Norsk kryptopolitikk

Forsvarsdepartementet
Justis- og beredskapsdepartementet

Forord

Norge er blant de fremste landene i verden til å ta i bruk ny teknologi, og digitalisering er en avgjørende del av vår verdiskaping og vekst. Bruken av internett og den raske utviklingen innen informasjons- og kommunikasjonsteknologi (IKT), gir helt nye muligheter for forsvarssektoren og det sivile samfunn. Digitaliseringen bidrar til å effektivisere mange av samfunnets oppgaver. Produkter og tjenester vi bare kunne drømme om for noen få siden, er nå en realitet. Med den økte bruken av digitale tjenester øker mengden av digital informasjon eksponentielt. Ved bruk av internett, offentlig digitale tjenester og mobiltelefon m.m., genereres det enorme menger digitale spor om våre bevegelser.

Nærings- og handelsdepartementet lanserte norsk kryptopolitikk i 2001. Det har vært en rivende utvikling av IKT og digitalisering siden den gangen. Krypto og kryptoteknologi har vært, og er i dag et viktigere verktøy enn noensinne for å sikre våre nasjonale, samfunnsmessige, forretningsmessige og private verdier.

Det globale digitale landskapet er endret, digitale verdikjeder krysser landegrenser og det etableres digitale avhengigheter som utfordrer nasjonale myndigheter. Den internasjonale sikkerhetssituasjonen er også i endring og har blitt mer krevende. Det stilles økte krav til et godt sivilt-militært samarbeid for å ivareta samfunnssikkerhet og statssikkerhet. Forsvaret blir stadig mer avhengig av sivile tjenester og infrastruktur. Å ivareta samfunnssikkerheten blir stadig mer betydningsfullt for forsvarssektoren og vår evne til å forsvare vårt land og opprettholde samfunnskritiske funksjoner. Trussel- og risikobildet internasjonalt og nasjonalt endres raskt og vi opplever flere alvorlige terroraksjoner, ekstremvær, digitale angrep og en krevende sikkerhetspolitisk utvikling. Hybride trusler er med på å viske ut skillelinjene mellom fred, krise og krig, og i det digitale domenet kan det være krevende å avgjøre hvilken aktør som står bak.

Ett av regjeringens virkemidler for å møte utfordringene er å videreutvikle det sivil-militære samarbeidet innenfor rammen av totalforsvarskonseptet. Kryptomateriell som er utviklet til bruk i forsvarssektoren brukes også i større grad av myndigheter og virksomheter i sivil sektor som er en del av totalforsvaret.

Regjeringen lanserte nasjonal strategi for digital sikkerhet i januar 2019. Strategien skal møte utfordringene som følger av teknologiutviklingen og den gjennomgående digitaliseringen av det norske samfunnet. Strategien understreker behovet for styrket offentlig-privat samarbeid, sivil-militært samarbeid og internasjonalt samarbeid. Samtidig ble det også lansert nasjonal strategi for digital sikkerhetskompetanse. Digital sikkerhetskompetanse er en viktig forutsetning for at vi skal lykkes med å sikre alle tjenester som digitaliseres. Grunnleggende digital sikkerhetskompetanse er igjen avgjørende for å kunne opprettholde nasjonal kryptokompetanse.

Bruken av kryptoteknologi er avgjørende for å bevare tilliten til nye digitale tjenester i det norske samfunnet, trygge våre digitale verdier og sørge for sikker kommunikasjon i militære operasjoner.

Vi vil med vår kryptopolitikk bidra til å bygge et sikkert samfunn, trygge den enkelte borger i det digitale rom, møte de digitale sikkerhetsutfordringene, opprettholde nødvendig nasjonal kryptokompetanse, understøtte totalforsvaret, stimulere til innovasjon og produktutvikling og videreføre Norges viktige posisjon som kryptoleverandør til NATO.

Oslo, november 2019

Foto: Sturlason/UD

Frank Bakke-Jensen
Forsvarsminister

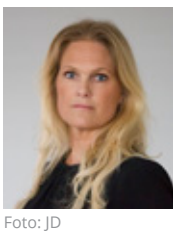

Foto: JD

Ingvil Smines Tybring-Gjedde
Samfunnssikkerhetsminister

Innhold

Foto: Getty Images

Innledning

Bruk av kryptoteknologi er helt avgjørende både for å beskytte informasjon om enkeltindividet og informasjon som har avgjørende betydning for nasjonale sikkerhetsinteresser. Norge har en lang og stolt tradisjon for å utvikle egen kryptoteknologi.

Norge er et av de mest digitaliserte landene i verden. Utviklingen av internett og den raske utviklingen innenfor informasjons- og kommunikasjonsteknologien (IKT) gir helt nye muligheter for samfunnet.

Det digitale rom har ikke de samme tradisjonelle nasjonale grenser som i den fysiske verden. I Norge er vi opptatt av å arbeide for at det digitale rom fortsatt skal fremme innovasjon og internasjonal handel, som vil bidra til internasjonal stabilitet og sikkerhet. Regjeringen er opptatt av at demokratiske verdier og universelle rettigheter også blir ivaretatt i det digitale rom. Regjeringen lanserte internasjonal cyberstrategi for Norge i 2017, som skal tjene norske interesser, sikre gode og forutsigbare rammevilkår og bidra til forebygging av og beskyttelse mot utfordringer og trusler i det digitale rom. Den internasjonale cyberstrategien fremhever Norges strategiske prioriteringer, som legger føringer også for utforming av norsk kryptopolitikk. Norsk kryptopolitikk skal understøtte nasjonale sikkerhetsinteresser, samfunnssikkerheten og bidra til å sikre borgernes og næringslivets digitale informasjon og kommunikasjon. Det er avgjørende for borgernes tillit til staten at den enkeltes trygghet ivaretas av politiet i det digitale rom. Norsk kryptopolitikk skal derfor også understøtte politiets forebygging, avdekking, stansing og etterforskning/iretteføring av lovbrudd – og bidrag til gjenoppretting av lov og orden – i det digitale rom.

Samfunnssikkerhet og statssikkerhet

Teknologiutviklingen og den økte bruken av IKT fører imidlertid også til økte sårbarheter, noe som er nærmere utredet i NOU 2015:13 *Digital sårbarhet – sikkert samfunn.* Utredningen er av regjeringen fulgt opp i Meld. St. 38 (2016–2017) *IKT-sikkerhet – Et felles ansvar.* Samfunnssikkerhetsmeldingen jf. Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn*, peker på verdien av og utfordringer med å dele og utveksle informasjon i en digital verden.

Samfunnets og borgernes sikkerhet er den viktigste av statens kjerneoppgaver. Et av regjeringens satsingsområder er derfor trygghet i hverdagen og styrket beredskap. Lov om nasjonal sikkerhet (sikkerhetsloven), jf. Prop. 153 L (2016-2017) skal legge rammene for at vi har de virkemidlene som er nødvendige for å ivareta nasjonale sikkerhetsinteresser og forebygge mot sikkerhetstruende virksomhet. Det vises forøvrig til regjeringens øvrige politikk for statssikkerhet, jf. Prop. 151 S (2015-2016) *Kampkraft og bærekraft – Langtidsplanen for forsvarssektoren.*

Behovet for og bruken av kryptoteknologi har tradisjonelt vært forbeholdt Forsvaret og ivaretagelse av statssikkerheten. Kryptoteknologi har vært anerkjent som et nødvendig verktøy for å hindre uvedkommende å få tilgang på sikkerhetsgradert og sensitiv informasjon.

Nasjonalt forebyggende sikkerhetsarbeid reguleres gjennom sikkerhetsloven. Kryptosikkerhet er en viktig del av nasjonalt forebyggende sikkerhetsarbeid. Forsvarsdepartementet valgte på denne bakgrunn å foreslå regulering av særlige krav i sikkerhetsloven til bruk av krypto for å beskytte sikkerhetsgradert informasjon, for å sikre at kryptoen som brukes er av en viss kvalitet. Det må bemerkes her at disse bestemmelsene ikke kommer i konflikt med regjeringens generelle holdning om at bruken av kryptografi verken bør forbys eller reguleres.

Sivil sektor har tatt i bruk kryptoteknologi i takt med bruken av IKT. Med økt digitalisering vil også behovet for å gi sikker tilgang til digitale tjenester og beskytte sensitiv informasjon og personopplysninger øke.

Teknologiutviklingen medfører også at det om noen år mest sannsynlig vil bli utviklet kvantedatamaskiner. En kvantedatamaskin baserer seg på kvantemekaniske prosesser. Dette gir en regnekraft som er overlegen dagens datamaskiner. Kvantedatamaskiner vil kunne brukes til kryptoanalyse og dette vil redusere sikkerhetsnivået og i noen tilfeller bryte sikkerheten i dagens kryptoalgoritmer, både i forsvarssektoren og i sivil sektor.

Regjeringen har høye ambisjoner om å fornye, forenkle og forbedre offentlig sektor gjennom digitaliseringen, samtidig som innbyggere og næringsliv har forventninger om en enklere hverdag, jf. Meld. St. 27 (2015-2016) *Digital Agenda for Norge.* Bruk av IKT og bevisst utnyttelse av digitaliseringens muligheter gjør at vi kan oppnå begge deler. Digital sikkerhet er en nødvendig forutsetning for tillit til digitale løsninger og bruken av kryptoteknologi i sivil sektor er derfor mer aktuell enn noensinne.

Foto: NATO

Opprettholdelse av en høykompetent nasjonal kryptoindustri er et viktig bidrag til Norges sikkerhetspolitiske samarbeid med andre land og Norges posisjon som kryptoleverandør til NATO.

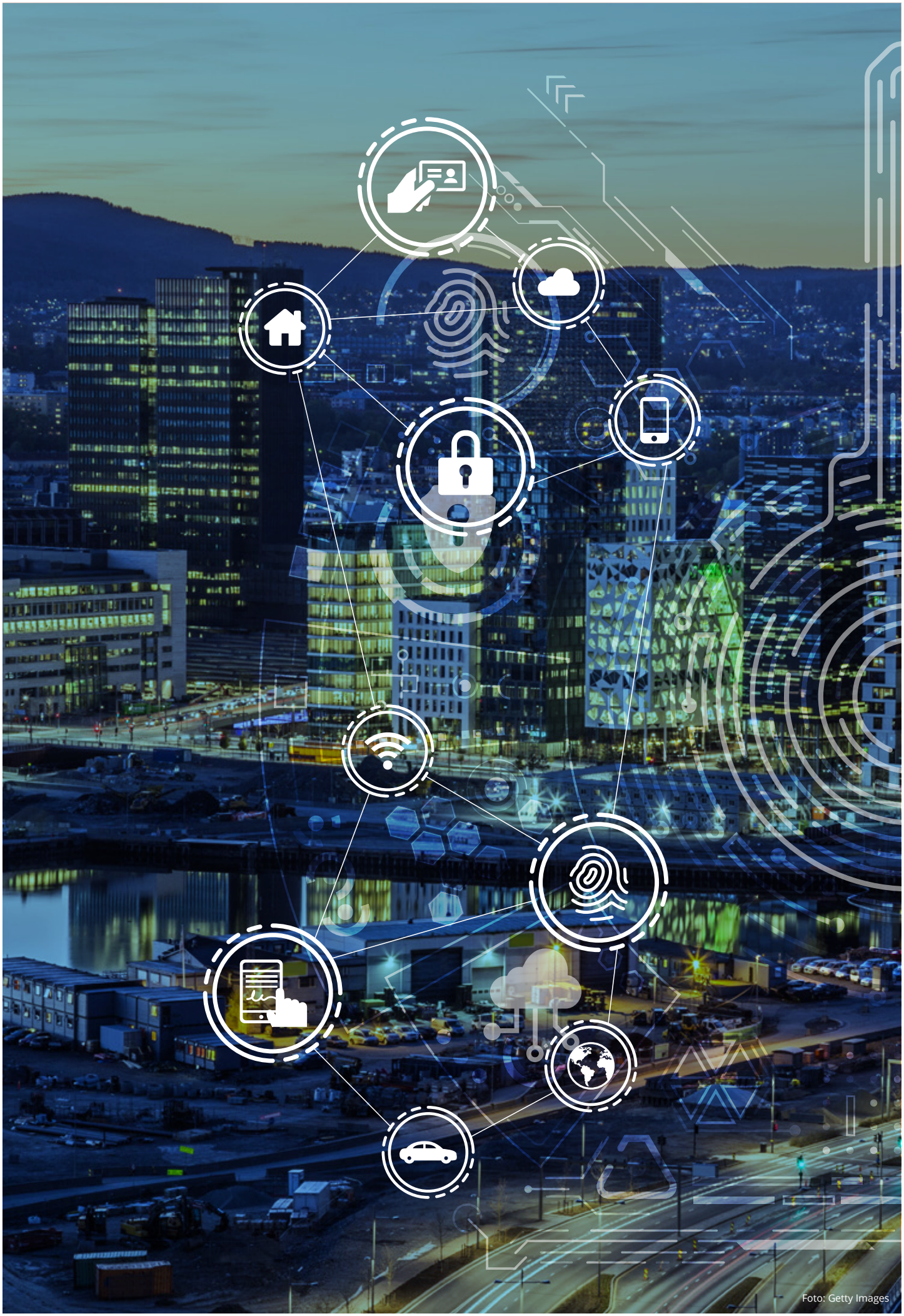

Foto: Getty Images

Bakgrunn og omtale av kryptoteknologi

Bakgrunn for kryptopolitikken

«Norsk kryptopolitikk», utgitt av det daværende Nærings- og handelsdepartementet i 2001, inneholder en rekke anbefalinger for utarbeidelse av en nasjonal kryptopolitikk, blant annet for å understøtte personvern og ytringsfrihet, utvikling av en nasjonal kryptoindustri, vitale nasjonale sikkerhetsinteresser og effektiv, elektronisk forvaltning. Forsvarsdepartementet og Nasjonal sikkerhetsmyndighet (NSM) har vært viktige premissleverandører for oppfølgingen av kryptopolitikken når det gjelder å sikre vitale nasjonale sikkerhetsinteresser. Utviklingen av internett, digitaliseringen av samfunnet og bruken av IKT gjør bruken av kryptoteknologi mer aktuell enn noen sinne. For å bidra til å sikre nødvendig nasjonal kryptokompetanse og stimulere til innovasjon og produktutvikling, bestemte regjeringen i Meld. St. 10 (2016-2017) *Risiko i et trygt samfunn*, at den norske kryptopolitikken fra 2001 skulle revideres.

Kryptopolitikken fra 2001 baserte seg på OECDs retningslinjer fra 1997 for kryptopolitikk. OECDs retningslinjer har jevnlig blitt evaluert siden utgivelsen i 1997. Siste gjennomgang ble foretatt høsten 2017. Konklusjonen av denne gjennomgangen var at retningslinjene fortsatt er relevante, men at fortalen bør oppdateres med hensyn på utvikling og bruk av ny digital teknologi de siste 20 årene. Retningslinjene har vært førende for kryptopolitikken i svært mange OECD-land. Retningslinjene har knesatt flere viktige prinsipper for hvordan kryptopolitikk bør utformes og håndheves. Det er derfor også i denne reviderte norske kryptopolitikken tatt utgangspunkt i OECDs retningslinjer for valget av hovedområder som kryptopolitikken omtaler.

Kryptoteknologi

Kryptering handler tradisjonelt om å gjøre informasjon uleselig. Man «låser» (krypterer) slik at det kun er den som har tilgang til den riktige «nøkkelen» som kan «låse opp» (dekryptere) informasjonen, og lese den. Kryptografiske metoder benyttes også for å beskytte informasjon mot uautorisert endring og for å knytte opphavet til informasjon til en person eller virksomhet.

Kryptering har vært brukt i mer enn tusen år med stadig mer avanserte beregningsmetoder. Moderne kryptoteknologi benytter matematiske rammeverk for å ivareta funksjonene den skal tilby.

For å anvende dagens kryptoteknologi må det brukes datamaskiner. I takt med utviklingen av datamaskiner har det stadig blitt utviklet mer avansert kryptoteknologi. Etter hvert som datamaskiner har blitt allemannseie og digitaliseringen har skutt fart, har også bruken av kryptoteknologi økt.

Den fundamentale beregningsmetoden for kryptoteknologi omtales ofte som kryptoalgoritmen. Sikkerheten for den krypterte informasjonen er avhengig av hvor lang nøkkelen som brukes er, og måles i antall bit. Dette kalles nøkkellengden.

Symmetrisk kryptografi refererer til krypteringsmetoder der sender og mottaker deler en felles hemmelighet som gjerne kalles en hemmelig kryptonøkkel. Utfordringen med å beskytte kommunikasjon eller datamengder blir redusert til utfordringen med å beskytte kryptonøkkelen, som typisk er av en liten størrelse. For å styrke sikkerheten i symmetrisk krypto

Foto: Getty Images

for høygraderte systemer, er også kryptoalgoritmen og nøkkellengden ukjent for uvedkommende. Det er da enda vanskeligere å analysere kryptert informasjon i forsøk på å dekryptere uten krypteringsnøkkelen.

I asymmetrisk krypto er sikkerheten basert på beregningsmessig kompleksitet av to matematiske problemer. Ett av dem er lett å beregne, mens det andre er svært vanskelig. Denne asymmetrien er nødvendig for å lage et offentlig og privat nøkkelpar. Hvis man lager en privat nøkkel, er det lett å beregne en tilhørende offentlig nøkkel. På den annen side er det vanskelig å beregne den private nøkkelen hvis man kun har den offentlige nøkkelen. Kryptoalgoritmene som brukes i asymmetrisk krypto er kjent.

Fordelen med asymmetrisk krypto er at det ikke nødvendig for partene å dele noen hemmeligheter på forhånd. Dette forenkler kryptonøkkelhåndteringen. Den offentlige nøkkelen publiseres gjerne på en nettside eller deles med alle som en skal kommunisere med, sammen med et elektronisk sertifikat.

Kvantedatamaskiner forventes å bli tilgjengelig i nær framtid. Disse vil utgjøre en stor trussel mot noen av de underliggende matematiske problemene som symmetrisk og asymmetrisk kryptografi er bygget på. I noen tilfeller er denne trusselen så stor, at vi vil måtte bytte ut de fundamentale byggesteinene som er i utbredt bruk i dag.

Hash-funksjoner brukes i tilknytning til asymmetrisk krypto og tar en vilkårlig datamengde og beregner en verdi av en forhåndsbestemt størrelse. For kryptografiske hash-funksjoner er det vanskelig å utlede noe fra den opprinnelige datamengden hvis man kjenner hash-verdien. Det betyr at to forskjellige datamengder (selv om det er en liten forskjell) vil gi helt forskjellige hash-verdier. Hash-funksjoner kaller derfor også ofte for en-veis-funksjoner. En hash-verdi kalles gjerne et fingeravtrykk og gir integritetsbeskyttelse av en datamengde.

Elektronisk signatur og digital signatur

En elektronisk signatur er et dataelement som følger et digitalt dokument, og som binder dokumentet til en virksomhet, en person, en datamaskin eller en datatjeneste.

En elektronisk signatur har disse egenskapene:

- **Den er entydig knyttet til undertegneren.**
- **Den kan identifisere undertegneren.**
- **Den er laget med midler som bare undertegneren har kontroll over.**
- **Den er knyttet til dokumentet på en slik måte at alle etterfølgende endringer i det kan oppdages.**

Kryptering handler tradisjonelt om å gjøre informasjon uleselig. Man «låser» (krypterer) slik at det kun er den som har tilgang til den riktige «nøkkelen» som kan «låse opp» (dekryptere) informasjonen, og lese den.

Elektroniske signaturer som brukes i forbindelse med Public Key Infrastructure (PKI) omtales som digitale signaturer. Fordelen ved bruk av PKI er at de tilordnes et elektronisk sertifikat til en person eller virksomhet. Dette elektroniske sertifikatet inneholder entydig informasjon om personene eller virksomheten og inneholder også den offentlige nøkkelen. Et elektronisk sertifikat kan også knyttes til et domenenavn og er da et sertifikat for nettstedautentisering og kalles ofte et SSL-sertifikat. Den som utsteder sertifikatet kalles en tiltrodd tredjepart, og er den som går god for at identiteten i sertifikatet er korrekt.

Teknologier som anvender kryptoteknologi

Blockchain er mye omtalt som teknologien som brukes i Bitcoin og andre digitale valutaer. Blockchain er en anvendelse av Merkel tre-konstruksjonen (et hash-tre). Merkel tre har blitt brukt og brukes i andre anvendelser som protokoller, revisjonskontrollsystemer (særlig i programvareutvikling) og det har i det siste vært en del snakk om å benytte teknologien i enkelte sikkerhetsfunksjoner.

Multi-party computation er et område det forskes mye på. Typisk eksempel på anvendelse er to virksomheter med hver sin database eller datamengde som de vil holde skjult for hverandre, men likevel utføre beregninger på hverandres data (statistikk, sammenligninger mv.)

Homomorfisk kryptografi er også lovende. Homomorfisk kryptografi er en metode for å gjennomføre annonymiserte databasesøk og behandling av krypterte elementer i databaser, uten at de dekrypteres.

Foto: Getty Images

Kryptopolitikken

Formål

Kryptopolitikken har flere formål. Den skal bidra til å bygge et sikkert samfunn gjennom å opprettholde nødvendig nasjonal kryptokompetanse, stimulere til innovasjon og produktutvikling, stimulere til at kryptoteknologi tas i bruk og videreføre Norges viktige posisjon som kryptoleverandør til NATO.

Kryptopolitikken skal også beskrive betydningen av kryptoteknologi for å understøtte norsk forsvars- og sikkerhetspolitikk og regjeringens politikk på de ulike samfunnsområdene som teknologiutvikling, digitalisering, offentlige digitale tjenester, sikker elektronisk kommunikasjon, forskning, sikring av personopplysninger mv. Kryptopolitikken beskriver regjeringens målsettinger, ambisjonsnivå og prioriteringer for anvendelse av kryptoteknologi.

Teknologiutviklingen og anvendelse av kryptoteknologi

Ny teknologi har effektivisert samfunnet på de fleste områder, både innenfor forsvarsektoren og de andre samfunnsområdene. Teknologiutviklingen siden 2001 har vært meget stor og digitaliseringen har endret samfunnet og vi er blitt helt avhengige av ulike digitale tjenester. Bruken av kryptoteknologi er teknikker som skal sikre informasjonenes opphav, hindre innsyn og avdekke endring. Kryptering har avgjørende betydning for beskyttelse av informasjon, og er derfor mer enn noen gang en forutsetning for sikkerhet i elektronisk kommunikasjon, både i forsvarssektoren og i sivil sektor.

Regjeringen konkluderte i Meld. St. 38 (2016-2017) *IKT-sikkerhet – Et felles ansvar* at kryptering ikke skal forbys eller begrenses gjennom lov. Dette berører ikke regulering av kryptosikkerhet i sikkerhetsloven. Sikkerhetsloven regulerer særlige krav til bruk av krypto for å beskytte sikkerhetsgradert informasjon for å sikre at kryptoen som brukes er av en viss kvalitet.

Regjeringen vil på denne bakgrunn oppfordre til bruk av kryptoteknologi for å understøtte sikkerhet i IKT-systemer, sikring av personopplysninger, offentlige digitale tjenester og sikker elektronisk kommunikasjon i forvaltningen og i næringslivet.

Forsvarssektoren har siden andre verdenskrig vært avhengig av bruken av kryptoteknologi for å ivareta nasjonale sikkerhetsinteresser. Kryptosikkerhet er en viktig del av nasjonalt forebyggende sikkerhetsarbeid. Forsvarsdepartementet understreket i Prop. 153 L (2016-2017) at de mest grunnleggende reglene om kryptosikkerhet bør gå klart frem av sikkerhetsloven. Loven ble tydelig på hvordan kryptosikkerheten skal forvaltes, og at det stilles særlige krav ved bruk av krypto for å beskytte sikkerhetsgradert informasjon. Det er nødvendig at kryptoteknologi som skal brukes til beskyttelse av sikkerhetsgradert informasjon er av en viss kvalitet, spesielt å ivareta behovet for beskyttelse av høygradert informasjon.

NSM har et tett samarbeid med norsk kryptoindustri for å utvikle høygraderte kryptoløsninger. Forsvars-departementet har en policy for samarbeid mellom Forsvaret og norsk industri på IKT-området som omfatter kryptosikkerhet for høygraderte løsninger. Policyen baserer seg på St.meld. nr. 38 (2006-2007)

Det er en langsiktig prosess å bygge opp kompetanse- og forskningsmiljøer, og kunnskap om kryptering må vedlikeholdes dersom den skal være relevant.

Forsvaret og industrien – strategiske partnere – Strategi for de næringspolitiske aspekter ved Forsvarets anskaffelser. Med bakgrunn i forsvarsindustriens betydning for nasjonal sikkerhet, blir forsvarssektorens forhold til forsvarsindustrien behandlet i stortingsdokumenter med jevne mellomrom. Strategien ble evaluert i 2014. Dette resulterte i Meld. St. 9 (2015-2016) *Nasjonal forsvarsindustriell strategi.*

Kvantedatamaskiner vil kunne brukes til kryptoanalyse, som vil redusere styrken i kryptoalgoritmene i høygraderte systemer. Det er derfor helt avgjørende at framtidens kryptoalgoritmer og kryptosystemer som brukes i høygraderte løsninger er resistente mot kvantedatamaskiner, slik at informasjonen som krypteres har beskyttelse i minst 30 år.

For å møte utfordringene med kvantedatamaskiner er det nødvendig å fokusere på flere forhold samtidig, slik som nasjonal kryptokompetanse, samarbeid mellom myndigheter og kryptoindustrien og internasjonalt samarbeid. Disse forholdene omtales nedenfor.

Nasjonal kontroll på høygradert kommunikasjon er viktig for norsk suverenitet og statssikkerhet, og en del av norsk forsvars- og sikkerhetspolitikk. Regjeringen har derfor som målsetting at kryptoteknologi som benyttes til å beskytte nasjonal høygradert informasjon fortsatt skal være underlagt nasjonal kontroll. Nasjonal kontroll innebærer at utviklingen av kryptoalgoritmer, implementasjon og produksjon av kryptomateriell gjøres i samarbeid mellom NSM og norsk kryptoindustri på oppdrag fra Forsvarsdepartementet.

- **Regjeringen har en klar målsetting om at kryptoteknologi som benyttes til å beskytte nasjonal høygradert informasjon fortsatt skal være underlagt nasjonal kontroll.**
- **Regjeringen oppfordrer til bruk av kryptoteknologi i alle samfunnssektorer for å understøtte sikkerhet i IKT-systemer, sikring av personopplysninger, offentlig digitale tjenester og sikker elektronisk kommunikasjon i forvaltningen og i næringslivet.**
- **Regjeringen ønsker å stimulere markedet til å tilby kryptoprodukter og -tjenester som er enkle å ta i bruk, både for borgerne og næringslivet.**

Stimulere til forskning, innovasjon og næringsutvikling

Norges forskningsråd skal bidra til å dekke samfunnets behov for forsking ved å fremme grunnleggende og anvendt forskning og innovasjon. Forskningsrådet arbeider for et kvalitetsmessig løft i norsk FoU og for å fremme innovasjon, i samspill mellom forskningsmiljøene, næringslivet og den offentlige forvaltningen. Forskningsrådet skal identifisere behov for forskning og foreslå prioriteringer. Gjennom målrettede finansieringsordninger skal Forskningsrådet bidra til å sette i verk nasjonale forskningspolitiske vedtak.

Justis- og beredskapsdepartementet har i samarbeid med Kunnskapsdepartementet utarbeidet en nasjonal strategi for digital sikkerhetskompetanse. Denne skal være et grunnlag for å utvikle kompetanse i tråd med samfunnets, arbeidslivets og den enkeltes behov.

I langtidsplanen for forsking og høyere utdanning 2019-2028, jf. Meld. St. 4 (2018-2019) er forskning på muliggjørende teknologier og IKT-sikkerhet omtalt. Det er opprettet forskningsprogrammer som IKTPLUSS og SAMRISK hos Forsningsrådet. Innenfor disse programmene vil det kunne initieres relevant forskning på digital sikkerhet og kryptologi.

Anvendelse av kryptoteknologi bidrar til å øke tilliten og sikkerheten i digitale tjenester og ny anvendelse kan legge grunnlag for ny muliggjørende teknologi. Blockchain er et godt eksempel der anvendelse av kryptoteknologi brukes til å skape ny teknologi, og som igjen skaper nye muligheter for innovasjon.

Departementene har i sine budsjetter diverse poster for støtte til forskningsaktiviteter. Det er viktig at det stimuleres til forskning og næringsutvikling på kryptoteknologi innenfor eksisterende forskingsprogrammer og i forbindelse med andre relevante forskningsaktiviteter i offentlig og privat regi.

> **Regjeringen vil arbeide for at det stimuleres til forskning og næringsutvikling på kryptoteknologi innen eksisterende forskningsprogrammer for digital sikkerhet og i andre relevante forskningsaktiviteter i offentlig og privat regi.**

Sikre nasjonal kryptokompetanse

FD har et tett samarbeid med NSM og norsk kryptoindustri for å utvikle høygraderte kryptoløsninger for forsvarssektoren. Det er en langsiktig prosess å bygge opp kompetanse- og forskningsmiljøer, og kunnskap om kryptering må vedlikeholdes dersom den skal være relevant. Uten kompetente nasjonale fagmiljøer vil norske myndigheter og bedrifter måtte forholde seg til utenlandske aktører, for å innhente kvalifiserte vurderinger og råd om kryptografiske systemer. Dette vil være uheldig sett fra et nasjonalt sikkerhetsperspektiv.

Nasjonal strategi for digital sikkerhetskompetanse omtaler behovet for å øke kompetanse innen kryptoteknologi. Strategien omtaler også flere tiltak som er satt i gang for å øke rekrutteringen og styrke kompetansen. Strategien trekker særlig fram behovet for å finne løsninger som kan bidra til at flere av de som rekrutteres kan sikkerhetsklareres. En ordning som kan vurderes nærmere er offentlig sektor ph.d-stillinger, der kvalifiserte kandidater som allerede er ansatt hos sikkerhetsmyndighetene/forskningsinstitusjonene kan søke. En vil her kunne legge inn som et vilkår at søkere må ha gyldig sikkerhetsklarering for å få tilsetting. Sikkerhetsindustrien kan oppfordres til å benytte nærings-ph.d-ordningen med det samme vilkåret om at søkere må ha gyldig sikkerhetsklarering. Grunnleggende digital sikkerhetskompetanse er avgjørende for å kunne rekruttere spesialister og opprettholde nasjonal kryptokompetanse.

Anskaffelse av høygraderte kryptoløsninger for forsvarssektoren gjøres ofte som direkteanskaffelser i samarbeid med en norsk industri i tråd med anskaffelsesregelverk for forsvarssektoren. NSM deltar med kryptokompetanse i denne typen prosjekter. For at dette skal være mulig å gjennomføre trengs kryptokompetanse på svært høyt nivå. Det må derfor legges til rette for at nordmenn i større grad enn tidligere kan kvalifisere seg til stipendiatstillinger og stillinger knyttet til relevante forskningsprogrammer. Regjeringens styrking av utdannings- og forskningsmiljøene knyttet til IKT-sikkerhet fra og med 2018 vil bidra til å styrke rekrutteringsgrunnlaget for å bedre den nasjonal kompetansen innen kryptoteknologi.

> **Regjeringen vil arbeide for at kryptokompetansen i NSM styrkes.**

> **Regjeringen oppfordrer arbeidslivet, utdannelses- og forskningsmiljøene og forvaltningen til å samarbeide for å heve nasjonal kryptokompetanse innen forskning og utdanning, slik at rekrutteringsgrunnlaget for stillinger i forsvarssektoren, industrien og næringslivet styrkes.**

> **Regjeringen vil arbeide for at personer som kan sikkerhetsklareres, kan kvalifisere seg til stipendiatstillinger og utvalgte forskningsprogrammer.**

Samarbeid mellom myndigheter og kryptoindustrien

For å sikre nasjonal kontroll på høygradert informasjon er Norge avhengig av en levedyktig nasjonal kryptoindustri. Regjeringen ønsker derfor å videreføre en tydelig satsing på samarbeid mellom forsvarssektoren og norsk kryptoindustri.

Forsvarssektoren er avhengig av kryptoteknologi i en rekke ulike materiellanskaffelser som både er modernisering og opprettholdelse av eksisterende systemers evne til å beskytte sikkerhetsgradert informasjon. Får å sikre at de høygraderte systemene er motstandsdyktige mot kvantedatamaskiner krever

Foto: KDA

dette et fortsatt samarbeid mellom forsvarssektoren, NSM og norsk kryptoindustri. Forsvarsdepartementet har etablert en policy for samarbeid mellom Forsvaret og norsk industri på IKT-området som inkluderer kryptosikkerhet for høygraderte løsninger. Opprettholdelse av en høykompetent nasjonal kryptoindustri er også et viktig bidrag til Norges sikkerhetspolitiske samarbeid med andre land og Norges posisjon som kryptoleverandør til NATO.

NSMs rolle innen kryptosikkerhet er definert i sikkerhetsloven som stiller særskilte krav til krypto for gradert informasjon. For å understøtte dette gjennomføres gradert forskning og utviklingsaktiviteter. Forskningen som har pågått gjennom mange tiår er høyt gradert og tilgang til å arbeide med denne krever en egen spesialisering og kvalifisering i NSM. Kunnskap om det nasjonale graderte teoretiske grunnlaget for kryptologi beskyttes strengt og gis ikke tilgang til med mindre det er strengt nødvendig. De graderte problemstillingene relatert til kryptologi i totalforsvaret løses hovedsakelig internt i NSM. For at NSM fortsatt skal være i stand til å samarbeide med norsk kryptoindustri for å utvikle høygraderte kryptoløsninger må kryptomiljøet i NSM styrkes utover dagens nivå.

Det er viktig at norsk kryptoindustri er konkurransedyktig internasjonalt og har mulighet for å levere norsk kryptoteknologi til nasjoner Norge har et sikkerhetsmessig samarbeid med og til NATO. Dette er en forutsetning for en levedyktig norsk kryptoindustri som kan utvikles og være i stand til å levere høyteknologiske nasjonale kryptoløsninger til forsvarssektoren. Det bør søkes å videreutvikle eller etablere nye samarbeidsarenaer som kan legge til rette for godt samarbeid og økt kompetanse innen kryptoteknologi. Eksport av visse typer kryptoteknologi er underlagt eksportkontroll og krever tillatelse fra

Utenriksdepartementet. Norske aktører må være oppmerksomme på at regelverket for eksportkontroll også omfatter eksport av kunnskap som kan anvendes til militære formål. Forskningsinstitusjoner må derfor vurdere risikoen for ulovlig kunnskapsoverføring når sensitiv kunnskap deles med utenlandske studenter, forskere og samarbeidspartnere. Det må derfor også legges til rette for et godt samarbeid og informasjon mellom industrien og forvaltningen om gjeldende lovgivning på området.

> **Regjeringen vil videreføre en tydelig satsing på samarbeid mellom forsvarssektoren og norsk kryptoindustri, samt med utdannings- og forskningsinstitusjonene, for å understøtte nasjonal kontroll over høygradert kryptoteknologi.**

Digitalisering av offentlig sektor og offentlige digitale tjenester

Regjeringen har høye ambisjoner om å fornye, forenkle og forbedre offentlig sektor gjennom digitaliseringen, samtidig som innbyggere og næringsliv har forventninger om en enklere hverdag, jf. Meld. St. 27 (2015-2016) *Digital Agenda for Norge.* Bruk av IKT og bevisst utnyttelse av digitaliseringens muligheter gjør at vi kan oppnå begge deler. Digital sikkerhet er en nødvendig forutsetning for tillit til digitale løsninger og bruken av kryptoteknologi i sivil sektor er derfor mer aktuell enn noensinne.

Offentlige digitale tjenester er avhengig av tillit til løsninger for sikker autentisering ved innlogging på nett, sikring av konfidensialitet og sikker bruk av elektroniske signaturer. Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester) trådte i kraft 15. juni 2018. Loven med forskrifter gjennomfører eIDAS-forordningen i norsk rett og regulerer bruk av elektronisk identifikasjon (eID), samt definerer sikkerhetsnivåer til bruk i offentlig sektor. Loven regulerer også bruk av elektroniske tillitstjenester i offentlig sektor og i næringslivet. Elektroniske tillitstjenester er typisk sertifikater for elektroniske signaturer for både fysiske og juridiske personer samt sertifikater som brukes for å sikre nettsteder på Internett.

Regjeringen har revidert rammeverk for identifikasjon og sporbarhet i elektronisk kommunikasjon med og i offentlig sektor, som vil være retningslinjer for offentlige virksomheter som skal sikre digital samhandling med og i offentlig forvaltning. For å understøtte sikker tilgang til offentlige tjenester har regjeringen etablert ID-porten som en felles løsning for alle offentlige virksomheter.

Lov om elektroniske tillitstjenester legger også til rette for sikker samhandling og elektronisk handel på tvers av landegrensene i EØS og ivaretar interoperabilitet innen EUs indre marked.

Reguleringen er teknologinøytral. Mange av tjenestene vil realiseres gjennom anvendelse av kryptoteknologi.

> **Regjeringen vil arbeide for at prinsipper, rammeverk og tjenester som lov om elektroniske tillitstjenester omfatter, tas i bruk i offentlig sektor.**

> **Regjeringen oppfordrer næringslivet til både å tilby og anvende produkter og tjenester som omfattes av lov om elektroniske tillitstjenester og for øvrig anvende kryptoteknologi i produkter og tjenester i det norske markedet.**

Bekjempelse av kriminalitet

Teknologiutviklingen, herunder kryptoteknologi som brukes til å gjennomføre og skjule lovbrudd, utfordrer politiets evne til effektiv bekjempelse av kriminalitet. Dette gjelder både der IKT-teknologi anvendes for å gjennomføre en straffbar handling, og kriminalitet som er rettet mot IKT-systemer. Kriminalitetsbildet endres raskt i det digitale rom, og politiet må ha kompetanse og kapasitet til å bekjempe kriminalitet på disse nye områdene for å kunne avdekke, forebygge, avverge, etterforske og iretteføre kriminalitet, og for å kunne gjenopprette lov og orden i det digitale rom i henhold til politilovens krav og forutsetninger. Ved nesten all etterforskning av kriminalitet, kan det være behov for tilgang til digital informasjon, og særlig ved alvorlig kriminalitet har politiet i dag hjemler for innhenting av informasjon som finnes digitalt. Nødvendig informasjon kan finnes på ulike informasjonsbærere, som for eksempel mobiltelefoner eller PC'er, eller i «skyen». Selv om den nødvendige informasjonen er kryptert, vil politiet kunne ha behov for tidsriktig tilgang til informasjonsinnholdet. Det er viktig at politiet har hjemler, utstyr og kompetanse som gir mulighet til å få tilgang til informasjonsinnholdet. Uten slik tilgang vil politiet ikke kunne gjennomføre samfunnsoppdraget i det digitale rom. Det er et faktum at for tilnærmet alle straffbare handlinger i dag, vil informasjon av betydning for stansing eller etterforskning av forholdet kreve tilgang til en eller annen form for digitalt lagret informasjon.

For den aller mest alvorlige kriminaliteten har PST og det øvrige politiet adgang til å bryte eller omgå beskyttelse, for eksempel kryptering i datasystemet. Straffeprosessloven og politiloven regulerer politiets adgang til å iverksette dataavlesing, kommunikasjonskontroll og få tilgang til trafikkdata, og lov om elektronisk kommunikasjon gir tilbydere av elektronisk kommunikasjon plikt til å legge til rette for kommunikasjonskontroll. Dette er eksempler på reguleringer, som sørger for lovlig tilgang til informasjon som politiet har behov for, for å gjennomføre sitt samfunnsoppdrag.

Ut over dataavlesning, og eventuelt frivillig overlevering, kan politiet oppnå tilgang til kryptert informasjon gjennom f.eks. ransaking og utleveringspålegg. Ved ransaking har politiet også hjemmel til å bryte eller omgå beskyttelse, herunder kryptering, samt hjemmel til å pålegge "enhver" som har befatning med datasystemet, å gi politiet de nødvendige opplysninger for å gi tilgang til datasystemet.

For øvrig er politiet avhengig av at den som har rådighet over aktuelle krypterte opplysninger kan og er villig til å dekryptere informasjonen, og overlate denne til politiet, eller overlate kryptert informasjon og krypteringsnøkkel til politiet. Erfaring har vist at frivillig samarbeid har et stort uforløst potensiale. Politiet opplever imidlertid at tredjeparter som sitter med relevant informasjon samarbeider i varierende grad, og det er behov for å videreutvikle samarbeid med ulike tjenestetilbydere av kryptert lagring og kommunikasjon. Beskyttelse av informasjon er ofte sentralt for tjenestetilbyderne, og et frivillig samarbeid med politiet må derfor gjennomføres i henhold til deres kommersielle kontrakter, forpliktelser og øvrig lovverk.

Borgerne og næringslivet har behov for å sikre egen informasjon og kommunikasjon fra uvedkommende. Rettsikkerhet og personvern må ivaretas best mulig og sees i sammenheng med behovet for beskyttelse mot kriminalitet og angrep på lov og orden, når samfunnet skal sikre politiet tilgang til informasjon, som er nødvendig for å bekjempe kriminalitet.

> **Regjeringen vil arbeide for gode reguleringer som ivaretar rettssikkerheten og personvernet til norske innbyggere og bedrifter når politiet tar i bruk sin lovlige tilgang til informasjon, som er nødvendig for kriminalitetsbekjempelse og opprettholdelse av lov og orden i det digitale rom.**

> **Regjeringen vil arbeide for å gi politiet kompetanse, kapasitet og verktøy innen IKT-teknologi for å kunne sikre at de kan gjennomføre sitt samfunnsoppdrag.**

Sikring av personopplysninger

Teknologiutviklingen, digitaliseringen og bruken av IKT på alle samfunnsområder utfordrer personvernet. Hverdagen til borgerne er digital og over alt hvor borgerne ferdes legges det igjen elektroniske spor. Innsamling, lagring og bruk av personopplysninger gjennomføres i stor utstrekning. Borgernes grunnleggende behov for personvern, både personopplysningsvern og kommunikasjonsvern, må respekteres. Bruk av kryptoteknologi er sentralt for å oppnå dette.

Den nye personopplysningsloven gjennomfører EUs personvernforordningen (GDPR) i norsk rett. Kryptoteknologi er sentralt for å etterleve flere av forpliktelsene personvernforordningen oppstiller. Personvernforordningen setter blant annet krav til at aktører som behandler personopplysninger, iverksetter tekniske og organisatoriske tiltak for å sørge for sikker behandling av opplysningene. Kryptering er uttrykkelig nevnt i forordningen som et eksempel på et slikt tiltak. Forordningen fremhever også at tiltak skal tilpasses risikoen ved den konkrete behandlingen av personopplysninger. Det er derfor rom for å benytte kryptoteknologi av ulik kompleksitet og omfang avhengig av omstendighetene.

Kryptoteknologi vil være relevant ikke kun for å forhindre sikkerhetsbrudd ved behandling av personopplysninger, men også for å begrense risikoen dersom sikkerhetsbrudd inntreffer. Hvis personopplysninger skulle komme på avveie, vil blant annet forhåndskryptering kunne forhindre at uvedkommende kan nyttiggjøre seg av opplysningene i ettertid.

Tilsvarende vil gjelde for informasjon som er omfattet av kommunikasjonsvernet. Kryptering kan bidra til å sikre tillit til konfidensialitet gjennom beskyttelse av informasjon i transitt. Kryptoteknologi er derfor sentralt for tilbydere av elektroniske kommunikasjonstjenester. Samtidig kan borgerne selv iverksette tiltak for å beskytte sin kommunikasjon. Programvare for kryptering og annen kryptoteknologi vil da være et viktig supplement til tjenestetilbydernes andre sikkerhetstiltak for kommunikasjonsvern.

> **Regjeringen oppfordrer til bruk av kryptoteknologi for å fremme personopplysningsvern og kommunikasjonsvern og gjennom dette styrke tilliten til ny teknologi og nye digitale tjenester i samfunnet.**

Foto: Terje Pedersen / NTB scanpix

Internasjonalt samarbeid og standardisering

Bruken av anerkjente internasjonale standarder sikrer den nødvendige kvaliteten og tilliten til kryptoteknologi som anvendes i produkter og tjenester. Standarder sikrer også mulighet for samvirke mellom tjenester på tvers av landegrensene og gir mulighet for at produkter og tjenester som norske virksomheter utvikler kan markedsføres i et europeisk og globalt marked. Samtidig vil utenlandske produkter og tjenester kunne anvendes i nasjonale systemer. Bruken av kryptoteknologi bør derfor så langt det er hensiktsmessig basere seg på internasjonale anerkjente standarder og godkjente NATO-standarder.

Standardisering av kryptoteknologi og algoritmer gjøres i ulike internasjonale standardiseringsorganisasjoner der både myndigheter og næringsliv deltar. Noe standardisering foregår også i regi av andre myndigheter slik som National Institute of Standards and Technology (NIST) i USA. NIST utarbeider standarder innen kryptoteknologi og algoritmer. NIST er underlagt det amerikanske handelsdepartementet. NIST arbeider blant annet med å utvikle nye kvanteresistente asymmetriske algoritmer.

NSM deltar i NATO Communication and Information Systems Security Standards (CIS3) C&I partnership. Her bidrar NSM aktivt med utarbeidelse av kommunikasjonsstandarder som sikrer kryptografisk interoperabilitet med allierte. Interoperabilitet er avgjørende for alliert samhandling i hele krisespennet og i alle operative sammenhenger og har derfor stor betydning for kryptoutviklingsprosjekter i forsvarssektoren.

For norske kryptomiljøer i forsvarssektoren og sivil sektor, vil det være viktig å søke dialog og samarbeid og prioritere deltagelse i organer som utarbeider relevante standarder innen kryptoteknologi.

> **Regjeringen vil arbeide for å videreføre norsk deltagelse i relevante internasjonale fora.**

> **Regjeringen oppfordrer norske kryptomiljøer til aktiv deltagelse i relevante internasjonale fora, standardiseringsaktiviteter og relevant bilateralt samarbeid.**

Økonomiske og administrative konsekvenser

Økonomiske og administrative konsekvenser av politikken vil omfatte utgifter knyttet til gjennomføring i forvaltningen og i privat sektor. Målsettinger og ambisjonsnivå som er beskrevet i politikken skal fortrinnsvis dekkes innenfor departementenes og underlagte etaters gjeldende budsjettrammer. Framtidig understøttelse av kryptopolitikken dekkes innenfor fremtidige budsjettrammer.

Målsettingen om nasjonal kontroll over høygradert krypto har flere avhengigheter. En forutsetning er tilstrekkelig kryptokompetanse, både i NSM og i norsk kryptoindustri. En annen forutsetning er en levedyktig norsk kryptoindustri som er konkurransedyktig internasjonalt. Tilstrekkelig kryptokompetanse vil også være avhengig av at det utdannes tilstrekkelig antall personer med digital sikkerhetskompetanse og som kan spesialisere seg innen kryptoteknologi på master- og doktorgradsnivå samt postdoktor og i forskningsprogrammer. Det er lagt til rette for at studieplasser og stipendiatstillinger som inkluderer kryptoteknologi kan dekkes innenfor gjeldende budsjettrammer. Forskning innenfor sivil sektor og forsvarsektoren som vil omfatte forsking på kryptoteknologi prioriteres innenfor eksisterende forskningsprogrammer og -aktiviteter.

Aktiviteter som relevante departementer ønsker å initiere for å stimulere markedet til å tilby kryptoprodukter og -tjenester, håndteres innenfor gjeldende budsjettrammer. Regjeringen vil videreføre satsing på samarbeidet mellom forsvarssektoren og norsk kryptoindustri samt med utdannings- og forskningsinstitusjonene.

Regjeringens målsettinger innen digitalisering og arbeid med å legge til rette for bruk av eID, at forvaltningen tar i bruk ulike produkter og tjenester, og forvaltning av lov om elektroniske tillitstjenester vil måtte dekkes innenfor gjeldende budsjettrammer. Dersom målsettingen krever økte kostnader må dette vurderes opp mot andre formål i framtidige budsjetter.

Bekjempelse av kriminalitet er en prioritert oppgave. Å legge til rette for at politiet gis nødvendig tilgang til trafikkdata mv. dekkes innenfor berørte departementers budsjettrammer. Målsettingen om å gi politiet tilstrekkelig kompetanse og utvikle nye etterforskningsmetoder vil kunne medføre økte bevilgninger, og må vurderes i fremtidige budsjetter.

Hvor langt regjeringen lykkes med å nå målene, vil være avhengig av det framtidige økonomiske handlingsrommet og må vurderes opp mot andre behov og prioriteringer.

Utgitt av:
Forsvarsdepartementet
Justis- og beredskapsdepartementet

Bestilling av publikasjoner:
Departementenes sikkerhets- og serviceorganisasjon
www.publikasjoner.dep.no
Telefon: 22 24 00 00
Publikasjoner er også tilgjengelige på:
www.regjeringen.no
ISBN papirutgave: 978-82-7924-097-6
ISBN elektronisk utgave: 978-82-7924-098-3
Publikasjonskode: S-1029 B
Design og layout: Konsis Grafisk
Trykk: Departementenes sikkerhets- og serviceorganisasjon
11/2019 – opplag 100