Dr juris Lee A Bygrave
Institutt for rettsinformatikk
Det juridiske fakultet
Universitetet i Oslo

Et grunnlag for utvikling av en helhetlig nasjonal kryptopolitikk

6. april 2001

Innholdsfortegnelse

Forord

Denne rapporten er skrevet på oppdrag av Nærings- og handelsdepartementet (NHD). Forfatteren er dr juris Lee A Bygrave ved Institutt for rettsinformatikk (IRI), Universitetet i Oslo. Professor dr juris Jon Bing ved IRI har bistått arbeidet. Nyttige innspill har også kommet fra stipendiatene Rolf Riisnæs og Jens Petter Berg ved IRI. Utforming av rapporten har skjedd i samråd med en interdepartemental styringsgruppe for kryptopolitikk ledet av NHD.

Rapporten bygger delvis på et rapportutkast skrevet av Endre Grøtnes ved Statskonsult[1] og en rapport fra 1997 skrevet i regi av daværende Rådet for IT-sikkerhet.[2]

Fremstillingen av kryptopolitikk i Storbritannia (jf vedlegg 4) bygger i stor grad på en oversikt skrevet av dr Ian Walden ved Centre for Commercial Law Studies, Queen Mary and Westfield College, University of London.

1 Jf *Utkast til rapport om kryptopolitikk*, versjon 0.11, 2.1.2001.
2 Jf Rådet for IT-sikkerhet, *Sluttrapport fra utvalg for vurdering av behov for kryptopolitikk*, 10.11.1997.

1 Sammendrag

Rapporten gir en kortfattet oversikt over visse kryptopolitiske problemstillinger. Formålet er å danne et grunnlag for utarbeidelse av en helhetlig politikk for bruk av kryptografi i Norge (jf hovedpunkt 2).

En innledende introduksjon til hva kryptografi er, gis i hovedpunkt 3.

I hovedpunkt 4 presenteres de overordnede formål for bruk av kryptografi:

- Sikring av konfidensialitet (dvs at informasjon (i klartekst) ikke blir tilgjengelig for personer/organisasjoner som mangler autorisasjon for å få tilgang til den).
- Sikring av integritet (dvs at informasjon ikke kan endres eller tilintetgjøres på uautorisert vis uten at det kan oppdages).
- Sikring av autentisitet (dvs at informasjon og identiteten til dens brukere ikke forfalskes).
- Sikring av ikke-benekting (engelsk: "non-repudiation", dvs at den som sender informasjon ikke skal kunne benekte at handlingen fant sted).

Realisering av disse formål vil kunne bidra til å fremme andre formål, bl a:

- Sikring av enkeltindividers personvern (særlig interessene i diskresjon og ikke å bli forvekslet med andre).
- Sikring av bedriftshemmeligheter (og dermed f eks bedrifters konkurransefortrinn).
- Sikring av grunnlaget for trygg handel (særlig elektronisk handel).
- Sikring av vitale nasjonale sikkerhetsinteresser (herunder rikets sikkerhet).

I hovedpunkt 5 skisseres visse bruksområder for kryptografi og visse utviklingstrekk. Tidligere ble kryptografi ofte brukt for å sikre kommunikasjon mellom offentlige organer, og gjerne assosiert med forsvarets behov. I dag er dette en alt for snever ramme, snarere karakteriseres utviklingen av den sterkt økende bruk innen privat sektor, ikke minst i forbindelse med elektronisk handel. Tendensen forsterkes ved likestilling mellom papirbaserte og elektroniske dokumenter og visse trekk i virksomheters organisering og arbeidsmåte (økende geografisk desentralisering, bruk av hjemmekontor). Kryptering brukes også for å sikre personvern ved elektronisk kommunikasjon. For å sikre visse rettigheter (typisk opphavsrettigheter), bygges kryptering i økende grad inn i den grunnleggende teknologien.

Økt bruk av kryptering har utfordret politi og påtalemyndighet i utføringen av deres legitime oppgaver, fordi det er blitt vanskeligere å få tilgang til innholdet i kommunikasjon og lagrede data ved vanlig avlytting og beslag. Selv om kryptobruk i norske kriminelle miljøer hittil synes å ha hatt beskjeden innvirkning på politiets etterforskningsevne, er det forventet at denne situasjonen vil endre seg.

Utviklingen i sin helhet kan sammenfattes i tre punkter:

- Større etterspørsel og tilgengelighet av kryptoprodukter.

- Større vanskeligheter med å begrense anvendelse av kryptografi.
- Større kompleksitet og uforutsigbarhet når det gjelder hvorledes kryptografi vil bli brukt og regulert i framtiden.

I hovedpunkt 6 diskuteres forskjeller i dagens kryptobruk mellom enkeltindivider, bedrifter og offentlige organer. Det pekes på at enkeltindivider stort sett bruker kryptering som en integrert del av tilbudte tjenester. Bedrifter bruker både kryptering i sin kommunikasjon eksternt og internt. Det offentlige bruker alle former for kryptering – ikke bare innen forsvaret og utenrikstjenesten, hvor kryptering er svært utbredt, men også f eks innen helseforvaltningen, hvor sensitive personopplysninger utnyttes.

I hovedpunkt 7 diskuteres overordnede interesser som kan fremmes ved bruk av kryptering. Oppsummeringsvis er disse:

- Personvern og ytringsfrihet.
- Transaksjonstrygghet.
- Bedrifters interesse i økt inntjening og konkurranseevne, inklusive fremming av en kryptoindustri.
- Vitale nasjonale sikkerhetsinteresser, herunder rikets sikkerhet og geopolitisk suverenitet.
- Effektiv, elektronisk forvaltning.
- Reduksjon av sårbarhet for ytre angrep.
- Økt tillit til datamaskinbaserte systemer.

I hovedpunkt 8 diskuteres overordnede interesser som kan skades ved økt bruk av kryptering:

- Etterforskning og bekjempelse av kriminalitet, spesielt organisert kriminalitet.
- Personvern (som svekkes gjennom større krav til registrering av personopplysninger i forbindelse med den infrastruktur som er nødvendig for velfungerende krypterte tjenester).

I hovedpunkt 9 diskuteres rettslige krav til bruk av kryptering. Kort gjennomgås de bestemmelser som *direkte* regulerer kryptering:

- Lov om elektroniske signaturer (definerer bl a krav til avanserte elektroniske signaturer, kvalifiserte sertifikater, utstedere av slike sertifikater og sikre signaturfremstillingssystemer).
- Personopplysningsloven (i forskrift er det pålegg om kryptering eller annen sikring av personopplysninger som overføres utenfor den databehandlingsansvarliges fysiske kontroll).
- Sikkerhetsloven (ikke trådt i kraft, inneholder regler om godkjenning og bruk av krypteringssystemer for sikkerhetsgradert informasjon, og etablerer bl a Nasjonal sikkerhetsmyndighet).
- Eksportkontrolloven, sammen med det såkalte Wassenaar-arrangementet (regulerer eksport av kryptoprodukter fra Norge til utlandet, administrert av Utenriksdepartementet i samråd med Nasjonal sikkerhetsmyndighet).

Det finnes også bestemmelser som mer *indirekte* omhandler kryptering:

- Personopplysningsloven, hvor krav til konfidensialitet, integritet og tilgjengelighet kan

realiseres ved kryptering.
- Straffeloven, hvor bestemmelser om forskjellige typer datakriminalitet kan beskytte krypterte opplysninger og krypteringsmekanismer.
- Den europeiske menneskerettskonvensjonen som i artikkel 8 fastslår retten til "respect for private life, family, home and correspondence"; også relevante er artikkel 10 om ytringsfrihet og artikkel 6 om retten til "fair hearing".

I hovedpunkt 10 gjennomgås de internasjonale rammer for norsk kryptopolitikk med særlig fokus på:

- *Standardisering*. Det mangler offisielle internasjonale standarder på området. Amerikanske standarder (DES og snart etterfølgeren AES) fungerer som *de facto* standarder. Standardisering har vesentlig betydning for å oppnå funksjonelt samvirke (interoperabilitet) mellom kryptosystemer.
- *Eksportkontroll*. USA har liberalisert sin eksport av produkter og tjenester relatert til kryptering. EU har en egen forordning om kontroll med bl a visse kryptoprodukter.
- *Adgang til klartekst i forbindelse med kriminalitetsbekjempelse*. Det pågår en diskusjon om hvorvidt politi og andre organer for håndhevelse av loven skal få adgang til kryptert informasjon i klartekst, og under hvilke omstendigheter. EU har fastsatt hovedprinsipper i en handlingsplan fra 1997, mens G8 har vedtatt en handlingsplan i ti punkter for kriminalitet relatert til høyteknologi, hvor enkelte punkter berører kryptering. Det nærmeste en kommer internasjonale rettslige normer er Europarådets utkast til konvensjon om "cybercrime" som ventes ferdigstilt i løpet av 2001. Her er spesielt artikkel 19 interessant, som angir hvilken plikt en ratifiserende stat vil ha til i nasjonal lovgivning sikre politi mv tilgang til datamaskinbaserte systemer og informasjon lagret i slike.
- *OECDs retningslinjer for kryptopolitikk fra 1997*. Disse skal veilede OECD medlemslandene i deres utarbeidelse av nasjonal kryptopolitikk. Norge har sluttet seg til retningslinjene. Kjernen i retningslinjene er åtte innbyrdes avhengige prinsipper som bl a oppfordrer til økt og markedsdrevet bruk av kryptografi.

I hovedpunkt 11 skisseres interesseavveininger i forbindelse med bruk av kryptering. Det fremheves at ofte vil det ikke være noen interessemotsetninger mellom enkeltpersoners, bedrifters og offentlige organers interesser.

Som den viktigste interessekonflikten nevnes i hvilken grad enkeltpersoner eller bedrifter skal kunne sikre sin kommunikasjon og informasjon med kryptering på bekostning av politiets og andre offentlige organers mulighet for i praksis å få innsyn i denne. Problemstillingen kompliseres ved at visse former for kryptering kan være midler for å sikre seg mot kriminalitet (f eks uberettiget utnyttelse av åndsverk). Argumentene for å gi politi eller andre myndigheter innsyn gjennomgås kortfattet, og stilles opp mot motargumenter. Spørsmålet om obligatorisk nøkkeldeponering diskuteres særskilt.

Beslektet er reguleringen av eksport av sterke kryptoprodukter til utlandet, hvor hensynet til nasjonal sikkerhet kan komme i konflikt med næringspolitiske interesser.

Diskusjonen kan ikke skilles ut fra den mer generelle politiske diskusjon av hvordan en utformer

informasjonssamfunnet. Og den gjøres vanskeligere ved at den i stor utstrekning må basere seg på hypoteser og prognoser det lett vil kunne være saklig uenighet om.

I hovedpunkt 12 fremmes visse anbefalinger for en nasjonal kryptpolitikk:

- En grunnleggende positiv holding til bruk av kryptering.
- Avvisning av obligatorisk deponering av krypteringsnøkler som en innehar som privatperson.
- Oppmerksomhet rettet mot koordinering på et internasjonalt, ikke bare europeisk nivå.
- Tilrettelegging av forholdene for sterkere vekst i nasjonal kryptoindustri.
- Minst mulig belastning av brukergrupper ved implementering av politikken.
- Utforming av politikken i tråd med forslaget om bruk av elektroniske signaturer (jf NOU 2001:10).
- Utforming av politikken slik at den ikke krever endring i de alminnelige regler for saksbehandling i offentlig forvaltning, men sikrer bedre realisering av forvaltningslovens målsettinger ved overgang til elektronisk forvaltning.

I hovedpunkt 13 fremmes visse problemstillinger som videre arbeid bør ta stilling til:

- *Samordning*, bl a spørsmålet om man bør sondre mellom bruk av kryptering i forsvaret og sivil sektor, og om en bør sondre mellom tiltak for sikring av konfidensialitet og tiltak for sikring av integritet, autentisitet og ikke-benektning.
- *Anskaffelse*, dvs om det bør tas stilling til hvordan verktøy eller systemer anskaffes.
- *Reguleringsmåte*, dvs om det bør tas stilling til hvordan en skal regulere kryptering, fra selvregulering til lover.

Det antydes at kryptopolitikk bør finne sitt grunnlag i det som er fremmet for elektronisk handel og forretningsdrift (jf St meld nr 41 (1998–99), dvs:

- "Elektronisk handel vil bli drevet frem av markedet i form av produkter og tjenester som bedrifter og forbrukere vil etterspørre".
- "Der myndighetene griper inn, må dette skje i full åpenhet og dialog med de berørte parter".
- "Reguleringene må være nøytrale i forhold til teknologi og ikke være bundet til bestemte teknologiske løsninger".

Vedlegg

I vedlegg 1 oppsummeres OECDs retningslinjer for kryptopolitikk. I vedlegg 2–4 gjøres det kort rede for hovedtrekk i Sveriges, Danmarks og Storbritannias kryptopolitkk. Hovedtrekkene kan oppsummeres slik:

- *Overordnet kryptopolitikk*. Dette er utformet av Sverige i en skrivelse fra regjeringen (1998–99) og videreført i en proposition for 1999/2000. I Danmark er det sammenfattet i et felles brev fra april 2000 fra Erhvervs-, Forsvars-, Justits- og Forskningsministeren til IT-sikkerhetsrådet. I Storbritannia er det ikke utformet noen tilsvarende overordnet politikk.
- *Eksportkontroll*. Sverige, Danmark og Storbritannia har implementert EU-Rådets forordning nr 1334/2000.

- *Elektroniske signaturer*. Sverige, Storbritannia og Danmark har implementert EU direktivet (1999/93/EF) om elektroniske signaturer.
- *Obligatorisk nøkkeldeponering*. I Sverige har det vært liten debatt om dette, hverken der eller i Danmark synes det å være aktuelt. I Storbritannia er det innført et eksplisitt forbud, dog åpner loven for at regjeringen kan vedta deponering i visse tilfeller. I Storbritannia finnes det også hjemmel for at politiet kan innhente informasjon som inneholder nøkler i visse tilfeller, unntatt slike som brukes for generering av elektroniske signaturer, og med et unntak som spesielt tar sikte på forholdet til Den europeiske menneskerettskonvensjon artikkel 6.
- *Andre relevante initiativ*. Sverige har etablert en arbeidsgruppe "för skydd mot informationsoperationer", Danmark en "Følgegruppe om Kryptering". I Storbritannia er det hjemlet et register over godkjente tilbydere av kryptotjenester, som ikke er implementert i påvente at bransjen etablerer selvregulering (et eksempel er tScheme).

I vedlegg 5 gis en kort gjennomgang av norske regler vedrørende politiets evne til å etterforske kriminalitet, med særlig fokus på tilfeller der kommunikasjon og lagrede data i det kriminelle miljøet er kryptert. Det pekes på visse rettslige problemer knyttet til kommunikasjons-/informasjonstjenesteleverandørers registrering av abonnent- og trafikkdata. Problemene kan medføre vanskeligheter for politiet i å innhente opplysninger om kriminelles identitet og kommunikasjon.

2 Rapportens formål

Formålet med rapporten er å danne et grunnlag for utarbeidelse av en helhetlig politikk for bruk av kryptografi i Norge.

Kryptopolitikken skal fastsette målsettinger for hvordan kryptografi brukes i Norge, samt angi retningslinjer for oppnåelse av målsettingene. OECDs retningslinjer for kryptopolitikk[3] fra 1997 skal legges til grunn. Politikken skal dekke nåtidig og fremtidig bruk av kryptografi i både offentlig og privat sektor. Den skal legge særlig vekt på spørsmål knyttet til:

- Enkeltindividets, næringslivets og myndighetenes behov for og nytte av sikker kommunikasjon.
- Hensynet til kriminalitetsbekjempelse.
- Norges holdning i internasjonalt samarbeid, bl a om eksportkontroll av kryptoprodukter.
- Ivaretagelse av vitale nasjonale interesser, f eks vedrørende handel, suverenitetskontroll, offentlighet og sikkerhetspolitikk.[4]

Nærings- og handelsdepartementet har i felleskap med Justisdepartementet hovedansvar for utforming av kryptopolitikken.

Et hovedelement i denne rapporten er å fremstille ulike aktørers interesser angående kryptobruk, samt eventuelle spenninger mellom disse. Rapporten forsøker dessuten å tydeliggjøre konsekvensene av ulike interesseavveininger og tilhørende handlinger. Selv om rapporten fokuserer på norske forhold, inneholder den også en oversikt over utviklingen av kryptopolitikk i visse andre land og på internasjonalt nivå.

3 Kryptografi i et nøtteskall

På et overordnet nivå handler kryptografi om forskjellige systemtekniske tiltak som omformer data slik at visse personers/organisasjoners evne til å forstå dataenes semantiske innhold (dvs informasjonen som dataene er ment å uttrykke i ukryptert format)[5] blir vanskeliggjort. Omformingen betegnes som *kryptering*. Det å reversere en krypteringsprosess betegnes som *dekryptering*. Kryptering foregår i de edb-systemer som gjerne anvendes i dag, ved bruk av en *algoritme* (beregningsmetode som definerer hvordan dataene skal omformes) med tilhørende *nøkkel* (sekvens av symboler som kontrollerer krypterings- og dekrypteringsoperasjonene).

Det finnes tre måter å få tilgang til innholdet i krypterte data på. En må enten kjenne krypteringsnøkkelen, "knekke" algoritmen/nøkkelen ved hjelp av kryptoanalyse, eller kjenne til en eventuell teknisk-organisatorisk "bakdør" til innholdet.

---

[3] Jf OECD, *Guidelines for Cryptography Policy*, vedtatt 27.3.1977. Nærmere opplysninger om retningslinjene finnes i hovedpunkt 10 og vedlegg 1.

[4] Jf Nærings- og handelsdepartementet, *Utgangspunkter for arbeidet med politikk for bruk av kryptering*, Notat av 7.9.2000, pkt 4.

[5] Også kalt informasjon *i klartekst*.

Hvor lett en krypteringsnøkkel – i edb-sammenheng – kan knekkes av personer/organisasjoner som i utgangspunkt ikke kjenner til nøkkelen, avhenger delvis av antall *bits* (0- eller 1-tall) som inngår i nøkkelen. Jo flere bits, desto vanskeligere er det i praksis å knekke nøkkelen.[6]

Det finnes to hovedkategorier av kryptografi: *symmetrisk* og *asymmetrisk*. Et symmetrisk kryptosystem betegner en prosess der både kryptering og dekryptering av ett sett opplysninger/data foregår ved bruk av samme nøkkel. I forbindelse med datakommunikasjon innebærer et symmetrisk kryptosystem at avsenderen og mottakeren av dataene deler en felles (men ellers hemmelig) nøkkel.

Et *asymmetrisk* kryptosystem innebærer derimot anvendelse av forskjellige (dog matematisk relaterte) nøkler til kryptering og dekryptering. Hver bruker av systemet får tildelt et nøkkelpar der den ene nøkkelen er privat og hemmelig, mens den andre er offentlig tilgjengelig. Den hemmelige nøkkelen benyttes til dekryptering av data; den offentlige nøkkelen brukes til kryptering.

Asymmetrisk kryptografi muliggjør langt på vei systemer for *digitale/elektroniske signaturer*. En elektronisk melding kan "signeres" ved bruk av avsenderens hemmelige nøkkel. Verifisering av signaturen kan skje ved (mottakerens) bruk av den offentlige nøkkelen som tilhører avsenderen. For at verifiseringen skal være sikker må det opprettes et system som på uavhengig vis kan godtgjøre forbindelsen mellom avsenderen og den offentlige verifiseringsnøkkelen. Slike systemer tilbys av *sertifikatutstedere* innenfor rammen av en *infrastruktur for offentlignøkkel-kryptografi* (såkalt "Public Key Infrastructure" (PKI), dvs en samling av sikkerhetstjenester, sikkerhetskomponenter og aktører som muliggjør storskala bruk av digitale signaturer). Sertifikatutstederens hovedvirksomhet består av å utstede og administrere sertifikater som dokumenterer tilhørigheten mellom en viss (offentlig) verifiseringsnøkkel og en viss bruker.

Terminologiforklaringene ovenfor legges til grunn i denne rapporten.[7]

4 Bruksformål for kryptografi

På et overordnet nivå fremmer bruk av kryptografi, sett under ett, følgende formål:

- Sikring av *konfidensialitet* (dvs at informasjon (i klartekst) ikke blir tilgjengelig for personer/organisasjoner som mangler autorisasjon for å få tilgang til den).
- Sikring av *integritet* (dvs at informasjon ikke kan endres eller tilintetgjøres på uautorisert vis uten at det kan oppdages).
- Sikring av *autentisitet* (dvs at informasjon og identiten til dens brukere ikke forfalskes).

---

[6] For hver bit en øker krypteringsnøklenes lengde med, dobles antall mulige nøkler som er benyttet i forbindelse med algoritmen. En 56-bits nøkkel gir 2^{56} eller ca 72 millioner milliarder mulige nøkler. I dag er dette antallet ansett som knapt tilstrekkelig til å beskytte systemer med høye sikkerhetsbehov.

[7] For en mer utførlig beskrivelse av de tekniske og organisatoriske sider ved kryptografi, med hovedfokus på digitale signaturer og PKI, vises det til NOU 2001:10, *Uten penn og blekk – Bruk av digitale signaturer i elektronisk samhandling med og i forvaltningen*, særlig kapittel 3 og vedlegg 4.

- Sikring av *ikke-benekting* (engelsk: "non-repudiation", dvs at den som sender informasjon ikke skal kunne benekte at denne handlingen fant sted).

Oppnåelse av hvert av disse sikringsformålene vil i tur kunne bidra til å fremme av en lang rekke andre formål. Typiske eksempler her er:

- Sikring av enkeltindividers personvern (særlig interessene i diskresjon og ikke å bli forvekslet med andre).
- Sikring av bedriftshemmeligheter (og dermed f eks bedrifters konkurransefortrinn).
- Sikring av grunnlaget for trygg handel (særlig elektronisk handel).
- Sikring av vitale nasjonale sikkerhetsinteresser (herunder rikets sikkerhet).

Når det gjelder sikring av dataintegritet bør det understrekes at kryptobruk i seg selv ikke kan stoppe uautorisert endring eller tilintetgjøring av data, men bruk av asymmetriske krypteringsmetoder muliggjør at slike integritetskrenkelser blir oppdaget.

Det bør videre presiseres at hvor velegnet kryptografi er for å oppnå hvert av de ovennevnte formål delvis vil avhenge av hvilken krypteringsmetode som anvendes. Symmetriske metoder er velegnet til sikring av konfidensialitet, særlig når det er behov for rask kryptering av store datamengder. De kan også bidra til oppnåelse av en viss grad av autentisitet (mellom kommunikasjonspartene dog ikke overfor omverden), men er dårlig egnet for utførelse av ikke-benektingsfunksjoner.

Asymmetriske krypteringsmetoder er derimot velegnet for bruk til autentiserings- og ikke-benektingsformål. De kan dessuten bidra til sikring av konfidensialitet, men kan ikke kryptere store datamengder like raskt som symmetriske metoder. Systemer for elektroniske signaturer med tilhørende PKI vil derfor ofte basere seg på en kombinasjon av asymmetrisk og symmetrisk kryptografi der sistnevnte brukes i forbindelse med den primære krypteringen av dataene som skal lagres eller overføres.

Kryptografi i sin alminnelighet er for det meste en *befordrende* faktor snarere enn en *nødvendig* forutsetning for oppnåelse av alle de ovennevnte formål. Samtidig er det ikke til å underslå at kryptobruk er i ferd med å bli uunværlig for at visse typer elektroniske transaksjoner skal kunne utføres på en hensiktsmessig måte (jf neste hovedpunkt). Dessuten er det per dags dato vanskelig å fremstille digitale/elektroniske signaturer (i alle fall de som er definert som "kvalifiserte signaturer" etter loven om elektroniske signaturer)[8] uten bruk av asymmetrisk kryptografi.

5 Bruksområder for kryptografi – generelle utviklingstrekk

Kryptografi sett under ett anvendes i dag på svært mange og ulike områder. Tidligere ble kryptografi oftest brukt for å sikre kommunikasjon mellom offentlige organer samt sikre lagrede data. Særlig var dette aktuelt i forsvarssektoren og utenrikstjenesten. Nå blir kryptografi i økende

[8] Jf hovedpunkt 9.

grad brukt for å sikre kommunikasjon mellom aktører i den private sektor (både næringsdrivende og enkeltindivider) og for å sikre kommunikasjon mellom disse og den offentlige sektor.

Parallelt med at kryptobruk sprer seg fra offentlig til privat sektor, foregår det globaliseringsprosesser som innebærer økt tilgjengelighet av og etterspørsel etter kryptoprodukter på tvers av nasjonale grenser. Disse prosessene er blitt holdt noe tilbake av visse lands (i hovedsak USAs) strenge regler for eksport av sterke kryptoprodukter, men en liberalisering av eksportreglene har nylig funnet sted (jf hovedpunkt 10).

Betydningen av kryptografi for sikring av integritet, autentisitet og ikke-benekting har samtidig blitt større i forhold til betydningen for konfidensialitetssikring. Denne utviklingen har skjedd i og med fremveksten av pålitelige systemer for elektroniske/digitale signaturer. Hovedtyngden av dagens kryptobruk er fremdeles rettet inn mot sikring av konfidensialitet, men profilen vil sannsynligvis endre seg så snart allment utbredte og velfungerende PKI-systemer er på plass.

Kryptografi er i ferd med å bli uunværlig hvis en skal oppnå den ønskede utviklingen av handel og kommunikasjon over åpne nettverk. På en rekke områder der tjenester som tradisjonelt krever en betydelig grad av konfidensialitet (f eks legetjenester, banktjenester, apotektjenester, tjenester for voldgift/megling, ulike offentlige forvaltningstjenester) i økende grad utføres "online", blir bruk av forholdsvis sterk kryptering essensiell.

Viktigheten av kryptografi forsterkes av en tendens til at elektroniske dokumenter mv rettslig sett likestilles med papirbasert dokumentasjon når det gjelder elektronisk saksbehandling i offentlig forvaltning generelt. Visse trekk ved virksomheters organisering og arbeidsmåte (bl a økende geografisk spredning av bedrifters virksomhet og økende bruk av hjemmekontor), samt den sterkt voksende økonomiske verdisettingen av data og databehandling i seg selv, bidrar også til at kryptografi får stadig større betydning.

Kryptomekanismer blir videre i økende grad bygget inn i ulike informasjonssystemers grunnleggende arkitektur. Eksempler her er SSL (Secure Sockets Layer, en Internett-standard for sikker tilkopling til en web-server) og Microsoft Windows 2000 (som tilbyr innholdskryptering). Integreringen er ikke bare resultat av nye teknologiske muligheter; den skjer også som følge av ønsker om å forsterke ivaretagelse av ulike rettigheter (f eks opphavsrett, personvernrettigheter) spesielt i online-sammenheng.

Kryptomekanismer blir i større grad utformet etter premisser fastlagt av private kommersielle aktører. Det vokser frem en industri som har spesialisert seg på å utvikle og markedsføre stadig mer sofistikerte kryptoprodukter.

Noen av disse produktene har sammen med annen informasjons- og kommunikasjonsteknologi (IKT) gjort det svært vanskelig for politi og påtalemyndighet å få tilgang til klartekst i kommunikasjon og lagrede data ved vanlig avlytting og beslag. Dette har skapt frykt for at kryptering skal kunne brukes til illegitime formål uten at myndigheter har en reell sjanse til å gripe inn. Slike vanskeligheter har imidlertid ofte vært av forbigående karakter. Innsnevringen av muligheter for å få adgang til klartekst har ofte blitt oppveid av utvikling av mer sofistikerte avlyttings-/dekrypteringsteknologier og/eller regler som medfører at myndigheter kan få adgang til klartekst (f eks ved at det bygges inn en teknisk-organisatorisk "bakdør" til innholdet). Dette

gjelder bl a myndigheters avlyttingsmuligheter i forhold til mobiltelefoni over GSM-nettet.

Når det gjelder kryptobruk i kriminelle miljøer er det verdt å merke seg at politi og påtalemyndighet i Norge hittil har erfart at de aller fleste databeslag foretatt i etterforskningsøyemed ikke er krypterte.[9] Dette skyldes trolig i stor grad at mange datamaskiners operativsystemer inntil nylig har manglet standard kryptofunksjoner. Politi og påtalemyndighet har likevel erfart en del problemer med kryptering av lagrede data i forbindelse med etterforskning av saker angående besittelse av barnepornografi. De har også merket noe bruk av kryptering ved kommunikasjon blant kriminelle. Generelt sett synes kryptobruk i norske kriminelle miljøer hittil å ha hatt beskjeden innvirkning på politiets etterforskningsevne. Det kan imidlertid ikke forventes at denne situasjonen vedvarer, særlig i lys av økende utbredelse av IKT-produkter som inneholder standard kryptofunksjoner.

Den rivende teknologiutviklingen betyr et kontinuerlig kappløp mellom krypterings- og dekrypteringsmuligheter. Den betyr også at sikkerheten som oppnås ved kryptering forblir midlertidig og relativ.[10]

Sammenfatningsvis medfører de utviklingstrekk som er beskrevet her:

- Større etterspørsel og tilgjengelighet av kryptoprodukter.
- Større vanskeligheter med å begrense anvendelse av kryptografi.
- Større kompleksitet og uforutsigbarhet når det gjelder hvorledes kryptografi vil bli brukt og regulert i framtiden.

6 Forskjeller i dagens kryptobruk mellom enkeltindivider, bedrifter og offentlige organer

Behovet for kryptografi samt måten den benyttes i dag kan variere mellom enkeltindivider, bedrifter og offentlige organer.

I utgangspunktet kan det grovt sett skilles mellom kryptoprodukter og -tjenester som anvendes ved lokal lagring av data og de som anvendes ved overføring av data mellom personer/organisasjoner. Det kan videre skilles mellom krypteringsprosesser som er integrert i et større tjenestetilbud og de som en tjenestebruker selv må ta initiativet til å igangsette. Skillelinjene i begge tilfeller vil ofte være nokså diffuse i praksis.

Når det gjelder enkeltindivider er deres kryptobruk i hovedsak iverksatt som integrert del av de tjenestene de benytter (som f eks GSM-mobiltelefoni og betalingsformidling ved nettbanker). Noen tar i bruk kryptering av eget tiltak i forbindelse med kommunikasjon (f eks e-post).

---

[9] Ifølge opplysninger gitt av ØKOKRIM (Den sentrale enhet for etterforskning og påtale av økonomisk kriminalitet og miljøkriminalitet) i anledning lukket møte den 4.4.2001 mellom Katarina de Brisis (NHD), Lee A Bygrave (IRI) og to representanter fra ØKOKRIM (Inger Marie Sunde og R Fløisbonn).

[10] Det er nylig rapportert om at en respektert amerikansk kryptolog, Michael Rabin, nettopp har utviklet en uknekkelig (symmetrisk) kryptoteknikk, men stor usikkerhet knyttes til hvorvidt teknikken er praktisk anvendbar. Jf "Unknackbare Verschlüsselung: Wirbel um die Krypto-Revolution", Spiegel Online 2001, <http://www.spiegel.de/netzwelt/technologie/0,1518,120312,00.html>.

Bedrifter både etablerer og bruker tjenester som benytter kryptering. Mange bedrifter bruker også kryptering i kommunikasjonen med sine samarbeidspartnere. Store bedrifter har ofte interne nettverk hvor all eller mye informasjon overføres kryptert.

Det finnes lite tilgjengelig empiri om hvor vanlig det er at enkeltindivider og bedrifter benytter kryptering ved lokal lagring av data. Det er imidlertid kjent at finansinstitusjoner og forsikringsselskaper pleier å oppbevare sensitive data i kryptert form. Det er grunn til å tro at det samme gjøres av et økende antall store bedrifter i andre bransjer av næringsliv.

Offentlige organer benytter alle former for kryptering. I forsvaret og utenrikstjenesten er kryptobruk allerede meget utbredt. Noen av de kryptoproduktene som her brukes, har vært utviklet innenfor staten og ikke vært tilgjengelige for andre. Mange steder, spesielt innen helsesektoren, blir dokumenter lagret kryptert. Sensitive personopplysninger vil også overføres kryptert. I tillegg vil arbeid på hjemmekontor ofte forutsette kryptobruk ved dataoverføring. Det finnes videre utstyr som krypterer informasjon sendt mellom statsrådene. Enkelte myndigheter (f eks Rikstrygdeverket) har dessuten etablert tjenester som benytter kryptering.

7 Overordnede interesser som kryptobruk kan fremme

Bruk av kryptografi kan fremme en rekke ulike interesser som enkeltindivider, bedrifter og offentlige organer kan sies å ha.

For enkeltindivider er interessene først og fremst av personvernmessig art; dvs at interessene i stor grad angår beskyttelse av personlig integritet, privatliv og autonomi. Ytringsfrihet er en annen ideell interesse som er nært knyttet til personverninteressene, spesielt i nåværende sammenheng. Både personvern og ytringsfrihet handler bl a om enkeltindividers muligheter for selvutfoldelse.

Disse interessene blir i hovedsak ivaretatt av kryptografiens evne til å sikre datakonfidensialitet. Det bør samtidig understrekes at kryptering ikke er ensbetydende med anonymisering. Kryptering medfører ikke nødvendigvis en fullstendig anonymisering av en transaksjon og dens parter. Kryptobruk kan skjule innholdet i datakommunikasjon uten å skjule identiteten til de som kommuniserer. Dessuten kan kryptobruk ikke hindre overvåking av generelle trafikk- og kommunikasjonsmønstre, selv om disse i stor grad er anonymiserte.

I tillegg til interessene tilknyttet personvern og ytringsfrihet har enkeltindivider en rekke interesser som mer direkte vedrører transaksjonstrygghet, dvs at en transaksjon (i vid forstand) utføres i tråd med transaksjonspartenes rimelige forventninger. Transaksjonstrygghet betyr dermed også at alle rammene for transaksjonen er relativt godt kjent for partene (og eventuelt andre som er berørt av transaksjonen). Interessene som er direkte knyttet til transaksjonstrygghet vil ofte være av økonomisk, teknisk og/eller prosedyremessig karakter. De angår pålitelighet, effektivitet, hurtighet mv i forbindelse med bl a betalingsformidling og offentlig saksbehandling.

Interessene i transaksjonstrygghet vil først og fremst kunne fremmes av kryptografiens evne til å sikre integritet, autentisitet og ikke-benekting. Samtidig vil også evnen til å sikre konfidensialitet kunne spille en betydelig rolle. Det bør videre fremheves at skillelinjen mellom interessene vedrørende transaksjonstrygghet og interessene vedrørende personvern og ytringsfrihet ikke er fast. Begge interessesett overlapper hverandre.

For bedrifter er deres interesser som kryptografi kan fremme, i stor grad tilknyttet transaksjonstrygghet. En annen viktig interesse – som delvis teller blant interessene vedrørende transaksjonstrygghet – er beskyttelse av bedriftshemmeligheter. I tillegg kommer interessen i å ivareta visse rettigheter (f eks opphavsrettigheter) i forbindelse med salg og annen tilgjengeliggjøring av digitale produkter. Kryptografi muliggjør også en mer effektiv deling av sensitiv informasjon f eks i utviklingssamarbeid ("nettverking") mellom kommersielle aktører.

På et mer overordnet nivå vil kryptobruk kunne gagne bedrifters interesser i økt fortjeneste og konkurranseevne. For bedrifter som lever av å utvikle og/eller selge kryptoprodukter og –tjenester, vil disse interessene også understøttes av et miljø som tilbyr kryptobruk gode vekstvilkår i både privat og offentlig sektor. En blomstrende kryptoindustri burde kunne få positive ringvirkninger for IKT-industrien generelt og for elektronisk handel spesielt.

Når det gjelder offentlige organer, er betydningen av kryptobruk tradisjonelt blitt fremhevet i forbindelse med beskyttelse av rikets sikkerhet og geopolitisk suverenitet. Men med overgangen til en omfattende elektronisk forvaltning vil kryptografi, sett under ett, bli viktig for effektiv gjennomføring av de aller fleste av offentlige organers sentrale oppgaver. Elektronisk forvaltning innebærer at rutiner for intern saksbehandling, økonomiforvaltning, innkjøp og innrapportering, samt rutiner for kontakt med eksterne aktører, i stor grad vil basere seg på elektronisk informasjonsutveksling. Slike rutiner vil åpenbart måtte understøttes av utstrakt bruk av kryptosystemer. Alle av kryptografiens primærfunksjoner (sikring av konfidensialitet, integritet, autentisitet og ikke-benekting) vil spille vesentlige roller her.

I den forbindelse vil kryptobruk kunne fremme en lang rekke interesser. Mange av disse vedrør oppnåelse av transaksjonstrygghet. Mer overordnede interesser omfatter bl a ønsker om kostnadsbesparelse og forbedring av kvaliteten på tjenesteytelse.

Kryptobruk er viktig også i et sårbarhetsperspektiv. Stans i, eller andre grunnleggende forstyrrelser av, informasjonssystemet til en organisasjon (i privat eller offentlig sektor) kan lamme organisasjonens virksomhet – noe som av og til kan få betydelige negative følger for samfunnet som helhet. Et velfungerende kryptosystem (brukt f eks i forbindelse med adgangskontroll) vil som regel kunne bidra til å redusere denne risikoen.

Et forholdsvis lite påaktet aspekt ved sårbarhetsbetraktninger vedrør *tilliten* til at et system fungerer på tilsiktet vis. Rykkes grunnlaget for denne tilliten bort kan selve systemet lammes, selv om det ikke foreligger noen konkrete angrep på systemet. *Muligheten* for forstyrrelse eller kompromittering av systemet kan i seg selv være nok til at systemet lammes. Velfungerende – inklusive velpubliserte (dog innenfor visse grenser!) – krypteringstiltak kan forhindre slik tillitssvikt.

Tillitsaspektet er særlig viktig for fremveksten av elektronisk handel over Internett. Det er høyst

sannsynlig at handel på Internett i overskuelig framtid vil utgjøre en stadig større andel av handel generelt. En forutsetning for denne utviklingen er at kjøpere og selgere skal kunne ha gjensidig tillit til at de mange forskjellige transaksjoner som inngår i elektronisk handel, gjennomføres på en minst like sikkert måte som ved ikke-elektroniske handel. Tilgang til pålitelige kryptomekanismer er essensielt for å fremme denne tilliten.

8 Overordnede interesser som kryptobruk kan skade

Bruk av kryptografi kan få negative ringvirkninger for etterforskning og bekjempelse av kriminalitet. Denne kriminaliteten vil være mangeartet, men vil i særlig grad gjøre seg gjeldende med organisert kriminalitet. Den vil f eks kunne omfavne terrorisme såvel som lagring og overføring av ulovlig (pornografisk, rasistisk mv) innhold. Svekkelse av myndighetenes evne til å bekjempe den vil få åpenbare skadefølger for samfunnet generelt.

Det er kryptografiens evne til å sikre datakonfidensialitet som er problematisk her, ikke dens evne til å sikre autentisitet, integritet og ikke-benekting. Problemet oppstår først og fremst når datakommunikasjon mellom kriminelle eller lagrede data oppbevart av kriminelle, krypteres ved bruk av algoritmer/nøkler som politiet eller andre statlige sikkerhetsorganer ikke er i stand til å knekke. Hvor vanskelig knekking er, vil avhenge av ikke bare algoritmens/nøkkelens kompleksitet, men også hvilke ressurser og kompetanse som myndighetene har i forhold til oppgaven. I den forbindelse er det verdt å merke seg at den forestående etablering av Politiets Datakrimsenter ved ØKOKRIM vil innebære en betydelig forbedring av myndighetenes ressurser og kompetanse på feltet.[11]

Det bør også påpekes at en (for myndighetene) "uknekkelig" kryptering av lagrede data hos kriminelle eller datakommunikasjon mellom kriminelle ikke nødvendigvis vil innebære at etterforskningen mislykkes. Myndighetene vil ofte ha flere bein å stå på i etterforskningsøyemed (jf vedlegg 5).

Det er likevel ikke til å underslå at slik kryptering vil kunne medføre betydelige praktiske problemer for myndighetenes evne til å bekjempe kriminalitet på en kostnadseffektiv måte. Disse problemer vil trolig forsterkes av flere faktorer (jf vedlegg 5):

- Usikkerhet om hvorvidt visse etterforskningsmetoder (f eks hemmelig online "ransaking") som kunne bidra til å lette adgang til klartekst, har tilstrekkelig lovhjemmel.
- Utilstrekkelig registrering av abonnent- og trafikkdata hos kommunikasjons-/informasjonstjenesteleverandører.
- Kriminelles bruk av egne lukkede kommunikasjonsnettverk (med f eks krypterte eller fiktive/falske Internet Protocol (IP) adresser).

Visse typer anvendelser av kryptografi har også et potensial for indirekte svekking av personverninteresser. PKI-systemer vil kunne svekke personvern i og med at slike systemer

[11] Jf ØKOKRIM, *Økt innsats for bekjempelse av datakriminalitet – Forslag om etablering av Politiets datakrimsenter, ØKOKRIM*, 18.12.2000. Regjeringen har nylig gitt klarsignal om at senteret skal opprettes.

forutsetter registrering og sentralisering av visse opplysninger om nøkkelbrukere ved utstedelse eller verifikasjon av sertifikater. I tillegg vil den videre bruken av personlige digitale signaturer kunne skape "elektroniske spor" som lett knytter signatur-/nøkkelbrukeren til en rekke transaksjoner. Hvor alvorlig svekkelsen av personvernet blir, vil naturligvis avhenge av hvilke opplysningstyper som registreres og hvilke type personvernmessig regulering som anvendes.

Til slutt kan kryptering innebære ytterligere en feilkilde/risiko som kan føre til svikt i datatilgjengelighet f eks som følge av mangelfull nøkkeladministrasjon.[12] På samme måte vil svekking av tilliten til sertifikatutsteder kunne lamme virksomheten til deler av norsk næringsliv eller offentlig forvaltning fordi tilliten til deres sertifikater blir revet bort som konsekvens av den svekkede tilliten til sertifikatutsteder.

9 Rettslige krav til kryptobruk

Følgende fremstilling er ikke ment å være uttømmende; den peker ut de mest sentrale regler som fordrer og utfordrer kryptobruk.

Innledningsvis bør det understrekes at det i dag ikke finnes noen restriksjoner på import og bruk av kryptografi i Norge, derimot finnes det krav, f eks til bruk av kryptografi av en viss styrke, på bestemte områder. Det finnes også krav til eksport av kryptoprodukter (jf nedenfor).

Rettsregler som direkte omhandler kryptobruk

Det er forholdsvis få rettsregler som *direkte* omhandler bruk av kryptografi. Slike regler finnes i hovedsak i loven om elektroniske signaturer, sikkerhetsloven, forskriftene til personopplysningsloven og eksportkontrolloven med tilhørende forskrifter.

Lov om elektroniske signaturer

Lov om elektroniske signaturer implementerer Direktiv 1999/93/EF av 13.12.1999 om en felleskapsramme for elektroniske signaturer (heretter "Direktivet om elektroniske signaturer").[13] Lovens formål er å legge til rette for sikker og effektiv bruk av elektroniske signaturer (§ 1). Den berører som sådan bruk av (asymmetrisk) kryptografi til hovedsakelig autentiseringsformål.

Loven definerer krav til såkalt avanserte elektroniske signaturer, kvalifiserte sertifikater, utstedere av slike sertifikater og til sikre signaturfremstillingssystemer (jf § 2, jf kap II og III).[14] Videre har loven bestemmelser om tilsyn med tilbydere av kvalifiserte sertifikater, samt bestemmelser om sanksjoner og erstatning (kap IV).

---

[12] Jf R Risnæs, *Skisse til retningslinjer for bruk av digital signatur og kryptering i offentlig forvaltning*, Notat til PKI-utvalget, 27.11.2000, kapittel 3.

[13] Loven ble vedtatt av Stortinget desember 2000, men er i skrivende stund ikke sanksjonert av Kongen. Frist for implementering av direktivet er 19.7.2001. Loven med tilhørende forskrift skal etter planen tre i kraft innen denne fristen. Et utkast til forskrift ble sendt på høring 14.2.2001 med høringsfrist 17.4.2001.

[14] En avansert elektronisk signatur er en elektronisk signatur som: (i) Er entydig knyttet til undertegneren; (ii) Identifiserer undertegneren; (iii) Er laget ved hjelp av midler som kun undertegneren kontrollerer; og (iv) Er knyttet til det elektroniske dokumentet slik at alle endringer av dokumentets innhold kan oppdages. En avansert elektronisk signatur som er basert på et kvalifisert sertifikat, og som er framstilt av et sikkert signaturframstillingssystem, kalles for kvalifisert elektronisk signatur.

Loven regulerer bare i liten grad andre typer av elektroniske signaturer, sertifikater og sertifikatutstedere enn de som er nevnt ovenfor. Den berører heller ikke spørsmål om kryptering av kommunikasjonsinnhold, og inneholder ikke omfattende normer for *bruk* av elektroniske signaturer. Dagens situasjon er imidlertid slik at kvalifiserte elektroniske signaturer bare kan fremstilles ved hjelp av kryptografi.

Personopplysningsloven
Lov om behandling av personopplysninger (personopplysningsloven)[15] implementerer Direktiv 95/46/EF av 24.10.1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger. Forskriften til personopplysningsloven[16] inneholder pålegg om kryptering eller annen sikring av personopplysninger "som overføres elektronisk ved hjelp av overføringsmedium utenfor den behandlingsansvarliges fysiske kontroll", dersom "konfidensialitet er nødvendig" (§ 2-11). Justisdepartementets veiledning om forskriften angir det "offentlige telenett" som eksempel på et slikt overføringsmedium. Veiledningen påpeker i tillegg at krypteringsreglene også gjelder for overføring "via private datalinjer som er utenfor det området virksomheten har sikret mot uautorisert adgang". Som eksempler på andre tilstrekkelige sikringstiltak enn kryptering angis anonymisering og/eller oppsplitting av tekst.

Det bør videre påpekes at Datatilsynets politikk hittil har vært at det skal benyttes kryptering ved ekstern dataoverføring av sensitive personopplysninger. Krypteringsstyrke skal minst tilsvare det som oppnås ved bruk av DES-algoritmen med 56-bits nøkkel.[17] Krypteringen av data skal skje fra ende-til-ende mellom to sikrede soner, dvs at kryptering/dekryptering skal skje i sikret sone.

Sikkerhetsloven
Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven)[18] inneholder regler om godkjenning og bruk av kryptosystemer for beskyttelse av sikkerhetsgradert informasjon. Loven bl a etablerer Nasjonal sikkerhetsmyndighet (NSM)[19] som hovedansvarlig for godkjenning, leveranse og eksport av slike kryptosystemer (jf § 14).

Detaljerte regler om bruk av symmetrisk kryptografi for beskyttelse av gradert informasjon er gitt i utkast til "forskrift om kryptosikkerhet". Forskriftsutkastet inneholder bl a krav om utvikling, merking, forsendelse, oppbevaring og tilintetgjøring av kryptomateriell.

Eksportkontrolloven
Lov om kontroll med eksport av strategiske varer, tjenester og teknologi (eksportkontrolloven),[20] med tilhørende forskrift,[21] regulerer eksport av kryptoprodukter fra Norge til utlandet. Eksportkontroll administreres formelt av Utenriksdepartementet (dog i samråd med NSM). Reglene følger linjer trukket opp i henhold til det såkalte Wassenaar-arrangementet.

---

15 Lov av 14. april 2000 nr 31, i kraft 1.1.2001.
16 Forskrift av 15. desember 2000.
17 DES står for Data Encryption Standard, en symmetrisk kryptoalgoritme utviklet i USA. En arvtager til DES er nylig blitt adoptert: Advanced Encryption Standard (AES).
18 Lov av 20. mars 1998 nr 10, ennå ikke i kraft.
19 NSM er synonymt med Forsvarssjefen og Forsvarets overkommando/Sikkerhetsstaben (FO/S).
20 Lov av 18. desember 1987 nr 93.
21 Forskrift av 10. januar 1989 nr 51 (sist endret 4. januar 2000 nr 2).

Wassenaar-arrangementet er et samarbeid mellom 33 land.[22] Arrangementet har som hovedformål å hindre spredning av konvensjonelle våpen og høyteknologiprodukter som kan brukes til oppbygging av offensiv militær kapasitet. Samarbeidet medfører at det utøves samordnet eksportkontroll av høyteknologiprodukter med både sivil og militær anvendelsesmulighet ("dual-use"). Visse kryptoprodukter faller inn under denne kategorien.

Eksportkontroll rammer først og fremst utførsel av kryptoprodukter som benytter (symmetriske) nøkler med lengde av mer enn 56 bits. Tillatelse (lisens) må innhentes fra Utenriksdepartementet før slike produkter kan eksporteres. Et unntak fra lisensplikt gjelder for kryptoprodukter med en nøkkellengde som ikke overstiger 64 bits og som i henhold til oppsatte kriterier kan klassifiseres som massemarkedsprodukter.

Det bør understrekes at det innenfor Wassenaar-arrangementet pågår en kontinuerlig oppdatering av kriteriene for eksportkontroll. En nærmere beskrivelse av den nåværende ordningen når det gjelder EU-medlemsland finnes i hovedpunkt 10.

Rettsregler som indirekte omhandler kryptobruk

Bruk av kryptografi vil kunne påvirkes i betydelig grad av regler som krever eller forutsetter sikring av datakonfidensialitet og -integritet.

Et sentralt eksempel er personopplysningsloven som inneholder forholdsvis omfattende krav til sikring av personopplysningers konfidensialitet, integritet og tilgjengelighet. Selv om loven ikke nevner bruk av kryptografi, er det innlysende at kryptobruk langt på vei vil kunne oppfylle disse krav. Det samme gjelder for alminnelige regler om taushetsplikt (se særlig forvaltningsloven § 13 flg[23]) samt taushetspliktsbestemmelser i sektorlovgivning (som f eks legeloven § 31[24] og telekommunikasjonsloven § 9-3[25]). Krav til kryptobruk kan dessuten være avtalebasert.

Forskjellige bestemmelser i straffeloven[26] vedrørende datakriminalitet vil også kunne bidra til beskyttelse av krypterte data og krypteringsmekanismer. Mest sentrale er bestemmelser som straffer:

- Datainbrudd (jf § 145 annet ledd) – dvs å skaffe seg tilgang til data/programutrustning ved å bryte en beskyttelse (f eks en krypteringsalgoritme);
- Beskyttelsesbrudd i forbindelse med radio- og fjernsynssignaler (jf § 262) – dvs å skaffe seg adgang til krypterte fjernsyns- eller radioprogrammer, ved bruk av såkalte piratdekodere;
- Databedrageri (jf § 270 første ledd nr 2) – dvs å manipulere, slette eller endre data/programutrustning for å oppnå økonomisk vinning;
- Dokumentfalsk (jf §§ 182 og 183; jf § 179) – dvs å forfalske et dokument, herunder datalagret

[22] Argentina, Australia, Belgia, Bulgaria, Canada, Danmark, Finland, Frankrike, Hellas, Irland, Italia, Japan, Luxembourg, Nederland, New Zealand, Norge, Polen, Portugal, Romania, Russland, Den slovakiske republikk, Spania, Storbritannia, Sveits, Sverige, Sør-Korea, Den tsjekkiske republikk, Tyrkia, Tyskland, Ukraina, Ungarn, USA og Østerrike.
[23] Lov om behandlingsmåten i forvaltningssaker 10. februar 1967.
[24] Lov om leger 13. juni 1980 nr 42.
[25] Lov om telekommunikasjon 23. juni 1995 nr 39.
[26] Almindelig borgerlig straffelov 22. mai 1902 nr 10.

informasjon, som har betydning for bevisspørsmål (f eks en digital signatur);
- Informasjonsheleri (jf § 317) – dvs å motta eller skaffe seg eller andre del i utbytte av en straffbar handling (f eks anskaffelse av ulovlig ervervede krypteringsnøkler);
- Skadeverk (jf §§ 291, 292 og 391) – dvs å skade en gjenstand, herunder datalagringsmedium (f eks harddisk), som tilhører en annen, og/eller ødelegge en informasjonssamling eller kommunikasjonsanlegg (f eks PKI) med omfattende forstyrrelse i offentlig forvaltning eller samfunnsliv som følge (jf § 151 b).

Andre relevante regler finner vi i straffelovens bestemmelser om spionasje (jf §§ 90, 91, 91 a og 93 når det gjelder spionasje som truer rikets sikkerhet; jf § 294 nr 2 og 3, § 405 a når det gjelder industrispionasje).

I tillegg finnes folkerettslige regler som indirekte bidrar til å beskytte kryptobruk. Kanskje den viktigste bestemmelse av dette slag er artikkel 8 i Den europeiske menneskerettskonvensjon (EMK) – formelt inkorporert i norsk rett.[27] Artikkel 8 fastslår retten til "respect for private life, family, home and correspondence" som grunnleggende menneskerettighet, og nedfeller vilkår for når offentlige organers inngrep i denne rettigheten kan rettferdiggjøres. Overvåking av enkeltindivider og deres kommunikasjon foretatt av statlige organer må vanligvis betraktes som i strid med artikkel 8, med mindre overvåkingen har tilstrekkelig hjemmel i nasjonal rett, er nødvendig for å oppnå et legitimt formål og proporsjonal i forhold til oppnåelsen av dette formålet.

EMK artikkel 10 om retten til ytringsfrihet kan også tenkes å kunne understøtte kryptobruk i og med at ytringsfrihet vil kunne fremmes gjennom tiltak for sikring av kommunikasjonskonfidensialitet (jf hovedpunkt 7).

Det er videre mulig at EMK artikkel 6 vil kunne påvirke myndigheters evne til å få tilgang til klartekst i etterforskningsøyemed. Vern mot selvinkriminering er ansett som en grunnleggende del av artikkel 6 første ledd (som fastslår retten til "fair hearing"). Vernet innebærer muligens at mistenkte ikke kan *tvinges* til å dekryptere informasjon de besitter.

Det er alminnelig antatt at lovlig avlytting av datakommunikasjon ikke krenker vernet mot selvkinkriminering. Mer usikkert er det om slik avlytting krenker uskyldspresumpsjonen (dvs at en person er uskyldig inntil det motsatte er bevist) etter artikkel 6 andre ledd.

10 Internasjonale rammer for norsk kryptopolitikk

Dette hovedpunkt gir en oversikt over internasjonale rammer for utvikling av norsk kryptopolitikk. Fokus legges på følgende tre problemstillinger: standardisering, eksportkontroll og myndigheters adgang til klartekst som ledd i kriminalitetsbekjempelse. I tillegg gis en kort oversikt over innholdet i retningslinjer for kryptopolikk vedtatt av OECD.

[27] Jf lov om styrking av menneskerettighetenes stilling i norsk rett 21. mai 1999 nr 30.

Standardisering

Mange ulike kryptoprodukter og -tjenester er i dag kommersielt tilgjengelige, men offisielle internasjonale standarder på området finnes ennå ikke. Når det gjelder algoritmer er den amerikanske Data Encryption Standard (DES) blitt mye brukt som de facto standard internasjonalt. Den nylig adopterte arvtageren til DES, med navnet Advanced Encryption Standard (AES), vil antagelig innta samme rolle. Samtidig er det høyst usannsynlig at vi i nær fremtid vil få kun én offisiell internasjonal standard for krypteringsalgoritmer eller andre kryptomekanismer. Dette vil muligens kunne vanskeliggjøre oppnåelse av uttalte mål om å øke kryptomekanismers interoperabilitet (funksjonelt samvirke). Det finnes imidlertid mange ulike regionale og internasjonale standardiseringsinitiativer på området.[28]

Eksportkontroll

Hovedtendensen når det gjelder eksportkontroll av kryptoprodukter er liberalisering av kontrollreglene. Tendensen er markant. Liberalisering har skutt fart spesielt etter at USA bestemte seg for betydelig å lempe på landets forholdsvis strenge kontrollregelverk. Denne oppmykingen skjedde først i januar 2000, deretter i oktober. Den innebærer bl a at alle krypteringsprodukter (dog ikke *kryptoanalytiske* produkter) fritt kan eksporteres fra USA til EU-medlemsland samt Norge, Australia, Tsjekkia, Ungarn, Japan, New Zealand, Polen og Sveits.

Når det gjelder EUs regler om eksportkontroll, er disse nedfelt i Rådets forordning (EF) nr 1334/2000 af 22.6.2000 om fællesskabsordning for kontrol med udførslen af produkter og teknologi med dobbelt anvendelse. Forordningen trådte i kraft 28.9.2000 og er, som sådan, direkte gjeldende i alle EU-medlemsstaters rettssystemer.

Forordningens regler om eksport av kryptoprodukter skiller mellom 4 kategorier av mottakerland:

- Eksport til andre EU-medlemsstater skal ikke reguleres, med unntak for overføring av produkter med *kryptoanalytiske* funksjoner og for overføring av kryptoprodukter via en medlemsstat til et tredjeland;
- Eksport til følgende ti land – USA, Japan, Canada, Sveits, Australia, New Zealand, Norge, Tsjekkia, Ungarn og Polen – som krever en forenklet "Community General Export Authorisation";
- Eksport til land som er underlagt våpenembargo – Afghanistan, Angola, Armenia, Azerbaidjan, Bosnia-Hercegovina, Burma, Burundi, Kroatia, Etiopia, Eritrea, Jugoslavia, Irak, Liberia, Libya, Rwanda, Sierra Leone, Sudan, Somalia, Tanzania, Uganda.
- Eksport til andre land som underlegges vanlige konsesjonsprosedyrer.

Forordningens regler gjelder kun for eksport av kryptoprodukter av en viss styrke, dvs når nøkkellengden overstiger 56 bits for en symmetrisk krypteringsalgoritme og 512 eller 112 bits (avhengig av metode) for en asymmetrisk algoritme.

Det finnes dessuten en rekke viktige unntak fra forordningens kontrollregler bl a for utførsel av såkalte "mass market" produkter og for utførsel av visse produkter for kopibeskyttelse, betalingsformidling, elektroniske signaturer, mobiltelefoni mv.

---

[28] Jf f eks European Electronic Signature Standardization Initiative (EESSI).

Adgang til klartekst i forbindelse med kriminalitetsbekjempelse

Flere internasjonale initiativer er blitt igangsatt i et forsøk på å koordinere og/eller harmonisere tiltak for bekjempelse av datamaskinrelatert kriminalitet. Initiativene drives langs to hovedlinjer:

- Innføring og/eller forsterkning av strafferettslige sanksjoner rettet mot ulike former for datakriminalitet;
- Forsterkning av metoder for etterforskning av kriminalitet generelt og håndhevelse av angjeldende sanksjoner.

Bruk av kryptografi er relevant i begge sammenhenger, da den kan fungere både som middel for å forebygge kriminalitet og som middel for å beskytte kriminalitet (jf hovedpunkt 7, 8 og 11).

Det er i forbindelse med innsatsen vedrørende forsterkning av etterforskningsmetoder mv at diskusjon om kryptobruk har skutt fart. Diskusjonen angår hvorvidt politiet og andre statlige sikkerhetsorganer bør kunne få kryptert informasjon i klartekst og under hvilke omstendigheter. Diskusjonen har fokusert ganske mye på hensiktsmessigheten ved systemer for obligatorisk nøkkeldeponering mv.[29] Den setter på spissen den betydelige spenningen som eksisterer her mellom interessen i kriminalitetsbekjempelse og personvern-relaterte interesser. Nærmere behandling av denne spenningen finnes i hovedpunkt 11.

Hittil gir internasjonale initiativer på området kun forholdsvis vage og diffuse føringer.

Hovedprinsippene for EUs politikk på området er fastsatt i EUs handlingsplan for bekjempelse av organisert kriminalitet (*Action plan to combat organized crime*), vedtatt 28.4.1997.[30] Av særlig relevans for kryptobruk er rekommandasjon 5 som bl a fastsetter:

> "[…] While avoiding undue restrictions, law enforcement and judicial authorities should have the means, as a complement to the specific responsibilities incumbent on the technology and service-providers, to prevent and combat the misuse of … new technologies. Attention should be paid both to illegal practices (such as the use of these technologies by criminal organizations to facilitate their activities) or illegal contents (such as child pornography or dissemination of synthetic drug recipes)".[31]

Når det gjelder G8 er en ti-punkt handlingsplan for bekjempelse av "high-tech crime" blitt vedtatt

---

[29] Litt forenklet kan obligatorisk nøkkeldeponering (engelsk: "key escrow") betegnes som et tiltak der nøkkelen som skal benyttes til å dekryptere kommunikasjon/informasjon også må oppbevares av en tredjepart. Sistnevnte vil kunne utlevere nøkkelen etter en rettslig kjennelse slik at klartekst av den krypterte kommunikasjonen/informasjonen kan fremskaffes.

[30] Jf Official Journal C 251, 15.08.1997, s 1–16. Se videre Commission of the European Communities, *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime* (COM(2000) 890 final, Brussels, 26.1.2001).

[31] Se også avsnitt 26(f) ("In the field of money-laundering and confiscation of the proceeds from crime, the following measures should be envisaged: […] (f) addressing the issue of money-laundering on the Internet and via electronic money products and requiring, in electronic payment and message systems, that the messages sent give details of the originator and the beneficiary") og avsnitt 29 ("Legislation to combat organized crime in connection with fiscal fraud should be developed in conformity with the relevant rules relating to data protection").

10.12.1997.[32] Av særlig interesse er pkt 4 ("Legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized"), pkt 5 ("Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime") og pkt 9 ("To the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence").

Det nærmeste en har kommet i utarbeidelse av internasjonale *rettslige* normer på området er innenfor Europarådets regi. Europarådet – sammen med en del land som ikke tilhører organisasjonen (først og fremst USA, Canada, Japan og Sør-Afrika) – er i gang med å ferdigstille en internasjonal konvensjon om Internett-kriminalitet ("cybercrime"). Det hittil siste offentliggjorte utkast til konvensjonsteksten er datert 22.12.2000.[33] Konvensjonsteksten ventes ferdigstilt i løpet av 2001.

Konvensjonen viderefører og utvider Europarådets rekommendasjon R (95) 13 "Concerning Problems of Criminal Procedure Law Connected with Information Technology", vedtatt 11.9.1995. Av særlig interesse i denne rekommendasjonen er anbefaling nr 14 som slår fast at en bør vurdere tiltak for å minimere de negative effektene som bruk av kryptografi medfører for etterforskning av straffesaker, uten å begrense dennes legitime bruk mer enn strengt nødvendig.[34]

Når det gjelder den planlagte konvensjonen finner vi de mest kontroversielle bestemmelsene i forhold til kryptobruk i artikkel 19(1) og 19(4). Disse angir hvilken plikt en ratifiserende stat vil ha til i nasjonal lovgivning sikre politi mv tilgang til datamaskinbaserte systemer og informasjon lagret i slike. Artikkel 19(1) lyder:

> "1. Each Party shall take such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
> a. a computer system or part of it and computer data stored therein; and
> b. computer-data storage medium in which computer data may be stored,
> in its territory."

Artikkel 19(4) lyder:

> "4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable,[35] the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2."

---

32 Tilgjengelig via <http://ue.eu.int/ejn/index.htm>.

33 Se <http://conventions.coe.int/treaty/EN/projets/cybercrime25.htm>.

34 Se også anbefaling nr 6 (om innhenting av trafikkdata i kriminaletterforskning) og anbefalinger nr 9–12 (om samarbeid med etterforskende myndigheter i forbindelse med beslag og sikring av data).

35 En fotnote til bestemmelsen påpeker at "[t]he reference to the 'reasonable' nature of the measure should be interpreted as not requiring those subject to it to collect information other than that which is already available to them, nor as requiring anyone other than those who have a direct relationship to the computer system to assist."

Det er noe uklart om artikkel 19(4) omfatter dekrypteringspåbud. Svaret er trolig ja siden "measures applied to protect the computer data" er bredt nok formulert til å romme krypteringstiltak.

Bestemmelsenes gjennomslagskraft er imidlertid kvalifisert i artikkel 19(5) som fastslår at "[t]he powers and procedures referred to in this article shall be subject to Articles 14 and 15." Artikkel 15 lyder:

> "The establishment, implementation and application of the powers and procedures provided for in this Section shall be subject to the conditions and safeguards provided for under the domestic law of each Party concerned, with due regard for the adequate protection of human rights, in particular as provided in applicable international human rights instruments, and, where applicable, the proportionality of the power or procedure to the nature and circumstances of the offence."

Til tross for initiativene nevnt over synes det i det store og hele å være lite eksplisitt støtte for innføring av systemer for obligatorisk nøkkeldeponering og lignende – i hvert fall når det gjelder nøkler som brukes til rent private/personlige formål. Få europeiske land har innført eller har planer om innføring av slike systemer. Skepsis til obligatorisk nøkkeldeponering har også vært uttrykt av EU-kommisjonen.[36]

OECDs retningslinjer for kryptopolitikk

OECD vedtok 27.3.1997 retningslinjer for kryptopolitikk (*Guidelines for Cryptography Policy*).[37] Som OECD medlemsland har Norge offisielt sluttet seg til retningslinjene. Formålet med retningslinjene er å veilede OECD medlemslandene i deres utarbeidelse av nasjonal kryptopolitikk. Selv om retningslinjene ikke er rettslige bindende, har de likevel stor politisk tyngde. De utgjør som sådan et svært viktig utgangspunkt for det videre arbeidet med utforming av en overordnet kryptopolitikk for Norge. Retningslinjene er imidlertid ikke ment å skulle anvendes i forbindelse med offentlige myndigheters beskyttelse av "informasjon som krever sikkerhet utfra nasjonale interesser".[38]

Kjernen i retningslinjene er åtte generelle prinsipper. Disse er gjengitt i vedlegg 1. Ifølge retningslinjene er alle åtte prinsipper "innbyrdes avhengige av hverandre og bør iverksettes som en helhet".[39] Prinsippene understreker bl a at regjeringer bør samarbeide for å samordne nasjonale kryptopolitikker, og at nasjonale kryptostandarder bør samsvare med internasjonale standarder. Kryptobruk bør i stor grad styres av brukergrupper selv i et åpent og konkurrende marked. I tillegg bør personvernrettigheter respekteres, noe som bør medføre visse begrensninger på rettshjemlet adang til klartekst eller kryptonøkler (jf prinsipp 6).

---

[36] Jf Commission of the European Communities, *Towards a European Framework for Digital Signatures and Encryption* (COM(97) 503 final, Brussels, 10.10.1997), del III. Merk også pkt 18 i fortalen til direktivet om elektroniske signaturer: "The storage and copying of signature-creation data could cause a threat to the legal validity of electronic signatures".

[37] Tilgjengelig via <http://www.oecd.org/dsti/sti/it/ec/index.htm>. Retningslinjene presiserer og bygger på OECDs retningslinjer for sikkerhet knyttet til informasjonssystemer (*Guidelines for the Security of Information Systems*), vedtatt 26.11.1992.

[38] Retningslinjene pkt II ("Virkefelt").

[39] Retningslinjene pkt IV ("Integrasjon").

11 Interesseavveininger i forbindelse med kryptobruk

Enkeltindividers, bedrifters og offentlige organers respektive interesser i forhold til kryptobruk vil ofte være sammenfallende og i relativ harmoni, dog kan det finnes forskjeller når gjelder hvor viktig oppnåelse av disse interessene er for hver part. De aller fleste offentlige organer vil f eks være interessert – både av prinsipielle og pragmatiske grunner – i at den enkelte borger får opprettholdt en betydelig grad av personvern. Alle parter vil dessuten være interessert i en oppblomstring av elektronisk handel.

I tillegg forsterkes interessesammenfall av visse utviklingstendenser. Det såkalte "Echelon"-systemet – et omfattende overvåkingssystem etablert av USA med hjelp av visse allierte[40] – er muligens et eksempel på en slik utvikling. Systemet er angivelig blitt brukt til å samle inn informasjon om handlinger, planer mv av private bedrifter og enkeltindivider i andre land, i tillegg til informasjon om handlinger mv utført av offentlige organer i disse land. Et overvåkingssystem som Echelon aktualiserer dermed ikke bare spørsmål om rikets sikkerhet men også personvern og nasjonale næringspolitiske spørsmål. Det viser at tiltak for beskyttelse av rikets sikkerhet (politisk suverenitet) langt på vei også bør anses som viktige ut fra personvern og næringspolitiske hensyn, og omvendt.

Det kan likevel ikke underslås at en betydelig grad av spenning foreligger mellom noen interesser. I forhold til kryptobruk oppstår spenningen i hovedsak mellom enkeltindividers personvern-relaterte interesser og offentlige organers interesser i å bekjempe kriminalitet mv.

Den grunnleggende (og mest brennbare) problemstillingen som en nasjonal kryptopolitikk må ta stilling til, gjelder hvorvidt enkeltindivider og bedrifter skal kunne sikre deres kommunikasjon/informasjon mot innsyn fra uvedkommende på bekostning av offentlige organers behov for tilgang til den samme kommunikasjon/informasjon. En beslektet problemstilling angår hvorvidt eksport av sterke kryptoprodukter og -tjenester til utlandet skal reguleres.

Disse to problemstillingene utgjør hovedtemaet for dette hovedpunktet. Den følgende diskusjon fokuserer også på spørsmål om hensiktsmessigheten av obligatorisk nøkkeldeponering da slik deponering setter problemstillingene på spissen.

Problemstillingene er vanskelige å løse fordi begge de ulike interessesett som må avveies, er viktige. Den store samfunnsmessige betydningen av kriminalitetsbekjempelse er åpenbar. Litt mindre åpenbar er det forhold at hvorvidt personvern og ytringsfrihet blir ivaretatt, er av vesentlig betydning ikke bare for enkeltindivider, men for kvaliteten av samfunnsliv generelt, særlig dets grad av pluralisme og demokrati. Dette betyr at personvern og ytringsfrihet bør anses som tungtveiende interessesett. Delvis på grunn av deres ideelle karakter blir de ofte lett tilsidesatt av (legitime) behov grunnet i mer konkrete og målbare verdier (som f eks kriminalitetsbekjempelse) – en utvikling som er blitt kalt for "det gode hensikters tyranni". Samtidig krever EMK og andre rettsregler at inngrep i personvern og ytringsfrihet skjer innenfor visse rammer.

---

[40] Jf bl a European Parliament, Scientific and Technological Options Assessment (STOA), *Development of Surveillance Technology and Risk of Abuse of Economic Information*, desember 1999 (PE 168.184/Vol 1/5/EN).

Ytterligere en faktor som kompliserer interesseavveiningene her er at kryptobruk kan bidra til bekjempelse av kriminalitet samtidig som den kan vanskeliggjøre slik bekjempelse. Kryptobruk kan bidra til å begrense kriminalitet ved å gjøre det praktisk vanskelig å krenke opphavsrettigheter, utføre industrispionasje, begå bedrageri mv. Effekten av kryptobruk i denne sammenheng er med andre ord tveegget.

Det bør også påpekes at offentlig debatt omkring disse problemstillingene lett vil kunne bli en debatt om følelser. Dette skyldes i noen grad problemstillingenes prinsippielle karakter. Det skyldes også at løsninger i stor grad vil måtte bæres frem av hypotetiske prognoser. En viktig utfordring ligger derfor i å legge til rette for at debatten også blir båret frem av argumenter med empirisk belegg.

Diskusjonen kan ikke skilles ut fra den mer generelle politiske diskusjon av hvordan en utformer informasjonssamfunnet.

La oss nå se på argumenter som tilsier at myndigheters behov for å få adgang til klartekst bør prioriteres i forhold til enkeltindividers personvern-relaterte interesser.

Det første argumentet baserer seg på antakelsen om at kriminalitet øker i omfang og alvorlighetsgrad. Det er særlig fremveksten i *organisert* kriminalitet som fremheves. Utviklingen tilsier at arbeidet med kriminalitetsbekjempelse bør prioriteres.

Nært knyttet til dette argumentet er følgende: Dersom myndighetenes muligheter for å få tilgang til klartekst under etterforskning av kriminalitet blir *vedvarende* svekket som følge av bruk av sterke krypteringsmekanismer, vil denne svekkelsen i seg selv muligens kunne oppmuntre til nye og kanskje mer dristige kriminelle handlinger.

Et tredje argument er at teknologisk innsnevring av myndighetenes avlyttingsmuligheter i forhold til datakommunikasjon, kan bety økt press fra politiet mv på å få utvidede fullmakter til å foreta avlytting, ransaking mv på andre områder – noe som muligens vil kunne svekke personvern-relaterte interesser i større grad.

Et fjerde argument fremhever at det ville være ulogisk dersom overvåking av datakommunikasjon over Internett ikke skal være mulig når andre kommunikasjonskanaler (som f eks vanlige brev og telefoni) kan (under visse vilkår) overvåkes av hensyn til rikets sikkerhet og bekjempelse av alvorlig kriminalitet.

Motargumenter er følgende.

Internett er ikke en kommunikasjonskanal som vanlige brev og telefoni; Internett er i tillegg en transaksjonskanal der stadig flere av våre daglige gjøremål utføres. Internett er samtidig et medium hvor vi på mange måter er svært sårbare overfor ulike registrerings-/overvåkingstiltak. Det er også et medium der vi føler oss usikre for rammene for våre handlinger, særlig når disse er av økonomisk betydning for oss (f eks betalingsformidling mv). Vår tillit er med andre ord satt på prøve. Det er samtidig mye som tyder på at denne tilliten er meget skjør. Elektronisk handel har ikke tatt av som forventet, delvis grunnet utstrakt frykt blant folk og bedrifter for at deres

interesser i personvern og transaksjonstrygghet ikke er godt nok beskyttet på Internettet.[41] I tillegg kommer økende skepsis til statlige systemer for sikkerhetskontroll – en skepsis fostret bl a av Lundkommisjonens avsløringer.[42]

Videre kan det argumenteres at personvern på mange samfunnsområder er på vikende front. Vi beveger oss mot et stadig mer transparent samfunn uten avlyttings-/overvåkings-/registreringsfrie soner. Denne utviklingen er bekymringsfullt med hensyn til samfunnets grad av pluralitet og demokrati.

Hvorvidt alle disse argumentene vektlegges, vil langt på vei avhenge av hvilken stilling en tar til følgende grunnleggende spørsmål:

1. Bør politiet mv i visse tilfeller kunne få adgang til klartekst i forhold til datakommunikasjon over Internett?
2. Hvis ja, hvordan bør adgangen sikres? Bør adgang kunne gis etter samme kriterier/regler som gjelder for overvåking av andre kommunikasjonskanaler?

En kan ikke ta stilling til slike spørsmål uten å ta i betraktning politiets etterforskningsmuligheter som helhet.

Når det gjelder obligatorisk nøkkeldeponering vil dette støttes av alle de fire argumentene som tilsier at myndigheters behov for å få adgang til klartekst bør prioriteres i forhold til enkeltindividers personvern-relaterte interesser. Et femte støtteargument er at obligatorisk nøkkeldeponering vil kunne lette nøkkelgjenoppretting (engelsk: "key recovery"), noe som vil kunne tjene både enkeltindivider (f eks leger som har mistet nøkler til kryptert pasientinformasjon) og bedrifter (f eks behov for å få tilgang til kryptert informasjon etter ansatte som har sluttet), i tillegg til offentlige organer.

Motargumenter kan oppsummeres slik:

- Obligatorisk nøkkeldeponering kan minske sikkerheten ved kryptobruk.
- Det kan dermed minske allmennhetens tillit til kryptobruk og dermed til bruk av kommunikasjonskanaler underlagt systemet.
- Svekkelsen medfører at det positive potensialet av IKT-anvendelse ikke kan realiseres fullt ut.
- Det er økt fare for at allmennhetens tillit svekkes fordi tilliten allerede er skjør.
- De som står bak organisert kriminalitet vil neppe bruke kommunikasjonskanaler underlagt obligatorisk nøkkeldeponering og/eller neppe innlevere sine nøkler.
- Opprettelse og vedlikehold av deponeringssystemet vil medføre store økonomiske kostnader.
- Det er fare for at obligatorisk nøkkeldeponering kommer på kant med EMK artikkel 6.
- Det er mulig å etablere systemer for nøkkelgjenoppretting uten at nøklene dermed blir gjort tilgjengelige for etterforskningsmyndigheter mv.

---

41 Jf bl a A Bhatnagar; S Misra og H Raghav Rao, "On Risk, Convenience, and Internet Shopping Behavior", *Communications of the ACM*, november 2000, bind 43, nr 11, s 98–105.

42 Jf Dokument nr 15 (1995–96), *Rapport til Stortinget fra kommisjonen som ble nedsatt av Stortinget for å granske påstander om ulovlig overvåking av norske borgere* (Lund-rapporten).

Disse argumentene er sterkest i forhold til deponering av nøkler som enkeltindivider innehar som privatpersoner og som brukes til rent personlige formål. Dette gjelder særlig argumentene angående tillit og EMK artikkel 6. Slike argumenter mister styrke i forhold til deponering av nøkler som innehas i kraft av en stilling i et offentlig organ eller en bedrift og som skal brukes i forbindelse med utøvelse av denne stillingen. Innholdet i informasjon/kommunikasjon som krypteres ved bruk av slike nøkler vil (og bør) vanligvis angå organisasjonen. Det er videre viktig å påpeke at selv om kriminelle neppe vil bruke kommunikasjonskanaler underlagt obligatorisk nøkkeldeponering, vil dette samtidig ha den positive effekten at de blir avskåret fra å kunne bruke disse (effektive) kanalene.

Når det gjelder eksportkontroll av kryptoprodukter kan det hevdes på den ene siden at full frihet til å eksportere og bruke sterke kryptoprodukter øker risiko for terroristanslag og lignende.

På den andre siden kan det hevdes at eksportkontroll kan bli stadig vanskeligere å håndheve med overgangen til en online verden. I tillegg vil eksportkontroll kunne tynge utviklingen av elektronisk handel mv. Kontrollen vil også øke risiko for at utviklingen av norsk kryptoindustri og dermed IKT-industrien generelt, svekkes. Dessuten er det fare for at et internasjonalt system for eksportkontroll, sett under ett, medfører konkurransevridninger ved at bedrifter i visse land (først og fremst USA) som er i det IKT-messige føresetet, få tilgang til nye og forbedrede kryptosystemer, mens bedrifter i andre land (f eks Norge) kun få tilgang til annenrangs teknologi. Det må samtidig medgis at en slik fare for norske bedrifter nå er blitt betydelig minsket etter liberaliseringen av USAs eksportregler overfor europeiske land.

12 Normative forslag til kryptopolitikken

Dette hovedpunkt inneholder anbefalinger om hvilke målsettinger en nasjonal kryptopolitikk bør ha. Anbefalingene er ikke ment å utgjøre en uttømmende liste over hensiktsmessige målsettinger. De er snarere fremsatt for å stimulere og strukturere diskusjonen om kryptopolitikkens mulige innhold.

Grunnleggende holdning til kryptobruk

Hovedspørsmålet som kryptopolitikken bør ta stilling til, er hvilken grunnleggende holdning politikken skal innta i forhold til kryptografi i sin alminnelighet. Den økende betydningen av kryptografi for realisering av en rekke legitime interesser tilsier at politikken i utgangspunkt bør omtale kryptografi i positive ordelag. Dette vil også være i tråd med den grunnleggende linjen i de tilsvarende politikkene for Danmark og Sverige.

Mer kontroversielt blir spørsmålet om hvilken holdning som bør inntas i forhold til bruk av sterk kryptering. Med "sterk" kryptering menes bl a at det benyttes en nøkkellengde av minst 128 bits for symmetrisk kryptering og minst 1024 bits for asymmetrisk kryptering.[43] I lys av analysen i

[43] Disse tall gjelder naturligvis kun for dagens teknologisk tilstand; de vil måtte oppjusteres kontinuerlig i takt med økningen i datamaskiners kapasitet.

hovedpunkt 11 er det gode grunner som tilsier at holdningen her også bør være positiv – noe som medfører at staten bør vise stor forsiktighet ved å innføre begrensninger på folks rett til å ta i bruk sterke kryptoprodukter og -tjenester. Den prioritering av personvern og forbrukervern som en slik holdning innebærer, vil være i tråd med grunnpolitikken for e-handel som er lagt frem i Stortingsmeldingen om elektronisk handel og forretningsdrift.[44]

Holdning til obligatorisk nøkkeldeponering

På bakgrunn av analysen i hovedpunkt 11 (jf også hovedpunkt 10) er det gode grunner som tilsier at kryptopolitikken bør ta avstand fra obligatorisk nøkkeldeponering i alle fall i visse tilfeller, først og fremst når nøkkelen innehas av privatpersoner og skal brukes til rent personlige formål.[45] Dette vil være i tråd bl a med dansk, svensk og (til en viss grad) britisk kryptopolitikk. Avstand bør også tas fra obligatorisk deponering av nøkler som kun brukes til autentiserings-/signeringsformål. Dette vil være i tråd bl a med OECDs retningslinjer (jf prinsipp 6).[46] Det er derimot gode grunner for å tillate obligatorisk nøkkeldeponering i forhold til nøkler som innehas av ansatte i en organisasjon og som skal brukes i forbindelse med organisasjonens virksomhet.[47]

Særlig om internasjonalisering

I lys av globaliseringsprosesser er det lite meningsfylt å fokusere kun på nasjonale forhold. Effektive løsninger på kryptospørsmål må i stadig større grad etableres på det internasjonale planet.

Kryptopolitikken bør fordre og legge til rette for interoperabilitet av kryptosystemer på *globalt* (ikke kun europeisk) nivå.[48] En utfordring her er å sikre at fremveksten av regionale standardiseringsinitiativer (særlig i regi av EU) ikke bremser oppnåelse av målet om økt globalt interoperabilitet.

Kryptopolitikken bør understøtte liberalisering av regler om eksportkontroll. Eksisterende regler i henhold til Wassenaar-arrangementet mv bør anvendes på romslig vis slik at eksport av sterke kryptoprodukter for sivil bruk kan finne sted forholdsvis enkelt og fritt.[49]

Import av kryptoprodukter bør forbli fri.

Særlig om nasjonal kryptoindustri

Kryptopolitikken bør bidra til en sterkere vekst av norsk kryptoindustri og dermed norsk IKT-industri generelt.[50] Norsk kryptoindustri er i dag liten, men har et stort utviklingspotensial både

---

[44] Jf St meld nr 41 (1998–99), særlig avsnitt 4.5 ("For å inngi tillit og tiltro må forbrukerrettigheter, personvern og andre hensyn ivaretas på den elektroniske markedsplassen: Det skal arbeides for aktiv ivaretakelse av sosiale og samfunnsmessige hensyn som sikkerhet, personvern og forbrukervern … og håndtere dette slik at det kan bli et konkurransefortrinn for norske aktører").

[45] Jf også NOU 2001:10, s 149 (jf også s 140).

[46] Jf også NOU 2001:10, s 149.

[47] Jf også NOU 2001:10, avsnitt 11.3.8 og 11.6.2.

[48] Jf også OECDs retningslinjer prinsipp 4, gjengitt i vedlegg 1.

[49] Dette vil være i tråd med svensk og dansk politikk på området, jf vedlegg 2 og 3.

[50] Jf også St meld nr 41 (1998-99) der det vektlegges behovet for rettslige og økonomiske rammebetingelser for elektronisk handel som ivaretar norske bedrifters konkurranseevne nasjonalt og internasjonalt.

nasjonalt og internasjonalt, særlig når det gjelder utvikling av nisjeprodukter. Det er blitt påpekt at samspillet mellom staten og norsk kryptoindustri hittil har vært altfor passivt; den ene har ventet på initiativer fra den andre med det resultat at en tilfredsstillende utvikling av norske kryptoprodukter til gjensidig nytte er uteblitt.[51] En av kryptopolitikkens sentrale målsettinger bør være fornyelse av dette samspillet for å stimulere fremveksten av en konkurransedyktig norsk kryptoindustri.

Det bør samtidig understrekkes at staten ikke kan opptre som *garantist* for utvikling av en slik industri.[52]

Særlig om elektroniske signaturer og PKI

Her er det naturlig at det videre arbeidet med utforming av en overordnet kryptopolitikk legger til grunn lov om elektroniske signaturer samt forslaget til en politikk for bruk av elektroniske signaturer som er fremmet i NOU 2001:10 (jf særlig kapittel 11).

Særlig om arbeidsbyrde for brukergrupper

Kryptopolitikken bør være slik at dens implementering innebærer minst mulig ekstra arbeid for brukergrupper.[53]

Særlig om administrativ saksbehandling

Kryptopolitikken bør ikke bryte med de alminnelige regler for administrativ saksbehandling som følger av forvaltningsloven, men snarere legge til rette for at reglenes målsettinger kan oppnås ved overgangen til elektronisk saksbehandlingen.[54]

13 Momenter som bør drøftes i det videre arbeidet med utforming av kryptopolitikken

Dette hovedpunktet lister opp noen problemstillinger som det videre arbeidet med kryptopolitikkens utforming bør ta stilling til. I motsetning til problemstillingene drøftet i hovedpunkt 11 er problemstillingene her av mer teknisk enn verdimessig karakter. Listen er ikke ment å være uttømmende.

Samordning

Hvor går grensene for samordning og harmonisering i forhold til en kryptopolitikk? Er det fare for gjentagelse av de problemer som oppsto med forsøket på å utarbeide og få gjennomslag for et

---

[51] Jf Rådet for IT-sikkerhet, *Sluttrapport fra utvalg for vurdering av behov for kryptopolitikk*, 10.11.1997, s 40.

[52] Jf også St meld nr 41 (1998-99).

[53] Jf også St meld nr 41 (1998-99) der det fastslås som mål at utvikling av elektronisk infrastruktur skal forenkle brukergruppers arbeidsoppgaver.

[54] Dette er i tråd bl a med anbefalingene fremsatt i NOU 2001:10 (jf særlig kapittel 11).

samordnet regelverk for informasjonssikkerhet tidlig på 90-tallet? Bør kryptopolitikken i lys av slike problemer skille klart mellom kryptobruk i forsvarssektor og bruk i sivil sektor?

Bør det videre skilles klart mellom målsettinger/retningslinjer for bruk av kryptering for å skjerme innhold for innsyn fra uvedkommende og målsettinger/retningslinjer for bruk av elektroniske signaturer?[55] Bør politikken med andre ord skille mellom tiltak for sikring av konfidensialitet og tiltak for sikring av integritet, autentisering og ikke-benekting? Bør politikken dessuten avgrense mot behandling av spørsmål vedrørende elektroniske signaturer?

Anskaffelse

Bør kryptopolitikken ta stilling til hvordan verktøy/system for kryptering og digitale signaturer bør anskaffes?

Normtyper

Bør kryptopolitikken ta stilling til hvilken typer normer som bør styre utvikling og bruk av kryptoprodukter og -tjenester? Er det videre et behov for å innføre særskilt kryptoregulering, særlig av kryptobruk til sikring av konfidensialitet?

Normer kan favne alt fra såkalte "myke regler" (f eks anbefalinger, adferdskodekser utarbeidet av brukergrupper selv) til lovhjemlet pålegg fra myndighetene.

Det er antagelig hensiktsmessig at kryptopolitikken her legge til grunn samme utgangspunkt som finnes i Stortingsmeldingen om elektronisk handel og forretningsdrift.[56] Meldingen fastslår følgende grunnprinsipper for regulering av e-handel:

- "Elektronisk handel vil bli drevet frem av markedet i form av produkter og tjenester som bedrifter og forbrukere vil etterspørre;[57]
- Der myndighetene griper inn, må dette skje i full åpenhet og dialog med de berørte parter;
- Reguleringene må være nøytrale i forhold til teknologi og ikke være bundet til bestemte teknologiske løsninger".

Samtidig kan regulering være hensiktsmessig for å fremskynde tillitsbygging i forhold til ny teknologi (som f eks elektroniske signaturer). Dessuten kan bruk av en mindre teknologinøytral regulering rettferdiggjøres ved at den gir større grad av forutberegnelighet (dog på bekostning av reglenes tilpasningsmulighet).

Dersom bruk av kryptografi som sikkerhetsmekanisme skal fungere etter hensikten er det påkrevet at reglene som utløser kryptobruk ikke er mer komplekse enn at de saksbehandlene som berøres kan forholde seg til dem i sin daglige virke (jf hovedpunkt 12). For eksempel vil det være unødig kompliserende om sikkerhetskrav etter personvernlovgivningen og taushetspliktsreglene

---

[55] En slik sondring er foreslått bl a av Riisnæs. Jf *Skisse til retningslinjer for bruk av digital signatur og kryptering i offentlig forvaltning*, Notat til PKI-utvalget, 27.11.2000. Samme linje tas i NOU 2001:10 (jf særlig kapittel 11) og dansk kryptopolitikk (jf vedlegg 3).

[56] St meld nr 41 (1998–99).

[57] Jf også OECDs retningslinjer prinsipp 3 (gjengitt i vedlegg 1).

etter forvaltningslovgivningen gir anvisning på ulike løsninger på tilfeller som ligner hverandre.[58] Usikkerhet med hensyn til bruksområde kan i seg selv utgjøre en sikkerhetstrussel.

[58] Jf Riisnæs, *Skisse til retningslinjer for bruk av digital signatur og kryptering i offentlig forvaltning*, Notat til PKI-utvalget, 27.11.2000, avsnitt 3.2; NOU 2001:10, avsnitt 11.3.2 og 11.7.

Litteratur[59]

- Andrews, S: "Who Holds the Key? A Comparative Study of US and European Encryption Policies", *Journal of Information, Law & Technology*, 2000, nr 2, <http://elj.warwick.ac.uk/jilt/00-2/andrews.html>.
- Berg, J P: "Overvåking av kryptert datakommunikasjon på internettet", i R Punsvik (red), *Elektronisk handel – rettslige aspekter* (Tano Aschehoug, 1997), s 76–87.
- Bhatnagar, A; Misra, S og Raghav Rao, H: "On Risk, Convenience, and Internet Shopping Behavior", *Communications of the ACM*, november 2000, bind 43, nr 11, s 98–105.
- Commission of the European Communities: *Towards a European Framework for Digital Signatures and Encryption* (COM(97) 503 final, Brussels, 10.10.1997).
- Commission of the European Communities: *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime* (COM(2000) 890 final, Brussels, 26.1.2001).
- Diffie, W og Landau, S: *Privacy on the Line. The Politics of Wiretapping and Encryption* (MIT Press, 1998).
- Dokument nr 15 (1995–96), *Rapport til Stortinget fra kommisjonen som ble nedsatt av Stortinget for å granske påstander om ulovlig overvåking av norske borgere* (Lund-rapporten).
- European Union: *Action Plan to Combat Organised Crime* (Official Journal C 251, 15.08.1997, s 1–16).
- European Parliament, Scientific and Technological Options Assessment (STOA): *Development of Surveillance Technology and Risk of Abuse of Economic Information*, desember 1999 (PE 168.184/Vol 1/5/EN).
- Froomkin, A M: "The Metaphor is the Key: Cryptography, The Clipper Chip, and the Constitution", *University of Pennsylvania Law Review*, 1995, bind 143, s 709–897.
- Koops, B-J: *Crypto Law Survey*, versjon 18.4, januar 2001, <http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm>.
- NOU 2001:10, *Uten penn og blekk – Bruk av digitale signaturer i elektronisk samhandling med og i forvaltningen*.
- OECD: *Guidelines for Cryptography Policy* (OECD, 1997); samt norsk oversettelse av retningslinjene – jf Nærings- og handelsdepartementet: *Kryptopolitikk. Retningslinjer og problemstillinger* (NHD, 1998), <http://odin.dep.no/nhd/norsk/regelverk/prinsipputtaleser/024005-990135/index-dok000-b-n-a.html>.
- OECD: *Revised Inventory of Controls on Cryptography Techniques*, 8.2.2001 (DSTI/ICCP/REG(2000)5REV1).
- Riisnæs, R: *Skisse til retningslinjer for bruk av digital signatur og kryptering i offentlig forvaltning*, Notat til PKI-utvalget, 27.11.2000, tilgjengelig ved <http://www.statskonsult.no/prosjekt/pki/index.htm>.
- Rådet for IT-sikkerhet: *Sluttrapport fra utvalg for vurdering av behov for kryptopolitikk*, 10.11.1997.
- Spiegel Online: "Unknackbare Verschlüsselung: Wirbel um die Krypto-Revolution", mars

[59] Noen arbeider er ikke direkte referert i rapporten.

2001, <http://www.spiegel.de/netzwelt/technologie/0,1518,120312,00.html>.
- St meld nr 41 (1998–99), *Om elektronisk handel og forretningsdrift*.
- Storbritannia, Department of Trade and Industry: *Consultation on EC Directive 1999/93/EC of the European Parliament and Council on a Community Framework for Electronic Signatures*, March 2001.
- Sverige: Regeringens skrivelse 1998/99:116 om kryptografi.
- ØKOKRIM: *Økt innsats for bekjempelse av datakriminalitet. Forslag om etablering av Politiets datakrimsenter, ØKOKRIM*, 18.12.2000.

Vedlegg 1: OECDs retningslinjer for kryptopolitikk

OECD vedtok 27.3.1997 retningslinjer for kryptopolitikk (*Guidelines for Cryptography Policy*). Retningslinjene nedfeller følgende generelle prinsipper for OECD medlemslandenes utvikling av nasjonal kryptopolitikk [utdrag]:

> "1. *Tillit til kryptometoder*
> Kryptometoder bør være pålitelige for å skape tillit til bruk av informasjons- og kommunikasjonssystemer. […]
>
> 2. *Valg av kryptometoder*
> Brukerne bør ha rett til å kunne velge hvilken som helst kryptometode, innen rammen av gjeldende rett. […]
>
> 3. *Markedsdrevet utvikling av kryptometoder*
> Kryptometoder bør utvikles for å dekke personers, næringslivets og offentlige myndigheters behov, etterspørsel og ansvar.
>
> Utviklingen og tilveiebringelsen av kryptometoder bør bestemmes av markedet i et åpent og konkurrerende miljø. […] Utviklingen av internasjonale tekniske standarder, kriterier og protokoller knyttet til kryptometoder bør også drives fram av markedet. […]
>
> 4. *Standarder for kryptometoder*
> Tekniske standarder, kriterier og protokoller for kryptometoder bør utvikles og gjøres kjent på nasjonalt og internasjonalt plan.
>
> […] Eventuelle nasjonale standarder for kryptometoder bør være i samsvar med internasjonale standarder for å lette global interoperabilitet, flyttbarhet og mobilitet. […]
>
> 5. *Sikring av personvern og persondata*
> Enkeltpersoners grunnleggende rett til beskyttelse mot inngrep i personvernet, herunder hemmeligholdelse av kommunikasjonsinnhold og sikring av persondata, bør respekteres i nasjonal kryptopolitikk og ved iverksetting og bruk av kryptometoder. […]
>
> 6. *Rettshjemlet adgang*
> Nasjonal kryptopolitikk kan tillate rettshjemlet adgang til klartekst eller kryptonøkler for krypterte data. Slik politikk må i størst mulig grad respektere de øvrige prinsippene som inngår i Retningslinjene.
>
> […] Prosessen som fører til at rettshjemlet adgang oppnås, bør registreres slik at avdekkingen av kryptonøkler eller data kan revideres eller gjennomgås i samsvar med nasjonal lovgivning. […] Prosesser for rettshjemlet adgang til kryptonøkler må anerkjenne skillet mellom nøkler som brukes til å sikre konfidensialitet, og nøkler som bare brukes til andre formål. En kryptonøkkel som bare *sørger* for identitet eller integritet (til forskjell fra en nøkkel som bare *verifiserer* identitet eller integritet) bør ikke gjøres tilgjengelig

uten samtykke fra den personen eller virksomheten som er i lovlig besittelse av nøkkelen.

7. *Ansvar*
Uansett om det er fastslått ved avtale eller lovgivning, bør ansvaret som påhviler personer eller virksomheter som tilbyr kryptotjenester eller innehar eller har adgang til kryptonøkler, være angitt på en klar måte. […]

8. *Internasjonalt samarbeid*
Regjeringene bør samarbeide for å samordne kryptopolitikker. Som et ledd i slike bestrebelser bør regjeringer fjerne utilbørlige handelshindringer eller unngå at kryptopolitikk i seg selv skaper slike hindringer.

[…] For dette formålet bør Retningslinjene anvendes ved utforming av nasjonal politikk. Dersom det er utviklet nasjonale nøkkelforvaltningssystemer, må disse, dersom det er formålstjenlig, muliggjør internasjonal bruk av krypto. […] Ingen regjering bør hindre den frie flyten av krypterte data som strømmer gjennom dens jurisdikjson utelukkende med begrunnelse i kryptopolitikk. For å fremme internasjonal handel bør regjeringene unngå å utvikle kryptopolitikk og –rutiner som skaper utilbørlige hindringer for global elektronisk handel. Regjeringene bør unngå å skape utilbørlige hindringer for kryptometoders internasjonale tilgjengelighet."

Retningslinjene kap IV påpeker at prinsippene "er innbyrdes avhengige av hverandre og bør iverksettes som en helhet …" Videre bør "[i]ngen av prinsippene iverksettes isolert fra de øvrige".

Vedlegg 2: Hovedtrekk i Sveriges kryptopolitikk

Overordnet kryptopolitikk

Sverige har utarbeidet en overordnet nasjonal kryptopolitikk som i hovedsak er formalisert i Regeringens skrivelse 1998/99:116 om kryptografi. Politikken sammenfattes på følgende vis:

- "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.

Tilblivelsen og oppfølgingen av den svenske regjeringens skriv om kryptografi er i Sverige i stor grad ansett å være en suksess.[60] Alle departementer deltok i utarbeidelsesprosessen og har sluttet seg til politikken. Skrivet har skapt lite debatt i etterkant av utferdigelsen.

Skrivet sier lite om rollefordelingen mellom privat og offentlig sektor. Dette er fordi et utgangspunkt for svensk politikk de siste 20 årene har vært at hovedansvar for å utvikle og ta i bruk sikkerhetssystemer ligger hos den enkelte.

Hovedlinjene i skrivet er videreført i Regeringens proposition 1999/2000:86, *Et informationssamhälle för alla*. Propositionen uttrykker den svenske regjeringens generelle informasjonspolitikk for perioden 2000–2004. Kryptobruk omtales i svært positive ordelag:

- "Regeringen välkomnar en bred användning av kryptografi. Det ökar tilliten till kommunikationssystemen och stärker informationsfriheten. Det är därför också viktigt att användarna får god tillgång till säkra kryptosystem, svenske eller importerade, så att de själva kan välja teknik" (avsnitt 5.3.4, s 49).
- "Betryggande säkerhetsfunktioner baserade på krypteringsteknik och elektroniska signaturer måste uvecklas och göra allmänt tillgängliga i sammhället så att förutsättningar skapas för ökad elektronisk kommunikasjon och elektronisk handel" (avsnitt 5.3.3, s 47).

Eksportkontroll

Svensk regelverk om eksportkontroll av kryptoprodukter følger Rådets forordning (EF) nr

[60] Ifølge muntlige opplysninger gitt den 15.2.2001 av Anne-Marie Eklund Löwinder (IT-kommissionen) og Göran Axelsson (Utrikesdepartementet) til Lee A Bygrave.

1334/2000. Ansvaret for anvendelsen av regelverket ligger hos Inspektionen för strategiska produkter.

I Regeringens skrivelse 1999/2000:110 bekreftes holdningen om eksportkontroll av krypto som er nedfelt i skrivelse 1998/99:116. Regjeringen erkjenner et sikkerhetspolitisk behov for å begrense eksport til visse land, men uttaler bl a også at Sverige "verkar … för en friare handel med kryptoprodukter med beaktande av de säkerhetspolitiska hänsynen." Regjeringen uttrykker som målsetting "att den begränsade exportkontroll av kryptoteknik som är motiverad skall upprätthållas på ett så snabbt och smidigt sätt att den i jämförelse med andra länders kontrollprocedurer inte skall medföra en konkurransenackdel för svensk industri, utan helst ge en konkurransefördel." Samtidig erkjenner regjeringen at en "internationell samsyn måste dock uppnås vad gäller bl a. EU-ländernas kontroll mot tredje land".

Elektroniske signaturer

Direktivet om elektroniske signaturer er implementert i svensk rett ved lag (2000:862) om kvalificerade elektroniska signaturer, i kraft 1.1.2001.

Nøkkeldeponering

Det har vært forholdsvis lite debatt om spørsmål vedrørende obligatorisk nøkkeldeponering. Innføring av et system for obligatorisk nøkkeldeponering synes å være utelukket – i hvertfall i nær fremtid.

Andre relevante initiativer

Det svenske försvarsdepartementet har opprettet en arbeidsgruppe "för skydd mot informationsoperationer" (tidligere "arbetsgruppen för skydd mot informationskrigföring"). Arbeidsgruppen skal utrede trusler og risiki knyttet til såkalte "informationsoperationer" (dvs "samlade och samordnade åtgärder i fred, kris och krig till stöd för politiska eller militära mål genom att påverka eller utnyttja motståndares eller annan utländsk aktörs information och informationssystem", jf Regeringens protokoll av 21.6.2000). Arbeidsgruppen skal avslutte sin virksomhet 31.12.2001.

I tillegg er en offisiell utredning om visse sårbarhetsspørsmål under ferdigstillelse. Utredningen, som skrives av Åke Pettersson, skal foreslå prinsipper for å få til en mer helhetlig planleggingsstrategi "för civilt försvar och beredskapen mot svåra påfrestningar på samhället i fred" (jf Direktiv 1999:63). Det forventes at utredningen vil berøre kryptospørsmål.

Vedlegg 3 – Hovedtrekk i Danmarks kryptopolitikk

Overordnet kryptopolitikk

Den danske regjeringens holdning til kryptospørsmål er sammenfattet i et brev av 7.4.2000 fra Erhvervsministeren, Forsvarsministeren, Justitsministeren og Forskningsministeren til det danske IT-sikkerhedsrådet. I følge brevet skal Danmarks fremtidige kryptopolitikk basere seg på følgende hovedlinjer:

- "Den nuværende danske krypteringspolitik, som baserer sig på fri anvendelse og fri import af kryptering, skal fastholdes, og Danmark vil aktivt fremme brug af stærk kryptering til støtte for sikker elektronisk kommunikation og handel.
- Med henblik på at fremme IT-udviklingen, skal der iværksættes initiativer til udbredelsen af stærk kryptering i Danmark. Dette bør ske gennem initiativer, der sigter på at skabe øget opmærksomhed i befolkningen omkring nødvendigheden af at sikre kommunikationen ved hjælp af kryptering og på, at det offentlige gennem sin efterspørgsel fremmer opbygningen af den nødvendige infrastruktur og udbredelsen af standardiserede krypteringsprodukter.
- Danmark bør ikke gennemføre reguleringer med nøgledeponering. Vi bør dog fortsat følge den internationale udvikling på området og samtidig være opmærksom på behovet for, at politiet i overensstemmelse med retsplejelovens retssikkerhedsgarantier fortsat kan gøre brug af eksisterende efterforskningsmidler til forebyggelse og opklaring af kriminalitet.
- Der arbejdes for størst mulig liberalisering af eksportkontrollen med varer og teknologi med dobbelt anvendelse (dual-use goods), i EU og Wassenaar, dog med behørig hensyntagen til behovet for fortsat at kunne kontrollere spredningen af meget sensitive produkter til sensitive slutbrugere.
- Det er hensigten med de ovenstående hovedlinier at præcisere, at regeringen ønsker at fremme IT-udviklingen mest muligt, og at det er en væsentlig forudsætning, at der er tillid til sikkerheden i anvendelsen af elektronisk kommunikation. Regeringen vil fortsat nøje følge den internationale udvikling på krypteringsområdet."

Som brevet antyder er både *anvendelse* og *import* av kryptoprodukter i Danmark ikke blitt underkastet særskilt lovregulering.

Eksportkontroll

Det danske regelverket for eksportkontroll av kryptoprodukter følger EU Rådets forordning (EF) nr 1334/2000. Hovedansvaret for implementering av regelverket ligger hos Erhvervsfremmestyrelsen under Erhvervsministeriet.

Elektroniske signaturer

Direktivet om elektroniske signaturer er implementert i dansk rett ved lov nr 417 av 31.5.2000 om elektroniske signaturer, i kraft 1.10.2000.

Nøkkeldeponering

Innføring av et system for obligatorisk nøkkeldeponering synes å være utelukket – i hvertfall i nær fremtid.

Andre relevante initiativer

Regjeringen har opprettet en interdepartemental "Følgegruppe om Kryptering". Gruppen skal sørge for statlig implementering og koordinering av dansk kryptopolitikk, samt holde øye med den internasjonale utviklingen. Problemstillinger knyttet hovedsakelig kun til bruk av elektroniske signaturer faller utenfor gruppens arbeidsområde. En tett kobling av politikk om kryptobruk til konfidensialitetssikringsformål med politikk vedrørende bruk av elektroniske signaturer er hittil blitt ansett av regjeringen som uhensiktsmessig.

Vedlegg 4 – Hovedtrekk i Storbritannias kryptopolitikk

Overordnet kryptopolitikk

Det finnes ingen overordnet nasjonal kryptopolitikk for Storbritannia som tilsvarer den svenske regjeringens skrivelse 1998/99:116 om kryptografi.

Eksportkontroll

Hovedansvaret for eksport kontroll ligger hos Export Control and Non-Proliferation Directorate innen Department of Trade and Industry. Det relevante regelverket finnes i The Dual-Use Items (Export Control) Regulations 2000. Forskriftene følger Rådets forordning (EF) nr 1334/2000. Eksportbegrepet defineres i forskriftene til å omfatte elektronisk overføring av programvarer mv i tillegg til overføring av fysiske produkter.

Importkontroll

Import av kryptoprodukter er ikke regulert.

Elektroniske signaturer

Deler av direktivet om elektroniske signaturer er implementert ved The Electronic Communications Act 2000, Del II. Et forslag til implementering av direktivets øvrige deler ble sendt ut på høring i mars 2001 med frist for tilbakemeldinger medio juni 2001.[61]

Nøkkeldeponering

Et eksplisitt forbud mot innføring av systemer for obligatorisk nøkkeldeponering er nedfelt i The Electronic Communications Act 2000 § 14(1). Men § 14(2) av loven åpner for at en regjeringsbeslutning kan kreve nøkkeldeponering i visse tilfeller:

> "(a) a requirement to deposit a key for electronic data with the intended recipient of electronic communications comprising the data; or
> (b) a requirement for arrangements to be made, in cases where a key for data is not deposited with another person, which otherwise secure that the loss of a key, or its becoming unusable, does not have the effect that the information contained in a record kept in pursuance of any provision made by or under any enactment or subordinate legislation becomes inaccessible or incapable of being put into an intelligible form".

En slik beslutning er ennå ikke truffet.

---

[61] Jf Department of Trade and Industry, *Consultation on EC Directive 1999/93/EC of the European Parliament and Council on a Community Framework for Electronic Signatures*, March 2001.

Andre relevante initiativer

Selvregulering
Del I av The Electronic Communications Act 2000 fastsetter opprettelsen av et register over godkjente tilbydere av kryptotjenester (for konfidensialitetssikring og/eller sikring av autentisitet mv). Regjeringen har imidlertid valgt ikke å implementere dette registreringssystemet. Den håper i stedet at industrien skal etablere selv-regulatoriske registreringssystemer. Det er allerede etablert et slikt system, det såkalte "tScheme".[62] Dersom regjeringen ikke implementerer registreringssystemet som er hjemlet i loven innen en fem-års periode, vil de angjeldende bestemmelsene i loven bli opphevet (§ 16(4)).

Etterforskning av kriminalitet
Del III av Regulation of Investigatory Powers Act 2000 gir politiet hjemmel til å innhente informasjon som kan inneholde (de)krypteringsnøkler. Bestemmelsene angår kryptert informasjon som på lovlig vis har kommet i politiets besittelse etter ransaking. Personer som politiet tror er i besittelse av dekrypteringsnøkkelen for denne informasjonen, vil som utgangspunkt kunne pålegges å oppgi informasjonen i klartekst, men ikke nøkkelen. Loven åpner imidlertid muligheten for at nøkkelen også vil måtte frigis under spesielle forhold:

> "(a) that there are special circumstances of the case which mean that the purposes for which it was believed necessary to impose the requirement in question would be defeated, in whole or in part, if the direction were not given; and
> (b) that the giving of the direction is proportionate to what is sought to be achieved by prohibiting any compliance with the requirement in question otherwise than by disclosure of the key itself" (§ 51(4)).

Bestemmelsen gjelder ikke for krypteringsnøkler som kun skal brukes for generering av elektroniske signaturer og kun er blitt brukt til dette formålet (§ 49(9)).

Under forberedelsene til loven ble det uttrykt bekymring for at en person kunne bli tiltalt for ikke å gi fra seg en nøkkel selv når vedkommende ikke lenger hadde nøkkelen eller hadde glemt den. En slik tiltale ble ansett som i strid med EMK artikkel 6 (retten til "fair hearing"). På grunn av bekymringen stipulerer loven at

> "a person shall be taken to have shown that he was not in possession of a key to protected information at a particular time if sufficient evidence of that fact is adduced to raise an issue with respect to it, and
> the contrary is not proved beyond a reasonable doubt." (§ 53(3)).

Dessuten stipuleres det at enhver anvendelse eller lagring av nøkkelen må være nødvendig og proporsjonal i forhold til anvendelses-/lagringsformålet (§ 55). Disse bestemmelsene i loven er ennå ikke trådt i kraft da regjeringen ønsker å foreta en videre høringsrunde om visse aspekter ved dem.

---

[62] Jf <www.tscheme.org>.

Vedlegg 5 – Oversikt over norske regler som har betydning for etterforskning av kriminalitet

Her gis en kort gjennomgang av norske regler vedrørende politiets evne til å etterforske kriminalitet, med henblikk på tilfeller der kommunikasjon og lagrede data i det kriminelle miljøet er kryptert. Fokus rettes mot reglenes begrensninger.

Mistenkte/siktede har i straffesaker ingen plikt til å samarbeide med politiet eller retten (jf bl a straffeprosessloven §§ 90 og 92 annet ledd[63]). Dette betyr at mistenkte/siktede i forhold til politiet/påtalemyndighet ikke er forpliktet til å dekryptere data eller oppgi en krypteringsalgoritme/-nøkkel. Dersom krypteringsalgoritmen/-nøkkelen er kjent av en annen person, kan retten pålegge vedkommende å utlevere den etter strpl § 210 (såframt personen plikter å vitne i saken). Algoritmen/nøkkelen eller klartekst vil muligens også kunne fremskaffes gjennom avlytting av telekommunikasjon, og ellers ved bruk av ekstraordinære etterforskningsmetoder som f eks bruk av informanter som befinner seg i mistenktes miljø, infiltrasjon i miljøet mv.

Bruk av ekstraordinære etterforskningsmetoder er i hovedsak ikke direkte lovregulert. Dette kan skape vanskeligheter i vurdering av hvorvidt visse metoder er lovlige. Et eksempel her gjelder hemmelig online "ransaking" som i visse tilfeller kunne gi politiet tilgang til informasjon før den blir kryptert. Det er usikkert om slik ransaking har tilstrekkelig hjemmel i henhold til straffeprosessloven (jf § 192).

Avlytting av telekommunikasjon er derimot direkte lovregulert. Avlytting er tillatt i forbindelse med etterforskning av grov kriminalitet og i saker vedrørende rikets sikkerhet (jf strpl § 216 a). I begge tilfeller kreves det rettslig kjennelse før avlyttingen kan finne sted. Verdien av avlyttingen vil selvfølgelig forringes når innholdet i kommunikasjonen er kryptert og politiet ikke har tilgang til krypteringsalgoritmen/-nøkkel.

Dette problemet vil kunne oppveies i noen grad ved at politiet får tilgang til opplysninger om hvem som kommuniserer, samt sted, tidspunkt og varighet for kommunikasjonen. Slike opplysninger er vanligvis registrert og lagret hos teleoperatører. Opplysningene er i utgangspunktet underlagt taushetsplikt etter telekommunikasjonsloven (jf § 9-3 første ledd), men taushetsplikten "er ikke til hinder for at det gis opplysninger til påtalemyndigheten eller politiet om en abonnents navn, adresse, telefonnummer eller datakommunikasjonsadresse" (jf § 9-3 tredje ledd). Anmodning om slike opplysninger skal etterkommes "med mindre særlige forhold gjør det utilrådelig" (jf § 9-3 fjerde ledd).

Høyesterett har i en kjennelse av 20.12.1999 (jf Rt 1999 s 1944) under dissens (4–1) fastslått at utlevering av slike opplysninger i utgangspunktet verken er i strid med EMK artikkel 8 eller andre personvernregler. Rettens flertall uttalte dog at personvernhensyn tilsier en innskrenkende tolkning av § 9-3 tredje ledd slik at det må stilles krav til hvilke opplysninger politiet må gi teleoperatørene for å få de opplysningene bestemmelsen nevner. Bestemmelsen kan mao ikke

[63] Lov om rettergangsmåten i straffesaker 22. mai 1981 nr 25 – heretter "strpl".

brukes av politiet til å få tak i opplysninger (f eks trafikkdata) som ellers er taushetsbelagte etter § 9-3 første ledd. I den aktuelle sak fastslo rettens flertall at teleoperatøren måtte oppgi abonnentens navn når politiet oppga et dynamisk IP-nummer som abonnenten angivelig brukte samt tidspunkt for abonnentens nett-tilkobling.

Etter anmodning fra politiet, påtalemyndigheten eller retten kan Post- og Teletilsynet (PT) også oppheve taushetsplikten for andre opplysninger som er taushetsbelagte etter § 9-3 første ledd (jf strpl § 118 første ledd). Teleoperatørene kan til tross for PTs fritak nekte å gi fra seg opplysningene til politiet. Alternativt kan PT nekte å oppheve taushetsplikten. Da kan politiet kreve en rettslig kjennelse. Når kjennelsen foreligger, er operatøren pliktig til å utlevere opplysningene som politiet ber om.

En del problemer knytter seg til teleoperatørenes registrering av abonnent- og trafikkdata. Problemene kan vanskeliggjøre politiets evne til å oppspore identiteten til gjerningspersonen. Enkelte av disse problemene er snarere av praktisk enn rettslig art (f eks dårlige rutiner for å kontrollere at oppgitte abonnentopplysninger er korrekte). Når det gjelder rettslige problemer, er følgende av særlig interesse:

- Hjemmelen som PT har til å pålegge registrering av abonnentdata synes å være uklar og muligens utilstrekkelig hvis registreringspålegg skjer av hensyn til etterforskning av kriminelle handlinger (jf teleforskriften § 2-7; jf telekommunikasjonsloven § 4-6 andre avsnitt). Problemet har dukket opp spesielt i forbindelse med at tilbydere av mobiltelefontjenester selger forhåndsbetalte SIM-kort med uregistrert abonnement. PT har bedt Samferdselsdepartementet om en avklaring av rettstilstanden på dette punktet (jf brev av 28.5.1999; ref 98/15302 411.2).
- Det er usikkert om telekommunikasjonsloven omfatter tilbydere av teletjenester (f eks universiteter og skoler) som ikke tilbyr tjenestene "i næringsøyemed" (jf § 1-6 (d)).
- Det er videre usikkert hvorvidt telekommunikasjonsloven omfatter visse andre typer tjenesteleverandører, f eks innehaveren av en såkalt Internett-café eller et web-hotell.
- Hvor lenge teletjenesteleverandører bør oppbevare logger med trafikkdata, er omstridt. Datatilsynet har fastsatt tre måneder som maksimum lagringstid i henhold til sine konsesjonsvilkår for behandling av personopplysninger i telesektoren (jf personopplysningsforskriften § 7-1). ØKOKRIM mener at dette ikke er tilstrekkelig for etterforskningsformål, og vil ha ett års lagringstid.