Veiledning til forskrift om elektronisk kommunikasjon med og i forvaltningen

Forskrift om elektronisk kommunikasjon med og i forvaltningen trådte i kraft 1. juli 2002. Formålet med forskriften har vært å utarbeide et felles regelverk som legger rammene for sikker og effektiv bruk av elektronsk kommunikasjon med og i forvaltningen. Forskriften skal fremme forutsigbarhet og fleksibilitet, samt legge til rette for samordning av sikre og hensiktsmessige tekniske løsninger.

Temaet i forskriften vil være ukjent for mange. Arbeids- og administrasjonsdepartementet har derfor gitt Statskonsult i oppdrag å utarbeide en veileder til forskriften. Veilederen inneholder en generell introduksjon til temaet "elektronisk kommunikasjon", samt forklaringer til de enkelte bestemmelsene i forskriften.

Veilederen som publiseres er under stadig forbedring, blant annet på bakgrunn av innspill fra brukerne av forskriften. Vi anbefaler derfor brukerne jevnlig å sjekke nettstedet for oppdateringer.

Veiledning til forskrift om elektronisk kommunikasjon med og i forvaltningen

Del I Moderne e-forvaltning krever moderne regelverk

Denne veiledningen handler om hvordan forvaltningen skal legge til rette for å kommunisere elektronisk i forbindelse med saksbehandling og forvaltningsvirksomhet på en måte som er brukervennlig, effektiv og tilstrekkelig sikker. Veiledningen knytter seg til en ny forskrift til forvaltningsloven. Forskriften gjelder fra 1.7. 2002. Arbeids- og administrasjonsdepartementet forvalter forskriften.

Fjerne hindre, legge til rette

Et stort dugnadsarbeide fra departementenes side har kartlagt og fjernet, ved regjeringens og Stortingets hjelp, juridiske hindre for elektronisk kommunikasjon i lover og forkrifter.[1] Neste fase er positivt å legge til rette for elektroniske løsninger, også med juridiske virkemidler. Det er nettopp dette forskriften om elektronisk kommunikasjon gjør, på sitt område. Den gir et viktig rammeverk og utgangspunkt, med adgang til å gi mer detaljerte regler på enkelte punkter. Forskriften bidrar til at et formelt grunnlag for elektronisk kommunikasjon i forvaltningen, mellom forvaltningsorganer, og mellom forvaltningen og privat sektor (publikum og næringsliv), er kommet på plass.

Noe av det som gjør elektronisk kommunikasjon forsvarlig, skyldes de positive mulighetene som gis av utviklingen knyttet til elektroniske signaturer og innholdskryptering. Begrepene forklares senere.

Reglene i den nye forskriften erstatter ikke andre regler for forvaltningens arbeid, men kommer som utdypende tillegg i forhold til elektronisk kommunikasjon.

Forskriftens regler gjør det ikke obligatorisk å kommunisere elektronisk, men hvis man gjør det, for eksempel med bruk av elektroniske signaturer og innholdskryptering, skal reglene følges. Reglene gir imidlertid betydelig valgfrihet til virksomhetene, innenfor visse rammer.

Forskriften er ikke ment som en uttømmende regulering av alt som er relevant i forhold til elektronisk saksbehandling, arkivering og kommunikasjon i forvaltningen. Noen temaer er angitt med stikkordene ”digitale eller elektroniske signaturer” og ”innholdskryptering”. Fordi disse temaene er litt fremmede og vanskelige for de fleste, er hensikten med denne veiledningen å bidra til å gjøre temaet mer kjent - alminneliggjøre det (del I) - og i tillegg gi

[1] Se e-Regelprosjektet i regi av Nærings- og handelsdepartementet http://www.dep.no/nhd/norsk/p10001272/eRegelprosjektet/index-b-n-a.html

noen konkrete kommentarer til de enkelte paragrafene (del II). På denne måten håper vi det blir lettere både å forstå meningen med forskriften, og å følge den.

Forskriftens plass i regeljungelen

I Norge har vi flere sentrale lover og forskrifter som gir regler om hvordan saksbehandlingen i forvaltningen skal foregå; forvaltningsloven, offentlighetsloven, arkivloven og personopplysningsloven, alle med forskrifter. Det er sammen med disse sentrale lovene og forskriftene den nye forskriften har sin plass, med hele forvaltningen som virkeområde, kommuner, fylkeskommuner og staten. Vi har også en instruks internt i statsforvaltningen om beskyttelse mot uvedkommendes innsyn i dokumenter, beskyttelsesinstruksen. I tillegg har vi, for hele landet, sikkerhetsloven med mange forskrifter, som skal forebygge mot trusler som spionasje, sabotasje og terrorhandlinger. Objekt for disse truslene er rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. I sikkerhetsloven med forskrifter gis det også regler knyttet til elektronisk kommunikasjon og kryptering, men da i forhold til informasjon som er sikkerhetsgradert for å forebygge de nevnte truslene mot rikets sikkerhet mv.

I tillegg til disse sentrale lovene finnes det en rekke særlover med forskrifter på sektorområder. Som eksempel kan nevnes regelverket på skatte-, toll og avgiftsområdet. Til sammen gir de sentrale og sektorvise regelverkene et relativt komplekst og fragmentarisk bilde av rettstilstanden, som nok kan være uoversiktlig, men som gir atskillig fleksibilitet. Reglene er først og fremst forsøkt tilpasset de enkelte livs- og saksområdene og i mindre grad tilpasset den summen av ulike regelverk som en del må etterleve. Dette er også en grunn til å være bevisst på hva de enkelte regelverkene handler om og på hvilke områder de gjelder, hvor det ene slutter og det andre begynner og hvor det er overlappinger. I denne veiledningen er det ikke plass til å gjøre rede for alle disse forholdene, men vi vil prøve å plassere den nye forskriften inn i dette noe sammensatte regel-terrenget.

Forvaltningsloven og ny forskrift – effektivitet og rettssikkerhet

Forvaltningsloven kom i 1967 etter et langt forarbeid. Rettssikkerheten for borgerne skulle ikke være dårligere ved saksbehandling i forvaltningen enn for domstolene. Dette var et ambisiøst mål, som reglene skulle bidra til å nå.

Når forvaltningsorganer treffer vedtak som angår enkeltpersoner eller juridiske personer, er de bundet av regler som ikke overlater for mye til forvaltningens skjønn. En god del må i praksis likevel overlates til forvaltningens skjønn i det enkelte tilfelle, men innenfor de rammene regelverket setter. Slike regler skal generelt være enkle å finne, lette å forstå og ikke endres for hyppig. I tillegg til å være bundet av regler om innholdet i vedtakene, er forvaltningen bundet av regler om saksbehandlingen. Dermed blir det lettere for den enkelte å forutberegne sin rettsstilling, å se at like saker behandles likt, kort sagt at rettssikkerheten ivaretas. I tillegg, eller som en del av dette, skal forvaltningen balansere mellom henholdsvis betryggende og rask behandling.

Effektivitet og rettssikkerhet var slagord i forbindelse med tilblivelsen av forvaltningsloven. De gjelder også for denne nye forskriften om elektronisk

kommunikasjon , som er hjemlet i en ny § 15 a i forvaltningsloven. Den er også hjemlet i § 5 i lov om elektronisk signatur, som omtales senere.

Forskriften skal ta vare på viktige normer i forvaltningsloven, pluss noen til, når vi beveger oss over i en forvaltning med elektronisk kommunikasjon mellom publikum, næringsliv og forvaltningen og internt i forvaltningen. Men husk at det er mye forskriften ikke tar opp, f eks gir den ikke konkrete regler for *hvordan* forvaltningen skal *lagre* signatur og sertifikat (begrepene blir forklart senere), og den gir ikke konkrete oppskrifter på *interne rutiner* for arkiv, postmottak og ansatte for øvrig ved behandling av digitalt signerte og/eller krypterte dokumenter. Dette overlates til det praktiske liv. Forskriften gir derimot en rekke regler av overordnet karakter på et område som fremdeles lukter av pioner-ånd, og der regelgivningen faktisk ligger noe i forkant av utviklingen.

En forutsetning for at reglene i forskriften skal kunne virke etter hensikten, er selvsagt at både forvaltningen og de private parter kjenner reglene og faktisk er i stand til å følge dem. Ved behov kan man kontakte Arbeids- og administrasjonsdepartementet for nærmere avklaringer og mer informasjon. Se i menyen på nettsiden; **kontaktinformasjon**, for nærmere opplysninger om hvem man kan kontakte og stille spørsmål til.

Hva handler elektroniske signaturer og innholdskryptering om?

Disse begrepene brukes i forskriften, og er en del av temaet *informasjonssikkerhet*, som er et fagfelt som kan bidra til tryggere kommunikasjon over usikre nettverk som Internett.

For å bidra til en bedre forståelse av en viktig side ved forskriften gir vi nedenfor en kort omtale av deler av fagfeltet informasjonssikkerhet og forklaring på en del viktige begreper. Kjernen i dette er det som kalles s*ikkerhetstjenester* (ikke å forveksle med nasjoners "hemmelige tjenester" eller lignende). Sikkerhetstjenestene vi her omtaler, er i hovedsak følgende: autentisering, integritet, ikke-benekting og konfidensialitet. Disse tjenestene er uttrykk for teknikkuavhengige behov, som er relativt stabile over tid.

Sikkerhetstjenester kan ivaretas av sikkerhets*teknikker* eller *–mekanismer*, som kryptering og digitale signaturer. Disse er teknikkavhengige og tidsavhengige forhold – Cæsar krypterte på sin måte med suksess ca 50 år før Kristus, og Thomas Jefferson krypterte på en annen måte tidlig på 1800-tallet. I dag gjøres det elektronisk ut fra de produktene som til enhver tid er på markedet. Den aktuelle forskriften bygger på bl.a. kryptering og digitale signaturer, med det som kalles offentlig nøkkelkryptografi[2], med hjelp fra tredjeparter, som viktige ingredienser. Men også vanlig kryptering med like nøkler kan være aktuelt. Mer om slike ting senere.

[2] At teknikken kalles *offentlig* nøkkelkryptografi må ikke forveksles med *det offentlige.* Begrepet har ingenting med det offentlige å gjøre, men at den ene nøkkelen i et nøkkelpar skal være offentlig tilgjengelig for alle. Dette er en forholdsvis ny teknikk, i motsetning til den gamle, der begge nøklene måtte holdes absolutt hemmelige, - med de problemer dette førte med seg, ikke minst i forhold til distribusjon av nøkler til (alle) de som skulle delta i kommunikasjonen.

Hva oppnår en ved å bruke disse teknikkene? Jo, avsendere av elektroniske meldinger kan identifisere seg. Mottakerne kan få bekreftet eller sannsynliggjort at identiteten stemmer når det gjelder personer, roller, maskiner og systemer. Vi kan oppdage om innholdet i det vi sender kommer frem uten endringer, og vi kan få bevis som gjør det vanskelig for mottaker eller avsender i ettertid å benekte det som er gjort. Dessuten kan vi sende og motta meldinger med behov for skjerming mot uvedkommendes blikk. Alt dette kan vi gjøre, selv om vi kommuniserer ved hjelp av åpne og utrygge nettverk.

Som vanlige brukere trenger vi ikke fullt ut å forstå hvordan teknikken fungerer, enten vi er ansatte i forvaltningen, i privat sektor eller er borgere, bare vi klarer å bruke den i praksis, - og med tilstrekkelige kunnskaper til å være skeptiske og på vakt der hvor det kan være grunn til det. For brukerne blir dette muligheter man med letthet velger på skjermen, som et klikk eller to på en meny. Mye av det tekniske som skal skje, tar systemet seg av, ofte automatisk - forutsatt at visse ting er på plass, og at dette skjer på en trygg måte, med kunnskapsrike og aktsomme brukere. Forskriften vil med sine regler bidra til at vi får disse viktige forutsetningene på plass, og dermed legge til rette for en bedre og sikrere elektronisk offentlig forvaltning.

Litt mer om informasjonssikkerhet – sentrale begreper

Utviklingen av det moderne informasjonssamfunnet har ført til at de fleste former for informasjon skapes, behandles og utveksles i digital form. Nasjonale og internasjonale infrastrukturer har åpnet for nye veier i elektronisk samhandling. Utviklingen innebærer at prosedyrer forankret i papirbaserte rutiner i stadig flere tilfeller må finne nye og digitale former. Bruk av elektroniske signaturer er eksempelvis en teknikk som kan benyttes til å ”signere” digital informasjon. Metoden ivaretar flere av de samme funksjonene som en håndskreven signatur i forhold til et papirdokument, og en del av dem til og med på en bedre måte. I tillegg har metoden nyttige funksjoner som den håndskrevne underskriften ikke har. Teknikken får betydning for jussen (og omvendt) bl.a. i sammenhenger hvor det å ”skrive under” spiller en rolle.

Samtidig med den teknologiske utviklingen er det skapt et stort og voksende behov for å integrere sikkerhetsløsninger i de vanlige systemene vi bruker i hverdagen, både i forvaltningen, i næringslivet og som privatpersoner. Den nye forskriften om elektronisk kommunikasjon bygger på en spesiell teknologisk utvikling, som vi skal se litt mer på nedenfor.

Fagfeltet informasjonssikkerhet har til oppgave å utvikle metoder og teknikker som kan bidra til en trygg og sikker elektronisk hverdag og forvaltning. Et informasjonssystem kan sikres ved at vi anvender veldefinerte sikkerhetstjenester, som beskytter informasjonen mot identifiserte trusler. Sikkerhetstjenestene kan bidra til å realisere muligheter som uten disse tjenestene ville vært vanskelige eller umulige. Denne forskriften er et eksempel på dette.

Sikkerhetstjeneste er i denne sammenhengen en overordnet betegnelse på en egenskap eller ytelse som vi ønsker eller trenger i et system, og som *ikke sier*

noe om hvilken teknologi som benyttes for å realisere løsningen. Begrepet brukes i forskriften. En sikkerhetstjenester realiseres eller implementeres ved hjelp av spesifikke sikkerhetsmekanismer eller sikkerhetsteknikker. Noen av de viktigste sikkerhetstjenestene er omtalt kort nedenfor:

- Autentisering er en sikkerhetstjeneste som skal sikre at opplysninger som identifiserer en enhet (person, maskin, system, nettside, prosess) virkelig stemmer. I forbindelse med utveksling av elektroniske meldinger vil bruk av autentisering sannsynliggjøre at avsenderen av en melding faktisk er den vedkommende gir seg ut for å være og dermed knytte avsenderen til meldingens innhold. Brukerautentisering av personer som logger seg på et elektronisk datasystem er spesielt viktig og danner grunnlaget for at vi kan stole på tilknyttede sikkerhetstjenester. Behovet for autentisering vil avhenge av hvilken type melding det er tale om å utveksle. I de fleste transaksjoner vil det være ønskelig eller nødvendig å få etablert tilfredsstillende autentisering, f eks av hensyn til økonomiske verdier, korrekt saksbehandling, personvern, mv.

- Integritet er en sikkerhetstjeneste som skal sørge for at informasjon ikke kan endres under lagring eller transport uten at det oppdages. Hvis skade kan oppstå ved at innholdet i en melding blir endret, vil det være behov for å benytte en integritetstjeneste. Denne typen integritet for data, informasjon, melding eller dokument må ikke forveksles med informasjonens kvalitet, som er knyttet til riktigheten av de opplysninger som er formidlet. Informasjonens integritet kan være i behold selv om opplysningene objektivt sett er uriktige, dersom det var disse opplysningene avsenderen faktisk sendte (”Shit in, shit out”).

- Ikke-benekting er en sikkerhetstjeneste som gir mottakeren av et dokument en rimelig grad av sikkerhet for at den angitte avsender ikke senere kan nekte å ha sendt dokumentet. Hvis avsenderen av et dokument har behov for å vite med en viss grad av trygghet at sendingen er mottatt, må imidlertid mottakeren ved en handling gi fra seg en kvittering for mottaket, slik at han eller hun ikke senere kan nekte å ha mottatt dokumentet.

- Konfidensialitet er en sikkerhetstjeneste som skal sikre at informasjon ikke blir gjort tilgjengelig for uvedkommende. Informasjonen kan ved kryptering beskyttes mot innsyn under transport og lagring. Selv om uvedkommende skulle få tak i informasjonen, vil den være uleselig uten den riktige nøkkelen til å gjøre teksten leselig eller forståelig. Forvaltningsloven pålegger taushetsplikt om det som kalles noens personlige forhold og konkurranseutsatte opplysninger, uten å si hvordan plikten skal ivaretas utover kravet om at det skal være *på betryggende måte*. Næringslivet har behov for å skjerme sine forretningshemmeligheter, også i kommunikasjon med forvaltningen, mens privatpersoner har behov for å skjerme bl a sin personlige korrespondanse eller sine personlige opplysninger. På enkelte områder finnes det konkrete regler for sikker elektronisk behandling av slike opplysninger, f eks på personvernområdet og når det gjelder rikets sikkerhet.

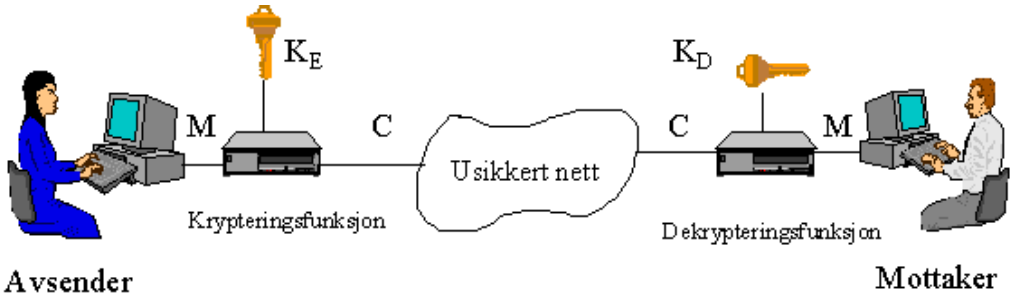
- Sporbarhet er en sikkerhetstjeneste som skal sikre at viktige hendelser i systemet kan spores til ansvarlige personer eller prosesser. Autentiseringstjenester er ofte nødvendige for sporbarhet.

- Tilgjengelighet er en sikkerhetstjeneste som skal sørge for at informasjon og ressurser er tilgjengelige for brukere som har rettmessig adgang til informasjonen, når de har behov for det, og på en effektiv måte. Dette er generelt viktig for å få ”hjulene til å gå rundt” under ulike forhold, kanskje særlig tidskritiske.

Sikkerhetsmekanismer eller ***sikkerhetsteknikker*** realiserer, som tidligere nevnt, sikkerhetstjenester. Slike mekanismer eller teknikker kan være av fysisk, organisatorisk eller logisk (systemteknisk) karakter. Tradisjonelt har vi løst konfidensialitet ved bruk av forseglede konvolutter og kurérpost, mens tilsvarende elektronisk kommunikasjon blir beskyttet ved hjelp av kryptering. Kryptering forvrenger det digitale signalet slik at bare rettmessig avsender og mottaker ser det opprinnelige innholdet i klartekst. Kryptografi er et omfattende teknologisk fagfelt, men de grunnleggende idéene er enkle. For å lette forståelsen av underliggende problemstillinger på dette området, noe forskriften i atskillig grad bygger på, gir vi her en kortfattet fremstilling av noen sentrale begreper.

Se NOU 2001:10, Uten penn og blekk, for nærmere omtale og illustrasjoner mv. : http://www.dep.no/aad/norsk/publ/utredninger/NOU/002001-020005/index-dok000-b-n-a.html

Symmetrisk krypto
Forsvar og diplomati har i århundrer gjort bruk av kryptering for å sikre kommunikasjon. Figuren under gir et inntrykk av hva som skjer når kryptering foregår ved hjelp av moderne teknikk.



Figur a: Kryptering av dataforbindelse

Avsenderen har et dokument M i lesbar form, ofte kalt klartekst. Før den kan sendes over til mottakeren må klarteksten gjennomgå en krypteringsfunksjon (”kvern”), der den blandes med en krypteringsnøkkel K_E. Resultatet blir en uforståelig melding, chiffertekst (C i figuren), som uvedkommende ikke kan tyde. Bare den rettmessige mottakeren sitter på den korrekte dekrypteringsnøkkelen K_D , som gjør det mulig å omforme C tilbake til klarteksten M. Det er derfor helt avgjørende for sikkerheten i systemet at ikke uvedkommende får tak i denne nøkkelen.

I konvensjonelle eller symmetriske kryptosystemer benyttes samme nøkkel til kryptering og dekryptering i den forstand at de er like. Vi vet altså at $K_E = K_D$. Det betyr at kryptonøkler må distribueres på en sikker måte til begge parter før

den krypterte forsendelsen kan gjennomføres. Slik nøkkelfordeling stiller store organisasjonsmessige og sikkerhetsmessige krav og er derfor en kostbar og krevende løsning dersom antall brukere blir stort.

Selve krypteringsfunksjonen skjer ved hjelp av en krypto-algoritme, som beskriver på en eksakt måte hvordan klartekst og nøkkel skal blandes sammen. Det finnes mange ulike algoritmer som er kommersielt tilgjengelige, men foreløpig ingen felles internasjonal standard på området. Den amerikanske standarden DES (Data Encryption Standard) benyttes mye, men denne er over 25 år gammel, og arbeidet med å få frem en erstatning er nå gjennomført. National Institute of Standards and Technology (NIST), som er et organ under næringsdepartementet i USA, har nylig vedtatt en ny standard symmetrisk krypteringsaltoritme, Advanced Encryption Standard (AES). Den skal kunne brukes av den amerikanske forvaltningen og av andre. Den kan eksporteres til andre land.

Datatilsynet anbefalte pr september 2001 å bruke DES128, opplyst å være en 112 bits effektiv nøkkel.

Asymmetrisk krypto
I et asymmetrisk eller offentlignøkkel kryptosystem (eng. public key cryptosystem) er det ikke lenger noen enkel sammenheng mellom krypteringsnøkkel og dekrypteringsnøkkel. I figuren ovenfor vil det bety at det ikke lenger er noe krav om at krypteringsnøkkelen K_E skal holdes hemmelig. I slike systemer vil hver bruker i systemet få laget sitt eget nøkkelpar (K_E , K_D). Den offentlig tilgjengelige nøkkelen K_E kan nå fritt distribueres til alle som vil sende krypterte meldinger til den aktuelle brukeren. At den kalles *offentlig* må ikke misforstås i retning av at den som sådan har noe med *det offentlige* å gjøre. Poenget er bare at den ene nøkkelen rett og slett kan og skal gjøres tilgjengelig for alle som har eller får behov for den. Det er dette som er det fundamentalt nye, og som de siste tiårene har rokket ved det som var etablerte sannheter gjennom tusener av år innenfor dette faget, at begge nøkler måtte være like, og hemmelige. Kravet til hemmelighold av nøkkelen fra symmetrisk krypto er erstattet av et krav om at den offentlig tilgjengelige krypteringsnøkkelen må være ekte eller autentisk, samt krav om sikre opplysninger om hvem den hører til.

Dette betyr at asymmetrisk krypto er best egnet til å løse de klassiske problemene knyttet til nøkkelfordeling. Men også her kreves det omfattende organisasjonsmessige og tekniske løsninger for å etablere den infrastrukturen som skal til for å distribuere offentlige nøkler på en god måte. Bruk av nøkkelsertifikater og katalogtjenester er viktig for å få til dette.

I praksis er alle asymmetriske kryptosystemer for langsomme til å kryptere store mengder data eller trafikk i sanntid. Det er derfor vanlig å lage blandingssystemer, der man benytter det asymmetriske systemet til å fordele trafikknøkler som går inn i symmetrisk kryptering av selve meldingen.

Det mest utbredte asymmetriske kryptosystemet kalles RSA, etter opphavsmennene Rivest, Shamir og Adleman. Men det finnes også en rekke

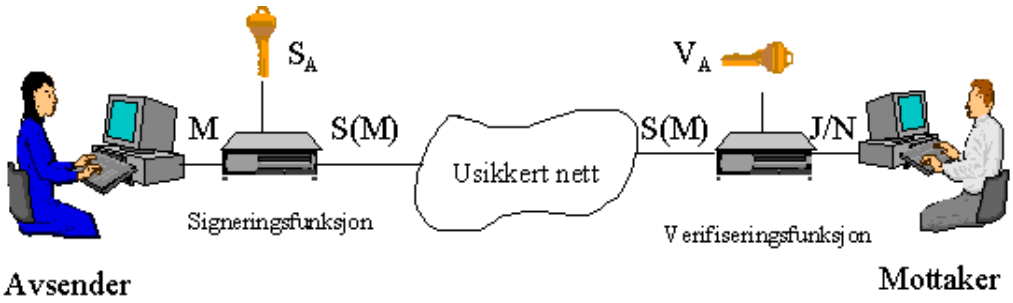
andre teknikker som særlig benyttes til å etablere et godt opplegg mellom de kommuniserende partene.

Teknologien i asymmetriske systemer er en helt annen enn i de symmetriske systemene, bl a vil kravene til nøkkellengder være helt forskjellige. En kan derfor ikke sammenligne nøkkellengder mellom DES og RSA. En god egenskap ved mange asymmetriske løsninger er at de enkelt kan skaleres opp til et ønsket sikkerhetsnivå.

Digitale signaturer
Omtalen av krypto ovenfor beskriver hvordan teknikkene brukes for å oppnå konfidensialitet, altså gjøre det tekstlige innholdet uleselig for uvedkommende. Omvendt kan den som rår over den hemmelige nøkkelen bruke den på en tekst, og sende dette av gårde, men ettersom alle som har tilgang til den tilhørende offentlige nøkkelen da kan åpne teksten, er det uaktuelt å sende tekst på denne måten som ikke skal kunne leses av andre enn noen få. Derimot vet mottakeren(e) at det er den *ene* hemmelige nøkkelen som er brukt, siden de får åpnet dokumentet med den *andre*, tilhørende offentlig tilgjengelige nøkkelen. Avsender oppnår dermed å identifisere seg, i hvert fall hvis vi kan stole på at det er avsender som har brukt den hemmelige nøkkelen til å signere.

En spesiell variant er det som kanskje litt villedende kalles digitale signaturer. Digitale signaturer er også eksempel på en teknologi innenfor området kryptering (asymmetrisk krypto), og her brukes nøklene denne andre veien (som ikke skjuler innholdet). Teknikken har som hovedoppgave å realisere andre sikkerhetstjenester som autentisering, integritet og ikke-benekting. Det betyr at innholdet i det som signeres, eller som teknikken digital signatur brukes på, ikke skjuler teksten for uvedkommende. Men hvis meldingen lar seg åpne eller verifisere, vil mottakeren vite hvem som har sendt den, og slik sett ”skrevet under” (oppgitt identitet er mulig å bekrefte/autentisere), at meldingen er kommet uforandret frem (meldingens integritet er i behold), og det foreligger ut fra disse kjensgjerninger bevis som gjør det vanskelig for avsender å hevde at ”det var ikke han!”. Dette er den ”enkle og folkelige forklaringen”. Nedenfor kommer en litt mer presis fremstilling.

Figuren illustrerer hvordan et digitalt signatursystem fungerer.



Figur b: Bruk av digitale signaturer

Avsenderen i et slikt system genererer et nøkkelpar som består av en hemmelig signeringsnøkkel S_A og en offentlig verifiseringsnøkkel V_A. Når avsenderen ønsker å signere et elektronisk dokument M, sendes M sammen med

signeringsnøkkelen S_A inn i en signeringsfunksjon. Resultatet av denne prosessen er en signert melding S(M). I de fleste signatursystemene består den signerte meldingen i praksis av den opprinnelige meldingen uberørt og i klartekst, etterfulgt av et signaturfelt, hvor selve signaturen er en komplisert blanding av M og S_A.

Når mottakeren får en slik signert melding, vil han altså ha direkte tilgang til selve M i klartekst. For å verifisere at dette virkelig er en ekte melding fra avsenderen, vil han sende M sammen med den offentlige verifiseringsnøkkelen $V_{A,}$ som tilhører avsenderen, inn i en verifikasjonsfunksjon. Resultatet av denne prosessen vil være et godkjent eller ikke-godkjent utfall. Operasjonen skjer automatisk, ved museklikk på korrekt valg. Ved et godkjent utfall vil mottakeren vite følgende:

?? M kommer sannsynligvis fra avsenderen, siden det bare er hun som besitter den hemmelige signaturnøkkelen som må til for å lage den digitale signaturen. Vi har altså autentisering av melding og avsender.

?? Meldingen eller signaturfeltet kan ikke bevisst eller ubevisst ha blitt endret under overføringen. Det betyr at krav om meldingens integritet er oppfylt.

?? Avsenderen kan vanskelig i ettertid nekte for å ha sendt meldingen. Mottakeren kan sannsynliggjøre overfor en tredjepart (f eks domstol) at det var avsenderens hemmelige nøkkel som ble benyttet for å signere meldingen, ved gjentatt demonstrasjon av verifikasjonsfunksjonen. Den digitale signaturen gir derfor en ikke-benektingstjeneste.

?? Signaturen beskytter også mot at mottakeren endrer meldingen og prøver å få den akseptert som en ekte melding. Mottakeren kjenner ikke signeringsnøkkelen S_A som er nødvendig for å lage en signatur som passer på den modifiserte meldingen.

For et digitalt signatursystem vil det være nødvendig å etablere en infrastruktur som sikrer at alle parter får tilgang til de ulike nøklene som trengs. Alle skal ha tilgang til alle verifiseringsnøklene.

Kort oppsummert kan vi si om nøkkelsystemer der den ene nøkkelen er offentlig tilgjengelig og den andre fortsatt må holdes hemmelig:

I et signatursystem er det kun en person som kan signere ved hjelp av den hemmelige signeringsnøkkelen, men det er mange som kan verifisere (få bekreftet (få sannsynlighet for) ektheten i) signaturen ved hjelp av den offentlig tilgjengelige verifiseringsnøkkelen. I et system for kryptering er det mange som kan kryptere innholdet i meldinger (gjøre teksten uleselig) ved hjelp av den offentlige krypteringsnøkkelen, men det er kun en som kan dekryptere (få frem leselig tekst) ved hjelp av den tilhørende hemmelige dekrypteringsnøkkelen.

Sertifikater
Når de offentlige nøklene blir så viktige, hvordan kan en vite at den offentlige nøkkelen for henholdsvis kryptering av innholdet i en melding, og/eller den offentlige nøkkelen for verifisering av en signatur, faktisk hører til den vi vil kommunisere med og ikke noen andre? Det gis ikke noe enkelt svar på dette spørsmålet.

For å få etablert sikkerhet for at en signatur er korrekt, kan man søke hjelp hos en tredjepart (av og til flere, kanskje med litt ulike roller), som kan *bekrefte* at en bestemt offentlig nøkkel faktisk hører til en bestemt person, som altså har den tilhørende hemmelige nøkkelen i nøkkelparet. Dette forutsetter at tredjeparten kontrollerer og/eller går god for at en person er rette vedkommende (entydig navn), f eks ved personlig møte hvor det er fremvist akseptabelt identifikasjonsbevis. På grunnlag av dette utsteder eller lager tredjeparten de to nøklene som må til for å få til den aktuelle kommunikasjonen (krypteringen og/eller signeringen). Samtidig lages det en erklæring fra utstederen som bekrefter at *den bestemte offentlige nøkkelen hører til den identifiserte personen*. Det er denne bekreftelsen som kalles ”offentlig nøkkelsertifikat”.

Vi får altså et sertifikat eller en bekreftelse på en sammenheng, som sannsynliggjør at vi har med rett person å gjøre, i hvert fall hvis tredjeparten er til å stole på. Dette siste er et kapittel for seg, som vi ikke kan gå særlig inn i her. I NOU 2001:10 Uten penn og blekk er det sagt mer om det, se bl.a. kapitel 3.2.5. Hvilket grunnlag man har for å stole på en sertifikatutsteder og de sertifikatene som utstedes, vil variere i mange sammenhenger, ut fra ulike sikkerhetsbehov og hva som tilbys på markedet.

Ny lov om elektronisk signatur og kvalifiserte sertifikater

I Norge fikk vi i 2001 en lov om elektronisk signatur, som i hovedsak gir regler nettopp om sertifikatutstedere i signatursammenheng, og det loven kaller kvalifiserte elektroniske *signaturer* og sertifikater. Det er opp til de utstederne som finnes på markedet om man vil kalle sine sertifikater for *kvalifiserte*. Men *hvis* man gjør det, er det en *plikt* å følge loven med forskrifter. Da kommer sertifikatutstederen inn under et regime som skal gjøre det trygt for brukerne å kjøpe tjenester fra utstederen. Reglene i Norge er i overensstemmelse med et EU-direktiv om dette, slik at det er felles, harmoniserte regler i hele EØS-området, til glede bl a for alle som skal kommunisere på tvers av disse landegrensene. Det gjenstår imidlertid å se om de relativt få markedsaktørene på dette smale området vil finne det attraktivt å kalle sine sertifikater for kvalifiserte og dermed underlegge seg de aktuelle reglene om bl a erstatningsansvar, kvalitetssikring av egen organisasjon og produksjon, mv. Hvis det er penger å tjene, blir det selvfølgelig attraktivt.

Loven om elektronisk signatur har *to* paragrafer som gir regler som gjelder *alle* signaturer med sertifikater, enten de er kvalifiserte eller ikke. I korthet går det ut på å erklære at også ikke-kvalifiserte signaturer kan oppfylle krav om rettslig gyldighet (slik som de kvalifiserte) (jf § 6), dessuten at enhver sertifikatutsteder må følge grunnleggende viktige personvernregler (gitt i § 7), og at Datatilsynet er tilsynsorgan for at disse reglene overholdes. Det bestemmes bl a at en sertifikatutsteder bare får innhente personopplysninger direkte fra den det

gjelder, eller med uttrykkelig samtykke, og at slike opplysninger bare må brukes hvis det er absolutt nødvendig i forbindelse med sertifikatet (som altså bekrefter at en bestemt offentlig nøkkel tilhører en bestemt person, virksomhet, eller lignende). Datatilsynet forvalter og fører tilsyn også med personopplysningsloven med forskrifter, som også gjelder på dette området, men de nevnte reglene i § 7 er altså spesielt rettet inn mot virksomheten til alle sertifikatutstedere, enten sertifikatene kalles kvalifisert eller ikke. Dermed får §§ 6 og 7 i loven om elektronisk signatur et virkeområde som er betydelig større på disse to punktene, mens virkeområdet for resten av loven er begrenset til utstedere av kvalifiserte sertifikater.

Hvis det i fremtiden viser seg at utviklingen skjer mest på det såkalte ikke-kvalifiserte nivået, vil loven om elektronisk signatur få mindre direkte virkning. På den annen side er det lite ved loven som hindrer markedet i å velge andre og eventuelt enklere løsninger, innenfor rammene av de to generelle §§ 6 og 7. I en tidlig fase av utviklingen for elektroniske signaturer vil det ikke være unaturlig om både forvaltningen og privat sektor, og de få sertifikatutstederne, prøver seg frem med forholdsvis enklere løsninger til mer erfaring er vunnet.

Uansett hvordan dette utvikler seg, vil forskriften om elektronisk kommunikasjon med og i forvaltningen gi regler på selvstendig grunnlag, uavhengig av loven om elektroniske signaturer.

I loven om elektronisk signatur er det mest generelle og (antatt) teknologiuavhengige begrepet brukt (altså elektronisk signatur), men det er relativt klart at det er den mer presise teknologien eller mekanismen kalt digital signatur som ligger bak loven, og dessuten direktivet fra EU, som den bygger på. Dette gjelder for det loven kaller avansert elektronisk signatur, som forskriften om elektronisk kommunikasjon også omfatter (jf identiske definisjoner). De to omtalte paragrafene med større virkeområde omfatter også andre elektroniske signaturer, som ikke bygger på digitale signaturer. Digital signatur kan inngå som ett av flere tenkelige underbegrep under elektronisk signatur. Biometrisk baserte teknikker med for eksempel øye/iris-gjenkjenning og fingeravtrykk kan være et annet. PIN-koder kan være et tredje.

Forholdet mellom kryptering og signering

Dersom en har behov for beskyttelse av både integritet og konfidensialitet, kan digital signatur kombineres med påfølgende kryptering av innholdet i dokumentet eller informasjonen (innholdskryptering). Valg av tjenester må gjøres ut fra den verdien informasjonen har og de truslene eller mulighetene vi står overfor.

Innholdskryptering vil hindre uvedkommende innsyn i klarteksten eller innholdet i en kommunikasjon. Når slik teknikk brukes av forbrytere, vil det naturlig nok vanskeliggjøre eller umuliggjøre etterforskning og avlytting i regi av politi og myndigheter. Dette griper inn i forhold som kan ha med alvorlige forbrytelser å gjøre (narkotika og annen organisert kriminalitet) og med nasjonal sikkerhet.

De fleste land har lenge ført en streng eksportkontroll med teknologi som kan benyttes til kryptering. I mange dataprogrammer som selges fra USA er kryptofunksjonalitet hittil blitt fjernet eller sterkt redusert. Andre land fører også en streng regulering med nasjonal bruk av krypteringsteknologi. Konfidensialitet er derfor et område der det er langt vanskeligere å komme frem til internasjonale løsninger enn når det gjelder digitale signaturer og rene autentiseringstjenester.

OECD vedtok i mars 1997 retningslinjer for kryptopolitikk (som er oversatt til norsk, se Nærings- og handelsdepartementets nettsider). I retningslinjene anbefales medlemslandene å unngå umotiverte hindringer for bruk av kryptering, og at brukerne må fritt kunne velge mellom ulike krypteringsteknologier, og at teknologi og standarder må være styrt av markedets behov. Individets rett til å kommunisere uten andres uautoriserte innsyn må respekteres, og lovhjemlet adgang til kryptert kommunikasjon må respektere de nevnte prinsippene. Dette innebærer i henhold til retningslinjene at det er hensiktsmessig eller nødvendig å skille mellom krypteringsteknologi benyttet for henholdsvis innholdskryptering og signering, autentisering og intgritet. OECDs retningslinjer har som mål å fremme bruk av krypto og skape tillit til infrastrukturer, nettverk og systemer.

Flere land har senere endret sin politikk, bl.a. USA, som gradvis har lettet sine eksportrestriksjoner betydelig. Tendensen er at sivil sektor er en økende bruker av ulike kryptoløsninger, i forvaltning og næringsliv, og etter hvert for enkeltindivider. Tiden da krypto ble sett på som forbeholdt militærvesen og diplomati er forbi.

Problemstillingene rundt bruk og regulering av krypto er sammensatte. Det finnes asymmetriske kryptosystemer som også kan benyttes som signatursystemer. Den infrastrukturen som må etableres for å få systemene til å spille sammen, er lik fra land til land, og det må tas hensyn til at sikker elektronisk kommunikasjon ofte krever at tjenestene for både innholdskryptering og autentisering og signering er på plass.

Hovedtrekk i forskriften om elektronisk kommunikasjon med og i forvaltningen

Forskriften er som nevnt hjemlet i en ny § 15a i forvaltningsloven. Det er ikke foreslått å stille særskilte krav til kvalifiserte elektroniske signaturer som eventuelt skal benyttes ved kommunikasjon med og i offentlig sektor, slik det er adgang til etter lov om elektronisk signatur § 5. Forskriften er imidlertid også hjemlet i den nevnte paragrafen.

I samsvar med sitt mandat tok en arbeidsgruppe for forskriftsarbeidet i regi av Arbeids- og administrasjonsdepartementet utgangspunkt i anbefalinger fra PKI-utvalget, jf. NOU 2001:10 *Uten penn og blekk – Bruk av digitale signaturer i elektronisk samhandling med og i forvaltningen*, del IV, *Forslag til regulering av elektronisk kommunikasjon med og i forvaltningen*. Arbeidsgruppen ble orientert om høringsuttalelsene til NOU'en. Det ble gjennomført en rekke redaksjonelle og språklige endringer i forhold til anbefalingene i NOU'en, og noen nye bestemmelser har kommet til. Innholdsmessig er likevel forskriften i

det vesentlige i samsvar med anbefalingene. Det ble holdt en høringsrunde høsten 2001, med påfølgende bearbeiding og sluttføring våren 2002. Den ble vedtatt i statsråd 28.06.02, og gjelder fra 1.7.02.

Forskriftens formål og anvendelsesområde
Elektronisk kommunikasjon for annet enn litt uformelle eller private formål er fremdeles forholdsvis nytt for de fleste. Meddelelser av betydning sender de fleste av oss fortsatt på papir. I tråd med NOU'en om at det i alle fall på det nåværende tidspunkt er riktig å gå forholdsvis detaljert til verks i reguleringen, slik at partene vet *når* det kan benyttes elektronisk kommunikasjon og *hvordan* de skal gå frem, er forskriftsutkastet forholdsvis detaljert. På denne måten ønsker man å redusere usikkerhet, skape forutsigbarhet og trygghet og stimulere til økt bruk av elektronisk kommunikasjon. Samtidig er det lagt vekt på å beholde størst mulig grad av fleksibilitet for det enkelte forvaltningsorgan i forhold til å velge de fremgangsmåter og sikkerhetstjenester som er nødvendige og hensiktsmessige på det enkelte forvaltningsområde.

Forskriften gjelder for elektronisk kommunikasjon mellom forvaltningen og publikum og for elektronisk saksbehandling og kommunikasjon i forvaltningen (§ 1 nr. 2). Forskriften gjelder derimot ikke elektronisk kommunikasjon mellom private parter. En rekke av de hensyn forskriften bygger på gjør seg imidlertid gjeldende også ved kommunikasjon mellom private parter. I alle fall for virksomheter som driver utstrakt bruk av elektronisk kommunikasjon kan det være fornuftig å vurdere om enkelte av forskriftens prinsipper bør implementeres også i deres virksomhet.[3]

Alminnelige regler om elektronisk saksbehandling og tilrettelegging for elektronisk kommunikasjon
Innenfor rammen av relevant sektorlovgivning får det enkelte forvaltningsorgan stor grad av frihet til selv å velge i hvilken grad, og i så fall på hvilken måte, de vil legge til rette for elektronisk kommunikasjon. Publikum som vil kommunisere elektronisk med forvaltningen må benytte den fremgangsmåte som forvaltningsorganet har tilrettelagt for eller gitt anvisning på, f.eks. at all kommunikasjon vedrørende et forvaltningsområde skal foregå via en bestemt nettside, jf. § 2.

Henvendelser som ikke er underlagt spesielle krav til form eller fremgangsmåte i eller i medhold av lov eller forskrift, og som forvaltningsorganet heller ikke har stilt andre krav til, f.eks. ved å kreve bruk av en særskilt papirblankett eller angitt en spesiell nettside, kan rettes til forvaltningsorganets generelle elektroniske adresse, jf. § 3. Dette kan være en nettside for alminnelige henvendelser til organet eller en e-postadresse.

Det enkelte forvaltningsorgan kan stille krav om at bestemte sikkerhetstjenester skal benyttes hvis det kommuniseres elektronisk med forvaltningsorganet. Slike krav kan fastsettes individuelt eller generelt, f.eks. for et forvaltningsområde eller for en eller flere bestemte typer saker eller henvendelser. Valg av sikkerhetstjenester skal være i henhold til organets sikkerhetsstrategi, jf. om §

[3] http://www.dep.no/aad/norsk/publ/hoeringsnotater/002061-990018/#fotnote_4

11 nedenfor. På områder der det finnes krav til form eller fremgangsmåte som kan oppfylles ved hjelp av elektronisk kommunikasjon, skal forvaltningsorganet gi anvisning på hvilken fremgangsmåte og hvilke sikkerhetstjenester som kan eller skal benyttes for å oppfylle kravene, jf. § 4 nr. 5. Et eksempel kan være at loven krever at det skal benyttes en "… betryggende metode som autentiserer avsender …" e.l., jf. Ot.prp. nr. 108 (2000-2001) om fjerning av juridiske hinder mv, jf. e-regelprosjektet.

Forskriften inneholder videre bestemmelser om behandlingsmåten for henvendelser som ikke tilfredsstiller de krav som er stilt i eller i medhold av forskriften (§ 6), om betingelsene for når og hvordan underretning om vedtak og forhåndsvarsling kan skje i elektronisk form (§ 7), samt bestemmelser om bruk av elektronisk kommunikasjon i forbindelse med klage over enkeltvedtak (§ 8), innsyn i opplysninger og dokumenter (§ 9) og høring av forskrifter mv.(§ 10). Det er også gitt bestemmelser om arkivering av avansert elektronisk signatur og andre autentiseringsmekanismer (§ 26).

I denne del av forskriften er det kommet til to bestemmelser som er nye i forhold til NOU 2001:10. Dette gjelder for det første et krav om at forvaltningsorgan som mottar henvendelser i elektronisk form skal gi *bekreftelse* til avsender om at en henvendelse er mottatt (§ 5). Bestemmelsen er tatt inn for å unngå usikkerhet hos publikum med hensyn til hvorvidt en henvendelse er mottatt eller ikke og for å forebygge uheldige virkninger av tekniske eller andre feil som måtte føre til at en melding ikke kommer frem som forutsatt.

Det er også tatt inn en ny bestemmelse om oppbevaring og utlevering av sertifikater og bekreftede meldinger mv.(§ 27). Bestemmelsen innebærer at publikum, i forbindelse med en begjæring om innsyn i dokumenter som er signert med avansert elektronisk signatur, ikke skal kunne avspises med tilgang til dokumentets innhold, men også skal få tilgang til sertifikater og andre opplysninger som er nødvendige for verifisering av signaturen dersom den som begjærer innsyn ber om det.

Forvaltningsorganet skal også sørge for at publikum om nødvendig kan få tilgang til dokumentenes innhold i en annen form som gjør det mulig å dokumentere innholdet også overfor tredjepart. Dette kan f.eks. være i form av en elektronisk melding som er signert av forvaltningsorganets arkiv, etter at den er bekreftet og konvertert i henhold til forskriftens § 26, eller i form av en bekreftet papirutskrift dersom tredjepart f.eks. ikke kan behandle en signert elektronisk melding.

Krav til utarbeiding av sikkerhetsstrategi og koordinering av forvaltningens sikkerhetstjenester

Forvaltningsorgan som benytter eller ønsker å benytte sikkerhetstjenester for elektronisk kommunikasjon i sin saksbehandling skal utarbeide en strategi for informasjonssikkerhet i virksomheten ("sikkerhetsstrategi"), jf. § 11. Sikkerhetsstrategien vil være grunnlaget for bl.a. krav til bruk av sikkerhetstjenester i henhold til § 4. Sikkerhetsstrategien skal utarbeides i henhold til anerkjente prinsipper for informasjonssystemers sikkerhet,

eksempelvis relevante norske standarder på området (jf NS-ISO/IEC 17799 Utgave 1, 2001 Informasjonsteknologi - Administrasjon av informasjonssikkerhet). Det er i bestemmelsen angitt en del forhold som sikkerhetsstrategien skal inneholde.

Det er gitt hjemmel i forskriften til å utpeke et organ med koordineringsansvar for forvaltningens bruk av sikkerhetstjenester for elektronisk kommunikasjon, jf. § 28. Dette er ikke gjort ennå. Organet skal utarbeide krav til løsninger som anses hensiktsmessige for forvaltningens bruk av elektronisk kommunikasjon i ulike situasjoner og på ulike områder. Koordineringsorganet skal også vurdere hvorvidt sikkerhetsløsninger som er tilgjengelige i markedet tilfredsstiller de krav organet har stilt. Hensikten er å sikre samvirke mellom løsninger i ulike forvaltningsorgan og å lette anskaffelsesprosessen for det enkelte organ ved å gjøre krav og vurderinger tilgjengelige Hensikten er også å sikre forvaltningsorganene fleksibilitet og utvikling i markedet ved at det kan velges mellom ulike løsninger. Koordineringsorganet kan også iverksette andre koordinerende tiltak.

Anskaffelse og bruk av tjenester for sikring av autentisering, ikke-benekting, integritet og konfidensialitet
Forskriften inneholder videre bestemmelser om bruk av sertifikat som identifiserer forvaltningsorgan og ikke den enkelte saksbehandler ("virksomhetssertifikat") (§§ 12 og 13), om anskaffelse av utstyr og data til ansatte for bruk av sikkerhetstjenester (§ 24), om veiledning av ansatte og publikum (§§ 17 og 20), om restriksjoner på bruk av sertifikat mv.(§ 14),om krav til oppbevaring og bruk av signaturfremstillingsdata og dekrypteringsdata mv.(§ 15) samt varslingsplikt ved tap eller mistanke om misbruk av slike data (§ 16).

Det er tatt inn en bestemmelse om adgang til å hindre bruk av sertifikat mv. i forvaltningssammenheng dersom en person misbruker sine signaturfremstillingsdata eller adgangen til å kommunisere elektronisk med forvaltningen (§ 19). Det er også tatt inn bestemmelser om innholdskryptering mv. (§§ 21 til 23).

Det er kommet til en bestemmelse om krav til kontroll av sertifikater og tilbaketrekkingslister (§ 18). Bestemmelsen gjelder på områder der det er krav om bruk av avansert elektronisk signatur. Der det måtte finnes et slikt krav i lovgivningen, eller der et slikt krav er fastsatt av forvaltningsorganet, antas det å være et reelt behov for å oppnå den sikkerhet som en avansert elektronisk signatur kan gi. Det er derfor stilt krav til kontroll av at signaturen kan verifiseres, at sertifikatet er egnet for den aktuelle anvendelse og at det er utstedt av en sertifikatutsteder som er anerkjent av koordineringsorganet eller kan aksepteres i henhold til forvaltningsorganets sikkerhetsstrategi.

Det skal også kontrolleres at relevante sertifikater fortsatt er gyldige og ikke trukket tilbake. Hvor oppdaterte opplysningene om sertifikatets status bør være kan variere fra område til område, men skal fremgå av forvaltningsorganets sikkerhetsstrategi, f.eks. om det skal sendes forespørsel til sertifikatutsteder om

oppdaterte opplysninger ved hver verifisering, eller om det kan benyttes tilbaketrekkingslister som oppdateres f.eks. daglig.

For henvendelser der det er benyttet annen sikkerhetsteknikk enn avansert elektronisk signatur, må nødvendige kontroller vurderes i forhold til sikkerhetsbehovet på det aktuelle området. Dette bør fremgå av forvaltningsorganets sikkerhetsstrategi.

Del II Kommentarer til de enkelte paragrafer i forskriften

Nedenfor følger små og store kommentarer til de enkelte paragrafer. Fordelen er at man slipper å gjenta bestemmelsene som kommenteres. Ulempen kan være at kommentarene i denne delen av veiledningen blir litt mindre orientert mot helheten i forskriften, og detaljorientert. På bakgrunn av den generelle gjennomgangen i veiledningens del I, *Moderne e-forvaltning krever moderne regelverk*, regner vi med at fremstillingen er noenlunde harmonisk i forholdet mellom helhetlig og detaljert fremstilling og kommentar.

Alle kommentarene i denne del II er gitt i form av fotnoter til selve forskriftsteksten.

Kapittel 1 Innledende bestemmelser

§ 1 *Forskriftens formål og anvendelsesområde*

(1) Forskriftens formål er å legge til rette for sikker og effektiv[4] bruk av elektronisk kommunikasjon[5] med og i forvaltningen. Den skal fremme forutsigbarhet[6] og fleksibilitet[7] og legge til rette for samordning[8] av sikre og hensiktsmessige tekniske løsninger. Forskriften skal legge til rette for at

[4] Sikker og effektiv bruk oppnås både ved tekniske, organisatoriske og rettslige virkemidler, ut fra et helhetlig perspektiv. Det er ikke bare teknikken som må være til å stole på, men også organisasjonen(e) og personene som er involvert. Jussen må ikke gi dårligere rettssikkerhet i den elektroniske forvaltningen enn i den papirbaserte forvaltningen. Effektiviteten må balanseres mot sikkerheten. En fornuftig blanding kan gi det beste resultatet.

[5] Med elektronisk kommunikasjon tenkes det på den elektroniske informasjonsflyten eller – utvekslingen, som er knyttet til saksbehandlingen eller forvaltningsvirksomheten, innhenting og vurdering av informasjon, vedtak, forsendelse av vedtak mv.

[6] Forutsigbarhet er et viktig rettsprinsipp, likhetsprinsippet et annet. Til sammen utgjør de hoveddeler i begrepet rettssikkerhet. Det skal med andre ord være mulig å forutsi sin rettssituasjon, og det er et mål at rettsreglene i denne forskriften skal bidra til dette.

[7] Fleksibilitet knyttet til valg av kommunikasjonsform og sikkerhetstjenester er et mål. Dette kan i visse sammenhenger stå i motsetning til, eller måtte balanseres mot, hensynet til koordinering eller samordning, der felleshensyn tilsier dette.

[8] Å legge til rette for samordning betyr å ivareta fellesinteresser mellom de som samordnes, forvaltningen får fellesregler på et nytt område, publikum og næringslive får ett sett regler for elektronisk kommunikasjon mot forvaltningen, uansett hvilket forvaltningsorgan man forholder seg til. Forskriftsreglene er i seg selv uttrykk for slike fellesinteresser i at forvaltningen skal opptre ut fra fellesnormer på dette området (som gir den ønskede forutsigbarhet, likhet og dermed rettssikkerhet). Et behov for fleksibilitet kan kanskje sies å stå i et motsetningsforhold til dette, men forskriften legger til grunn at begge hensyn skal veies mot hverandre, og ivaretas rimelig balansert. Det er i § 28 gitt adgang til å utpeke et koordinerende organ for forvaltningens sikkerhetstjenester ved kommunikasjon med og i forvaltningen. Begrepet sikkerhetstjenester må ikke forveksles med tjenester som har med rikets sikkerhet og andre vitale nasjonale sikkerhetsinteresser å gjøre. I denne sammenhengen er sikkerhetstjenester et samlebegrep som omfatter tilgjengelighet, integritet, autentisitet, konfidensialitet og ikke-benekting. Disse kan ivaretas/realiseres ved sikkerhetsteknikker som elektroniske signaturer og innholdskryptering. Se nærmere omtale i veiledningens del I.

publikum på en enkel måte kan utøve sine rettigheter og oppfylle sine plikter i forhold til det offentlige.

(2) Denne forskrift gir ikke grunnlag for å gjøre unntak fra de alminnelige reglene om forsvarlig saksbehandling i forvaltningsloven.[9]

(3) Forskriften gjelder for elektronisk kommunikasjon mellom forvaltningen og publikum[10] og for elektronisk saksbehandling og kommunikasjon i forvaltningen.[11]

§ 2 *Definisjoner*

(1) I denne forskriften menes med:

1. *elektronisk signatur*: data i elektronisk form som er knyttet til andre elektroniske data og som fungerer som autentiseringsmetode,[12]
2. *avansert elektronisk signatur*: en elektronisk signatur som
   a. er entydig knyttet til undertegneren,
   b. kan identifisere undertegneren,
   c. er laget ved hjelp av midler som bare undertegneren har kontroll over, og
   d. er knyttet til andre elektroniske data på en slik måte at det kan oppdages om disse har blitt endret etter signering,[13]
3. *undertegner*: en fysisk eller juridisk person som handler på vegne av seg selv eller på vegne av en annen fysisk eller juridisk person,[14]

---

[9] Lov av 10. februar 1967 om behandlingsmåten i forvaltningssaker. Denne forskriften utfyller/kommer i tillegg til loven, og skal bidra til at også ved elektronisk kommunikasjon skal kravene i loven følges, ikke uthules eller utfordes.

[10] Med publikum menes både enkeltpersoner og næringslivet/juridiske personer.

[11] Internt i forvaltningen vil reglene angå kommunikasjon og saksbehandling mellom forvaltningsorganer og i det enkelte organ.

[12] Definisjonen avviker noe fra den tilsvarende i lov om elektronisk signatur. Den er derimot relativt lik den i EUs direktiv. Dataene som det refereres til er nok i praksis nøklene i et nøkkelpar, som består av en hemmelig/privat og en offentlig nøkkel. Brukt til henholdsvis å signere og bekrefte/autentisere signeringen med. Man signerer med den hemmelige nøkkelen, slik at alle som har tilgang til den offentlige nøkkelen kan få en bekreftelse på at dette faktisk kommer fra den ene som har den hemmelige nøkkelen. Den mest kjente og presist beskrevne teknikken for dette kalles digital signatur. I direktivet og i den norske loven er imidlertid "elektronisk signatur" brukt som et juridisk overordnet begrep, og forsøksvis teknologinøytralt. Hvis det kommer nye måter å gjøre det på i markedet, er tanken at direktiv og lov (kanskje) ikke trenger forandres. Biometriske metoder (for eksempel fingeravtrykk og øyegjenkjenning) og pin-koder kan sies å gå inn under begrepet elektronisk signatur. Det er imidlertid hevet over tvil at det er teknikken kalt digital signatur som ligger til grunn for direktivet om elektronisk signatur, den norske loven om elektronisk signatur – og langt på vei ligger til grunn for denne forskriften om elektronisk kommunikasjon med og i forvaltningen. *Autentiseringsmetode* vil si metode for å bekrefte at oppgitt identitet på person, virksomhet eller annen enhet faktisk stemmer. Det er med andre ord dette som er kjernen i bruken av elektronisk signatur.

[13] Denne definisjonen er identisk med tilsvarende i lov om elektronisk signatur (§3 nr 2). Dette er i praksis en beskrivelse av krav som nettopp teknikken kalt digital signatur (med infrastruktur) kan tilfredsstille. Den innebærer en høyere grad av sikkerhet enn den vanlige, elektroniske signaturen, med ivaretakelse av de funksjonene som nevnes i bokstavene § 2 nr 2.

[14] Definisjonen er noe justert i forhold til lov om elektronisk signatur (§ 3 nr 4) for klart å angi at undertegner også kan være en virksomhet/juridisk person. Jf bl.a. reglene om virksomhetssertifikat i forskriftens § 12.

4. *signaturfremstillingsdata*: unike data, som for eksempel koder eller private nøkler, som undertegneren benytter for å fremstille en elektronisk signatur,[15]
5. *signaturverifikasjonsdata*: unike data, som for eksempel koder eller offentlig nøkkel, som benyttes til å verifisere en elektronisk signatur,[16]
6. *sertifikat*: en kopling mellom signaturverifikasjonsdata og undertegner som bekrefter undertegners identitet og er signert av sertifikatutsteder,[17]
7. *sertifikatutsteder*: en fysisk eller juridisk person som utsteder sertifikater eller tilbyr andre tjenester relatert til elektronisk signatur,[18]
8. *virksomhetssertifikat*: sertifikat som identifiserer forvaltningsorganet,[19]
9. *autentisering*: en prosess som har som mål å bekrefte en påstått identitet,[20]

[15] Identisk med § 3 nr 5 i lov om elektronisk signatur.

[16] Tilnærmet lik § 3 nr 7 i lov om elektronisk signatur. Forskjellen er at i lovteksten står "offentlige nøkler" i flertallsform, mens i forskriften er det blitt entallsformen "offentlig nøkkel". Dette innebærer ingen forskjell i innholdet.

[17] Identisk med § 3 nr 9 i lov om elektronisk signatur. Sertifikatet bekrefter at den offentlige nøkkelen hører til den hemmelige nøkkelen som en nærmere identifisert person disponerer. Sertifikatet (bekreftelsen) kan inneholde flere relevante opplysninger. Uten en slik bekreftelse vil mulighetene for feil og falsknerier bli flere. Sertifikatet garanterer (eller øker sannsynligheten for) at det er riktig person (virksomhet/enhet) som har brukt den hemmelige nøkkelen til å signere med. Sertifikatet anses som viktig for å kunne ha tillit til løsningene. Sertifikatet signeres elektronisk av utstederen, med de sikkerhetsfunksjoner dette innebærer.

[18] Identisk med § 3 nr 10 i lov om elektronisk signatur. Når et sertifikat er så viktig (jf forskriftens § 2 nr 6 og omtalen i forrige fotnote), blir det også av betydning at den som utsteder (lager) sertifikatet faktisk er til å stole på. Det forutsettes at utstederen er en virksomhet som "alle" kjenner og har tillit til, samt tilgang og tillit til utstederens offentlige nøkkel. Grunnlaget for tilliten kan variere. De sertifikatutstedere som velger å la seg registrere hos Post- og teletilsynet som utstedere av *kvalifiserte* sertifikater, kommer inn under reglene i lov om elektronisk signatur. Disse er utformet for å gi et særskilt grunnlag for tillit til både aktørene og sertifikatene (i hele EU/EØS-området, jf EU-direktivet som den norske loven er en gjennomføring av). Hvilke sertifikatutstedere som har sendt inn melding og registrert seg kan man få opplyst ved henvendelse til Post- og teletilsynet. En sertifikatutsteder kan ha flere roller/tilby flere tjenester, herunder identitetskontroll, tildeling av navn, katalog- og tilbaketrekkingstjenester, valideringstjenester, tidsstempling, arkivering eller konsulenttjenester i forbindelse med elektroniske signaturer. Mange av disse oppgavene kan også løses av andre. Sertifikatutstedere skal arbeide ut fra nærmere regler for slik virksomhet, kalt sertifikatpolicy.

[19] Definert spesielt i denne forskriften (dvs. den fins ikke i lov om elektronisk signatur). Den er laget for å gjøre det mulig for den enkelte virksomhet å benytte elektroniske signaturer på en enklere måte. Et virksomhetssertifikat identifiserer virksomheten som sådan, ikke enkeltindivider i form av ansatte ledere, mellomledere og saksbehandlere. Virksomhetssertifikatet bekrefter at den offentlige nøkkelen er knyttet til en virksomhet med en tilhørende hemmelig nøkkel. En borger som er part i en sak kan være trygg på at dokumenter, sakspapirer eller vedtak som er signert med for eksempel Rikstrygdeverkets (RTV) virksomhetssertifikat, faktisk kommer fra RTV og ikke noen som gir seg ut for å være RTV. Hvem i RTV som internt har signert eller er ansvarlige for vedtaket, kan angis på vanlig måte med navn i tastet/skrevet inn vedtaket, men uten at det er nødvendig å bruke den spesielle sikkerhetsteknikken som en elektronisk signatur representerer. Den kan følgelig brukes der hvor den trengs best, der et usikkert Internett er kommunikasjonsmiddelet mellom forvaltningen og borgeren. Internt i forvaltningsorganet vil man antakelig sjelden trenge denne typen sikkerhet, fordi alle aktørene er velkjente, og fordi organet i sin interne virksomhet vanligvis er godt beskyttet mot ytre risiki, virus, andre angrep, mv ved hjelp av brannmurer og annet.

[20] Definert spesielt i denne forskriften (dvs. finnes ikke i lov om elektronisk signatur). Å kunne få bekreftelse på at en oppgitt ("påstått") identitet faktisk stemmer, er verdifullt i mange

10. *ikke-benekting*: en mekanisme som kan knyttes til elektronisk samhandling, og som er slik at de deltakende partene ikke kan benekte å ha deltatt i deler eller hele samhandlingen,[21]
11. *integritet*: en egenskap ved data som gjør det mulig å oppdage om data har blitt endret på en uautorisert måte eller på grunn av feil,[22]
12. *innholdskryptering*: en prosess som fører til forvrengning av innholdet i en meddelelse slik at bare mottaker med riktige dekrypteringsdata kan få det frem og lese det,[23]
13. *krypteringsdata*: en sekvens av symboler som kontrollerer operasjonene for kryptering av en meddelelse,[24]
14. *dekrypteringsdata*: en sekvens av symboler som kontrollerer operasjonene for dekryptering av meddelelsen.[25]

---

sammenhenger, enten det dreier seg om identiteten til avsender, mottaker, brukere av systemet, eller systemet selv. Jo høyere verdi informasjonen i en melding, et brev, et dokument eller vedtak har, jo viktigere blir det at det er mulig å autentisere (verifisere, bekrefte) identiteten til den eller de som er involvert. Teknikken med autentisering bygger på at det bare er én som har tilgang til den hemmelige nøkkelen. Vellykket bruk av den tilhørende åpne, offentlig tilgjengelige nøkkelen for verifisering, gir sterk indikasjon på at det er riktig aktør i den andre enden.

[21] Definert spesielt i denne forskriften (dvs. finnes ikke i lov om elektronisk signatur). Ikke-benekting bygger (også) på prinsippet om at bare én skal ha tilgang til den private/hemmelige nøkkelen som ble brukt i samhandlingen. En mottaker av et signert dokument får styrket sin antakelse om hvem som signerte dokumentet ved å verifisere/få bekreftet signaturen. Den som signerte kan imidlertid bare vite at dokumentet har kommet frem hvis han eller hun får en (signert) bekreftelse på mottak i retur.

[22] Integritet er den egenskapen ved krypteringsalgoritmer at en melding eller dokument må komme frem uforandret for at man skal kunne lese meldingen etter dekrypteringen. Går det ikke, kan det bety at et komma er flyttet eller et ord er forandret. Mer skal det ikke til. Tilsvarende vil man ikke få verifisert en digital signatur knyttet til en melding hvis meldingen er endret underveis. Meldingen kan være lesbar, men endret. Om endringen er utført bevisst av noen, eller om det er en teknisk feil, spiller ingen rolle. Poenget er at feilen gjør at man ikke kan stole på den elektroniske signaturen, eller ikke får lest meldingen.

[23] Innholdskryptering betyr å gjøre det tekstlige innholdet i en melding uleselig (da krypterer man med en nøkkel), slik at bare den tilhørende nøkkelen (her kalt dekrypteringsdata) i et nøkkelpar kan gjøre teksten leselig igjen (da dekrypterer man med nøkkelen). Se del I foran i veiledningen om symmetrisk og assymmetrisk kryptering. Innholdskryptering gir konfidensialitet, skjerming av innholdet mot uvedkommende. I denne sammenhengen omfattes ikke den kryptering som skjer av innhold i forbindelse med systemer for betal-TV, rettighetsadministrasjon mv. Innholdskryptering er et stadig mer praktisk tiltak for å beskytte taushetsbelagt informasjon, sensitive personopplysninger, opplysninger som er unntatt fra offentlighet iht offentlighetsloven mv., i en elektronisk forvaltning og –kommunikasjon.

[24] Med en såpass lyrisk definisjon er det nesten for enkelt å si at *krypteringsdata* er den omtalte *nøkkelen* for kryptering av innholdet i en tekst. Den sekvens av symboler som nevnes er tall. Enormt lange tall og regneregler/algoritmer, som gjør det svært vanskelig eller i praksis umulig å avsløre hvilket tall som er nøkkelen. Styrken i nøkkelen ligger i hvor stort tallet er, og hvor komplisert "kvern" man bruker for å lage nøkkelen. Nøklene oppbevares forsvarlig i smartkort eller i datamaskiner. Det finnes stor faglitteratur på området for mer presise forklaringer.

[25] Dekrypteringsdata er, som navnet og de foregående to fotnotene tilsier, data/tall/algoritmer/nøkler som brukes på tekst som er kryptert (lukket, gjort uleselig) for å åpne teksten igjen, gjøre den leselig. Kryptering og dekryptering kan bare gjøres av nøkler som hører sammen. Begrepene kryptering og dekryptering er i forskriften knyttet bare til innholdskryptering, for å skille dette begrepsmessig fra den noe parallelle, kryptobaserte aktiviteten som skjer ved signering og verifisering av signering, jf (de relativt lyriske)

Kapittel 2 Alminnelige krav til saksbehandling ved elektroniske henvendelser

§ 3 *Fremgangsmåte ved henvendelser i elektronisk form til forvaltningsorgan*

(1) Henvendelse til et forvaltningsorgan[26] kan[27] skje i elektronisk form når henvendelsen fremsettes på den måte[28] og til den elektroniske adresse[29] forvaltningsorganet har gitt anvisning på[30] for den aktuelle type henvendelse.

(2) Hvis ingen særskilt form eller fremgangsmåte er angitt for den aktuelle type henvendelse kan henvendelsen rettes til forvaltningsorganets generelle elektroniske adresse.[31]

---

begrepene signaturfremstillingsdata og signaturverifiseringsdata definert over. Nøklene oppbevares forsvarlig i smartkort eller i datamaskiner.

[26] Som forvaltningsorgan regnes i denne forskriften et hvert organ for stat eller kommune på samme måte som definisjonen i forvaltningsloven § 1. Reglene i forskriften gjelder etter sin ordlyd for forvaltningsorganet, men vil også gjelde for henvendelser som sendes direkte til en saksbehandler. Det er gitt noen regler som begrenser muligheten for direkte henvendelser til saksbehandler, se fotnotene til § 3 (3) og (4).

[27] Når forvaltningsorganet har lagt til rette for elektronisk kommunikasjon, kan den som vil sende en henvendelse til forvaltningsorganet velge om det skal gjøres elektronisk eller på papir. Avsender har ingen plikt til å sende henvendelser i elektronisk form.

[28] Henvendelser kan fremsettes på forskjellige måter. E-post blir av mange ansett som den vanligste i øyeblikket, men det vil bli mer vanlig å ta i bruk vevbaserte skjemaer på forvaltningsorganets hjemmeside. Bruk av slike skjemaer gir flere fordeler i forhold til e-post. Blant annet kan det føres automatisk kontroll med at alle relevante opplysninger er gitt. Videre vil informasjonen kunne struktureres, slik at den videre behandlingen internt i forvaltningsorganet blir mer effektiv. Slike løsninger er neppe mulig ved bruk av ordinær e-post. Dokumenter kan sendes som vedlegg til e-post, men det er ingen garanti for at IT-systemet hos mottaker håndterer det formatet som avsender bruker. Det kan i noen tilfeller føre til at dokumentet blir uleselig for mottaker. Også en del krav til sikkerhet vil lettere kunne løses ved hjelp av vevbaserte tjenester.

[29] Dette vil enten være en adresse på forvaltningsorganets hjemmeside (url) eller en e-postadresse. For å unngå at alle henvendelser sendes til en felles adresse, kan det være hensiktsmessig å stille krav om at bestemte typer henvendelser skal rettes til spesielle elektroniske adresser. Ved bruk av nettbaserte skjemaer, kan det legges inn funksjonalitet som styrer henvendelsene til riktig mottaker avhengig av hva slags type henvendelse det er eller hvilket saksområde henvendelsen gjelder. Dersom det ikke finnes en særskilt nettside for det forhold saken gjelder og det heller ikke er opprettet spesielle e-postadresser for bestemte typer henvendelser, skal det være mulig å sende e-post til forvaltningsorganets generelle elektroniske adresse, se fotnote 6.

[30] Informasjon om riktig fremgangsmåte og adresse for bestemte typer henvendelser kan være angitt på forvaltningsorganets hjemmeside, i en annonse, kunngjøring e.l. For eksempel kan det i en stillingsannonse gis informasjon om at søknader skal sendes via en angitt nettside, adresseres til navngitt saksbehandler eller bestemt avdeling i forvaltningsorganet. Selv om det er gitt anvisning om at henvendelser skal rettes til en bestemt adresse, har forvaltningen en generell veiledningsplikt til publikum som retter en henvendelse til feil organ eller bruker feil adresse, se forskriften § 6 og forvaltningsloven § 11. Flere kommuner har også etablert informasjons- eller servicesentre for å hjelpe publikum i å finne frem i forvaltningen.

[31] I tillegg til å opprette særskilte vevbaserte tjenester for bestemte saksområder eller brukere, bør forvaltningsorganet ha en generell side som gir publikum anledning til å ta kontakt med

(3) Henvendelse i elektronisk form direkte til saksbehandler,[32] av meldinger som angår forvaltningsorganet,[33] skal kun skje hvis forvaltningsorganet har lagt til rette for det,[34] eller det er avtalt i det enkelte tilfelle.[35]
(4) Forvaltningsorganet kan bestemme at adressering direkte til saksbehandler kan skje når meldingen sendes fra annet forvaltningsorgan.[36]

§ 4 *Krav til sikker identifisering, bruk av sikkerhetstjenester mv.*

(1) Henvendelser til forvaltningsorgan, som kan fremsettes i elektronisk form, og som ikke er underlagt særskilte formkrav[37] eller krav til konfidensialitet

---

forvaltningsorganet. Henvendelser via denne nettsiden bør sendes til arkivtjenesten. Alle forvaltningsorganer som åpner for bruk av e-post, har plikt til å ha en generell elektronisk adresse. Dette følger av arkivforskriften § 3-2 annet ledd: "Organ som nyttar e-post, skal ha eit sentralt e-postmottak for post til organet. E-post til det sentrale postmottaket skal opnast av arkivtenesta." En slik e-postadresse kan for eksempel være postmottak@skoleetaten.oslo.no. Denne adressen kan brukes dersom publikum er usikre på hvilken måte henvendelser skal fremsettes eller til hvem de skal sendes.

[32] Det er noen ulemper ved å tillate at henvendelser sendes direkte til saksbehandler. Vanligvis er det ikke mulig for andre å lese e-post som sendes direkte til en person. Dermed vil ingen kunne behandle henvendelsen før mottakeren er tilbake på jobb. Hvis saksbehandler har sluttet eller har et lengre fravær, kan det føre til store forsinkelser i saksbehandlingen og i verste fall til at henvendelsen aldri blir lest. E-post kan også sendes til feil forvaltningsorgan. Kunnskapen om håndtering av feilsendte meldinger og hvilken informasjon avsender har krav på og behov for, kan være mindre hos den enkelte saksbehandler enn hos arkivet som håndterer postmottaket. Direkte adressering bør derfor være forbeholdt tilfeller eller typer av saksbehandling der det enten er særskilt behov for det eller det i alle fall er på det rene at det ikke har spesielle ulemper.

[33] Henvendelser av privat eller personlig karakter som sendes direkte til saksbehandler reguleres ikke av denne bestemmelsen eller forskriften for øvrig.

[34] Et eksempel på at det er lagt til rette for direkte henvendelser til saksbehandler kan være når forvaltningsorganet benytter elektronisk saksbehandling, arkiv- og journalsystem. Da kan det også være lagt til rette for at saksbehandler selv kan foreta registrering av inngående post. Dersom saksbehandler ikke kan foreta journalføring selv, må organet ha rutiner som sikrer at henvendelsen blir videresendt til arkivtjenesten. Dette følger også av arkivforskriften § 3-1 annet ledd, jf. arkivforskriften § 3-2 første ledd.

[35] Det åpnes for at saksbehandler i enkelttilfeller kan åpne for direkte kommunikasjon selv om forvaltningsorganets rutiner generelt ikke er tilrettelagt for dette. Saksbehandler har da ansvaret for at organets interne rutiner for håndtering av ekstern kommunikasjon følges. Forvaltningsorganet bør ha interne rutiner for hvordan saksbehandlere skal håndtere direkte elektronisk kommunikasjon. Det er også viktig å gi informasjon til partene hvis saksbehandler har planer om lengre fravær, se fotnote 32.

[36] I prinsippet har det i forhold til reglene om journalføring og arkivering ingen betydning om henvendelser kommer fra andre forvaltningsorganer eller fra private. Saksbehandler må også behandle henvendelser fra andre forvaltningsorganer i tråd med de generelle rutinene som gjelder for journalføring og arkivering.

[37] Særskilte formkrav kan for eksempel være krav om underskrift, skriftlighet eller bruk av bestemte skjemaer. I eRegelprosjektet i NHD ble det gjennomført en kartlegging av hindringer for elektronisk kommunikasjon. Et resultat av dette arbeidet var blant annet at det ble foretatt en rekke lovendringer som fjerner mange av hindringene. Lovforslagene ble fremsatt i Ot.prp. nr. 108 (2000-2001). Selv om de rettslige hindringene er fjernet og det nå er åpnet for å ta i bruk elektronisk kommunikasjon, er det mange krav som forutsetter at bestemte fremgangsmåter, sikkerhetstjenester og -produkter tas i bruk. Et eksempel på slike krav er § 7, som bestemmer at forvaltningsorganet skal sikre at enkeltvedtaket ikke gjøres tilgjengelig for uvedkommende. Når det er gitt slike krav, skal forvaltningsorganet fastsette hvordan disse kravene skal oppfylles ved

mv.[38], kan fremsettes uten bruk av sikkerhetstjenester med mindre annet er bestemt i medhold av nr. 2-4 nedenfor.

(2) Forvaltningsorganet kan i det enkelte tilfelle[39] be om opplysninger[40] som bekrefter avsenders identitet eller fullmakter dersom dette er av betydning for håndtering av henvendelsen.

(3) Forvaltningsorganet kan også stille krav om at bestemte fremgangsmåter, sikkerhetstjenester og -produkter skal tas i bruk for å sikre autentisering, ikke-benekting, integritet og konfidensialitet.[41]

(4) Forvaltningsorganet kan fastsette at krav som nevnt i nr. 2 og 3 ovenfor skal gjelde generelt for nærmere angitte typer av henvendelser.[42]

(5) På områder der det er åpnet for elektronisk kommunikasjon, men der henvendelser er underlagt særskilte formkrav eller krav til konfidensialitet mv., skal forvaltningsorganet fastsette hvilke fremgangsmåter,

---

bruk av elektronisk kommunikasjon, se § 4 (5). Det vil fortsatt være mange praktiske hindringer for å kunne ta i bruk elektronisk kommunikasjon, blant annet fordi vi foreløpig ikke har etablert en felles infrastruktur for elektroniske signaturer.

[38] I tillegg til konfidensialitet, kan det forekomme krav til andre sikkerhetstjenester, som for eksempel autentisering, integritet, tilgjengelighet eller ikke-benekting. Det er dette som ligger i uttrykket "mv.". Se del I i veiledningen for en nærmere beskrivelse av relevante sikkerhetstjenester og -teknikker.

[39] Hvis det normalt fungerer greit uten spesiell bekreftelse, er det ingen grunn til å stille generelt strengere krav generelt ved elektronisk kommunikasjon enn ved bruk av papirpost. Bruk av elektronisk kommunikasjon kan likevel skape en særlig risiko eller usikkerhet som gjør det rimelig å stille strengere krav i enkelttilfeller.

[40] Det er ikke alltid nødvendig å stille krav om elektronisk signatur for å få bekreftet avsenders identitet eller fullmakter. Forvaltningsorganet kan for eksempel be avsender oppgi sin fødselsdato, bostedsadresse, kundenummer eller lignende opplysninger som i det enkelte tilfelle anses tilstrekkelig som bekreftelse på identitet. Bekreftelse på fullmakter kan fåes ved å ta direkte kontakt med fullmaktsgiver.

[41] Forvaltningen kan stille krav til sikkerhet uten at det nødvendigvis følger av andre regler. Hvilke behov det er for å ta i bruk bestemte fremgangsmåter, sikkerhetstjenester og -produkter må vurderes konkret av det enkelte forvaltningsorgan. I noen sammenhenger er det av stor betydning å kunne verifisere avsenders identitet, mens det i andre sammenhenger er viktigere å sikre at opplysningene ikke gjøres kjent for uvedkommende. Vurderingen må blant annet sees i sammenheng med hvilke typer saker forvaltningsorganet behandler og hvilke opplysinger som utveksles. Valg av løsning må også vurderes i forhold til kostnader og nytte. Det vil for eksempel være grunn til å stille strengere krav til identifisering av personer som søker om studielån enn av personer som ber om generell informasjon fra Statens lånekasse. I vurderingen bør det også tas hensyn til når sikkerhetsløsningene må benyttes. Det kan for eksempel være tilstrekkelig å ha god sikkerhet ved utbetaing av studielån, mens innsendelse av lånesøknad trolig kan skje uten spesielle krav.

[42] Det kan være behov for å la kravene gjelde generelt for henvendelsene som normalt inneholder bestemte typer opplysninger eller som gjelder bestemte typer saksområder. For eksempel kan det være aktuelt for et forvaltningsorgan å gi generelle regler om autentisering ved lovpålagt innlevering av opplysninger til et offentlig register e.l. Et annet eksempel kan være opplysninger som forvaltningsorganet har taushetsplikt om. Selv om forvaltningsorganet har plikt til å forhindre at uvedkommende får tilgang til opplysningene, vil ikke den som sender inn opplysningene nødvendigvis ha en slik plikt. For eksempel har ikke privatpersoner taushetsplikt om opplysninger som angår dem selv. Men skal forvaltningsorganet kunne ivareta sin taushetsplikt, kan det være behov for å stille krav om at henvendelser krypteres. I de fleste tilfeller vil dette også være av interesse for den som sender henvendelsen. Se også merknadene til § 20.

sikkerhetstjenester og -produkter som oppfyller kravene til form eller konfidensialitet mv.[43]

(6) Forvaltningsorganet skal tilby eller gi anvisning på sikkerhetstjenester og -produkter som oppfyller de krav forvaltningsorganet har stilt i henhold til nr. 3-5 ovenfor.[44]

§ 5 *Bekreftelse på at en henvendelse er mottatt*

(1) Forvaltningsorgan som mottar henvendelser i elektronisk form skal gi bekreftelse til avsender om at en henvendelse er mottatt, med mindre henvendelsen er av en slik art at den ikke utløser saksbehandling eller mottaket fremgår på annen måte.[45]

(2) Bekreftelse bør gis straks henvendelsen er mottatt.[46] Den bør inneholde et referansenummer[47] eller lignende og angi på hvilket tidspunkt henvendelsen ble mottatt.

---

[43] Vurderingene som må gjøres i forhold til § 4 (5) vil i stor grad være de samme som i forhold til § 4 (3), se fotnote til denne bestemmelsen. Men etter § 4 (5) vil behovet for bestemte tiltak følge av at det er gitt spesielle formkrav etter krav til sikkerhet i regelverket. Forvaltningsorganet har da plikt til å informere om hvilke tiltak som konkret kan oppfylle et generelt angitt form- eller sikkerhetskrav. Ingen skal behøve å gjette seg frem til hvordan krav i regelverket kan oppfylles. Et eksempel på slike generelle krav er personopplysningsloven § 13 om informasjonssikkerhet. I personopplysningsforskriften § 2-11 tredje ledd, gitt i medhold av loven, er det bestemt at elektronisk overføring av personopplysninger "ved hjelp av overføringsmedium utenfor den behandlingsansvarliges fysiske kontroll, skal krypteres eller sikres på annen måte når konfidensialitet er nødvendig". Forvaltningsorganet skal vurdere og gi informasjon om hva som er tilstrekkelig for å sikre konfidensialiteten. Et annet eksempel er lov om offentlige tjenestetvister § 12 tredje ledd. Når oppsigelse skal sendes i rekommandert brev, kan dette også gjøres ved bruk av elektronisk kommunikasjon "dersom det er benyttet en betryggende metode for å sikre at varselet er mottatt". Forvaltningsorganet må definere hva som er en "betryggende metode".

[44] Forvaltningsorganet skal konkret angi hvorledes de krav de selv har stilt kan oppfylles. Dette kan gjøres ved enten selv å tilby produkter eller å navngi tjenesteytere og produkter, som tilfredsstiller kravene. For eksempel kan det være i form av utsending av PIN-koder eller henvisning til signaturtjenester som er anbefalt av koordinerende organ, se § 28 i forskriften. Et konkret eksempel på anvisning om bestemt sikkerhetstjeneste og -produkt er Datatilsynets anbefaling om å kryptere overføring av sensitive personopplysninger med en krypteringsstyrke tilsvarende "DES128" (112 bits effektiv nøkkel).

[45] Det vil være mulig å kontrollere automatisk om henvendelser utløser saksbehandling eller ikke, men henvendelsen må da være strukturert slik at IT-systemet forstår hva den gjelder. Dersom forvaltningsorganet tilbyr vevbaserte søknadsskjemaer, kan IT-systemet som mottar søknader kunne definere dette som et saksdokument og sende bekreftelse til avsender automatisk. Ved bruk av e-post kan det gis automatisk bekreftelse på at en henvendelse er mottatt, men automatiske løsninger klarer ikke å skille mellom henvendelser som utløser saksbehandling og henvendelser som ikke gjør det. Det enkleste vil ofte være å legge opp til bekreftelse på alle mottatte henvendelser.

[46] Det bør tas i bruk systemer som sender bekreftelser automatisk. Da vil bekreftelse kunne sendes i det øyeblikket henvendelser er mottatt av forvaltningsorganet. Dersom bekreftelser gis manuelt bør de sendes senest innen utløpet av neste virkedag, jf. § 8 annet ledd.

[47] Når henvendelser sendes i strukturert form via nettbaserte skjemaer vil det være mulig å opprette saksnummer automatisk. Referansenummeret som oppgis i bekreftelsen kan da være det samme som saksnummeret. Dersom avsender bruker e-post, må forvaltningsorganet først vurdere om en henvendelse skal journalføres og få et saksnummer. Siden denne manuelle behandlingen kan ta noe tid, bør det opprettes et eget referansenummer slik at bekreftelse kan gis straks henvendelsen er mottatt.

§ 6 *Henvendelser som ikke tilfredsstiller aktuelle krav*[48]

(1) Henvender noen seg til urette myndighet eller benytter uriktig elektronisk adresse[49] ved en henvendelse til et forvaltningsorgan, skal det forvaltningsorgan som mottar henvendelsen gi avsender beskjed om feilen og om mulig vise vedkommende til rett organ og rett elektronisk adresse, jf. forvaltningslovens § 11.

(2) Er en henvendelse avgitt i en annen form eller på en annen måte enn det som er angitt i eller i medhold av forskriften her, skal organet gi avsenderen beskjed om dette dersom feilen har betydning for behandling av saken[50] eller det av andre grunner finnes nødvendig.[51] Organet bør samtidig gi frist til å rette opp feilen og gi veiledning om hvordan dette kan gjøres.

(3) Forvaltningsorganet skal registrere tidspunkt for når det er sendt melding etter nr. 1 og 2 ovenfor, og til hvem meldingen ble sendt. Dersom feilen er av en slik art at det ikke er mulig å identifisere avsender, og varsel ikke kan sendes, skal det registreres opplysning om dette.

§ 7 *Underretning om enkeltvedtak og enkelte andre meddelelser fra forvaltningsorgan*[52]

(1) Underretning om enkeltvedtak kan skje i elektronisk form dersom parten har uttrykkelig godtatt dette[53] og oppgitt den elektroniske adresse forvaltningsorganet skal benytte for melding etter nr. 2 nedenfor.

---

[48] Reglene i § 6 følger også av forvaltningsloven § 11 om veiledningsplikt.

[49] Et forvaltningsorgan kan ha flere elektroniske adresser, for eksempel inndelt geografisk, etter saksområder eller avdelinger. Benytter avsender feil adresse, skal det gis veiledning om hva som er korrekt adresse for den aktuelle type henvendelse. I tillegg til veiledning bør det også internt i forvaltningsorganet være rutiner for å videresende slike feilsendte henvendelser til rett instans. Avsender bør i så fall få beskjed om at henvendelsen er videresendt.

[50] Dersom en henvendelse til et forvaltningsorgan inneholder feil, misforståelser, unøyaktigheter eller andre mangler som avsenderen bør rette, skal organet om nødvendig gi beskjed om dette. Et eksempel på at henvendelsen har en feil som er av betydning for saksbehandlingen, er at en søknad mangler opplysninger som er nødvendige. Det kan også foreligge feil som kan være av mindre betydning for saksbehandlingen. Dersom en søknad ikke er undertegnet i de tilfellene dette er et krav eller at signaturen av tekniske grunner ikke kan verifiseres, kan forvaltningsorganet likevel være forpliktet til å behandle søknaden. Dette gjelder særlig hvis feilen ikke har betydning for saksbehandlingen og ikke andre forhold taler mot det, for eksempel hvis forvaltningsorganet sitter inne med andre opplysninger som bekrefter de aktuelle forhold. Uansett skal avsender få veiledning og en rimelig frist til å rette feilen.

[51] Forvaltningsorganet kan vanskelig forhindre at for eksempel sensitive personopplysninger sendes fra andre uten noen form for sikring av konfidensialitet. Dersom slike opplysninger sendes uten noen form for sikring, bør det gis veiledning til avsender slik at slike opplysninger sikres ved senere henvendelser. Se også fotnote 6 til § 4 (4).

[52] Hovedregelen om underretning om enkeltvedtak står i forvaltningsloven § 27, men denne bestemmelsen regulerer ikke nærmere hvordan underretning i elektronisk form skal gjøres. Klagefristen etter forvaltningsloven § 29 første ledd er tre uker fra det tidspunkt underretning om vedtaket er kommet frem til parten. Det vil derfor være viktig å kunne fastslå når en underretning i elektronisk form faktisk har skjedd og § 7 (6) i forskriften har regler om dette.

[53] Mange privatpersoner har e-postadresse, men er ikke derfor nødvendigvis forberedte på at viktige meldinger kan komme inn på denne måten. For å unngå at noen skal lide rettstap fordi

(2) Parten skal få melding om at enkeltvedtak er fattet, om hvor og hvordan vedkommende kan skaffe seg kunnskap om innholdet, samt en frist for når dette senest må skje.[54]
(3) Innholdet i enkeltvedtaket skal gjøres tilgjengelig fra egnet informasjonssystem[55], jf. blant annet kravene i nr. 2, 4 og 5.
(4) Forvaltningsorganet skal sikre at enkeltvedtaket ikke gjøres tilgjengelig for uvedkommende, jf. § 4.[56]

---

man har en annen holdning til sin elektroniske postkasse enn sin fysiske, er det bestemt at underretning om vedtak bare kan skje når mottakeren har uttrykkelig godtatt å motta meldinger på denne måten. Med *godtakelse* (eller samtykke) menes en frivillig erklæring om at man aksepterer å motta den type meldinger som godtakelsen omfatter. Godtakelsen må være informert, dvs. at avgiver av godtakelseserklæringen må forstå hva vedkommende har godtatt. Tillegget *uttrykkelig* viser for det første at det ikke må være tvil om at parten faktisk har godtatt, og at bevisbyrden for at det foreligger godtakelse vedrørende den aktuelle elektroniske melding, ligger hos forvaltningsorganet. Det oppstilles ikke noen formkrav, men det vil være fornuftig å ha godtakelsen skriftlig (på papir eller elektronisk). For det annet ligger det i *uttrykkelig* at godtakelsen må dekke den aktuelle melding og fra den aktuelle avsender.

For å unngå tvil, kan det være greit å innhente samtykke når parten henvender seg til forvaltningsorganet. En løsning kan være å be om samtykke samtidig som bekreftelse på mottak av henvendelsen etter reglene i § 5 sendes. Kravet om uttrykkelig samtykke vil neppe være oppfylt om parten leser enkeltvedtaket i elektronisk form, uten at det samtidig fremgår klart at parten har akseptert denne formen for underretning. Dersom samtykke ikke er innhentet på forhånd, bør det likevel være tilstrekkelig at parten gir et uttrykkelig samtykke i forbindelse med at parten henter frem enkeltvedtaket, særlig hvis alle enkeltvedtak rutinemessig gjøres tilgjengelige i elektronisk form. En løsning kan være å publisere enkeltvedtak på en egen nettside, og legge inn en sperre som forhindrer at parten får lese det uten først å gi et uttrykkelig samtykke. Konsekvensen av at det ikke foreligger et uttrykkelig samtykke, blir at de alminnelige reglene i forvaltningsloven § 27 skal gjelde, se forskriften § 7 (7).

[54] Underretning om enkeltvedtak omfatter to ting. For det første skal det sendes en melding om at vedtaket er truffet med en beskrivelse av hvor det kan hentes, for eksempel adresse til en nettside. Denne meldingen kan sendes som ordinær e-post, forutsatt at kravene i blant annet § 7 (4) kan ivaretas. For det andre skal parten ut fra den informasjonen som gis i meldingen kunne hente selve vedtaket fra det informasjonssystemet hvor vedtaket er gjort tilgjengelig. Parten har etter § 7 (7) en frist på en uke etter at meldingen ble sendt til å hente enkeltvedtaket. Går det mer enn en uke, skal enkeltvedtaket ettersendes på papir i posten, se fotnote 8.

[55] Et "egnet informasjonssystem" kan for eksempel være en nettside hvor enkeltvedtaket er publisert. Ved å tildele et unikt brukernavn og passord kan parten få tilgang til egne nettsider som inneholder alle opplysninger knyttet til sin sak. En slik løsning kan sammenlignes med en nettbank. Det er viktig at slike nettsider ivaretar de krav som er gitt i medhold av § 7 (4) og (5). Et egnet informasjonssystem gir også mulighet for at forvaltningen står for oppbevaring av vedtakene i elektronisk form på vegne av publikum. Da vil vedtaket være tilgjengelig uavhengig hvor brukeren befinner seg. Brukeren kan skrive ut eller lagre vedtaket på sin PC etter behov, men vil fortsatt ha tilgang til en verifiserbar elektronisk versjon hos forvaltningsorganet. Dersom vedtaket sendes som e-post, er brukeren avhengig av å kunne ta med seg meldingen hvis hun bytter e-postadresse eller PC.

[56] Som hovedregel er det innsynsrett i forvaltningens dokumenter, men innsyn blir først gitt etter begjæring og en konkret vurdering av forvaltningsorganet. Offentlighetsloven legger ikke opp til at forvaltningsorganet skal publisere sine dokumenter på eget initiativ, men det er heller ikke noe forbud mot det. I noen tilfeller velger forvaltningsorganet å publisere sine dokumenter offentlig, særlig hvis det gjelder saker av stor allmenn interesse. Men dersom publisering gjøres rutinemessig for alle enkeltvedtak, er det en fare for at noen dokumenter inneholder opplysninger som andre ikke vil ha innsynsrett i. Offentlig publisering av enkeltvedtak bør derfor skje etter en konkret vurdering. Ved å begrense andres tilgang til enkeltvedtak, unngår man at det i noen tilfeller kan oppstå brudd på taushetsplikten. Selv om det ikke er taushetsplikt, skal man være oppmerksom på at personvernhensyn nok tilsier at forvaltningsorganet ikke bør

(5) Informasjonssystemet skal registrere tidspunktet for når parten har skaffet seg tilgang til enkeltvedtaket og data som bekrefter at vedkommende har rett til å gjøre seg kjent med vedtaket.[57]
(6) Underretning om enkeltvedtak anses å ha kommet frem på det tidspunktet parten skaffet seg tilgang til vedtaket.[58]
(7) Har parten ikke skaffet seg tilgang til enkeltvedtaket innen én uke fra det tidspunkt det ble sendt melding om det, eller vedtaket ble gjort tilgjengelig, skal underretning skje i henhold til de reglene som gjelder når det ikke er gitt samtykke til elektronisk kommunikasjon, jf. forvaltningslovens § 27.[59]
(8) Det som er sagt om underretning om enkeltvedtak i nr. 1-5 ovenfor gjelder tilsvarende ved forhåndsvarsel etter forvaltningsloven § 16 og for andre meldinger som har betydning for mottakerens rettsstilling, for behandlingen av saken eller for meldinger som det av andre grunner er av særlig betydning å sikre at vedkommende mottar.
(9) I forbindelse med underretning om enkeltvedtaket skal det informeres om hvorvidt forvaltningsorganet har lagt til rette for mottak av klage i elektronisk form og hva som er rette elektroniske adresse. Det skal også informeres om at parten bør kontrollere at han mottar bekreftelse når klage leveres i elektronisk form, jf. § 8 nr. 2.

---

publisere offentlig alle sine dokumenter knyttet til enkeltpersoner. Gode mekanismer for autentisering kan sikre at parten får sin rettmessige tilgang og at forvaltningsorganet får bekreftet dette. Videre vil dette hindre at opplysninger gjøres tilgjengelig for uvedkommende, for eksempel hvis parten har oppgitt feil e-postadresse for henvendelser fra forvaltningen. Selv om melding etter § 7 (2) er sendt til feil adresse, vil feil mottaker ikke kunne få tilgang til vedtakets innhold. Hvilke mekanismer som skal benyttes for autentisering, avgjør forvaltningsorganet med støtte i § 4.

[57] Registrering av tidspunkt og kontroll med at parten har fått tilgang til enkeltvedtaket kan skje automatisk, ved å ha et system som loggfører tidspunkt og opplysninger som identifiserer parten. Det vil da være nødvendig å tildele parten en unik elektronisk identifisering som må brukes før parten kan hente frem enkeltvedtaket fra informasjonssystemet. Man skal likevel være oppmerksom på at PIN-koder og andre former for brukernavn og passord kan være en for svak sikkerhetsløsning, siden det kan gi uvedkommende tilgang til enkeltvedtaket dersom de har fått tak i disse opplysningene.

[58] Parten kan få underretning om enkeltvedtak raskere ved bruk av elektronisk kommunikasjon enn om enkeltvedtaket sendes på papir i posten. I noen tilfeller kan det likevel hende at elektroniske meldinger ikke kommer frem eller at parten ikke har mulighet til å lese meldingen. Derfor skal tidspunktet parten oppsøker informasjonssystemet hvor enkeltvedtaket er gjort tilgjengelig legges til grunn for når underretning har skjedd. Når underretning har skjedd etter denne regelen, begynner klagefristen i forvaltningsloven § 27 å løpe. Se også merknadene til § 7 (7) for de tilfellene hvor parten ikke skaffer seg tilgang til enkeltvedtaket innen en uke.

[59] Hvis det går mer enn en uke før parten skaffer seg tilgang, skal enkeltvedtaket sendes til parten som papirpost. Det er derfor viktig at forvaltningsorganet også har tilgang til partens postadresse, slik at enkeltvedtak kan sendes på denne måten. Ordningen skal blant annet sikre at ingen lider rettstap ved for eksempel å oversitte klagefrister eller ikke bli gjort kjent med vedtaket på grunn av tekniske feil, at de har oppgitt feil elektronisk adresse, er midlertidig avstengt fra sin nettforbindelse eller e-postkonto e.l. Siden det kan være vanskelig å føre manuell kontroll med når parten skaffer seg tilgang til vedtaket, bør det tas i bruk tekniske løsninger som holder rede på om og når dette skjer, se merknadene til § 7 (5). Systemet bør også sikre at vedtaket blir ettersendt som papirpost etter en uke, enten automatisk eller ved at saksbehandler får en melding om forholdet.

§ 8 *Klage*

(1) Klage over enkeltvedtak kan fremsettes i elektronisk form dersom forvaltningsorganet har lagt til rette for det, jf. §§ 3 og 4.[60]

(2) Klager bør kontrollere at han mottar bekreftelse etter § 5 innen utløpet av neste virkedag.[61] Dersom klagefristen løper ut etter at klagen er sendt, og klager ikke mottar bekreftelse som nevnt i første punktum, anses klagen likevel fremsatt i rett tid dersom klager sender klagen på nytt med angivelse av når den ble sendt første gang innen en uke eller - dersom den opprinnelige frist er kortere - innen en frist av samme lengde som denne.[62]

§ 9 *Innsyn i opplysninger og dokumenter i elektronisk form*

(1) Begjæring om innsyn i opplysninger eller dokumenter i en sak kan sendes forvaltningsorganet i elektronisk form, jf. §§ 3 og 4.

(2) Fører forvaltningsorganet elektronisk arkiv, kan det gis tilgang til opplysninger og dokumenter i elektronisk form dersom den som begjærer innsyn samtykker eller ber om dette.

(3) Med mindre innsyn kan kreves etter offentlighetsloven, gis innsyn i elektronisk form bare når det kan oppnås:
   a) tilfredsstillende bekreftelse på at vedkommende har krav[63] på innsyn, og
   b) tilfredsstillende sikkerhet for at dokumentene kun gjøres tilgjengelige for denne.

§ 10 *Høring*

(1) Høringsbrev til institusjoner og organer som har egen elektronisk adresse kan sendes i elektronisk form. I stedet for utsending av alle sakens dokumenter kan det sendes melding om hvor høringsdokumentene er gjort tilgjengelige.[64]

---

[60] Fremgangsmåten og autentiseringsmekanismen fastsettes av forvaltningsorganet etter §§ 3 og 4 i forhold til hva som anses nødvendig på det enkelte område.

[61] Etter § 5 skal bekreftelse sendes straks en henvendelse er mottatt. Sammenholdt med § 8 annet ledd vil fristen for å sende bekreftelse være senest innen utløp av første virkedag etter at klagen ble sendt.

[62] For klager som ikke kommer frem til forvaltningsorganet, følger det av forvaltningsloven § 30 at klagen må sendes på ny innen en uke etter at klageren har fått vite om dette eller burde ha forstått det. Når klager sendes elektronisk, regnes fristen for å sende klagen på nytt fra det tidspunktet klageren burde ha mottatt bekreftelse, det vil si senest ved utløpet av første virkedag etter at klagen ble sendt første gang, jf. første punktum. Dersom det går lenger tid før klageren får sjekket om det er gitt bekreftelse, vil fristen for å sende ny klage regnes fra den dagen klageren burde ha blitt oppmerksom på at det ikke var gjort. Reglene om frist for å sende klage på nytt gjelder kun i de tilfeller klagefristen i mellomtiden er gått ut. Dersom klagefristen ikke er gått ut og klageren oppdager at klagen ikke er mottatt, er det selvsagt full anledning til å sende klagen på nytt.

[63] Det kan være andre grunnlag for å gi innsyn. Særlig praktisk er partenes innsynsrett etter reglene i forvaltningsloven § 18 flg. Videre har pasienter innsynsrett i sin journal etter reglene i pasientrettighetsloven § 5-1 og helsepersonelloven § 14. Dersom pasientjournalen føres elektronisk, kan også innsyn gis elektronisk så lenge kravene i bokstav a) og b) er oppfylt.

[64] Muligheten for å sende høringsbrev elektronisk forutsetter at mottaker har egen elektronisk adresse. Et annet alternativ er kun å sende melding om at høringsbrev er publisert på forvaltningsorganets hjemmeside, med adresse til den nettsiden hvor høringsbrevet ligger.

(2) Uttalelser til høringen kan avgis i elektronisk form, jf. §§ 3 og 4.[65]

Kapittel 3 Tiltak for sikker elektronisk kommunikasjon

§ 11 *Sikkerhetsmål og sikkerhetsstrategi*[66]

(1) Forvaltningsorgan som benytter elektroniske signaturer, systemer for innholdskryptering eller andre sikkerhetstjenester, skal[67] ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten ("sikkerhetsmål" og "sikkerhetsstrategi").

(2) Sikkerhetsstrategien skal være utarbeidet i henhold til anerkjente prinsipper[68] for informasjonssystemers sikkerhet. Sikkerhetsstrategien skal bl.a. inneholde:

Dersom noen høringsparter ikke har mulighet til å motta eller lese høringsbrev i elektronisk form, må høringsbrevet også sendes ut på papir. Se også utredningsinstruksen kapittel 5, utarbeidet av Arbeids- og administrasjonsdepartementet.

[65] For å kunne effektivisere behandlingen av uttalelser til høringen, vil det være en fordel om høringsinstansene gir sin uttalelse ved å fylle ut et nettbasert skjema på forvaltningsorganets hjemmeside. Adresse, fremgangsmåte og eventuelle sikkerhetstjenester kan fastsettes etter behov med hjemmel i §§ 3 og 4.

[66] Begrepene er hentet fra personopplysningsforskriften (for 2000-12-15 1265) § 2-3. Sikkerhetsmål i denne sammenheng beskrives som virksomhetens formål med bruk av sikkerhetstjenester og overordnede føringer for bruk av informasjonsteknologi. Dette vil være blant annet å realisere formålbestemmelsen i § 1, om å legge til rette for sikker og effektiv bruk av elektronisk saksbehandling.

Valg og prioriteringer for bruk av sikkerhetstjenester beskrives i en sikkerhetsstrategi. Sikkerhet vil omfatte både fysiske og administrative sikkerhetstiltak. Sikkerhetsstrategien vil reflektere det valgte sikkerhetsnivå. Sikkerhetsbestemmelsene i forskrift til personopplysningsloven kapittel II vil kunne gi en god veiledning omkring innholdet i sikkerhetsmål og sikkerhetsstrategi. Se også nedenfor om BS 7799:1999 – British Standard 7799. Sikkerhetsstrategien vil også inneholde krav som vil være relevante ved valg av sertifikatpolicy og øvrige krav for bruk av elektroniske signaturer og kryptering, jfr paragrafens annet ledd. Sertifikatpolicyen kan være utarbeidet av sertifikatutstederen eller av en brukergruppe, bransjeorganisasjon, standardiseringsorgan e.l. Slik f.eks. FNS sertifikatpolicy nr 1. FSP-1:1.0 For forvaltningens del kan man tenke seg at en mulig sertifikatpolicy utarbeides av et koordineringsorgan for forvaltningens bruk av sikkerhetstjenester, jfr § 28. Den enkelte sertifikatutsteder vil utarbeide en sertifiseringspraksis som konkretiserer prosedyrer og teknikker for *hvordan* sertifikatpolicyen oppfylles.

[67] Det lille ordet *skal* er i denne sammenhengen stort. Det pålegger forvaltningsorganer å utarbeide sikkerhetsmål og sikkerhetsstrategi *før* man setter i gang med de aktuelle sikkerhetstjenester og tilhørende sikkerhetsteknikker som elektronisk signatur og innholdskryptering. Vi snakker med andre ord ikke bare om tillit til tekniske løsninger, men tillit til et forvaltningsorgans evne til å ivareta sikkerhetsbehovene i et helhetlig og organisasjonsmessig forsvarlig perspektiv. Sikkerhetsmål og –strategi anses som viktige virkemidler for at det enkelte forvaltningsorgan skal klare å gjennomføre dette på en trygg og effektiv måte, og som et grunnlag for publikum, den enkelte borger og næringslivet, for å ha tillit til forvaltningen.

[68] Anerkjente prinsipper er gjerne nedfelt i standarder. En meget viktig standard på dette området er BS 7799:1999 – British Standard 7799. Denne er også blitt Norsk Standard og ISO-standard NS-ISO/IEC 17799 Utgave 1, 2001 Informasjonsteknologi - Administrasjon av informasjonssikkerhet (ISO/IEC 17799:2000) / Information technology - Code of practice for information security management (ISO/IEC 17799:2000). Virksomheter kan derved utvikle, implementere og måle virksomhetens sikkerhetsarbeid og rutiner. BS 7799 er basert på den

a) prosedyrer for anskaffelse, bruk, oppbevaring og sikring av signaturfremstillingsdata[69], passord/PIN-koder og dekrypteringsdata[70] knyttet til personlige sertifikat[71] eller sertifikat for ansatt i forvaltningen, jf. §§ 14,15, og 24;
b) prosedyrer for anskaffelse, bruk, oppbevaring og sikring av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsdata knyttet til virksomhetssertifikat, jf. § 12 nr. 3 og 4 og § 13;[72]
c) prosedyrer for å etablere og opprettholde et sikkert brukermiljø[73] der det benyttes elektroniske signaturer, innholdskryptering eller andre sikkerhetstjenester, jf. § 24 nr. 2;
d) prosedyrer for varsling[74] og sperring[75] av sertifikat og passord/PIN-koder ved mistanke om tap eller misbruk, jf. § 16;

---

beste nåværende praksis innen arbeidet med informasjonssikkerhet både i England og i flere andre land. Den ligger til grunn for en norsk ordning for frivillig sertifisering av informasjonssikkerheten i organisasjoner, forvaltet av Norsk Akkreditering, se under *Informasjonssikkerhet* på nettsiden deres: http://www.justervesenet.no/na/.

Se også rapporten Elektroniske signaturer – Myndighetsroller og regulering av tilbydere av sertifikattjenester http://odin.dep.no/nhd/norsk/publ/rapporter/024005-994081/index-dok000-b-n-a.html.

[69] Se § 2 nr 4

[70] Se § 2 nr 14

[71] Personlig sertifikat er et sertifikat utstedt til den enkelte personlig uten tilknytning til ansettelsesforhold. Disse kan benyttes i tjeneste for forvaltningsorgan kun hvis de er godkjent for det, jf § 14 (2).

[72] Virksomhetssertifikat er omtalt foran, se fotnote til § 2 nr 8. Siden virksomhetssertifikatet identifiserer forvaltningsorganet som sådan, er det ekstra viktig at sikkerhetsstrategien inneholder god ivaretakelse av sikkerheten rundt virksomhetens eget sertifikat utad. Det er i § 12 (2) lagt opp til at virksomhetssertifikatet bør brukes ved underretning om enkeltvedtak og høringer. Se for øvrig kommentarene til de andre punktene i denne paragrafen, som i hovedsak er relevante også for virksomhetssertifikat.

[73] Det er behov for å sikre at signaturframstillingsdata, og de dataene som skal signeres, ikke «angripes» eller «misbrukes» via det informasjonssystemet de benyttes i, f.eks. som følge av virus e.l. Dette stiller krav til signaturframstillingssystemet, brukerens øvrige systemkonfigurasjon, det omkringliggende miljøet («brannmurer» o.l.) og PC-er som sådanne. Slike krav må i første omgang ivaretas av den enhet som står for anskaffelse og drift av informasjonssystemene i virksomheten. I neste omgang må det stilles krav til brukeren om ikke å foreta handlinger som kan true sikkerheten i systemet, som ukritisk nedlasting eller installering av ikke godkjent programvare e.l.

[74] Et ledd i forsvarlig bruk av koder, passord, nøkler og nøkkelbærende medier er omgående varsling dersom det oppstår mistanke om at nøkler er tapt, kommet på avveie eller på annen måte blir eller kan bli misbrukt. Eieren av signaturframstillingsdata eller autentiseringsdata skal straks varsle sertifikatutsteder eller den som ellers er utpekt til å motta varsel dersom det oppstår mistanke om at signaturframstillingsdata eller autentiseringsdata er tapt, kommet på avveie eller på annen måte blir eller kan bli misbrukt. Prosedyrene for hvordan dette skal gjøres vil fremgå av forvaltningsorganets sikkerhetsstrategi og av sertifikatpolicyen for vedkommende sertifikat. Sertifikatutsteder vil i de fleste tilfeller være et privat rettsubjekt, ikke forvaltningsorganet selv. For de tilfeller der forvaltningsorganet selv er utsteder av sertifikater, skal varselet sendes til den enheten som forestår utstedelse og administrasjon av sertifikatene.

[75] Resultatet av at et sertifikat blir sperret er at sertifikatet settes opp på sertifikatutsteders tilbaketrekkingsliste/revokeringsliste og at brukerne ikke lenger har grunnlag for å ha tillit til sertifikatet. Den forvaltningsansatte får utstedt et nytt sertifikat med tilhørende nøkkelpar. Benyttes passord/PIN-kode må dette endres.

e) prosedyrer for kontroll[76] av sertifikater og tilbaketrekkingslister[77] ved mottak av melding utstyrt med elektronisk signatur, herunder krav til hvor oppdatert[78] informasjon om sertifikaters status bør være for de ulike formål sertifikatene benyttes for, jf. § 18;
f) prosedyrer for sperring[79] av sertifikat mv. ved misbruk av elektronisk kommunikasjon med forvaltningen, jf. § 19;

---

[76] Ved mottak av melding utstyrt med signatur må det blant annet kontrolleres om signaturen kan verifiseres, om de relevante sertifikater fortsatt er gyldige og tilfredsstillende for den aktuelle anvendelsen, om sertifikatet tilhører rett person mv. Hvilke kontroller som skal gjennomføres og hvilken tilleggsinformasjon som skal innhentes, vil avhenge av hvilken tjeneste som benyttes, og hvor kritisk den enkelte anvendelse er. Kravene vil være definert i virksomhetens sikkerhetsmål og sikkerhetsstrategi, samt i sertifikatutstederens signaturpolicy.

Spørsmålet om i hvilken grad saksbehandler skal gjennomføre de aktuelle kontrollene, er avhengig av hvilke tjenester som finnes sentralt i organet og hvilke funksjoner som løses automatisk i den enkeltes lokale arbeidsstasjon. Dette er imidlertid oppgaver som i størst mulig grad bør løses automatisk. Hvis verifisering ikke lykkes, og dette innebærer at videre behandling av meldingen ikke kan skje, må saksbehandler initiere melding til avsender i henhold til reglene om meldinger som ikke tilfredsstiller kravene i § 6 (2).

[77] Rutinene for tilbakekalling av sertifikater, herunder hvem som er berettiget til å trekke et sertifikat tilbake er kritiske for påliteligheten i systemet. Det samme gjelder tilgang til oversikter over tilbaketrukne sertifikater. Sertifikatutsteder er ansvarlig for å ajourføre tilbaketrekkingslister/revokeringslister (CRL). Sertifikatpolicyen omtaler revokeringslistens oppdateringsfrekvens. Se også notene til § 11 (2) bokstav d) ovenfor.

[78] Forvaltningsorganet må fastsette sine egne krav til hvor oppdaterte opplysningene om sertifikaters status skal være for ulike anvendelser. For særlig kritiske anvendelser kan det være nødvendig å kreve tilgang til kontinuerlig oppdaterte opplysninger, i andre tilfeller kan en mer sporadisk oppdatering være tilstrekkelig. Forvaltningsorganet bør bare akseptere sertifikater utstedt under en sertifikatpolicy som støtter de kravene som er stilt. ETSI TS 101 456 sertifikatpolicy for kvalifiserte sertifikater, pkt 7.3.6 a) stiller krav om at det skal ta maksimum en dag (at most one day) fra anmodning om tilbaketrekking er mottatt av sertifikatutsteder til den skal være tilgjengelig på tilbaketrekkingslisten. Hvis det benyttes tilbaketrekkingslister skal disse som et minimum oppdateres daglig, jfr ETSI TS 101 456 pkt 7.3.6 G).

For sertifikater som er utstedt under ETSI's Lightweight Certificate Policy, se ETSI TS 102 042, skal tilbaketrekkingslister oppdateres minst hver 72 time, dvs hver tredje dag, jfr pkt 7.3.6 g). Det norske ZebSign's signaturpolicy har i pkt. 4.4.9 angivelse om at listen skal oppdateres hver 24 time eller hver gang et sertifikat er trukket tilbake.

[79] Elektronisk saksbehandling må bygge på tillit til de valgte sikkerhetsløsningene. Men sikkerheten avhenger av at brukerne opptrer aktsomt og lojalt. Dersom et antall brukere misbruker en sikkerhetsløsning, vil dette svekke tilliten til løsningen som helhet. Det bør derfor være mulig å sperre for brukere som misbruker løsningen. Sperring kan f.eks. skje ved at brukernavn sperres, eller at sertifikater trekkes tilbake.

Dette kan være et anliggende for den enkelte sertifikatutsteder, men kan også gjelde forvaltningsorganet direkte, enten fordi forvaltningsorganet selv administrerer koder eller passord, eller fordi forvaltningsorganet ikke lenger har grunn til å ha tillit til bruken av et bestemt sertifikat. Dersom borgeren benytter et sertifikat fra en frittstående sertifikatutsteder, og dette sertifikatet kan benyttes også til andre formål enn kommunikasjon med forvaltningen, er det ikke sikkert at et eventuelt misbruk i forbindelse med f.eks. rapportering til forvaltningen gir grunnlag for å trekke tilbake sertifikatet som sådant, i og med at slik tilbaketrekking også vil sperre for andre anvendelser. Det kan likevel være grunn for forvaltningsorganet til å sperre sertifikatet *for bruk mot forvaltningen*. Det kan i så fall skje ved hjelp av lokale sperrelister, eventuelt ved samkjøring med satsvis nedlastede sperrelister fra sertifikatutsteder. En slik løsning vil være mindre inngripende overfor sertifikateier enn sperring av sertifikatet i sertifikatutsteders sperreliste.

g) prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon, jf. §§ 20 og 22;[80]
h) prosedyrer for sikkerhetskopiering, oppbevaring og deponering av dekrypteringsdata[81] for opplysninger som angår forvaltningsorganet, jf. § 23.[82]

Samtidig må man ta høyde for at sperring av koder eller sertifikater kan ha inngripende virkning overfor den enkelte. Derfor må det etableres rutiner for kvalitetssikring av opplysninger som ligger til grunn for en slik avgjørelse, adgang til overprøving, håndtering av sertifikater mens klagen er under behandling, og prosedyrer som sikrer at slik behandling skjer raskt. Disse reglene finnes i § 19. Hjemmel for denne relativt inngripende bestemmelsen er forvaltningsloven § 15 a bokstav e).

[80] Forvaltningsorganet skal beskrive sine prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon, se også personopplysningsloven §§ 13 og 14 med utfyllende forskrifter. Forvaltningens plikt til å sikre informasjon etter reglene om taushetsplikt og behandling av personopplysninger bør, om ikke annet som et utslag av veiledningsplikten, også utløse plikt til å informere borgerne om de risikoer som hefter ved elektronisk formidling av (person)opplysninger, og til å legge til rette for at borgerne enkelt kan få tilgang til hensiktsmessige sikkerhetstjenester.

Taushetsplikten og behandlingsreglene gjelder normalt forvaltningsorganet som sådant. Den enkelte borger kan utvilsomt beslutte at vedkommende selv vil sende opplysninger ubeskyttet til forvaltningen. Men en slik beslutning bør være basert på relevant og tilstrekkelig informasjon slik at vedkommende fatter en «opplyst beslutning». Dersom forvaltningsorganet aktivt gjør tilgjengelig en kommunikasjonskanal som innebærer en risiko for brukerne, vil det formodentlig føre til skjerping av veiledningsplikten, slik at den enkelte bedre kan ivareta sine interesser.

Plikten må være begrenset til de tilfellene der forvaltningen faktisk har kontakt med vedkommende før opplysninger overføres, f.eks. ved at vedkommende slår opp på relevant web-side, laster ned et passende skjema eller på annen måte får tilgang til informasjon som opplyser om eller gir inntrykk av at opplysninger kan sendes elektronisk. Den helt egeninitierte sendingen av førstehenvendelse pr. e-post med personopplysninger eller annen informasjon som vil være taushetsbelagt på forvaltningens hånd, kan man vanskelig gjøre noe med.

[81] Jf § 2 nr 14.

[82] Det er naturligvis viktig at materiale ikke blir utilgjengelig for forvaltningsorganet som følge av at krypteringsnøkler går tapt. Det kan derfor være aktuelt å stille krav om sikkerhetskopiering og/eller deponering av krypteringsnøkler.

Det finnes motforestillinger av personvernmessig art når det gjelder krav om sikkerhetskopiering og deponering av krypteringsnøkler. Men dersom det etableres krav om at man skal benytte krypteringsnøkkel knyttet til forvaltningsorganet (og ikke til saksbehandler) ved kryptering av materiale til organet, og kravet til kopiering/oppbevaring eller deponering knyttes til slike nøkler, burde betenkelighetene bli mindre.

Hvis man legger restriksjoner på bruk av forvaltningsansattes krypteringsnøkler til kun å gjelde kommunikasjon i forvaltningens tjeneste, bør det heller ikke være store betenkeligheter knyttet til krav om sikkerhetskopiering og eventuell deponering av slike nøkler.

Det kan imidlertid tenkes tilfeller der rutiner for bruk av den forvaltningsansattes egen nøkkel er begrunnet i at organet ikke uten videre skal ha tilgang til den informasjon den enkelte saksbehandler mottar. I så fall må man vurdere strammere rutiner for deponering enn hva som ellers benyttes for organets nøkler. Det må likevel bare være i unntakstilfellene at det overhodet ikke skal være adgang til sikkerhetskopiering eller deponering av krypteringsnøkler som benyttes for materiale som gjelder forvaltningsorganets virksomhet.

Sikkerhetskopiering og/eller deponering av krypteringsnøkler forutsetter gode prosedyrer for sikring av kopiene slik at materiale ikke blir gjort tilgjengelig for uvedkommende. Tilgang til slikt materiale bør kunne gjøres tilgjengelig uten tidkrevende prosedyrer når behovet først oppstår. En begjæring fra lederen av den delen av forvaltningsorganet som det krypterte materialet sorterer under, eventuelt vedkommendes overordnede, bør antakelig være

§ 12 *Sertifikat for forvaltningsorgan (virksomhetssertifikat)*[83]

(1) Forvaltningsorgan som benytter elektronisk signatur kan[84] benytte virksomhetssertifikat.

(2) Ved underretning om enkeltvedtak etter § 7 og ved høringer etter § 10 bør det benyttes virksomhetssertifikat.[85]

(3) Ved bruk av virksomhetssertifikat skal forvaltningsorganet sikre at ikke uvedkommende får tilgang til eller kan benytte tilhørende signaturfremstillingsdata. Organet skal også sikre tilfredsstillende kontroll med og registrering av personell og aktiviteter som benytter slike signaturfremstillingsdata. Sikringstiltakene skal skje i henhold til organets sikkerhetsstrategi.

(4) Signaturfremstillingsdata knyttet til virksomhetssertifikat bør ikke deles av flere personer.

---

tilstrekkelig. Ettersom det krypterte materialet, etter den avgrensningen som er brukt her, gjelder forvaltningsorganets forhold, burde ytterligere begrensninger normalt ikke være nødvendig.

Hvis det skal være alminnelig adgang for den enkelte til også å benytte sin krypteringsnøkkel for private formål, bør man antakelig vurdere spørsmålet om sikkerhetskopiering/deponering om igjen. Det anbefales imidlertid at man reserverer bruken av forvaltningsorganets og saksbehandlers krypteringsnøkkel for materiale som angår forvaltningsorganet.

[83] Se også fotnote til § 2 nr 8, om virksomhetssertifikat, og fotnote til § 11 (2) b). Bestemmelsen om virksomhetssertifikat innebærer en litt ny måte å tenke på, i forbindelse med elektronisk saksbehandling og kommunikasjon. Det anbefales i mange sammenhenger, og som en hovedregel, å bruke sertifikat som identifiserer selve virksomheten, ved hjelp av den sikkerhetsteknikken som elektronisk signatur innebærer. Den ansvarlige saksbehandler og leder navngis selvfølgelig også, men da med "trykte bokstaver", ikke nødvendigvis med en mer eller mindre uleselig underskrift. Formalitetene og ansvaret for korrekt saksbehandling foreslås i utgangspunktet ikke forandret, bortsett fra selve underskriftsfunksjonen. Hvis man for interne formål likevel ønsker å beholde håndskrevne underskrifter på papir, vil en eventuell elektronisk kommunikasjon eksternt tilsi at disse *ikke kan* følge med. Da kunne man legge opp til at saksbehandlers og leders underskrifter isteden ble gjort ved hjelp av elektroniske signaturer, med bruk av tilhørende sertifikater. På det stadiet denne sikkerhetsteknikken er i dag, ville dette imidlertid kunne by på en del praktisk problemer, og det kunne være tungt å få til, ikke minst i en startfase. Dessuten har ikke publikum behov for den høye grad av sikker identifisering av enkeltpersoner som er involvert.

Publikums behov er først og fremst knyttet til å være trygg på at det faktisk er det konkrete forvaltningsorganet som har sendt vedtaket eller lignende, og at dette er til å stole på. Både ut fra hva som er de reelle behovene involvert, og av rene effektiviseringsgrunner, bør man derfor legge opp til at kommunikasjonen ut av huset blir påført elektronisk signatur kun ett sted, som sikkert identifiserer selve forvaltningsorganet overfor borgere og næringsliv. Dermed unngår man også å skyte spurv med kanoner. Det enkelte forvaltningsorgan kan plassere denne sikkerhetsfunksjonen på et dertil egnet sted, for eksempel som en oppgave hos arkivfunksjonen, eller et annet sentralt sted, som er i stand til også å ivareta andre viktige forhold som effektiv journalføring, bidra til gjennomføring av innsynsrett mv. Det kan også være aktuelt å vurdere om en slik sentral funksjon skal være automatisert, slik at meldinger kan sendes ut eller gjøres tilgjengelig på aktuelt informasjonssystem uavhengig av om arkiv/postmottak er bemannet.

[84] "Kan" betyr selvfølgelig ikke en plikt, men det ligger en sterk anbefaling i dette.

[85] Dette er en annen anbefaling, som gjenspeiler en tro på at det kan realiseres betydelige effektivitetsgevinster ved å legge opp til rasjonell bruk av sertifikater for virksomheten som sådan for viktig kommunikasjon, og ikke minst i forbindelse med store volumer.

§ 13 *Sikring av signaturfremstillingsdata og dekrypteringsdata ved bruk av virksomhetssertifikat*[86]

(1) Ved bruk av virksomhetssertifikat, jf. § 12, skal det være lagt opp rutiner som sikrer at systemet raskt kan settes i drift med nye signaturfremstillingsdata og nytt sertifikat dersom det sertifikatet som er i bruk blir trukket tilbake eller signaturfremstillingsdata går tapt.
(2) Det skal vurderes om forvaltningsorganet bør være utstyrt med signaturfremstillingsdata og virksomhetssertifikat fra mer enn én sertifikatutsteder.
(3) Signaturfremstillingsdata og dekrypteringsdata skal være sikret mot misbruk i henhold til forvaltningsorganets sikkerhetsstrategi.

§ 14 *Restriksjoner på bruk av sertifikat mv.*

(1) Signaturfremstillingsdata, sertifikat eller passord/PIN-koder som er ment for bruk i tjeneste for forvaltningen skal ikke benyttes for andre formål.
(2) Personlige sertifikat skal ikke benyttes i tjeneste for forvaltningen med mindre det er utstedt eller godkjent for slik bruk.
(3) Et forvaltningsorgan kan bestemme at sertifikat som er utstedt til publikum spesielt for kommunikasjon med forvaltningen eller et bestemt forvaltningsorgan ikke skal benyttes for andre formål. Slike begrensninger må fremgå av sertifikatet og brukeren skal opplyses om begrensningene.

§ 15 *Krav til oppbevaring og bruk av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsdata*[87]

(1) Innehaver av signaturfremstillingsdata skal oppbevare og benytte disse på en slik måte at de ikke gjøres tilgjengelige for andre.
(2) Innehaver skal aldri forlate arbeidsstasjon og lignende uten å sikre at signaturfremstillingsdata ikke er tilgjengelige for andre. Innehaver skal sikre:
    a) at signaturfremstillingsdata fjernes fra arbeidsstasjonen dersom dataene er lagret i smartkort e.l., og
    b) at arbeidssesjonen er avsluttet og eventuelle lagrede eller behandlede signaturfremstillingsdata er deaktivert, eller
    c) at signaturfremstillingsdata på annen måte er sikret mot misbruk.
(3) Innehaver av signaturfremstillingsdata skal ikke overlate disse til andre eller gi andre tilgang til dem. Skal noen handle på vegne av en annen skal dette skje med fullmektigens egne signaturfremstillingsdata.
(4) Bestemmelsene om oppbevaring og bruk av signaturfremstillingsdata gjelder tilsvarende for bruk av passord/PIN-koder o.l. og dekrypteringsdata.

[86] Reglene i § 13 skal sikre forvaltningsorganet mot sårbarhet ved bruk av virksomhetssertifikater. Det legges stor vekt på at organets sikkerhetsstrategi må inneholde et gjennomarbeidet opplegg for å ivareta de mest grunnleggende sikkerhetsbehovene, tilpasset det enkelte organs virksomhet og behov.

[87] Her følger det gode regler for å holde orden i eget hus. Siden dette er et nytt område, er reglene noe mer detaljerte, og de kan ved behov suppleres og tilpasses virksomheten i sikkerhetsstrategien.

§ 16 *Varslingsplikt ved tap eller mistanke om misbruk av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsdata*

(1) Innehaver av signaturfremstillingsdata skal straks varsle sertifikatutsteder eller den som ellers er utpekt til å motta varsel, dersom det oppstår mistanke om at signaturfremstillingsdata er tapt, kommet på avveie eller på annen måte blir eller kan bli misbrukt.[88] Det samme gjelder for bruk av passord/PIN-koder o.l. og dekrypteringsdata.

§ 17 *Informasjon til publikum*

(1) Forvaltningsorganet skal sørge for at publikum får informasjon som nevnt i § 25 i forbindelse med anskaffelse av sertifikat eller, hvis det ikke er mulig, ved første gangs bruk av slike tjenester ved kommunikasjon med et forvaltningsorgan.[89]

§ 18 *Krav til kontroll av sertifikater og tilbaketrekkingslister*

(1) Ved mottak av melding som er underlagt krav om bruk av avansert elektronisk signatur, skal forvaltningsorganet, i henhold til kravene fastsatt i organets sikkerhetsstrategi, kontrollere:
   a) at signaturen teknisk lar seg verifisere, herunder at meldingen ikke er endret,
   b) at tilknyttet sertifikat fortsatt er gyldig og ikke suspendert eller trukket tilbake,
   c) at sertifikatet er egnet for den aktuelle anvendelse, herunder sertifikatets sikkerhetsnivå og eventuelle begrensninger i sertifikatets anvendelsesområde,
   d) at sertifikatet er utstedt av en sertifikatutsteder som anbefales eller er anerkjent av koordineringsorganet, jf. § 28, eller som forvaltningsorganet kan akseptere i henhold til sin sikkerhetsstrategi.

(2) Hvis en melding som er signert med avansert elektronisk signatur ikke tilfredsstiller kontrollene i første ledd, og dette har betydning for behandling av meldingen i forvaltningsorganet, skal det sendes melding til avsender i henhold til reglene i § 6.

---

[88] Et ledd i forsvarlig bruk av koder, passord, nøkler og nøkkelbærende medier er omgående å varsle sertifikatutsteder, eller tjenesteyter utpekt av denne, dersom det oppstår mistanke om at nøkler er tapt, kommet på avveie eller på annen måte blir eller kan bli misbrukt. Dette gjelder uavhengig av hvem eieren er. Bestemmelsen retter seg altså både til forvaltningens tjenestemenn og til borgerne. For forvaltningens tjenestemenn skal varslingsprosedyrene være beskrevet i sikkerhetsstrategien som forvaltningsorganet har plikt til å utarbeide, se § 11 2.ledd bokstav d) og i samsvar med den anvendte sertifikatpolicy. For brukerne vil sertifikatutsteders sertifikatpolicy gi anvisning på varslingsprosedyrer og tidspunkter for innplassering i tilbaketrekkingslister mv. Se også kommentarene til § 11.

[89] De enkelte forhold som forvaltningsorganet har en plikt til å informere publikum om, er gjengitt tilsvarende i § 25 (om hva egne ansatte skal informeres om). Selv om dette involverer teknisk avanserte teknikker for sikkerhet, vil sikkerheten også avhenge av at menneskene har fått tilstrekkelige kunnskaper, og at de følger de vanligste spillereglene. …det svakeste ledd i en kjede… osv.

§ 19 *Sperring i et forvaltningsorgan av sertifikat mv. ved misbruk av elektronisk kommunikasjon med forvaltningen*

(1) Ved begrunnet mistanke om misbruk av signaturfremstillingsdata og sertifikat ved elektronisk kommunikasjon med forvaltningsorgan, kan forvaltningsorganet sperre sertifikatet eller tilknyttet brukeridentitet for videre bruk mot organet. Det samme gjelder dersom sertifikatinnehaver misbruker tillatelsen eller adgangen til å kommunisere elektronisk med organet.[90]

(2) Før sertifikatet sperres, skal forvaltningsorganet sende sertifikatinnehaver melding om at det vurderer å sperre sertifikatet og begrunnelsen for dette. Sertifikatinnehaver skal oppfordres til å uttale seg om grunnlaget for sperringen. Forvaltningsorganet skal sette en frist for slik uttalelse. I særlige tilfeller kan forvaltningsorganet sperre sertifikatet samtidig med at varsel sendes.[91]

(3) Dersom forvaltningsorganet etter å ha vurdert sertifikatinnehavers uttalelse, velger å sperre sertifikatet, skal forvaltningsorganet straks sende sertifikatinnehaver melding om dette.

(4) Sertifikatinnehaver kan påklage avgjørelse om sperring. Reglene i forvaltningsloven[92] kap. VI gjelder tilsvarende så langt de passer.

(5) Bestemmelsene gjelder tilsvarende for sperring av brukeridentitet med tilhørende passord/PIN-koder, i informasjonssystemer tilrettelagt av forvaltningsorganet, så langt de passer.

§ 20 *Informasjon til publikum ved formidling av taushetsbelagt informasjon og personopplysninger til forvaltningen*[93]

(1) Når et forvaltningsorgan legger til rette for elektronisk kommunikasjon av opplysninger som på forvaltingens hånd kan være underlagt taushetsplikt, krav til sikring etter reglene om behandling av personopplysninger eller tilsvarende regler, skal risiko for uberettiget innsyn i slike opplysninger være forebygget på tilfredsstillende måte.

---

[90] Dersom borgeren benytter et sertifikat fra en frittstående sertifikatutsteder, og dette sertifikatet kan benyttes også til andre formål enn kommunikasjon med forvaltningen, er det ikke sikkert at et eventuelt misbruk i forbindelse med f.eks. rapportering til forvaltningen gir grunnlag for å trekke tilbake sertifikatet som sådant, i og med at slik tilbaketrekking også vil sperre for andre anvendelser. Det kan likevel være grunn for forvaltningsorganet til å sperre sertifikatet for bruk mot forvaltningen. Det kan i så fall skje ved hjelp av lokale sperrelister, eventuelt ved samkjøring med satsvis nedlastede sperrelister fra sertifikatutsteder. En slik løsning vil være mindre inngripende overfor sertifikateier enn sperring av sertifikatet i sertifikatutsteders sperreliste.

[91] Før sperring skjer, må sertifikateier få anledning til å uttale seg. Ettersom sperring av sertifikat forutsetningsvis er en reaksjon på et grovt tillitsbrudd fra sertifikateier overfor forvaltningsorganet, og fortsatt misbruk vil kunne påføre forvaltningen eller andre tap eller merarbeid, bør ikke fristen være lenger enn det som er nødvendig for sertifikateier for å rette innvendinger mot sperring av sertifikatet. I tilfelle der det er tale om særlige grove brudd kan forvaltningsorganet sperre for bruk samtidig med at varsel sendes.

[92] lov av 10. februar 1967 om behandlingsmåten i forvaltningssaker

[93] Forvaltningen har en plikt til å sikre informasjon iht regler om bl.a. taushetsplikt, personvern. Når forvaltningen inviterer publikum til å kommunisere elektronisk, må eventuelle risiki varsles om, og det må informeres godt og grundig om hvordan publikum skal gå frem for å gjøre dette på en trygg måte.

(2) Forvaltningsorgan som legger til rette for å motta opplysninger som nevnt i nr. 1, skal på hensiktsmessig måte informere om eventuelle risiki ved elektronisk overføring av slike opplysninger og om hva som er rette elektroniske adresse.
(3) Forvaltningsorganet skal sørge for at nødvendige sikkerhetstjenester er lett tilgjengelige eller gi opplysninger som gjør at den enkelte lett kan få tilgang til slike tjenester.
(4) Forvaltningsorganet skal også opplyse om hvordan taushetsbelagt informasjon og personopplysninger sikres under behandling i forvaltningsorganet.

§ 21 *Kryptering av melding til forvaltningen*

(1) Ved kryptering av melding til forvaltningen skal forvaltningsorganets krypteringsdata eller krypteringsdata til en nærmere angitt enhet ved forvaltningsorganet benyttes.
(2) Kryptering med en saksbehandlers krypteringsdata kan bare benyttes dersom organet har lagt spesielt til rette for det.

§ 22 *Mottak av kryptert materiale*[94]

(1) Melding som mottas av forvaltningsorganet i kryptert form, skal straks dekrypteres.
(2) Hvis meldingen ikke lar seg dekryptere ved mottak, skal det straks sendes melding tilavsender med beskjed om at forvaltningsorganet ikke får tilgang til meldingens innhold. § 6 gjelder tilsvarende.
(3) Forvaltningsorganet skal sikre opplysningene under den videre behandling i organet i henhold til de regler som gjelder for de aktuelle opplysningene.

§ 23 *Sikkerhetskopiering av dekrypteringsdata mv.*

(1) Forvaltningsorganet skal sikre at opplysninger som er mottatt av organet ikke blir utilgjengelige som følge av at dekrypteringsdata går tapt. Det skal alltid finnes kopi av dekrypteringsdata for opplysninger som angår forvaltningsorganet.
(2) Prosedyrer for sikkerhetskopiering, oppbevaring, deponering og utlevering av dekrypteringsdata skal følge anerkjente prinsipper og skal fremgå av forvaltningsorganets sikkerhetsstrategi.

Kapittel 4 Regler for forvaltningsorgan - Krav til forvaltningsorganets utstyr og opplæring av ansatte

§ 24 *Anskaffelse av utstyr og data til ansatte*

(1) Et forvaltningsorgan skal gi sine ansatte anvisning[95] på hvilke sikkerhetstjenester[96] de skal benytte under tjeneste for organet, og hvorledes

[94] Ved mottak av kryptert materiale er det viktig å gjøre innholdet leselig for organet, og den bør sjekkes for virus mv før den behandles videre i det interne systemet. Beskyttelse deretter kan skje med andre midler enn kryptering overfor omverdenen, fordi det er kjente deltakere og truslene mot meldingen/dokumentet da er annerledes/mindre.

[95] For å kunne iverksette elektronisk saksbehandling i større skala må arbeidsgiver kunne pålegge den forvaltningsansatte å ta i bruk de sikkerhetstjenester som forvaltningsorganet har

de skal gå frem for å anskaffe nødvendig utstyr og data, herunder signaturfremstillingsdata[97] og dekrypteringsdata[98] med tilhørende sertifikat[99] samt passord og PIN-koder[100] mv.

(2) Forvaltningsansatte skal følge instruksene[101] arbeidsgiver har fastsatt om bruk og sikring[102] av virksomhetens informasjonssystemer, herunder om

---

valgt å benytte i sin saksbehandling. Dette kan være bruk av ansattsertifikater for den enkelte tjenestemann eller virksomhetssertifikater for den enkelte virksomhet. Det kan også gjelde andre sikkerhetstjenester som bruk av passord og PIN-koder, samt bruk av krypteringsutstyr mv. Hva som benyttes i det enkelte organ vil være avhengig av organets vurdering av dets behov.

På hvilken måte tildeling av nøkler, koder og sertifikater skal skje, og hvor den enkelte må henvende seg for registrering e.l., vil være avhengig av hvilke(n) tjeneste(r) som er valgt. Arbeidsgiver må derfor gi den forvaltningsansatte anvisning om dette.

Hvilke forhold som skal dokumenteres ved anskaffelse av nøkler, koder eller sertifikat mv., vil avhenge av hvilken sikkerhetsløsning som er valgt. For et ansattsertifikat vil det normalt være tilstrekkelig å få dokumentert brukers identitet og ansettelsesforhold. For andre typer av sertifikater kan det i tillegg være nødvendig med opplysning om vedkommendes fullmakter, profesjonstilknytting e.l.

Prosedyrer og krav til dokumentasjon i forbindelse med anskaffelse av sertifikat vil framgå av den sertifikatpolicy forvaltningsorganet har valgt, og som det skal utstedes sertifikat i henhold til. En sertifikatpolicy beskriver krav til hvordan sertifikater utstedes og behandles, og danner grunnlag for hvilken tillit man kan ha til sertifikatene. *Hvordan* kravene oppfylles konkretiseres vanligvis i en såkalt sertifiseringspraksis. Det kan være vanskelig for den enkelte å sette seg inn i en sertifikatpolicy. Derfor bør arbeidsgiver trekke ut det som er relevant for tjenestemannen.

[96] Sikkerhetstjeneste er i denne sammenheng en overordnet betegnelse på en egenskap eller ytelse som en ønsker eller trenger i et system, og sier ikke noe om hvilken teknologi som benyttes for å realisere løsningen. Sikkerhets*tjenester* realiseres eller implementeres ved hjelp av spesifikke sikkerhets*mekanismer* eller sikkerhets*teknikker*. Noen av de viktigste sikkerhetstjenestene er autentisering (§ 2 nr 9), integritet (§ 2 nr 11), ikke-benekting (§ 2 nr 10) og innholdskryptering (§ 2 nr 12). Disse kan ivaretas av sikkerhetsteknikker/-mekanismer som kryptering og digitale signaturer. Se mer om dette i den generelle delen av veiledningen.

[97] Jf § 2 nr 4

[98] Jf § 2 nr 14

[99] Jf § 2 nr 6. Se også avsnittet om sertifikater i den innledende del av veiledningen.

[100] Personal Identification Number (PIN)

[101] En har valgt å inkorporere retningslinjer som berører forvaltningsinterne forhold i forskriften. Se her for eksempel de fleste bestemmelsene i denne forskriftens kapittel 3. Disse kunne vært gitt som instruks. Dette kunne muligens gitt mer fleksibilitet i utvikling og tilpasning av regelverket, samt at en kunne unngått at forskrifter rettet mot allmennheten ble mer omfattende enn nødvendig.

Imidlertid ville det skape ekstra utfordringer med hensyn til regelverksadministrasjon og -vedlikehold, fordi det er en tett indre sammenheng mellom reglene som retter seg innad mot forvaltningen, og reguleringen av borgernes rettigheter og plikter når det gjelder kommunikasjon med forvaltningen. Fordi også kommunalforvaltningen omfattes, vil instruksjonsmyndigheten for et sentralt statlig organ ikke uten videre strekke til. Og det synes unaturlig å innføre en særskilt instruksjonsmyndighet på dette området. Det virker mer ryddig å operere med forskrifter forankret i lov for de reglene som skal være felles for alle forvaltningsorganer for stat og kommune.

[102] Bestemmelsen tar først og fremst sikte på å beskytte og sikre brukermiljøet. Det er behov for å sikre at signaturframstillingsdata, og de dataene som skal signeres, ikke «angripes» eller «misbrukes» via det informasjonssystemet de benyttes i, f.eks. som følge av virus e.l. Dette stiller krav til signaturframstillingssystemet, brukerens øvrige systemkonfigurasjon, det

kontroll med materiale som skal lastes ned eller installeres på den ansattes arbeidsstasjon.

(3) Når det benyttes elektroniske signaturer[103], skal forvaltningsorganet ha innhentet samtykke[104] fra de ansatte i henhold til lov om elektronisk signatur[105] §§ 7 og 14 annet ledd bokstav b) om utstedelse og utlevering av sertifikat.[106]

§ 25 *Forvaltningsorganets informasjonsplikt til ansatte*

(1) Ved anskaffelse av utstyr og data som nevnt i § 24(1), plikter forvaltningsorganet å sørge for at den ansatte får informasjon om:
   a) vedkommendes ansvar og plikter i forbindelse med oppbevaring og bruk[107] av signaturfremstillingsdata[108] og dekrypteringsdata[109] med tilhørende sertifikat[110] samt passord og PIN-koder mv.,

---

omkringliggende miljøet («brannmurer» o.l.) og PC-er som sådanne. Slike krav må i første omgang ivaretas av den enhet som står for anskaffelse og drift av informasjonssystemene i virksomheten. I neste omgang må det stilles krav til brukeren om ikke å foreta handlinger som kan true sikkerheten i systemet, som ukritisk nedlasting eller installering av ikke godkjent programvare e.l.

[103] Jf § 2 nr 1.

[104] I henhold til lov om elektronisk signatur (lov 15. juni 2001 nr. 81) kan opplysninger som skal benyttes i sertifikater, bare innhentes direkte fra den opplysningen gjelder, eller med dennes uttrykkelige samtykke, jf. § 7.

Videre kan sertifikatutsteder ikke utlevere sertifikat til andre uten sertifikateiers samtykke, jf. § 14 annet ledd, bokstav b. (§ 14 regulerer bare utstedelse av kvalifiserte elektroniske signaturer, jf § 2 om lovens virkeområde) Dersom det skal være åpning for at den forvaltningsansatte selv signerer utgående meddelelser, må det innhentes samtykke til utlevering av sertifikat.

Det er neppe praktisk eller holdbart at mottaker av en melding, signert av en forvaltningsansatt i tjeneste, ikke skal få tilgang til det aktuelle sertifikatet. Dersom slikt samtykke ikke blir gitt, bør konsekvensen være at den ansatte ikke kan drive utadrettet saksbehandling i elektronisk form.

I normaltilfellene vil relevant sertifikat være vedlagt meldingen slik at utlevering fra sertifikatutsteder ikke er nødvendig. Man bør imidlertid ikke utelukke muligheten for å hente sertifikat direkte fra utsteder (eller eventuelt forvaltningsorganets hjemmeside), og følgelig bør samtykke innhentes rutinemessig. Sertifikat som skal benyttes i forbindelse med kryptering (ved hjelp av mottakers offentlige nøkkel) må hentes hos sertifikatutsteder hvis ikke avsender er kjent med sertifikatet fra før. Slikt sertifikat omfattes imidlertid ikke av lov om elektronisk signatur.

[105] Lov om elektronisk signatur 15. juni 2001 nr. 81.

[106] Jfr § 2 nr 6 med fotnote.

[107] Uansett hvilken løsning som velges for den enkelte anvendelse, må det stilles krav til den enkeltes omgang med og bruk av signaturframstillingsdata eller autentiseringsdata. Dette er en forutsetning for at man kan ha tillit til løsningen.

Det er gitt detaljerte regler i § 15 om hvordan tjenestemannen skal forholde seg. Dette innebærer for det første å sikre at andre ikke får tilgang til koder og nøkler. Hvis signaturfremstillingsdata er lagret i smartkort skal dette fjernes fra arbeidsstasjonen når en selv forlater denne. Er signaturfremstillingsdata lagret i programvare i maskinen skal signaturfremstillingsdataene være deaktivert eller på annen måte sikret mot misbruk.(En del av disse problemene løses hvis signaturfremstillingsdataene beskyttes med passord som må brukes ved hver signering.) Tilsvarende må gjelde for oppbevaring og bruk av passord/PIN-koder. Disse skal oppbevares på en slik måte at de ikke blir kjent av uvedkommende.

b) restriksjoner[111] på bruk av data som nevnt i bokstav a),
c) egen og andres mulighet for å sperre[112] eller suspendere sertifikat,
d) utløp[113] av sertifikat,
e) hvilke opplysninger[114] om den enkelte som vil fremgå av sertifikatet og sertifikatutsteders behandling av personopplysninger, jf. personopplysningsloven[115] § 19, og
f) forvaltningsorganets sikkerhetsstrategi[116] for øvrig.

Tjenestemannen må omgående varsle dersom det oppstår mistanke om at nøkler er tapt, kommet på avveie eller på annen måte blir eller kan bli misbrukt. Dette er det gitt bestemmelse om i §16.

Restriksjoner på bruk av den ansattes sertifikat til bruk for private formål mv. finnes i § 14.

[108] Jf § 2 nr 4.

[109] Jf § 2 nr 14.

[110] Jfr § 2 nr 6 med fotnote.

[111] Instruksen kan angi at koder og nøkler bare benyttes til det formålet de er utstedt for. Dette er også gitt som regel i § 14. Eksempelvis skal de ikke brukes i private formål. Likeledes kan instruksen bestemme at private sertifikat ikke skal benyttes til tjenesteformål hvis de ikke er godkjent for slik bruk.

[112] Bestemmelsen knytter an til pliktene alle innehavere av signaturfremstillingsdata har etter § 16. Dette er viktig for å bevare tillit til sikkerhetsløsningene at den enkelte tjenestemann aktivt sikrer sertifikatene mot misbruk.

Det er først og fremst tjenestemannen selv som skal sørge for at sertifikatet sperres eller suspenderes når det har oppstått en mulighet for at dette kan misbrukes. Andre enn tjenestemannen selv vil først og fremst være arbeidsgiver, men også organ/organisasjon som forestår autorisasjon/godkjenning av profesjonsrettigheter kan ha anledning til å sperre/suspendere et sertifikat. Likeledes kan den som har utstedt en fullmakt til en annen for bestemte oppdrag, sperre eller suspendere sertifikatet.

Når et sertifikat blir sperret vil sertifikatet ikke kunne aktiveres igjen. Det kan derfor i visse tilfelle være mindre konsekvensfylt å suspendere et sertifikat der en er tvil om en skal sperre sertifikatet. Sertifikatpolicyen vil beskrive adgangen til å suspendere et sertifikat og fremgangsmåten for dette.

[113] Sertifikatene har en begrenset gyldighetsperiode som gjerne er to til tre år fra de er utstedt. Det norske firmaet ZebSign opererer f.eks. med tre års gyldighetsperiode for sine sertifikater, jfr Zeb Sign Certificate Policy ver 1.0 punkt 6.3.2.

[114] Hvilke typer opplysninger som fremkommer vil være avhengig av hva slags type sertifikat det er tale om. Et ansattsertifikat vil typisk inneholde personens navn, unik identifikator i virksomheten (ansattnummer, initialer el.), arbeidsgivers navn og organisasjonsnummer mv. For et profesjonssertifikat vil en i tillegg ha yrkes- eller utdanningstittel, unik identifikator for denne personen som hentes fra relevant register hos den myndighet eller organisasjon som har i oppgave å godkjenne yrket/utdanningen, samt dennes organisasjonsnummer.

[115] Lov om behandling av personopplysninger (personopplysningsloven) lov 2000-04-14 31 § 19 omhandler den behandlingsansvarliges informasjonsplikt overfor den registrerte. Se også lov om elektronisk signatur § 7 om innsamling og bruk av personopplysninger. Se også bestemmelsen i § 14 2.ledd b) om kravet om samtykke fra innehaveren for å gjøre et sertifikat offentlig tilgjengelig. Det siste gjelder kun for "kvalifiserte sertifikater", jf lov om elektronisk signatur § 4.

[116] Forvaltningsorgan som skal benytte sikkerhetstjenester må utarbeide sikkerhetsmål og sikkerhetsstrategi, jf § 11. Denne kan gjelde både fysisk sikkerhet og informasjonssikkerhet. Det første retter seg mot adgangskontroll, tilgangskontroll til soner mv. Informasjonssikkerhet omfatter tiltak iverksatt for å sikre at informasjon ikke er tilgjengelig uten autorisasjon (*konfidensialitet*), at informasjon ikke uautorisert endres eller ødelegges (*integritet*), og at informasjon er tilstede og anvendelig for medarbeidere slik at pålagte oppgaver kan utføres

§ 26 *Arkivering av avansert elektronisk signatur mv.*[117]

(1) Melding som er signert med en avansert elektronisk signatur[118], og som blir arkivert, skal arkiveres sammen med de opplysninger som er nødvendige[119] for å bekrefte signaturen.

(2) For meldinger som skal konverteres[120] til annet format, skal arkivet ved mottak verifisere signaturen, og deretter på hensiktsmessig måte bekrefte tilknytningen mellom meldingen, meldingens signatur og relevante opplysninger fra sertifikatet sammen med opplysning om tidspunktet for bekreftelsen. Arkivet skal sikre integriteten til meldingene og bekreftelsen av de nevnte forholdene i oppbevaringsperioden. Tilsvarende gjelder meldinger der tilhørende sertifikaters gyldighetsperiode[121] er kortere enn den tiden det kan være behov for å bekrefte meldingens innhold når det ikke benyttes tidsstempel[122] eller annen tjeneste som sikrer signaturens integritet.

(*tilgjengelighet).* Se i denne forbindelse også forskrift til personopplysningsloven kapittel 2 med kommentarer.

[117] For de tilfeller en benytter en avansert elektronisk signatur, jf lov om elektronisk signatur § 3 nr 2 må en også gjøre visse foranstaltninger når en skal arkivere disse for å bevare den tillit som ligger i bruken av denne typen signatur.

[118] Jf § 2 nr 2 se også lov om elektronisk signatur (lov 2001-06-15 81) § 3 nr 2

[119] Data som bekrefter signaturen er for det første opplysninger som kopler signaturverifiseringsdata til underskriveren, f.eks. navn og fødselsdato, og dernest data som bekrefter denne koplingen, typisk sertifikatutsteders signatur på sertifikatet. I tillegg vil det i mange tilfeller kreves bekreftelse på at både underskriverens og utstederens sertifikater ikke er trukket tilbake.Dersom dataene i sertifikatet ikke er tilstrekkelige til å identifisere personen kan det være nødvendig å gjøre oppslag i utsteders katalog f.eks. for å kople sertifikatet til innehaverens fødselsnummer. Av personvernhensyn vil ikke fødselsnummer bli brukt som unik identifikator i sertifikatene. Hva som ellers anses som nødvendig vil avhenge av den aktuelle transaksjon.

[120] Det er urealistisk for arkivet å ta vare på alle tidligere generasjoner av maskin- og programvare. Konvertering foretas for å gjøre informasjon flyttbar og håndterlig på nye teknologiplattformer, dvs det som til en hver tid er dagens utstyr. Konvertering kan også skje fordi arkivet ønsker å lagre alle dokumenter/meldinger i et bestemt NOARK-godkjent format med én gang. Ved konvertering oppheves bindingen mellom meldingen/dokumentet og signaturen. For å sikre fortsatt notoritet omkring knytningen mellom dokument og signatur, må arkivet oppbevare tilstrekkelige opplysninger til at man i ettertid kan sannsynliggjøre at signaturen ble tilfredsstillende verifisert på relevant tidspunkt.

Dette skjer ved at arkivfunksjonen innhenter nødvendige opplysninger og gjennomføre nødvendige verifiseringer, jf kommentarene til bestemmelsens første ledd. Deretter arkiveres meldingen sammen med arkivets bekreftelse på at korrekt verifisering fant sted på et bestemt tidspunkt. Tilliten til arkivfunksjonen og arkivets rutiner skal etablere den nødvendige bekreftelse på at knyttingen mellom meldingen og sertifikatet var i orden ved mottak, eller at det på annen måte ble gjennomført tilfredsstillende autentisering, og at arkivet deretter har sikret meldingens integritet (at meldingens innhold ikke bevisst eller ubevisst er endret) Arkivet kan også for eksempel tidsstemple den konverterte meldingen og de aktuelle informasjonsuttrekk fra det tilknyttede opprinnelige sertifikatet.

[121] En kan her som eksempel tenke seg en situasjon der et sertifikats gyldighetsperiode uløper i løpet av måneden (sertifikaters gyldighetstid er vanligvis to til tre år), og at dokumentet signaturen er knyttet til gjelder spørsmål om pengekrav der foreldelse er en relevant problemstilling.

[122] Tidsstempling er en sikkerhetsfunksjonalitet som dokumenterer at et dokument eksisterer eller faktisk var i noens besittelse på et gitt tidspunkt. Tidsstempling kan foretas av arkivet selv eller av en uavhengig og tiltrodd tredjepart. Eksempelvis vil mottaker av en melding motta det

Det enkelte forvaltningsorgan kan beslutte at denne fremgangsmåten skal benyttes også for andre meldinger.

(3) Dersom arkivet ikke lykkes i å verifisere signaturen, skal opplysning om dette lagres, om mulig sammen med opplysninger om årsaken til at verifisering ikke lyktes.

(4) Melding eller resultat av en automatisert databehandling som er bekreftet på annen måte enn ved avansert elektronisk signatur, bør lagres sammen med opplysninger om at korrekt bekreftelse har funnet sted, og om mulig hvilken teknikk som er blitt benyttet.[123]

§ 27 *Oppbevaring og utlevering av sertifikater og bekreftede meldinger mv.*

(1) Ved begjæring om innsyn[124] i dokumenter som er signert med avansert[125] elektronisk signatur, jf. § 9, skal relevante sertifikater og øvrige opplysninger som er nødvendige for verifisering[126] av signaturen utleveres sammen med dokumentet når den som begjærer innsyn har bedt om det. Forvaltningsorganet skal også sørge for at publikum kan få tilgang til

---

signerte dokumentet (vanligvis vil det være hash-verdien som er en matematisk representasjon av dokumentet som er signert), samt avsenders sertifikat. Dette vil mottaker videresende til tidsstemplingsfunksjonen sammen med opplysning om sertifikatets status som er hentet fra sertifikatutsteders base. Tidsstemplingsfunksjonen legger så til opplysning om tidspunkt for mottak og påfører sin signatur på det hele og returnerer det.

[123] Dette innebærer krav til arkivering av aktivitetslogger el. Lagring av autentiseringsdata bør ikke forekomme. I kode/passordsystemer kan dette innebære en sikkerhetsrisiko. Eventuelle alternativer er lagring av autentiseringsdata i kryptert form eller lagring av engangspassord. Det siste stiller krav til bevaring av samtlige benyttede engangspassord hos forvaltningsorganet og register over når de ble benyttet, og er neppe særlig praktisk.

[124]Det kan gis adgang til innsyn i elektronisk arkiv, jfr § 9 nr 2. Dette vil antakelig innebære en vesentlig styrking av innsynsretten ettersom terskelen for den enkeltes innsyn senkes. Man antar for det første at det er enklere å begjære innsyn direkte fra egen maskin enn via brev eller telefon, forutsatt at arkivet en ønsker innsyn i er hensiktsmessig organisert. For det andre slipper vedkommende å vente på brev fra organet eller møte opp personlig. Innsyn via skjerm kan i mange tilfelle oppnås umiddelbart etter at begjæring er sendt.
Dersom det begjæres partsinnsyn, og dokumentet ikke kan utleveres etter offentlighetsloven, er det viktig å sikre at begjæringen kommer fra parten selv, og at opplysningene ikke blir gjort tilgjengelige for uvedkommende i forbindelse med utleveringen. Etter personopplysningsloven kan begjæring om innsyn sendes i elektronisk form, og den behandlingsansvarlige kan kreve at den registrerte (den opplysningene gjelder og som ber om innsyn) identifiserer seg på en sikker måte, f.eks. ved hjelp av en avansert elektronisk signatur.
Innsyn kan som nevnt skje f.eks. ved autentisering direkte mot innsynsarkiv (speiling av dokumenter for innsynsformål), eller ved overføring av dokumenter i kryptert form. Dette kan skje ved bruk av en digital signatur i forbindelse med innsynsbegjæring, og ved at dokumenter sendes ut i kryptert form eller gjøres tilgjengelige på dedikert informasjonssystem på samme måte som ved underretning om vedtak, jf § 7.

[125] Jf. § 2 nr 2.

[126] Opplysninger som er nødvendige for å verifisere en signatur, skal oppbevares sammen med meldingen, jf § 26. Der dokumentet er konvertert til nytt format og man derved har brutt bindingen mellom dokumentet og signaturen skal en kunne etablere den nødvendige bekreftelse på at knytningen mellom dokumentet og signaturen var i orden ved mottak og at arkivet deretter har sikret dokumentets integritet. For de dokumenter der det kreves avansert elektronisk signatur vil det kunne være av betydning for den som begjærer innsyn å kunne foreta verifikasjon av avsender, at sertifikatet var gyldig på det tidspunkt dokumentet ble påført signaturen og for å verifisere dokumentets innhold mv. Dette kan det være like viktig å få innsyn i som selve dokumentet.

dokumentenes innhold i en form som gjør det mulig å dokumentere[127] innholdet også overfor tredjepart.

Kapittel 5 Diverse bestemmelser

§ 28 *Koordinerende organ*[128]

(1) Kongen kan utpeke et organ som har koordineringsansvar[129] for forvaltningens bruk av sikkerhetstjenester ved elektronisk kommunikasjon med og i forvaltningen.

(2) Koordineringsorganet skal utarbeide krav[130] til sikkerhetstjenester og -produkter som anbefales brukt ved elektronisk kommunikasjon med og i forvaltningen. Koordineringsorganet skal også vurdere om tilgjengelige sikkerhetstjenester eller -produkter tilfredsstiller[131] kravene.

(3) Koordineringsorganet kan bestemme[132] at det under tjeneste for forvaltningsorganer kun skal benyttes sertifikater fra sertifikatutstedere som har inngått rammeavtale om levering av slike tjenester til forvaltningen eller som er anerkjent av koordineringsorganet.

---

[127] For eksempel i form av en bekreftet utskrift dersom tredjepart ikke kan behandle elektroniske signaturer eller bekreftet med forvaltningsorganets elektroniske signatur dersom meldingen er arkivert i en form som utelukker verifisering med opprinnelig signatur, jf § 26 nr 2.

[128] Det er ved denne forskriftens ikrafttredelse ikke opprettet et slikt koordinerende organ.

[129] Koordinering er nødvendig fordi det kreves at det tas stilling til mange teknisk/organisatoriske/juridiske spørsmål for å sikre best mulig samhandling mellom forvaltningsorganene og at den tekniske infrastrukturen oppleves mest mulig enkel og enhetlig sett fra publikums side.

[130] Der forvaltningen går sammen om felles standarder, vil det være tjenlig med et felles organ som utarbeider krav og evaluerer slike produkter og tjenester. Et slikt organ vil også være viktig for å få et mest mulig likt brukergrensesnitt mot de forskjellige forvaltningsorganer. Det er i denne forskriften ikke definert krav til sikkerhetsprodukter og -tjenester som forvaltningen kan ønske å bruke. NOU 2001:10 "Uten penn og blekk" anbefaler bruk av tre sikkerhetsnivåer med tilhørende policyer. Dette vil være en oppgave for det koordinerende organ å utarbeide videre. Videre vil et koordinerende organ kunne utarbeide krav til dokumentasjon og eventuell sikkerhetsrevisjon av leverandører av sikkerhetstjenester til forvaltningsorganer.

[131] Det enkelte forvaltningsorgan skal slippe å evaluere de enkelte løsninger selv, men skal kunne basere seg på evalueringer som er gjort for forvaltningen sentralt. For kvalifiserte sertifikater må det vurderes om det skal stilles tilleggskrav. Eventuelle tilleggskrav må ligge innenfor rammen av direktiv 1999/93/EF om elektroniske signaturer, artikkel 3(7), jf. lov om elektronisk signatur § 5.

[132] Av koordineringshensyn, og for å sikre best mulig effektivitet i de interne kommunikasjonsprosessene i forvaltningen, bør sertifikater som skal benyttes av forvaltningsansatte under tjeneste for arbeidsgiver, kun utstedes av sertifikatutstedere som forvaltningsorganet, eller koordinerende organ for forvaltningen, har utpekt/godkjent og eventuelt inngått rammeavtale med. Dette gjør det mulig bl.a. å sikre interoperabilitet og tilgang til nødvendige sertifikatkataloger, at alle forvaltningsansatte har tilgang til de sertifikatene som er nødvendige for å verifisere andre tjenestemenns sertifikater, og kontroll med at tjenestene holder et tilfredsstillende sikkerhetsnivå. Dersom det er nødvendig av koordineringshensyn, eller fordi det enkelte forvaltningsorgan mangler kompetanse på området, kan det være hensiktsmessig å begrense valgmulighetene til sertifikatutstedere man har inngått rammeavtale med. Det forutsettes at ordningen med rammeavtaler innrettes i henhold til reglene for offentlige anskaffelser.

§ 29 *Ikrafttredelse og tidsbegrensing av forskriften*

(1) Forskriften trer i kraft 1. juli 2002.

(2) Forskriften opphører 1. juli 2004 dersom den ikke uttrykkelig fornyes.[133]

[133] Departementet tar sikte på å evaluere forskriften i god tid før utløpsdatoen, for eventuell fornyelse, endring eller opphør.