradiga krypton som inte är publika, dvs. programvara som ”berör nationell säkerhet”.

Utskottets överväganden

I skrivelse 1998/99:116 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.

För närvarande föreligger det inte skäl att begränsa användningen av kryptoteknik i Sverige, utan 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.

Regeringen anför också att 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.

Rätten att använda kryptering

I motion 1998/99:U16 (fp) yrkande 1 krävs att några svenska restriktioner i rätten att använda kryptering inte får finnas. Också i motionens yrkande 4 (delvis) samt i motion 1999/2000:T705 (fp) yrkande 8 (delvis) begärs fri användning av kryptoprogram. Yrkandena 2 och 3 i motion 1999/2000:U410 (m) samt motionerna 1999/2000:T703 (c) yrkande 16 och 1999/2000:T717 (m) yrkande 15 (delvis) har samma innebörd.

Utskottet noterar att regeringen välkomnar en ökad användning av kryptografi i Sverige. På öppna kommunikationsnät kan kryptografi, sägs det i skrivelsen, uppfylla grundläggande säkerhetskrav och skapa förtroende för kommunikationstjänster. Detta ligger i linje med riksdagens tidigare uttalande (bet. 1998/99:TU4) att det är en grundläggande förutsättning för elektronisk handel att företag, organisationer, myndigheter och enskilda har förtroende för och tillit till denna handel. Kryptografi är också ett medel för att skydda den personliga integriteten.

I sin skrivelse säger regeringen vidare att alla skall ha rätt att även i fortsättningen fritt använda sig av kryptoteknik och själva ha rätt att välja sådan teknik. I skrivelsen framhålls emellertid också, som nämnts ovan, att om utvecklingen skulle 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.

Utskottet delar den motionsvis framförda uppfattningen att överväganden utifrån demokratisynpunkt måste vara grundläggande då det gäller att bedöma behovet av regleringar i det framväxande IT-samhället. Utskottet vill emellertid samtidigt understryka att regeringens skrivelse ger uttryck just för detta synsätt och att inga regleringar i dagsläget föreslås.

Även om man är ense om att kryptografi är ett viktigt instrument för att försvåra eller förhindra brottslig verksamhet pågår i många länder, t.ex. i USA, Storbritannien och Frankrike, en livlig debatt om hur samhället skall kunna skyddas mot brottsligt missbruk av kryptografi. Utvecklingen på andra teknikområden har också visat att ett övergripande samhällsintresse inneburit att tvångsåtgärder, motsvarande dem som nämns motionsvis, måste införas i vissa väl definierade fall. Detta gäller exempelvis beträffande telefonavlyssning.

Utvecklingen på IT-säkerhetsområdet och riskerna för missbruk av kryptografi kan inte förutsägas, bl.a. på grund av att tekniken och användningen ständigt förändras. En svensk kryptopolitik måste därför, enligt utskottets uppfattning, präglas av flexibilitet och lyhördhet. I motsats till motionären menar utskottet således att beslut och åtgärder vid behov måste kunna omprövas. Utskottet anser därutöver att det vore principiellt betänkligt att för all framtid och oavsett utvecklingen, på sätt som motionärerna föreslår, förbinda sig att bevara ett visst rättsläge.

Därmed avstyrks motionerna *1998/99:U16 (fp) yrkandena 1 och 4 (delvis)*, *1999/2000:U410 (m) yrkandena 2 och 3*, *1999/2000:T703 (c) yrkande 16*, *1999/2000:T705 (fp) yrkande 8 (delvis)* samt *1999/2000:T717 (m) yrkande 15 (delvis)*.

Kryptonycklar m.m.

Frågan om elektroniska signaturer och kryptonycklar hänger nära samman. Regeringen anför i skrivelsen att en central fråga vid utformandet av svenska regler för elektroniska signaturer är hur hanteringen av certifikat och kryptonycklar skall utformas. Hur ett system för tillsyn och kontroll av signaturtjänster kommer att se ut i Sverige måste ses mot bakgrund av de regler som Europaparlamentets och rådets direktiv (1999/93/EG av den 13 december 1999) om ett gemenskapsramverk för elektroniska signaturer uppställer. En utgångspunkt 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 (Näringsdepartementet) har nyligen ett förslag till en framtida struktur och organisation av signaturtjänster utarbetats (Ds 1999:73 Elektroniska signaturer).

Enligt utskottets uppfattning innebär detta att de som berörs på ett lämpligt sätt får möjlighet att påverka det arbete som bedrivs på området och att de synpunkter som framförs i motion *1999/2000:U410 (m) yrkande 4* på ett allsidigt sätt kommer att kunna prövas. Regeringens och motionärens grundperspektiv är detsamma och innebär bl.a. att möjlighet skall skapas för att Sverige skall bli ett framgångsrikt IT-land.

Utskottet noterar också att statsrådet Pagrotsky inför utskottet påpekat att regeringen ej framlagt något förslag om obligatorisk deponering av kryptonycklar och att inga planer i den riktningen finns. En helt annan sak är att det kan vara lämpligt att statliga myndigheter och privata företag beslutar om

egna nyckelhanteringssystem för sådana kryptonycklar som används i tjänsten eller inom den egna organisationen.

1999/2000:UU7

De synpunkter som framförs i motion 1999/2000:U410 (m) yrkande 4 är således i huvudsak redan beaktade, varför utskottet anser att motionen kan besvaras med vad som ovan anförts.

Exportfrågor

Motionärerna bakom motion 1998/99:U16 (fp) menar (yrkande 2) att civila produkter med kryptoinnehåll bör jämföras med andra civila produkter i exporthänseende och inte beläggas med exportrestriktioner då det gäller handel med stater som inte står under embargo. I samma motion yrkande 4 (delvis) och i motionerna 1999/2000:U410 (m) yrkandena 1 och 5–7, 1999/2000:T703 (c) yrkandena 17–18, 1999/2000:T705 (fp) yrkande 8 (delvis) samt 1999/2000:T717 yrkandena 15 (delvis) och 16 efterlyser motionärerna olika typer av lättnader beträffande export av kryptoprogram, tillämpningen av gällande exportkontrollarrangemang samt, därutöver, visst internationellt agerande i dessa frågor.

Produkter med dubbla användningsområden, såsom avancerad kryptoteknik, är sådana som har en etablerad civil användning men som också kan användas för militärt bruk (strategiska produkter). Den svenska exportkontrollen när det gäller dessa regleras i lagen (1998:397) om strategiska produkter och rådets förordning (EG) nr 3381/94 om upprättandet av en gemenskapsordning för kontroll av export av varor med dubbla användningsområden. Utskottet har tidigare behandlat detta regelverk i sitt betänkande 1997/98:UU19.

Sedan utskottet senast (i bet. 1999/2000:UU3) beredde frågor om krypto har nya, interimistiska amerikanska regler trätt i kraft. Med ledning av gjorda erfarenheter skall man senare i år utfärda slutliga regler. De nya reglerna har tillkommit eftersom den amerikanska industrin funnit de gamla alltför restriktiva och därför hävdade att t.ex. europeisk kryptoindustri haft en konkurrensfördel.

De nya amerikanska reglerna innebär betydande lättnader i licenshanteringen, och i de allra flesta fall skall företagen inte längre behöva söka individuella licenser. Företag som vill exportera måste dock låta sina produkter granskas tekniskt och klassificeras av tillsynsmyndigheten. För den första klassen krävs ingen licens. För den andra klassens produkter ges generell licens (licence exception) och för den tredje klassens varor kommer alltför individuell licens att krävas. Vissa s.k. terroristländer är helt svartlistade. Därutöver krävs individuell licens för utförsel av starka kryptoprodukter till statliga mottagare i andra länder och möjligtvis gäller detta även till utländska företag med statliga minoritetsintressen. Exportföretagen har dessutom rapporteringsplikt till USA:s handelsdepartement om produkter och köpare.

Enligt vad utskottet erfarit är de svenska reglerna, jämfört med de amerikanska, alltfjämt lättare att tillämpa för företagen i det att licenshanteringen är snabb och genom att Inspektionen för strategiska produkter (ISP) inte ställer krav på att tekniskt granska *alla* kryptoprodukter. Med verkan fr.o.m. den 1 augusti 1999 har ISP beslutat om öppna generella tillstånd för massmarknadsprodukter med upp till 128 bitar till ett 60-tal länder utöver EU-staterna. Det rör sig därvid om ett tillstånd som man inte behöver söka, där man inte behöver gå igenom en teknisk prövning och som inte heller kräver att man redogör för vem köparen är. Ytterligare förenklingar av det svenska systemet övervägs, bl.a. införande av s.k. projektlicenser.

Utformningen av exportkontroll beträffande produkter med dubbla användningsområden innebär ofta en delikat avvägning mellan olika faktorer såsom säkerhetspolitiska överväganden, skyldigheten att fullgöra internationellt överenskomna åtaganden samt tillgängligheten av teknik för försvaret och näringslivet. De civila nyttjarnas behov och näringspolitiska intressen är andra faktorer som också måste beaktas.

Regeringen har aviserat att den under innevarande år kommer att underställa riksdagen förslag till ny lag om produkter med dubbla användningsområden. Denna lag kommer att utgå från en radsförordning som för närvarande är under beredning. Frågor om kryptoprodukter kommer att regleras i detta sammanhang.

Tillämpningen av EG-förordningen om kontroll av export av varor med dubbla användningsområden baseras på varulistor som fastställs inom det s.k. Wassenaararrangemanget (WA). WA har till huvuduppgift att hindra spridning av krigsmateriel och varor med dubbla användningsområden, som kan ha militärt destabiliserande verkan och hota internationell och regional fred. WA:s listor över strategiska produkter uppdateras vid behov så att de hålls aktuella i ljuset av utvecklingen på de säkerhetspolitiska, teknologiska och kommersiella områdena.

Varulistan för informationssäkerhet, som även innefattar civila kryptoprodukter med möjlig militär tillämpning, upprättades i december 1998. Som framgår av skrivelsen kommer viss teknologi på denna lista att undantas från exportkontroll i december 2000, såvida medlemsstaterna inte överenskommer att fortsätta kontrollen. Sverige deltar i detta arbete och kommer fortsättningsvis, enligt vad utskottet erfarit, att än mer verka för en friare handel med kryptoprodukter som ett led i utvecklingen av elektroniska tjänster men med hänsynstagande till att det kvarstår ett säkerhetspolitiskt betingat intresse av att försvåra åtkomsten av starka krypton för exempelvis sådana användare som är länkade till utveckling eller produktion av massförstörelsevapen. Vidare beaktas att Sverige, för att säkra egen tillgång till utländsk högteknologi, har ett behov av att upprätthålla samma kontrollnivå som viktigare leverantörländer. Enligt utskottets mening innebär detta en lämplig avvägning. Utskottet vill framhålla att ovan redovisade synsätt också bör vara vägledande för Sveriges insatser i samband med arbetet med den nya radsförordningen som är under utarbetande.

Själva tillämpningen av WA är i betydande utsträckning en nationell angelägenhet. Som framgått ovan har detta utnyttjats av Sverige för att på olika sätt förenkla för företagen. Utskottet, som vid statsrådet Pagrotskys föredragning erfarit att ytterligare arbete med denna inriktning pågår, understryker betydelsen härav.

Förhållandena beträffande exportkontroll av kryptoprodukter har, vilket framgått ovan, i icke oväsentlig grad förändrats sedan skrivelsen underställdes riksdagen och motionerna väcktes. Enligt utskottets bedömning är därmed flertalet av de krav som motionsledes framförts redan tillgodosedda, varför motionerna 1999/2000:U410 (m) yrkandena 1 och 5–7, 1999/2000:T703 (c) yrkandena 17 och 18, 1999/2000:T705 (fp) yrkande 8 (delvis) samt 1999/2000:T717 (m) yrkandena 15 (delvis) och 16 kan besvaras med vad utskottet anfört.

I motionerna 1998/99:U16 (fp) yrkandena 2 och 4 (delvis) förespråkas, med undantag av FN-sanktionerade handelsembargon, en fullständigt fri handel, utan några restriktioner, med kryptoprodukter.

Att bifalla dessa motioner skulle innebära att Sverige måste frånträda sina åtaganden gentemot EU och WA samt dessutom bortse från nationella säkerhetspolitiska intressen. Då så icke bör ifrågakomma anser utskottet att dessa motioner bör avstyrkas.

Import av kryptoprogram

I motionerna 1998/99:U16 (fp) yrkande 4 (delvis) och 1999/2000:T705 (fp) yrkande 8 (delvis) efterlyser motionärerna fri import av kryptoprogram.

Detta yrkande överensstämmer, som framgår av sammanfattningen av skrivelsen tidigare i detta betänkande, med regeringens intentioner.

I skrivelsen betonas bl.a. att det är av allmänt intresse att användarna får tillgång till starka kryptosystem samt att det skapas förutsättningar för bruk av elektroniska signaturer och för skydd av konfidentialitet. Regeringens bedömning är att en bred användning av kryptografi ökar tilliten till kommunikationssystemen.

Utskottet delar regeringens bedömning och vill i sammanhanget framhålla att det är av allmänt intresse att vi i Sverige har tillgång till produkter av god kvalitet, såväl svenska som importerade.

Något behov av ett riksdagens tillkännagivande på denna punkt föreligger ej, varför utskottet avstyrker motionerna 1998/99:U16 (fp) yrkande 4 (delvis) och 1999/2000:T705 (fp) yrkande 8 (delvis).

IT-samhällets sårbarhet m.m.

I motion 1998/99:U16 (fp) yrkande 3 begärs en översyn av IT-samhällets sårbarhet, och motionärerna anser att en plan för att minska riskerna med IT-användningen bör tas fram.

Riksdagen har tidigare (prop. 1998/99:74, bet. 1998/99:FöU5) gjort bedömningen att det finns behov av en sammanhållen strategi för informationskrigföring och samhällets IT-säkerhet.

I skrivelse 1998/99:33 Beredskapen mot svåra påfrestningar på samhället i fred har regeringen bl.a. anfört följande. Den breddade användningen av informationsteknik leder till nya typer av sårbarhet. Konsekvensen av tekniska fel, dataintrång m.m. blir större när alltfler system kopplas samman. Regeringen prioriterar därför åtgärder som syftar till att förbättra IT-säkerheten och skyddet mot informationskrigföring. Regeringens arbete syftar till att skapa förtroende för den nya tekniken och att säkerställa att samhällsviktiga funktioner skyddas. För säkerhet på längre sikt arbetas en strategi för samhällets IT-säkerhet fram. I ett kortare perspektiv är insatser för att säkra omställningen till år 2000 högprioriterade.

Enligt vad utskottet inhämtat behandlas frågan om IT-samhällets sårbarhet i det nu pågående arbetet med en IT-proposition, som beräknas bli överlämnad till riksdagen år 2000.

Enär motionärens önskemål därmed redan får anses tillgodosedda erfordras inget riksdagens tillkännagivande, varför motion 1998/99:U16 (fp) yrkande 3 avstyrks.

Utskottet föreslår därmed att riksdagen lägger regeringens *skrivelse 1998/99:116* Om kryptografi till handlingarna.

Hemställan

Utskottet hemställer

1. beträffande *restriktioner i rätten att använda kryptering*
att riksdagen avslår motionerna 1998/99:U16 yrkandena 1 och 4 (delvis), 1999/2000:U410 yrkandena 2 och 3, 1999/2000:T703 yrkande 16, 1999/2000:T705 yrkande 8 (delvis) samt 1999/2000:T717 yrkande 15 (delvis),
2. beträffande *kryptonycklar m.m.*
att riksdagen förklarar motion 1999/2000:U410 yrkande 4 besvarad med vad utskottet anfört,
3. beträffande *export av produkter med kryptoinnehåll m.m.*
att riksdagen med avslag på motionerna 1998/99:U16 yrkandena 2 och 4 (delvis) förklarar motionerna 1999/2000:U410 yrkandena 1 och 5–7, 1999/2000:T703 yrkandena 17 och 18, 1999/2000:T705 yrkande 8 (delvis) samt 1999/2000:T717 yrkandena 15 (delvis) och 16 besvarade med vad utskottet anfört,
4. beträffande *import av krypteringsprogram*
att riksdagen avslår motionerna 1998/99:U16 yrkande 4 (delvis) och 1999/2000:T705 yrkande 8 (delvis),
5. beträffande *en översyn av IT-samhällets sårbarhet m.m.*
att riksdagen avslår motion 1998/99:U16 yrkande 3,

6. beträffande *skrivelse 1998/99:116*
att riksdagen lägger regeringens skrivelse 1998/99:116 Om krypto-
grafi till handlingarna.

1999/2000:UU7

Stockholm den 24 februari 2000

På utrikesutskottets vägnar

Viola Furubjelke

I beslutet har deltagit: Viola Furubjelke (s), Berndt Ekholm (s), Lars Ohly (v), Holger Gustafsson (kd), Bertil Persson (m), Liselotte Wågö (m), Carina Hägg (s), Agneta Brendt (s), Murad Artin (v), Sten Tolgfors (m), Marianne Samuelsson (mp), Marianne Andersson (c), Karl-Göran Biörsmark (fp), Marianne Jönsson (s), Karin Enström (m), Birgitta Ahlqvist (s) och Kenneth Lantz (kd).

Sammanfattning.....	1
Skrivelsen	2
Motionerna	2
Motion väckt med anledning av skrivelsen.....	2
Motioner väckta under den allmänna motionstiden 1999/2000	2
Utskottet	3
Ärendets beredning	3
Sammanfattning av skrivelsen	4
Bakgrund.....	4
Regeringens överväganden och slutsatser	6
Regeringens bedömning	6
Skälen för regeringens bedömning	6
Sammanfattning av motionerna	10
Utskottets överväganden.....	12
Rätten att använda kryptering.....	13
Kryptonycklar m.m.	14
Exportfrågor	15
Import av kryptoprogram	17
IT-samhällets sårbarhet m.m.	17
Hemställan	18