Elektronisk samhandling med og i forvaltningen – eForvaltningsforskriften

Rolf Riisnæs, advokat dr. juris, Wikborg, Rein & Co. Advokatfirma DA

Innholdsfortegnelse

Elektronisk samhandling med og i forvaltningen – eForvaltningsforskriften[1]

Rolf Riisnæs, advokat dr. juris, Wikborg, Rein & Co. Advokatfirma DA

1. Innledning

1.1 Utfordringer ved elektronisk samhandling

Elektronisk samhandling med og i forvaltningen spenner over et stort og uensartet område. Men det er ikke slik at alt er nytt. Forvaltningen har allerede brukt datamaskinbaserte systemer og elektronisk kommunikasjon i lang tid. Muligheten for å kommunisere elektronisk med forvaltningens *brukere* over *åpne elektroniske nett* er imidlertid fortsatt forholdsvis nytt, og innebærer en rekke nye utfordringer for forvaltningsorganene – og for brukerne.

For det første er kommunikasjon over åpne nett preget av manglende gjennomsiktighet, i den forstand at det kan være vanskelig å få bekreftet at den man kommuniserer med virkelig er den vedkommende gir seg ut for å være. For det annet er det elektroniske mediet preget av manglende stabilitet, forstått på den måten at endringer kan finne sted uten å etterlate spor hvis det ikke tas forholdsregler. For det tredje innebærer elektronisk kommunikasjon at de ytre kjennetegn for kommunikasjonen endrer seg. Vi har for eksempel ikke lenger forhåndstrykte brevark og konvolutter å forholde oss til. For det fjerde er elektronisk kommunikasjon preget av manglende erfaring og tradisjon. I tradisjonelle kommunikasjonsprosesser har vi ofte hatt en mageølelse i forhold til når vi kan regne med at noe går bra eller er til å stole på. Ved elektronisk kommunikasjon vil vi ofte ikke ha noe grunnlag for en slik følelse. Det er nok tvilsomt om denne mageølelsen alltid er rasjonelt begrunnet, men i praksis bygger vi nok mange av våre daglige avgjørelser på nettopp en slik følelse. Og sist, men ikke minst, kan bruk av elektronisk kommunikasjon i samhandlingen mellom forvaltningen og dens brukere støte an mot utfordringer av rettslig art.

Det har etter hvert blitt vanlig å anta at elektroniske signaturer og kryptering kan bidra til å løse en del av de utfordringer vi står overfor når vi skal ta i bruk elektronisk kommunikasjon i samhandlingen mellom forvaltningen og brukerne. Og fra tid til annen hører vi spørsmål som: ”Er en elektronisk signatur gyldig?” eller ”Er en elektronisk signatur rettslig bindende?” Disse spørsmålene kan ikke besvares generelt, og er ikke egnet som problemstillinger. Mer fruktbart er det nok å spørre om det er noen rettslige krav til form eller fremgangsmåte som berører det aktuelle forholdet, for eksempel om det finnes noen rettslige krav til skriftlighet eller signatur. Hvis det er tilfellet må en vurdere om kravene kan oppfylles ved hjelp av elektronisk kommunikasjon. Se for eksempel forvaltningsloven som i § 2 definerer lovens krav til skriftlighet slik:

---

[1] Denne delen av veilederen er en ajourført utgave av Rolf Riisnæs’ artikkel ”Sikker elektronisk samhandling med og i forvaltningen (eForvaltningsforskriften)”, publisert i boken "Informasjonssikkerhet - Rettslige krav til sikker bruk av IKT", Arild Jansen og Dag Wiese Schartum (red.), Fagbokforlaget 2005.

”(g) skriftlig: også elektronisk melding når informasjonen i denne er tilgjengelig også for ettertiden”. Konsekvensen av ikke å overholde et krav om form eller fremgangsmåte behøver dessuten ikke være at transaksjonen blir ugyldig eller ikke kan påberopes mellom partene. Det kan for eksempel dreie seg om en ordensregel som, hvis man ikke overholder den, flytter bevisbyrden for et forhold fra en part til en annen. Slik er det for eksempel med deler av kravene til elektronisk avtaleinngåelse etter finansavtaleloven.[2] Er det ingen slike rettslig bestemte krav til form eller fremgangsmåte, må en vurdere om det av andre grunner er behov for å sikre dokumentasjon for den handlingen eller transaksjonen man vurderer å sette i gang. Slike dokumentasjonsbehov kan for eksempel være begrunnet ut fra bevismessige hensyn og kan medføre behov for å ta tekniske virkemidler i bruk. Men i mange tilfeller vil det heller ikke være noen slike behov for dokumentasjon, for eksempel fordi noe rettslig etterspill ikke vil være aktuelt. Det spørsmålet som da gjenstår, er hva som skal til for at de som vurderer å samhandle har den tillitt til systemet og til hverandre at de opplever bruk av løsningen som trygg og forsvarlig, og at de tør å gå videre med transaksjonen.

Hvilke utfordringer man står overfor, og hvilke parter som er involvert, har naturligvis betydning for hvilke tekniske virkemidler som bør tas i bruk. For eksempel vil det vanligvis ikke være behov for å få bekreftet en brukers identitet hvis vedkommende begjærer innsyn i dokumenter som etter loven skal være offentlig tilgjengelige. Derimot vil det være behov for å oppnå en rimelig grad av sannsynlighet for riktigheten av en brukers påståtte identitet hvis behandling av saken er avhengig av vedkommendes samtykke til behandling av personopplysninger etter personopplysningsloven[3]. Det samme gjelder hvis det begjæres partsinnsyn i dokumenter eller opplysninger som er underlagt taushetsplikt og derfor ikke kan utleveres til andre enn parten selv. Beskyttelsesbehovet, og de virkemidler som må tas i bruk, vil også variere med sakens og de aktuelle opplysningenes art.

1.2 Regler for samhandling med forvaltningen

Mye av vår daglige kommunikasjon gjelder hverdagslige forhold, og det er vanligvis ikke noen katastrofe om en e-post ikke kommer frem eller en melding på en telefonsvarer ikke blir spilt av. Men vår kommunikasjon med forvaltningen vil i mange tilfeller gjelde spørsmål som er av stor betydning for oss. Det er derfor ikke likegyldig hvorledes denne samhandlingen foregår. Det er derfor nedfelt regler for forvaltningens saksbehandling og kommunikasjon bl.a. i forvaltningsloven. Disse reglene har i stor utstrekning bygget på en forutsetning om papirbasert kommunikasjon eller direkte kontakt mellom den enkelte og representanter for forvaltningsorganet. Når kommunikasjonen nå flyttes over på elektroniske kanaler, oppstår det nye utfordringer.

Regjeringen besluttet i april 2012 at digital kommunikasjon skal være den foretrukne kanal for all skriftlig kommunikasjon mellom forvaltningen på den ene siden, og innbyggerne og næringslivet på den annen. Stortinget vedtok i juni 2013 endringer i

---

[2] Se forarbeidene til finansavtaleloven § 8 i Ot.prp. nr. 41 (1998-1999) om lov om finansavtaler og finansoppdrag (finansavtaleloven).

[3] Lov av 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).

forvaltningsloven[4] (fvl.) for å legge til rette for dette. Endringene i forvaltningsloven innebærer at forvaltningen som hovedregel har lov til å kommunisere digitalt. I februar 2014 ble også eForvaltningsforskriften[5] (efvf.) endret og supplert med nye bestemmelser. eForvaltningsforskriften fastlegger nærmere hvordan den elektroniske kommunikasjonen mellom forvaltningen og næringslivet og innbyggerne skal tilrettelegges. Det fremgår nå av fvl. § 15a og efvf. § 8 at forvaltningen kan henvende seg til næringsliv og innbyggere ved hjelp av elektronisk kommunikasjon. Det er imidlertid åpnet for at privatpersoner kan reservere seg mot bruk av elektronisk kommunikasjon, og i stedet motta tradisjonell post fra forvaltningen. Næringsdrivende skal som hovedregel ikke ha en slik reservasjonsrett. Det er også en forutsetning for bruk av elektronisk kommunikasjon at mottakeren er registrert med en elektronisk adresse som forvaltningsorganet kan benytte for å varsle vedkommende om at en henvendelse er sendt. Nærmere om dette i kap. 3.9 nedenfor.

Elektronisk kommunikasjon med og i forvaltningen omfattes av de alminnelige reglene i forvaltningsloven (fvl). Forvaltningsloven er også hjemmelslov for eForvaltningsforskriften. Det innebærer at forvaltningsloven danner det rettslige grunnlaget for forskriften og setter rammene for forskriftens virkeområde. Forskriften adresserer de fleste av de temaene som er introdusert ovenfor. Forvaltningsloven og eForvaltningsforskriften gjelder både statlig, kommunal, regional og lokal forvaltning, og kommer til anvendelse med mindre annet er bestemt i lov eller i medhold av lov.[6]

I det følgende skal vi se nærmere på hvordan forskriften er bygget opp og hvilke føringer den legger på bruk av elektronisk kommunikasjon i forvaltningen og mellom forvaltningen og dens brukere.

eForvaltningsforskriften bygger i store trekk på en anbefaling fra PKI-utvalget.[7] Drøftelsene i anbefalingen fra utvalget kan fortsatt bidra til å belyse forskriftens bakgrunn og innhold.[8] Anbefalingen var grunnlaget for mandatet til en arbeidsgruppe nedsatt av Arbeids- og administrasjonsdepartementet i 2001 og som fremla for departementet et forslag til forskrift. Forslaget var langt på vei i overensstemmelse med PKI-utvalgets anbefalinger. Forskriften ble første gang vedtatt i juni 2002 med en såkalt

---

[4] Lov av 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven).

[5] Forskrift av 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften).

[6] Bestemmelsene omfatter også den forretningsvirksomhet som forvaltningsorganene driver. Etter omstendighetene kan bestemmelsene også gjelde for private rettssubjekter, men det forutsetter at de treffer enkeltvedtak eller utferdiger forskrift, jf. fvl § 1 siste setning. Det er gjort unntak fra loven for bl.a. Stortinget, Riksrevisjonen, Sivilombudsmannen og domstolene, og for enkelte andre organer når de behandler saker etter rettspleielovene, jf. fvl § 4.

[7] PKI-utvalget ble oppnevnt i februar 2000 med representanter fra flere ulike departementer og offentlige etater. Utvalgets mandat var bl.a. å utrede innholdet i en policy for offentlig forvaltning på området for bruk av digitale signaturer, dokumentkryptering og tilhørende infrastruktur (PKI, Public Key Infrastructure). Utvalget skulle også fremme forslag til retningslinjer for bruk av digitale signaturer og dokumentkryptering i forvaltningen. Se referansen til utvalgets innstilling i noten nedenfor.

[8] Se NOU 2001:10, *Uten penn og blekk. Bruk av digitale signaturer i elektronisk samhandling med og i forvaltningen*, del IV.

"solnedgangsbestemmelse" som innebar at den ville opphøre å gjelde etter to år med mindre den ble fornyet. Forskriften ble evaluert vinteren 2003/2004. Evalueringen viste bl.a. at det var lite kunnskap om forskriften og at den ble oppfattet som til dels vanskelig å forstå. Det var imidlertid stor grad av enighet om at forskriftens innhold måtte videreføres. Det ble også fremmet forslag om at man burde flytte en del av de alminnelige bestemmelsene over i forvaltningsloven, men det ville blitt en mer omfattende prosess enn det man i denne omgang hadde tatt høyde for.

På den bakgrunn ble det sendt på høring et forslag til ny forskrift som inneholdt en rekke endringer i forskriftens struktur og der flere bestemmelser var skrevet om. Men innholdsmessig var det bare foreslått mindre endringer i forhold til forskriften av 2002. Forslaget ble godt mottatt av høringsinstansene og en oppdatert eForvaltningsforskrift trådte i kraft 1. juli 2004.

Forskriften er senere endret flere ganger, sist i februar 2014 i forbindelse med innføring av prinsippet om digitalt førstevalg, jf. ovenfor. Samtidig ble det innført regler om rett for enkeltpersoner til å reservere seg mot elektronisk kommunikasjon (§ 9), om bruk av fullmektig (§ 10), om opprettelse og bruk av et nytt register for kontaktinformasjon (kap. 7), og den tidligere bestemmelsen om sikkerhetsmål og sikkerhetsstrategi er endret og supplert med viktige krav til internkontroll mv (§ 15). Vi kommer tilbake til dette nedenfor.

2. eForvaltningsforskriftens formål og virkeområde

eForvaltningsforskriftens formål er å "legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen. Den skal fremme forutsigbarhet og fleksibilitet og legge til rette for samordning av sikre og hensiktsmessige tekniske løsninger. Forskriften skal legge til rette for at enhver på en enkel måte kan utøve sine rettigheter og oppfylle sine plikter i forhold til det offentlige", se § 1første ledd. Dette er en ambisiøs målsetning. Ikke minst kan det synes som en betydelig utfordring å skulle fremme forutsigbarhet samtidig som en skal fremme fleksibilitet. Tanken er imidlertid å legge til rette for behovstilpassede løsninger innenfor faste rammer, og med krav om å informere brukerne om de valg som er gjort og de krav som er stilt.

Forskriften gjelder for elektronisk kommunikasjon med forvaltningen og for elektronisk saksbehandling og kommunikasjon i forvaltningen, og er hjemlet i forvaltningsloven § 15a. Forskriften er etter sin ordlyd også hjemlet i esignaturloven[9] § 5. Forskriften benytter de samme definisjoner som i esignaturloven, se efvf. § 2, men utover dette synes det ikke å være behov for å påberope esignaturloven som hjemmel for forskriften med det innhold den har i dag. eForvaltningsforskriften viker for særregler som fremgår av eller i medhold av annen lov, og den gir ikke grunnlag for å fravike de alminnelige reglene om forsvarlig saksbehandling i forvaltningsloven, se efvf. § 1 annet og tredje ledd.

En rekke av de forhold forskriften adresserer, retter seg mot forvaltningsorganene og deres ansatte, og man kunne tenke seg at flere av bestemmelsene ble gitt som instrukser snarere enn i forskrifts form. Dette ville imidlertid ikke være tilfredsstillende bl.a. i forhold til kommunene. Av hensyn til den indre sammenhengen mellom bestemmelsene,

[9] Lov av 15. juni 2001 nr. 81 om elektronisk signatur (esignaturloven).

og for å oppnå et enhetlig og mest mulig samlet og oversiktlig regelverk, har man valgt å gi bestemmelsene i forskrifts form. Innenfor rammen av eForvaltningsforskriften, er det nå tilrettelagt for at forvaltningsorganene på en enkel og koordinert måte kan ivareta sine behov for sikkerhetstjenester, bl.a. gjennom "Kravspesifikasjon for PKI i offentlig sektor" og den såkalte "selvdeklareringsordningen".

Bruk av elektronisk identitetsbevis (e-ID) og elektronisk signatur i offentlig sektor er nå samordnet gjennom ID-porten som forvaltes av Direktoratet for forvaltning og IKT (Difi). Det fremgår av Digitaliseringsrundskrivet (H-7/2014), punkt 1.2 *Bruk av nasjonale felleskomponenter* at: «Virksomheten skal ta i bruk ID-porten for digitale tjenester som krever innlogging og autentisering.» Slike føringer er gjenstand for politiske beslutninger og kan endres over tid. Digitaliseringsrundskrivet oppdateres jevnlig.

3. Forsvarlig elektronisk saksbehandling og kommunikasjon

3.1 Fleksibilitet og behovstilpassede løsninger

Det er et gjennomgående trekk ved eForvaltningsforskriften at forvaltningsorganene har stor grad av frihet til selv å velge form og kanal for henvendelser til forvaltningsorganet. Det vil si at forvaltningsorganet, innenfor de rammer som lovgivningen ellers setter, selv avgjør hvorledes den enkelte skal kommunisere med organet, for eksempel ved å kreve bruk av spesielle blanketter eller elektroniske skjemaer, at visse typer henvendelser skal adresseres til en spesiell enhet innenfor organet osv., se efvf. § 3 første ledd. Hensynet til forvaltningsorganets mulighet for effektivt å organisere sin egen saksbehandling tilsier at de må ha en viss adgang til å stille slike krav. For eksempel vil bruk av standardiserte skjemaer bidra til å sikre at alle relevante opplysninger er med og gjøre det lettere for organet å identifisere de ulike opplysningstypene. Når opplysningene skal behandles i forvaltningsorganets datamaskinbaserte systemer, er behovet for strukturering av opplysningene desto større.

Når man snakker om elektronisk kommunikasjon med forvaltningen, vil nok mange først og fremst tenke på elektronisk post. Men for elektronisk kommunikasjon med forvaltningen er ikke nødvendigvis elektronisk post alene noen god løsning. Til det er det for mange usikkerhetsmomenter og for mange utfordringer knyttet til bl.a. strukturering av opplysninger, valg av riktig elektronisk adresse, sikkerhetsløsninger og muligheten for å drive automatisert behandling eller forbehandling av henvendelser organet mottar. Selv om man ikke skal utelukke bruk av elektronisk post i ulike former og for enkelte formål, vil det nok i mange sammenhenger være mer effektivt med for eksempel Web-baserte løsninger. I eForvaltningsforskriften er det først og fremst de Web-baserte løsningene man har for øye, men bruk av for eksempel elektronisk post eller SMS-tjenester er også omfattet, se efvf. § 3 første ledd, bokstav (b) og (c).

Et annet utgangspunkt i forskriften er at all bruk av sikkerhetsløsninger bør være behovstilpasset og basert på forvaltningsorganets sikkerhetsstrategi. Dette har kommet til uttrykk i efvf. § 4. Den løsningen som er valgt, skal dels forebygge at forvaltningsorganet "for sikkerhets skyld" krever mer sikkerhet enn nødvendig, men samtidig legge til rette for at man av koordineringshensyn, og for at løsningene skal være oversiktlige og brukervennlige, kan velge ett eller noen få sikkerhetsnivåer for kommunikasjon med organet fremfor fullt ut å tilpasse seg den enkelte situasjon.

Det kan nok av og til være vanskelig å finne den riktige balansen mellom fleksibilitet og enkelhet og mellom behovstilpasning og koordinering.

3.2 Valg av form og fremgangsmåte

Innenfor de rammer som lovgivningen på det enkelte forvaltningsområde setter, er det i stor grad opp til det enkelte forvaltningsorgan om de vil legge til rette for elektronisk kommunikasjon og hvordan det skal skje. Hvis loven for eksempel foreskriver at en spesiell type henvendelse skal inneholde noen bestemte opplysningstyper, eller være underskrevet og bekreftet av vitner, må en eventuell elektronisk løsning oppfylle de relevante kravene. Men for øvrig kan forvaltningsorganet tilrettelegge den elektroniske kommunikasjonskanalen slik de selv finner det mest praktisk, så lenge løsningen tilfredsstiller de alminnelige kravene til forsvarlig saksbehandling og behandling av personopplysninger.

Friheten til å velge form og fremgangsmåte tilligger forvaltningsorganet. Den enkelte bruker av forvaltningens tjenester har altså ikke noe krav på å få kommunisere elektronisk med forvaltningsorganet på annen måte enn det organet selv har lagt til rette for, se efvf. § 3 første ledd. Men har forvaltningsorganet først etablert en generell elektronisk adresse, og det ikke er stilt noen spesielle krav til den aktuelle typen henvendelse, kan den generelle adressen benyttes, se efvf. § 3 annet ledd. Den enkelte skal heller ikke adressere henvendelser direkte til en enkeltperson i forvaltningsorganet med mindre organet har lagt til rette for det eller det er avtalt i det enkelte tilfellet, se efvf. § 3 tredje ledd.

Det fremgår også av eForvaltningsforskriften at "forvaltningsorganet bør legge til rette for at elektronisk kommunikasjon med forvaltningsorganet er brukervennlig og tilgjengelig for alle", se efvf. § 3 femte ledd. I dette ligger bl.a. en påminnelse om at løsninger for elektronisk kommunikasjon bør være lette å forstå og anvende og at de også skal være tilgjengelige for personer med nedsatt funksjonsevne. Krav til universell utforming følger nå også av lov av 21. juni 2013 nr. 61 om forbud mot diskriminering på grunn av nedsatt funksjonsevne (diskriminerings- og tilgjengelighetsloven) § 13 og av forskrift 21. juni 2013 nr. 732 om universell utforming av informasjons- og kommunikasjonsteknologiske (IKT)-løsninger.

Selv om Regjeringen har innført prinsippet om digitalt førstevalg, gir eForvaltningsforskriften § 3 ikke grunnlag for å *kreve* at forvaltningens brukere benytter elektronisk kommunikasjon. For tjenester som den enkelte har rett på, er det antakelig utelukket å kreve bruk av elektronisk kommunikasjon. I slike tilfeller må forvaltningsorganets strategi snarere være å legge den elektroniske kanalen så godt til rette at den blir foretrukket av brukerne hvis forvaltningsorganet mener det er hensiktsmessig. Derimot kunne man tenke seg at typiske tilleggsytelser (servicetjenester), som forvaltningsorganet tilbyr på eget initiativ, og som det ikke vil være økonomisk eller praktisk mulig å tilby på andre måter, bare er tilgjengelige ved hjelp av elektronisk kommunikasjon. Det rettslige grunnlaget for å iverksette en slik ordning må forvaltningsorganet imidlertid finne andre steder enn i eForvaltningsforskriften, og løsningen må ikke innrettes på en måte som er i strid med god forvaltningsskikk. Men er det først grunnlag for å tilby en tjeneste utelukkende ved hjelp av elektronisk kommunikasjon, vil eForvaltningsforskriften komme til anvendelse på vanlig måte.

3.3 Sikkerhetsstrategi og internkontroll på informasjonssikkerhetsområdet

Alle virksomheter som benytter elektronisk kommunikasjon bør vurdere om det er behov for å sette i verk sikringstiltak. Behovet for tiltak vil avhenge av hva som eventuelt kan gå galt og konsekvensene hvis noe går galt. Ethvert forvaltningsorgan som benytter elektronisk kommunikasjon skal derfor, i henhold til efvf. § 15, etablere sikkerhetsmål og sikkerhetsstrategi og et tilfredsstillende system for internkontroll.

Sikkerhetsmålene beskriver hva som ønskes oppnådd på informasjonssikkerhetsområdet. De skal understøtte og bidra til realisering av forvaltningsorganets overordnede mål, etterlevelse av lover og regler og kostnadseffektiv drift. Sikkerhetsstrategien beskriver hvordan forvaltningsorganet skal nå sikkerhetsmålene.[10]

Informasjonssikkerhet er et ledelsesansvar. Det er viktig at ledelsen og forvaltningsorganet for øvrig har tilstrekkelig styring og kontroll med det som gjøres i forvaltningsorganet for å ivareta informasjonssikkerheten. Mål og strategi for informasjonssikkerhet (sikkerhetsmål og sikkerhetsstrategi) er ledelsens viktigste redskap i styringen av informasjonssikkerheten innenfor forvaltningsorganets ansvarsområde. Ledelsen bør derfor delta aktivt i utformingen og behandlingen av disse og ikke bare komme inn som avsluttende godkjennings- eller beslutningspunkt.

Videre inngår mål og strategi som grunnlaget i *internkontrollen*. Forvaltningsorganets internkontroll skal være basert på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen på informasjonssikkerhetsområdet bør være en integrert del av virksomhetens helhetlige styringssystem.

Det er virksomhetens kompleksitet, risiko og behov som bør avgjøre omfang, innretning og detaljeringsnivå på sikkerhetsmål, sikkerhetsstrategi og omfanget av internkontrollen.

Fordi forvaltningsorganene vanligvis også vil behandle personopplysninger, vil kravene etter efvf. § 15 være delvis sammenfallende med kravene til sikkerhetsstrategi etter personopplysningsloven § 13 og personopplysningsforskriften kap. 2. Men sikkerhetsstrategien og internkontrollen skal etter eForvaltningsforskriften også adressere en rekke andre temaer som er spesifisert i efvf. § 15 i den utstrekning det er relevant for virksomheten. Blant annet skal den beskrive nærmere krav til bruk, kontroll og sikring av sertifikater og krypteringsnøkler hvis det er aktuelt.

Sikkerhetsstrategien skal danne grunnlaget for forvaltningsorganets beslutninger om bruk av sikkerhetstjenester og -produkter og sikre at dette skjer på en helhetlig, planlagt, systematisk og dokumentert måte. Dette gjelder både de krav forvaltningsorganet stiller i henhold til efvf. § 4, og for organets egen tilrettelegging av tjenester som ytes ved hjelp av elektronisk kommunikasjon, for eksempel underretning om vedtak, klage, begjæringer om innsyn og utlevering av opplysninger osv. Sikkerhetsstrategien skal også "inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks", se efvf. § 15 første ledd, siste setning. Sikkerhetsstrategien bør altså gi en samlet oversikt over kravene til informasjonssikkerhet innenfor det enkelte forvaltningsorgans område.

Informasjonssikkerhet og internkontroll er et stort og sammensatt fagområde i stadig endring. Difi er tildelt en særlig oppgave med å gi anbefalinger til forvaltningen på dette

[10] Se også om bruk av sikkerhetsstrategien i kap 4.1 nedenfor.

området. Difis anbefalinger om standarder fremkommer i "Referansekatalog for IT-standarder i offentlig sektor" og på Difis veiledningssider for informasjonssikkerhet.[11]

3.4 Krav til bruk av sikkerhetstjenester og -produkter

Den som henvender seg til et forvaltningsorgan ved hjelp av elektronisk kommunikasjon i henhold til efvf. § 3, kan som utgangspunkt gjøre det uten å ta i bruk spesielle sikkerhetstjenester eller -produkter, se efvf. § 4(1). Men det kan forekomme mange unntak fra dette utgangspunktet. For det første kan det følge av lovgivningen på det aktuelle forvaltningsområdet at det gjelder spesielle krav til henvendelsen, for eksempel et krav om underskrift, bekreftelse av identitet eller lignende. For det annet kan det være nødvendig å beskytte dataene mot innsyn fra andre i henhold til efvf. § 5. Og for det tredje kan krav om bruk av sikkerhetstjenester være fastsatt av forvaltningsorganet selv i henhold til efvf. § 4 med støtte i forvaltningsorganets sikkerhetsstrategi.

Med *sikkerhetstjenester og -produkter* menes i § 4: "løsninger for å oppnå bl.a. bekreftelse av partenes identitet eller fullmakter (autentisering), at data ikke utilsiktet eller urettmessig endres (integritet), beskyttelse av informasjon mot innsyn fra uvedkommende (konfidensialitet), og at det er mulig å dokumentere henvendelser og aktiviteter og hvem som har sendt eller utført dem (ikke-benekting),[12] … Slike løsninger kan for eksempel være basert på bruk av elektronisk signatur og kryptering." Det er altså en rekke ulike tjenester og produkter som kan være aktuelle. I tillegg til de tjenestene som er nevnt, kan det være aktuelt å ta i bruk andre tjenester og produkter i henhold til de krav som følger av forvaltningsorganets sikkerhetsstrategi.

Selv om eForvaltningsforskriften også er hjemlet i esignaturloven, er det ingen direkte kopling til, eller krav om bruk av, de løsninger som beskrives der. Riktignok er begrepet 'elektronisk signatur' definert på en slik måte at det vil være dekkende for en rekke av de løsninger det kan være aktuelt å ta i bruk, se e-signatuloven § 3 nr. 1. Og begrepet 'avansert elektronisk signatur' benyttes i noen bestemmelser i forskriften for å angi i hvilke tilfeller den enkelte bestemmelse kommer til anvendelse. Det gjelder bl.a. efvf. §§ 12 fjerde ledd, 27 og 28. Men hvilke løsninger som skal benyttes i forbindelse med de enkelte tjenester, avgjør forvaltningsorganet med utgangspunkt i sikkerhetsstrategien. Det gjelder også i forhold til bruk av såkalt 'kvalifisert elektronisk signatur', se esignaturloven § 3 nr. 3. I esignaturloven er en kvalifisert elektronisk signatur først og fremst relevant i forhold til rettsvirkningsbestemmelsen i § 6. Men de relevante formkravene i lovgivningen er i mange tilfeller ikke uttrykt som krav om underskrift, men som krav om autentisering, skriftlighet eller lignende. Og svært ofte vil nok også "lettere" løsninger kunne være tilfredsstillende for å oppfylle eventuelle formkrav. En annen sak er at de relativt høye krav til sikkerhet som en kvalifisert elektronisk signatur reflekterer, kan være relevante i forbindelse med behov for autentisering og/eller innholdskryptering for enkelte typer tjenester.

Et forvaltningsorgan som legger til rette for at visse typer av henvendelser kan formidles elektronisk, vil gjerne fastsette generelle behandlingsregler for henvendelsene, herunder

---

[11] http://infosikkerhet.difi.no

[12] Med ikke-benekting menes i denne sammenheng at det er mulig å etablere en tilfredsstillende (forholdsvis høy) grad av sannsynlighet for at en person eller virksomhet har sendt en melding med et bestemt innhold eller utført en nærmere bestemt handling.

generelle krav til bruk av sikkerhetstjenester og -produkter, se efvf. § 4 tredje ledd. Men situasjonen kan være slik at det i normaltilfellene ikke vil være behov for slike tjenester. eForvaltningsforskriften åpner for at forvaltningsorganet da kan tilrettelegge en normalprosedyre uten bruk av slike tjenester og i stedet innhente eventuelle tilleggsopplysninger, bekreftelser mv., på individuell basis når de finner det nødvendig, se efvf. § 4 annet ledd. Formålet med bestemmelsen er å hindre at forvaltningsorganene stiller generelle krav om bruk av sikkerhetstjenester og -produkter "for sikkerhets skyld" hvis det bare er i unntakstilfellene det er behov for dem.

Når forvaltningsorganet stiller krav om bruk av sikkerhetstjenester og -produkter etter efvf. § 4 annet og tredje ledd, skal organet enten selv gjøre tjenestene tilgjengelige for brukerne eller anvise hvilke andre løsninger som kan benyttes. Det kan for eksempel tenkes, at en bruker kan velge mellom løsninger som er gjort tilgjengelige av forvaltningsorganet, eller løsninger som brukeren har anskaffet i en annen sammenheng og allerede har tilgjengelig, for eksempel for bruk i forbindelse med nettbank, mobilhandel eller annen elektronisk samhandling. Det er naturligvis en forutsetning at løsningen tilfredsstiller de funksjonelle behov forvaltningsorganet har, for eksempel at løsningen er egnet til å kontrollere de opplysninger som forvaltningsorganet trenger å få bekreftet. Tilsvarende må forvaltningsorganet gjøre sikkerhetstjenester tilgjengelige hvis det er stilt krav om slike tjenester eller produkter for å beskytte taushetsbelagte opplysninger eller personopplysninger etter efvf. § 5, se nærmere om dette i avsnitt 3.5 nedenfor.

eForvaltningsforskriften § 4 gir, etter sin ordlyd, forvaltningsorganene stor grad av frihet til å stille krav om bruk av spesielle sikkerhetstjenester og -produkter. Men friheten går neppe så langt som til å stille krav om hvilken nettleser, eller annet alminnelig utstyr, brukeren må benytte. I alle fall ikke hvis det er flere produkter som tilfredsstiller de funksjonelle behov som er identifisert i forvaltningsorganets sikkerhetsstrategi.

For det første fremgår det av forskriften selv, at forvaltningsorganene bør legge til rette for at tjenestene er brukervennlige og tilgjengelige for alle, se efvf. § 3 femte ledd. Dette retter seg for det første mot grupper med særlige behov, for eksempel personer med nedsatt funksjonsevne. Krav til universell utforming følger nå også av lov av 21. juni 2013 nr. 61 om forbud mot diskriminering på grunn av nedsatt funksjonsevne (diskriminerings- og tilgjengelighetsloven) § 13 og av forskrift 21. juni 2013 nr. 732 om universell utforming av informasjons- og kommunikasjonsteknologiske (IKT)-løsninger. Krav til brukervennlighet og tilgjengelighet omfatter imidlertid også krav til tilgang via ulike typer utstyr og oppkopling. For eksempel bør man forsøke å legge til rette for at det er mulig å få tilgang til sentral informasjon hos forvaltningen, både via PC med vanlig skjerm, nettbrett, og via mindre mobile enheter, og uavhengig av hvilken overføringshastighet det er på den enkeltes nettverkstilknytning. Det finnes også et grunnleggende krav om å unngå usaklig og urimelig forskjellsbehandling av forvaltningens brukere. Det må innebære, at når man legger til rette for bruk av elektroniske tjenester, bør de være tilgjengelige for alle som benytter en standard kommunikasjonsplatform.

Retten til å stille krav om bruk av spesielle sikkerhetstjenester og -produkter går heller ikke lenger enn det som er nødvendig for å oppnå en effektiv og sikker gjennomføring av tjenestene, og må sees i lys av formålet om enkle og brukervennlige løsninger, jf. efvf. § 1 (formålsbestemmelsen). Dette innebærer, blant annet, at det kan stilles krav om at

brukerens utstyr kan etablere en sikker forbindelse i henhold til anerkjente og alminnelige standarder. For eksempel må det kunne stilles krav om at det kan etableres en kryptert forbindelse mellom forvaltningens tjenermaskin og brukerens nettleser ved hjelp av protokoller som støttes av de fleste nettlesere, for eksempel SSL eller TLS.[13] Men det må tilrettelegges slik at vanlige nettlesere, som følger standardene, kan benyttes for å få tilgang til tjenestene. Også fra politisk hold har man påpekt viktigheten av at brukerne uavhengig av plattform skal kunne utnytte digitale tjenester.

Når det gjelder utstyr som ikke (foreløpig) inngår i en standard kommunikasjonsløsning, for eksempel utstyr for fremstilling av digitale signaturer ved hjelp av nøkler oppbevart på smartkort eller lignende, går nok forvaltningens frihet til å stille krav om spesielle tjenester og produkter noe lenger. Det er fortsatt så mange valgmuligheter innenfor rammene av de tilgjengelige standarder, at en nærmere presisering kan være nødvendig for å oppnå samvirke mellom løsningene. Men forvaltningsorganene skal i disse tilfellene enten selv gjøre tilgjengelig, eller konkret angi, tjenester og produkter som kan benyttes, se efvf. § 4 fjerde ledd. Et eksempel på at forvaltningen selv gjør relevante løsninger tilgjengelig er "MinID" som tilbys gjennom ID-porten og kan benyttes for innlogging på de fleste offentlige nettjenester.

Statlige etater er for øvrig pålagt å benytte løsninger som tilfredsstiller kravene i "Kravspesifikasjonen for PKI i offentlig sektor". Nærmere om dette i kap 4.8 nedenfor.

3.5 Formidling av taushetsbelagte opplysninger og personopplysninger til forvaltningen

Forvaltningsorganer har taushetsplikt om nærmere bestemte typer av opplysninger, se forvaltningsloven §§ 13 flg. Men taushetsplikten oppstår vanligvis først etter at opplysningene er kommet under forvaltningsorganets kontroll. Før forvaltningsorganet er gjort kjent med opplysningene, eller fått hånd om dem, har det ikke vært tale om taushetsplikt når opplysningene har vært formidlet muntlig eller på papir. Når forvaltningsorganet legger til rette for elektronisk kommunikasjon, kan det imidlertid oppstå ny risiko knyttet til formidling av slike opplysninger. Det kan ikke forventes at brukerne selv er kjent med, eller har forutsetninger for å vurdere følgene av, den risiko for uberettiget innsyn, eller at opplysninger kommer på avveie, som måtte forekomme i forbindelse med elektronisk kommunikasjon.

eForvaltningsforskriften pålegger derfor forvaltningsorganet et særlig ansvar for å forebygge slik risiko og å informere brukerne om eventuell restrisiko når det tilrettelegges for elektronisk kommunikasjon, se efvf. § 5 første og annet ledd. Dette innebærer at forvaltningsorganet må legge til rette for bruk av sikre kanaler for henvendelser som rutinemessig vil inneholde opplysninger som er taushetsbelagt på forvaltningsorganets hånd. For andre typer av henvendelser, som vanligvis ikke vil inneholde slike opplysninger, og hvor forvaltningsorganet derfor ikke har truffet spesielle tiltak, bør det gis informasjon til brukerne om den risiko som eksisterer hvis brukeren likevel velger å avgi slike opplysninger.

Når det benyttes kryptering for å sikre opplysninger under overføring til forvaltningsorganet, skal forvaltningsorganets (og ikke enkeltpersoners) krypteringsnøkkel benyttes med mindre det er spesielt tilrettelagt for andre løsninger, se

[13] SSL (Secure Sockets Layer) og TLS (Transport Layer Security protocol).

efvf. § 5 fjerde og femte ledd. Dette er dels begrunnet i kravet om tilgjengelighet til opplysninger som angår forvaltningsorganet, dels i avsenders mulighet for å sikre at opplysningene kun gjøres tilgjengelig for rette vedkommende. Den enkelte bruker vil vanligvis ikke være kjent med hvilken person i forvaltningsorganet som er rette vedkommende, men vil lettere kunne identifisere rette organ. Nærmere om dette i avsnitt 4.5 nedenfor.

3.6 Tilbakemeldinger på henvendelser som forvaltningsorganet mottar

Et forvaltningsorgan som mottar en henvendelse i elektronisk form skal gi bekreftelse til avsender om at henvendelsen er mottatt, se efvf. § 6. Bekreftelsen bør gis straks henvendelsen er mottatt og bør inneholde et referansenummer, journalnummer eller lignende og angi på hvilket tidspunkt henvendelsen ble mottatt, se efvf. § 6 annet ledd. For Web-baserte løsninger kan dette for eksempel skje i form av en kvitteringsmelding på skjermen som en del av dialogen med brukeren. I andre tilfeller kan det være aktuelt å sende kvittering ved hjelp av elektronisk post eller SMS.

Bruk av kvitteringsmeldinger er blitt vanlig i mange sammenhenger innenfor elektronisk samhandling og innebærer en økt servicegrad idet den dels fjerner usikkerhet omkring hvorvidt noe har kommet frem, dels gjør det mulig for partene å formidle referansenummer eller lignende som kan benyttes for raskt å følge opp eller etterspore en sak. Særlig i forhold til avbrytelse av tidsfrister kan bruk av kvitteringsmeldinger være viktig. Dette er lagt til grunn bl.a. i efvf. § 11 vedrørende erklæring om klage over vedtak. Også i forarbeidene til endring av domstolloven § 146 om fristavbrudd når det benyttes elektronisk kommunikasjon, er bruk av kvitteringsmeldinger fremhevet som et viktig poeng.[14]

Forvaltningsorganet skal også gi tilbakemelding til brukeren dersom en henvendelse er sendt til feil organ, til uriktig elektronisk adresse eller er avgitt i en annen form eller på en annen måte enn det som er bestemt og det har betydning for behandlingen av henvendelsen, se efvf. § 7. Bestemmelsen har sammenheng med forvaltningsorganets alminnelige veiledningsplikt, se fvl. § 11.

Det er gjort visse unntak fra forvaltningsorganets plikt til å sende bekreftelse på at en henvendelse er mottatt, se efvf. § 6 tredje ledd. For det første er det unødvendig å sende egen bekreftelse på mottak hvis henvendelsen håndteres av et automatisert system og umiddelbart blir besvart, eller når det gis melding etter efvf. § 7 annet ledd om at henvendelsen innholder feil eller er sendt til feil organ, se efvf. § 7 første ledd. For det annet kan man unnlate å sende egen bekreftelse hvis mottaket fremgår på annen betryggende måte, for eksempel hvis brukeren får tilbakemelding på skjermen om at en overføring er vellykket. Men i og med at bruk av referansenummer og tidsangivelser i kvitteringsmeldingene kan ha praktisk betydning for oppfølgingen av henvendelsen, bør nok dette siste unntaket benyttes med forsiktighet. For det tredje kan man unnlate å sende bekreftelse hvis henvendelsen er av en slik art at den ikke utløser saksbehandling og forvaltningsorganet heller ikke av andre grunner har plikt til å svare, for eksempel hvis det mottar ”spam”. I tillegg har forvaltningsorganet anledning til å inngå avtale med

[14] Se forarbeidene til domstolloven § 146 i Ot.prp.nr. 8 (2002-2003) om lov om endringer i rettergangslovgivningen mv. (elektronisk kommunikasjon med domstolene mv.), avsnitt 5.3.3.

næringsdrivende og andre forvaltningsorganer om unntak fra plikten til å sende bekreftelse i forbindelse med rutinemessig eller periodisk rapportering.

3.7 Underretning om enkeltvedtak mv.

Vi har tidligere vært inne på at vår samhandling med forvaltningen ofte vil ha slik betydning for oss at det ikke er likegyldig hvorledes det foregår eller hvilken sikkerhet vi har for at vi faktisk settes i stand til å ivareta våre rettigheter. Dette er bakgrunnen for eForvaltningsforskriftens forholdsvis omfattende krav til løsninger for underretning om vedtak ved hjelp av elektronisk kommunikasjon, se efvf. § 8.

Ved endring av forvaltningsloven i juni 2013, og senere endring av eForvaltningsforskriften i februar 2014, er prinsippet om digitalt førstevalg innført i norsk forvaltningsrett. Dette innebærer bl.a. at forvaltningen som hovedregel kan henvende seg til andre ved hjelp av elektronisk kommunikasjon, se fvl. § 15a første ledd, og efvf. § 8. Frem til regelendringen i februar 2014, var ordningen at forvaltningen kunne benytte elektronisk kommunikasjon ved underretning om enkeltvedtak og forhåndsvarsling mv, forutsatt at den saken gjaldt uttrykkelig hadde samtykket til dette. Kravet til samtykke er nå fjernet. For privatpersoner er det imidlertid innført rett til å reservere seg mot bruk av elektronisk kommunikasjon for formidling av enkeltvedtak, forhåndsvarsler mv, se efvf. § 9.

Enkeltvedtak, forhåndsvarsler og andre henvendelser som det er særlig viktig at mottakeren blir oppmerksom på, skal som hovedregel gjøres tilgjengelig fra "egnet informasjonssystem", se efvf. § 8 annet ledd, første setning. Det er i utgangspunktet forvaltningsorganet selv som avgjør *hvilket* "egnet informasjonssystem" som skal benyttes. Ved vurderingen av *hva* som anses som egnet informasjonssystem må det bl.a. sees hen til kravene om at bare rette vedkommende får tilgang til vedtaket (tilgangskontroll og konfidensialitet) i efvf. § 8 fjerde ledd. Kravene vil være oppfylt bl.a. av Altinn, som er etablert særlig for kommunikasjon med næringsdrivende. For privatpersoner etableres det egen løsning for bruk av digitale postkasser fra leverandører som har avtale med det offentlige.

For å sikre at den henvendelsen gjelder blir oppmerksom på den, og har foranledning til å følge den opp, inneholder eForvaltningsforskriften krav om at vedkommende skal varsles om henvendelsen og hvordan vedkommende kan gjøre seg kjent med innholdet i den. Det er etablert et eget register for kontaktinformasjon, der den enkelte kan registrere og vedlikeholde den eller de elektronisk adresser som vedkommende vil ha varsel sendt til. Kontaktregisteret vil også inneholde opplysninger om hvem som har reservert seg mot bruk av elektronisk kommunikasjon, se efvf. § 9 siste ledd. Etablering og bruk av kontaktregisteret er nærmere regulert i efvf. kap. 7.

Varsel om at vedtak er fattet, sendes til den elektroniske adressen mottaker er registrert med i kontaktregisteret. Dette kan for eksempel være en e-postadresse eller et mobiltelefonnummer (SMS). Varselet skal inneholde opplysninger om hvor og hvordan mottaker kan skaffe seg tilgang til vedtaket, se efvf. § 8 tredje ledd. For enheter som er registrert i Enhetsregisteret, skal varsel sendes til den elektroniske adressen som virksomheten har oppgitt i forbindelse med saken, eller til en adresse registrert i et digitalt kontaktregister for virksomheter hvis det blir etablert.

Med utgangspunkt i opplysningene i varselet bør parten lett kunne skaffe seg tilgang til vedtaket. Forvaltningsorganet må imidlertid sikre vedtaket mot risiko for uberettiget

innsyn på en tilfredsstillende måte, se efvf. § 8 fjerde ledd. Organet må altså sikre at bare rette vedkommende får tilgang til vedtaket. Vedtaket vil i mange tilfeller inneholde personopplysninger eller andre taushetsbelagte opplysninger. Hva som kreves av sikringstiltak er avhengig av vedtakets og opplysningenes art. Krav om at brukeren skal ta i bruk nødvendige tjenester og produkter kan forvaltningsorganet fastsette i henhold til efvf. § 4 og kan omfatte for eksempel løsninger for såkalt elektronisk identitetsbevis (e-ID) og kryptering. Forvaltningsorganet skal registrere data som viser at den som fikk tilgang var rette vedkommende, se efvf. § 8 femte ledd.

Forvaltningsorganet må også tilrettelegge systemet slik at det registrerer når parten har skaffet seg tilgang til vedtaket, se efvf. § 8 femte ledd. Det vil naturligvis være av betydning for parten å få kjennskap til innholdet i vedtaket. Dessuten vil et forvaltningsvedtak normalt kunne påklages. Det er derfor av betydning at ikke vedtaket kommer bort, eller klagefristen løper ut, uten at parten har fått anledning til å gjøre seg kjent med vedtaket. Fordi de elektroniske kanalene er mer mangfoldige, erfaringen foreløpig mindre og usikkerheten tilsvarende større enn for tradisjonell papirbasert kommunikasjon, er det bygget inn en reserveløsning i eForvaltningsforskriften som skal sikre parten mot slike utilsiktede hendelser. Det er for så vidt uavhengig av om årsaken er en teknisk svikt, uriktig adresse eller om parten rett og slett ikke følger opp, eller er ute av stand til å få oversikt over, for eksempel sin egen e-post. Reserveløsningen innebærer at dersom parten ikke har skaffet seg tilgang til vedtaket innen én uke fra varsel ble sendt første gang, skal vedkommende varsles på nytt, se efvf. § 8 femte ledd, annen setning.

I enkelte tilfeller kan det være forsvarlig å sende vedtaket direkte til en elektronisk adresse parten oppgir, uavhengig av kravene til "egnet informasjonssystem" som er nevnt over. Det kan f.eks. være hvis vedtaket ikke inneholder taushetsbelagte opplysninger eller personopplysninger som krever særlige sikringstiltak, og forvaltningsorganet står i direkte kontakt med parten, slik at denne har særlig foranledning til å følge opp henvendelsen. Det fremgår derfor av efvf. § 8 at: "Dersom parten ber om det, det ikke er hensiktsmessig å kommunisere digitalt med parten via egnet informasjonssystem, det er forsvarlig og annet regelverk ikke er til hinder for dette, kan vedtaket likevel sendes til en elektronisk adresse parten oppgir." Begrepet "likevel" viser at bestemmelsen er en unntaksregel. Det er viktig å merke seg at bestemmelsen har fire kumulative vilkår. Alle vilkårene må altså være oppfylt.

Hensiktsmessighetsvurderingen foretas av forvaltningsorganet som avsender. Ansvaret for å vurdere om det er *forsvarlig* å benytte ordinær e-post som kanal for formidling av vedtaket ligger også i det enkelte tilfellet til forvaltningsorganet som avsender. Forvaltningsorganet må her vurdere om hensynene bak bestemmelsen kan oppfylles uten at det som ellers regnes som et "egnet informasjonssystem" benyttes. Ordinær e-post vil som utgangspunkt ikke være egnet som kanal for formidling av vedtaket som inneholder taushetsbelagte opplysninger. Krav til informasjonssikkerhet, for eksempel krav fastsatt i personopplysningsforskriften kapittel 2, vil være til hinder for dette. Dersom parten ønsker bruk av en forsendelsesmåte som forvaltningsorganet ellers ikke ville kunne benytte, vil det påhvile forvaltningen et særlig ansvar for å sikre at situasjonen er slik at det likevel fremstår som forsvarlig og at parten har forstått og akseptert restrisikoen, jf. den tilsvarende veiledningsplikten i § 5 annet ledd for kommunikasjon til organet.

I utgangspunktet skal det sendes varsel etter annet ledd også i disse tilfellene, men her vil det nok ofte være slik at varslingsadressen er sammenfallende med den adressen parten

har bedt om å få vedtaket sendt til. Departementet bemerker i motivene til endringen i § 8 tredje ledd (på s. 11) at: "Dersom vedtaket er sendt via ordinær e-post, anses varslingen etter tredje ledd å være foretatt ved at vedtaket sendes e-postadressen." Forvaltningsorganet må ta dette med i sin forsvarlighetsvurdering.

Klagefrist etter forvaltningsloven § 29 begynner å løpe fra det tidspunkt vedtaket er gjort tilgjengelig for parten i henhold til efvf. § 8, og varsel om dette er sendt, se efvf. § 11 annet ledd. Bestemmelsen i § 11 innebærer en endring sammenliknet med tidligere § 8 sjette ledd i eForvaltningsforskriften, der prinsippet var at fristen begynte å løpe når parten faktisk hadde skaffet seg tilgang til vedtaket. Vedtaket skal inneholde opplysninger om hvorvidt forvaltningsorganet har lagt til rette for å motta klage ved hjelp av elektronisk kommunikasjon og hvilken adresse som i så fall skal benyttes, se efvf. § 11 første ledd.

Reglene for underretning om enkeltvedtak gjelder tilsvarende ved forhåndsvarsel etter fvl. § 16 og for andre meldinger som har betydning for mottakerens rettsstilling eller for behandlingen av saken, og meldinger som det av andre grunner er av særlig betydning å sikre at vedkommende mottar, se efvf. § 8 siste ledd.

3.8 Klage over enkeltvedtak

Klage over enkeltvedtak kan fremsettes ved bruk av elektronisk kommunikasjon dersom det forvaltningsorganet som skal motta klagen har lagt til rette for det, se efvf. § 11 første ledd. Etter forvaltningsloven § 32 første ledd, bokstav b), skal en klage være undertegnet eller "autentisert som fastsatt i forskrift, eller i medhold av forskrift". Formuleringen trekker i retning av at det først og fremst er bekreftelse på klagerens identitet eller fullmakter man er ute etter. Hvordan klagen skal fremsettes og hvilke sikkerhetskrav som stilles, bestemmer forvaltningsorganet i henhold til efvf. §§ 3 og 4. Det kan for eksempel dreie seg om å bruke et spesielt klageskjema og autentisering ved hjelp av elektronisk signatur.

Klager skal motta bekreftelse på innsendt klage i henhold til efvf. § 6. Hvis klager ikke mottar bekreftelse, skal klagen sendes på nytt.

3.9 Innsyn i og utlevering av opplysninger og dokumenter

Adgangen til å få innsyn i opplysninger og dokumenter som angår ens forhold til forvaltningsorganene er viktige rettigheter for den enkelte. Bestemmelser om allmenn innsynsrett finner vi i offentleglova.[15] Hovedregelen er formulert slik i § 3: "Saksdokument, journalar og liknande register for organet er opne for innsyn dersom ikkje anna følgjer av lov eller forskrift med heimel i lov. Alle kan krevje innsyn i saksdokument, journalar og liknande register til organet hos vedkommande organ." Innsynsretten etter offentleglova er noe videre enn etter offentlighetsloven av 1970. Av lovens § 30 fremgår det at: "Organet fastset ut frå omsynet til forsvarleg saksbehandling korleis eit dokument skal gjerast kjent. Det kan krevjast papirkopi eller elektronisk kopi av dokumentet." Innsynsrett for den opplysningene direkte gjelder finner vi bl.a. i forvaltningsloven § 18 og personopplysningsloven § 18.

---

[15] Lov av 19. mai 2006 nr. 16 om rett til innsyn i dokument i offentleg verksemd (offentleglova).

eForvaltningsforskriften har nærmere bestemmelser om når og hvordan man kan begjære innsyn ved hjelp av elektronisk kommunikasjon og hvorledes slikt materiale kan gjøres tilgjengelig, se efvf. § 12. eForvaltningsforskriftens bestemmelser om innsynbegjæringer gjelder på forvaltningslovens område. Men etter forarbeidene til personopplysningsloven kan også begjæring om innsyn etter personopplysningsloven § 18 fremmes i elektronisk form på visse nærmere vilkår, for eksempel ved bruk av elektronisk signatur, se forarbeidene til personopplysningsloven § 24.[16] For den som mottar en slik begjæring kan antakelig eForvaltningsforskriften gi veiledning om hvorledes dette kan håndteres.

Begjæring om innsyn i opplysninger eller dokumenter i en sak kan sendes til forvaltningsorganet ved hjelp av elektronisk kommunikasjon når den som begjærer innsyn, gjør det på den måten som forvaltningsorganet har bestemt etter efvf. §§ 3 og 4, se efvf. § 12 første ledd. Forvaltningsorganet kan altså etter denne bestemmelse kreve at innsynsbegjæringer sendes på eget skjema. Dette kan være særlig praktisk hvis løsningen er lagt opp slik at innsyn kan gis i elektronisk form.

Hvis forvaltningsorganet fører elektronisk arkiv, kan de velge å gi innsyn i opplysninger og dokumenter i elektronisk form. Hvis det kan kreves innsyn etter offentlighetsloven eller annen allmenn innsynsrett kreves ingen særskilte forholdsregler. Men hvis det ikke foreligger slikt grunnlag må forvaltningsorganet sikre at de har tilfredsstillende bekreftelse på at vedkommende har krav på innsyn og at risiko for uberettiget innsyn i opplysningene er forebygget på en tilfredsstillende måte, se efvf. § 12 annet ledd. Rent praktisk innebærer det at det må benyttes en eller annen form for autentiseringsløsning og sikker overføring av opplysningene, for eksempel ved bruk av kryptering. Igjen er kravene til slike løsninger avhengig av opplysningenes art. Dette skal være adressert i forvaltningsorganets sikkerhetsstrategi og danne grunnlaget for valg av løsninger, se efvf. §§ 15 og 4.

I tillegg finnes det særlige regler om utlevering av dokumenter som er signert med avansert elektronisk signatur. Hvis den som begjærer innsyn ber om det, skal slike dokumenter enten utleveres sammen med sertifikater og øvrige opplysninger som er nødvendige for å verifisere signaturen, eller forvaltningsorganet kan legge til rette for at vedkommende kan få signaturen bekreftet i forvaltningens system i forbindelse med utleveringen, se efvf. § 12 fjerde ledd. Bakgrunnen for regelen er, at hvis det først er krevd bruk av avansert elektronisk signatur,[17] må en anta at opplysningene er av en slik art at det er av betydning å kunne få dem bekreftet, hvis ikke kunne man valgt en enklere løsning.

Forvaltningsorganet må også legge til rette for at den enkelte kan få tilgang til opplysningene i en form som gjør det mulig å dokumentere innholdet overfor tredjepart, om nødvendig i form av en papirutskrift der forvaltningsorganet bekrefter innholdet, se efvf. § 12 femte ledd. Dette kan være aktuelt for eksempel hvis parten har behov for å dokumentere et vedtak overfor en annen part i forbindelse med søknad, forebyggelse av tvist eller lignende. Det er ikke gitt at en eventuell tredjepart, som ikke selv har vært part i saken, vil være i stand til å håndtere opplysninger og dokumenter i elektronisk form,

---

[16] Se Ot.prp.nr. 92 (1998-1999) om lov om behandling av personopplysninger (personopplysningsloven) i spesialmotivene til § 24.

[17] Om avansert elektronisk signatur se lov om elektronisk signatur § 3 nr. 2.

eventuelt med elektronisk signatur. Forvaltningsorganet må da sørge for at parten kan dokumentere forholdet på annen måte.

Det er grunn til å reflektere over at når forvaltningsorganene legger til rette for elektronisk kommunikasjon, mister vi som brukere våre tradisjonelle verktøy for arkivering og vedlikehold av relevant informasjon. De fleste av oss har verken kompetanse til, eller erfaring med, langtidslagring av elektroniske data. Data som opprinnelig forekommer i elektronisk form, kan ofte ikke overføres til papir på noen tilfredsstillende måte for lagring på den måte vi er vant til. Da må forvaltningen ivareta våre interesser når det gjelder oppbevaring av relevant materiale, i større grad enn tidligere. Sikring av, og tilgang til, forvaltningens arkiv, blir med andre ord ikke bare et forvaltningsinternt anliggende, men påvirkes av hensynet til den enkelte bruker i større grad enn før.

3.10 Reaksjoner mot misbruk av elektronisk kommunikasjon

Bruk av elektronisk kommunikasjon kan forenkle saksbehandlingen, og vil i mange tilfeller også gjøre det mulig med mer komplette og effektive kontrolltiltak enn ved manuell behandling. Men samtidig eksponeres man kanskje for annen risiko med hensyn til misbruk eller lureri. Og noen mener nok at terskelen for svindel på nettet kan være lavere enn i tradisjonell samhandling. eForvaltningsforskriften gir forvaltningsorganet adgang til å gripe inn overfor slikt misbruk ved helt eller delvis å nekte den det gjelder videre bruk av elektronisk kommunikasjon med organet, enten det nå dreier seg om misbruk av kommunikasjonsløsningen eller sikkerhetsmekanismene, se efvf. § 14 første ledd. Den som blir nektet videre bruk av elektronisk kommunikasjon med organet, må i stedet benytte tradisjonelle kommunikasjonskanaler.

Dette er en forholdsvis vidtgående sanksjon og den er adressert særskilt i hjemmelsbestemmelsen i fvl. § 15a bokstav g). I bestemmelsen gis det eksempler på hva forvaltningsorganets kompetanse etter § 15a kan omfatte. Etter sin ordlyd dekker bokstav g) først og fremst misbruk av "data ment for signering, autentisering, sikring av integritet eller konfidensialitet" og det kan gis bestemmelser om hva som regnes som misbruk. I forarbeidene påpekes det imidlertid at eksemplifiseringen ikke er uttømmende og at retten til å gripe inn mot misbruk vil følge allerede av hovedregelen i § 15a innledningen (nå annet ledd).[18] Dette må også gjelde annet misbruk av den elektroniske kanalen enn det som er nevnt i bokstav g).

Før forvaltningsorganet iverksetter beslutning om utestenging skal den det gjelder, varsles og oppfordres til å uttale seg om forholdet. Hvis det finnes nødvendig av sikkerhetsmessige årsaker, for eksempel hvis systemsikkerheten er truet, kan imidlertid beslutningen iverksettes straks, se efvf. § 14 annet ledd.

Beslutninger om å nekte videre bruk av elektronisk kommunikasjon etter efvf. § 14 kan påklages, se efvf. § 14 tredje ledd.

---

[18] Se Ot.prp. nr. 108 (2000-2001) om lov om endringer i diverse lover for å fjerne hindringer for elektronisk kommunikasjon, avsnitt 3.5.4.7.2 og spesialmotivene til § 15a.

4. Særlig om elektronisk signatur, kryptering og sertifikater

4.1 Sikkerhetsstrategien som ramme for forvaltningsorganets bruk av elektronisk signatur, kryptering og sertifikater

I avsnitt 3.3 ovenfor ble det påpekt at ethvert forvaltningsorgan som benytter elektronisk kommunikasjon skal etablere en sikkerhetsstrategi.[19] En slik strategi vil omfatte en rekke ulike forhold.

I tillegg til de forhold som ellers hører hjemme i virksomhetens sikkerhetsstrategi, bør enhver bruk av sikkerhetstjenester og –produkter, som f.eks. elektronisk signatur, kryptering og sertifikater i et forvaltningsorgan, være basert på og nærmere beskrevet i sikkerhetsstrategien, se efvf. § 15 fjerde ledd.

Sikkerhetsstrategien skal adressere bl.a.: prosedyrer for anskaffelse, bruk, oppbevaring og sikring av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsnøkler; prosedyrer for å etablere og opprettholde et sikkert brukermiljø; prosedyrer for varsling og tilbaketrekking av sertifikater ved mistanke om tap eller misbruk; prosedyrer for kontroll av sertifikater og statusopplysninger ved mottak og hvor oppdatert opplysningene må være; prosedyrer for å nekte noen bruk av elektronisk kommunikasjon med forvaltningsorganet; prosedyrer for behandling av personopplysninger og taushetsbelagte opplysninger og prosedyrer for sikkerhetskopiering, oppbevaring og deponering av dekrypteringsnøkler knyttet til forvaltningsorganet. Det er en rekke bestemmelser i kap. 4-6 i eForvaltningsforskriften som forutsetter at forvaltningsorganet har avklart bruken av sikkerhetstjenester og –produkter i sin sikkerhetsstrategi.

4.2 Sertifikat for forvaltningsorgan (virksomhetssertifikat)

Når man har diskutert bruk av sertifikater i forbindelse med elektroniske signaturer, har fokus gjerne vært på sertifikater knyttet til enkeltpersoner. Og forvaltningen vil nok i mange tilfelle ha nytte av, og behov for, å få bekreftet for eksempel identiteten til enkeltpersoner. Men for den enkelte bruker av forvaltningens tjenester vil det vanligvis ha større betydning å kunne identifisere selve forvaltningsorganet. For det første er det forvaltningsorganet som sådant, og ikke den enkelte saksbehandler, som er involvert i samhandlingen. For det andre vil den enkelte bruker sjelden ha mulighet for å verifisere saksbehandlerens identitet eller at vedkommende faktisk opptrer på vegne av forvaltningsorganet.

Forvaltningsorganet har derfor anledning til å benytte såkalte "virksomhetssertifikater" når organet benytter elektroniske signaturer. Virksomhetssertifikatet identifiserer forvaltningsorganet, se efvf. § 16. Det har i andre sammenhenger vært diskutert hvorvidt andre enn fysiske personer kan disponere en signatur, men det har ingen praktisk betydning for oss. Etter endringene i esignaturloven i 2003 er det helt på det rene at også andre enn enkeltpersoner, for eksempel automatiserte systemer, kan avgi elektroniske signaturer etter loven. En elektronisk signatur (i sin alminnelige form) er i loven først og fremst knyttet til en metode for autentisering, altså et rent faktisk spørsmål. Hvilke rettslige virkninger en slik elektronisk signatur skal ha, er et annet spørsmål, for eksempel om den eller det som påførte ”signaturen” var berettiget til å gjøre det.

---

[19] Se mer om sikkerhetsstratgien i kommentarutgaven til § 13 og i kap 3.3 ovenfor.

Virksomhetssertifikater kan disponeres av enkeltpersoner på forvaltningsorganets vegne eller av automatiserte systemer. Hvis flere skal kunne disponere på vegne av forvaltningsorganet, bør de ifølge forskriften utstyres med hvert sitt virksomhetssertifikat, se efvf. § 23 annet ledd. For den som mottar en melding signert med et slikt sertifikat, vil det normalt være likegyldig hvem som disponerer det på vegne av organet. Men for forvaltningsorganet selv vil det kunne lette de interne kontrollrutinene når de sertifikater som benyttes, direkte kan spores tilbake til individuelle personer eller enheter som disponerer tilhørende signaturfremstillingsdata. Hvis flere enkeltpersoner har tilgang til signaturfremstillingsdata som er lagret sentralt, kan prosessen eventuelt spores via mekanismer for tilgangskontroll.

Hvis det skal benyttes sertifikat i forbindelse med underretning om enkeltvedtak, fremgår det av eForvaltningsforskriften at det *bør* benyttes virksomhetssertifikat, se efvf. § 16 annet ledd. Det er utarbeidet en norsk profil for virksomhetssertifikater.[20]

4.3 Kontroll av sertifikater mv.

En viktig, men ofte undervurdert side ved sertifikatbruk, er prosessen rundt kontroll av sertifikater i forbindelse med mottak av meldinger som er signert eller i forbindelse med bekreftelse av en brukers identitet eller rolle. Denne prosessen kalles av og til verifisering av sertifikat (eventuelt verifisering av signatur, men det omfatter noen flere oppgaver). Litt forenklet fremstilles det ofte slik at sertifikatet etablerer koplingen mellom den offentlige nøkkelen i sertifikatet og den personen som sertifikatet identifiserer (eller den rolle vedkommende representerer). Det er i og for seg riktig, men før man kan legge et slikt resultat til grunn for en transaksjon er det visse kontroller som må gjennomføres. De viktigste av disse kontrollene fremgår av efvf. § 27 første ledd. De omfatter blant annet å kontrollere at sertifikatet er egnet for den aktuelle anvendelse, og at sertifikatet er gyldig ved mottak eller at det kan dokumenteres at det var gyldig på signeringstidspunktet, for eksempel i form av en tidsstemplet melding om sertifikatets status på det aktuelle tidspunkt. Det skal også kontrolleres at sertifikatet er utstedt av en sertifikatutsteder som forvaltningsorganet kan akseptere i henhold til sin sikkerhetsstrategi eller som er anerkjent av koordineringsorganet i henhold til efvf. § 36.[21] Dette er oppgaver som forvaltningsorganene er pålagt å gjennomføre i tilfeller der det er krav om å benytte avansert elektronisk signatur. Tanken er at når det først er stilt krav om bruk av slik signatur, har transaksjonen vanligvis en slik betydning at kontroll av sertifikatet er påkrevd. Hvilke krav som stilles til inndataene og resultatene fra verifiseringsprosessen, for eksempel hvor oppdatert statusinformasjon for sertifikatet må være, vil variere med transaksjonens betydning. Disse kravene skal fremgå av forvaltningsorganets sikkerhetsstrategi, se efvf. § 27 første ledd. Hvis den meldingen som kontrolleres ikke tilfredsstiller de aktuelle kravene, skal det sendes melding til avsenderen om det i henhold til efvf. § 7.

Kravene til sertifikatverifisering er minimumsregler. Det kan være behov for å foreta tilsvarende kontroller også når det ikke er stilt krav om avansert elektronisk signatur,

---

[20] I sertifikatprofilen har man spesifisert nærmere hvordan internasjonale standarder for sertifikater skal forståes og tilpasses for å kunne brukes for et norsk virksomhetssertifikat. SEID er et 'Samarbeidsprosjekt om Elektronisk ID og signatur'.

[21] Se mer om dette i kap 4.8 nedenfor.

men det likevel benyttes sertifikater. For eksempel vil det vanligvis være nødvendig å kontrollere sertifikater som benyttes i forbindelse med innholdskryptering.

4.4 Oppbevaring av avansert elektronisk signatur mv.

Det er mange utfordringer knyttet til bruk av elektroniske signaturer. En av dem er å oppbevare det signerte materialet på en slik måte at det også i ettertid er mulig å foreta en tilfredsstillende verifisering av signaturen og av at opplysningene ikke har endret seg. Det er naturligvis av betydning både for den enkelte og for forvaltningen selv at det er mulig å dokumentere forvaltningens virksomhet på en tilfredsstillende måte. Se også det som er sagt om behovet for tilgang til og utlevering av materiale fra forvaltningsorganer i avsnittet om innsyn ovenfor.

Forvaltningens oppbevaring av opplysninger reguleres generelt av arkivloven med forskrifter. Men i tillegg er det i eForvaltningsforskriften stilt visse nærmere krav til oppbevaring i de tilfellene der det er benyttet avansert elektronisk signatur med tilknyttet sertifikat.

Det er gitt anvisning på to hovedstrategier for slik lagring. Enten kan de signerte opplysningene (eller dokumentene om man vil) lagres sammen med de øvrige opplysninger som er nødvendige for senere verifisering av signaturen, se efvf. § 28 første ledd. Dette kan omfatte bl.a. sertifikatet selv, opplysninger om sertifikatets status da signaturen ble påført eller sertifikatet ble mottatt, tilsvarende opplysninger for andre sertifikater i sertifikatkjeden mv.

Alternativt kan de nødvendige opplysninger kontrolleres i forbindelse med overlevering til arkivet og deretter oppbevares på en slik måte at arkivet senere kan bekrefte på en tilfredsstillende måte at opplysningene ble kontrollert, tidspunktet for kontrollene, koplingen mellom meldingen, signaturen og relevante opplysninger fra sertifikatet, og at opplysningene ikke senere er endret, se efvf. § 28 annet ledd. Dette kan være nødvendig for eksempel hvis opplysningene i forbindelse med lagring må konverteres til et annet format slik at signaturen ikke lenger kan verifiseres, eller det av andre grunner finnes nødvendig. I slike tilfeller bør det legges til rette for at senere utlevering kan skje med tilfredsstillende bekreftelse fra arkivet hvis det for eksempel begjæres innsyn, se efvf. § 12 fjerde og femte ledd.

4.5 Kryptering av meldinger til forvaltningsorganet

Ved kryptering av melding *til* forvaltningen, skal man benytte forvaltningsorganets krypteringsnøkkel, se efvf. § 5 fjerde ledd. Overfor andre brukere enn forvaltningen selv vil dette i praksis bli håndtert i form av virksomhetssertifikater eller tilsvarende som inneholder de aktuelle krypteringsnøkler. Kryptering med en enkeltpersons krypteringsnøkkel kan bare benyttes dersom forvaltningsorganet har lagt spesielt til rette for det, se efvf. § 5 femte ledd. Meldinger som mottas av et forvaltningsorgan i kryptert form, skal straks dekrypteres. Den videre behandlingen av opplysningene i organet skal skje i henhold til de reglene som gjelder for de aktuelle opplysningene, se efvf. § 26.

Hvis et forvaltningsorgan benytter ekstern databehandler etter personopplysningsloven § 15, så kan databehandlerens krypteringsnøkler benyttes forutsatt at visse nærmere vilkår er oppfylt. Dette kan være for eksempel når det etableres en portal som er felles for flere virksomheter, f.eks. Altinn. En kryptert forbindelse for overføring av data, for eksempel ved bruk av SSL, vil i en slik løsning kunne settes opp med portalens

sertifikat, i stedet for sertifikatet til det forvaltningsorgan som er den endelige mottaker av de opplysningene som skal overføres. Det er imidlertid en betingelse for å benytte databehandlerens sertifikat at det kan dokumenteres, eller er alminnelig kjent, at databehandleren mottar opplysninger på vegne av forvaltningsorganet. Dessuten kan andre regler kreve en annen løsning, for eksempel av personvernhensyn eller hensyn som er dekket av beskyttelsesinstruksen.[22] I så fall går personvernbestemmelsene og beskyttelsesinstruksen foran.

4.6 Sikring av forvaltningsorganets krypteringsnøkler mv.

Det er en rekke sårbarhetsspørsmål knyttet til bruk av elektroniske signaturer og krypteringsløsninger. Blant annet må en sikre seg mot stans i forvaltningsorganets virksomhet dersom en sertifikattjeneste blir utilgjengelig eller et virksomhetssertifikat må trekkes tilbake for eksempel på grunn av misbruk. Dessuten må en sikre at ikke data blir utilgjengelige som følge av at dekrypteringsnøkler går tapt.

eForvaltningsforskriften anbefaler derfor at et forvaltningsorgan som benytter virksomhetssertifikat, vurderer anskaffelse av sertifikat fra to uavhengige sertifikattjenester, slik at forvaltningsorganets systemer raskt kan sette nye sertifikater i drift om nødvendig, se efvf. § 23 tredje og fjerde ledd. Og forvaltningsorganene pålegges å oppbevare kopi av dekrypteringsnøkler som benyttes til data som angår forvaltningsorganet, se efvf. § 24. Sikkerhetsstrategien skal adressere rutiner for sikkerhetskopiering, deponering og utlevering av slike nøkler.

4.7 Bestemmelser om anskaffelse og forsvarlig bruk av sikkerhetstjenester mv. og om veiledning til brukerne

I tillegg til alle bestemmelsene om hvordan samhandlingen mellom den enkelte og forvaltningsorganene bør eller skal foregå når det benyttes elektronisk kommunikasjon, inneholder eForvaltningsforskriften en rekke bestemmelser om anskaffelse og forsvarlig bruk av bl.a. krypteringsnøkler og sertifikater og krav til forvaltningsorganene om veiledning av ansatte og eksterne brukere, se forskriftens kapittel 4 og 5. Bestemmelsene er forholdsvis detaljerte og kan nok tjene som sjekkliste også i andre sammenhenger.

Bestemmelsene reflekterer nok langt på vei det som må regnes som ”god skikk” på området. Tilsvarende krav til forsvarlig bruk vil for eksempel ofte følge av avtalen med den eller dem som leverer sikkerhetstjenestene og -produktene. Fordi tilliten til samhandling med forvaltningen også er avhengig av forsvarlig bruk av slike tjenester og produkter i alle ledd, har man valgt å presisere kravene i forskriften fremfor å overlate dette til avtalen med den enkelte leverandør.

Den enkelte har krav på veiledning med hensyn til hvilke sikkerhetstjenester og -produkter som skal benyttes og hvordan de kan anskaffes, om eventuelle bruksrestriksjoner, om den enkeltes ansvar og plikter i forbindelse med forsvarlig bruk, om behandling av personopplysninger i sertifikater og enkelte andre forhold, se efvf. § 17. Tilsvarende informasjon skal gis eksterne brukere i den utstrekning det er

---

[22] Man kan for eksempel tenke seg at de opplysningene som utveksles er av sensitiv karakter, og at man av den grunn vil kreve at de sendes kryptert helt frem til det forvaltningsorganet som skal motta dem, uten at de underveis blir dekryptert hos databehandleren. Da kan man ikke bruke databehandlerens krypteringsnøkler.

nødvendig, se efvf. § 21. Det påpekes at den forvaltningsansatte har plikt til å følge de retningslinjer arbeidsgiver har fastsatt for bruk av forvaltningsorganets informasjonssystemer og å følge forvaltningsorganets sikkerhetsstrategi for øvrig, se efvf. § 20.

Hvis det skal benyttes elektronisk signatur, skal det innhentes samtykke fra den enkelte til bruk og utlevering av sertifikat i henhold til lov om elektronisk signatur §§ 7 og 14(2)(b), se efvf. § 18.

Sertifikater som er beregnet for bruk i tjeneste for et forvaltningsorgan, skal ikke benyttes på annen måte, se efvf. § 19 første ledd. Det innebærer at for eksempel et ansattsertifikat ikke kan benyttes for private formål. Tilsvarende begrensninger kan om nødvendig fastsettes også for sertifikater som er utstedt til andre *spesielt for bruk ved kommunikasjon med forvaltningen*, se efvf. § 19 tredje ledd.

Den som er innehaver av signaturfremstillingsdata, dekrypteringsdata, passord/PIN-koder mv., skal oppbevare og benytte disse på en slik måte at de ikke gjøres tilgjengelige for andre. Vedkommende skal ikke forlate arbeidsstasjon og lignende uten å sikre at slike data ikke er tilgjengelige for andre, se efvf. § 22 første og annet ledd. Signaturfremstillingsdata skal aldri overlates til andre. Skal noen handle på vegne av en annen skal dette skje med fullmektigens egne signaturfremstillingsdata, se efvf. § 22 tredje ledd. Den enkelte har plikt til å varsle sertifikatutsteder og andre relevante instanser dersom signaturfremstillingsdata, dekrypteringsnøkler, passord, PIN-koder eller lignende kommer på avveie eller blir misbrukt, se efvf. § 25. Den enkelte skal motta veiledning fra forvaltningsorganet om prosedyrene for dette og til hvem varsel skal gis, se efvf. § 17 annet ledd, bokstav a) og c).

4.8 Koordinering av forvaltningens bruk av elektronisk kommunikasjon mv.

Det er utvilsomt gevinster å hente ved å koordinere forvaltningens bruk av elektronisk kommunikasjon, elektronisk signatur og sertifikattjenester mv.

Det er utpekt et organ med ansvar for koordinering av forvaltningens bruk av sikkerhetstjenester og -produkter i henhold til efvf. § 36. Det er nå Kommunal- og moderniseringsdepartementet, som er oppnevnt som koordineringsorgan etter denne bestemmelsen.[23]

I henhold til efvf. § 36, skal koordineringsorganet utarbeide krav til sikkerhetstjenester og -produkter som anbefales brukt ved elektronisk kommunikasjon med og i forvaltningen. Det er besluttet at "Kravspesifikasjonen for PKI i offentlig sektor", skal utgjøre slike krav. Alle statlige etater som anskaffer PKI-baserte sikkerhetstjenester etter 1. november 2005 skal benytte denne kravspesifikasjonen.[24]

---

[23] Se forskrift 7. oktober 2005 nr. 1117, sist endret (per desember 2014) ved forskrift 11. april 2014 nr. 530. Det tidligere 'Koordineringsorganet for PKI i offentlig sektor', som også var forankret i efvf. § 36 (den gang § 27), ble avviklet i forbindelse med etableringen av 'Koordineringsorganet for eForvaltning'.

[24] Se brev fra Moderniseringsdepartementet til alle statsetater, datert 7. juni 2005, vedrørende "Felles sikkerhetsportal for elektronisk kommunikasjon med offentlig sektor". Se også brev fra Fornyings- og administrasjonsdepartementet til samtlige statsetater datert 20. september 2006, vedrørende "Felles sikkerhetsinfrastruktur for elektronisk kommunikasjon med offentlig sektor", på s. 3.

Sikkerhetstjenester og –produkter som skal benyttes i ID-porten skal være omfattet av en frivillig selvdeklarereringsordning som er forankret i esignaturloven § 16a. Ordningen er regulert gjennom forskrift, og administreres av Post- og teletilsynet. Ordningen skal bl.a. sikre at kravene i kravspesifikasjonen[25] er oppfylt, og kan også gjøre det enklere for brukerne å orientere seg blant de sikkerhetstjenester og –produkter som er tilgjengelige i markedet, og bidra til å etablere tillit til deres pålitelighet.

[25] Kravspesifikasjonen for PKI i offentlig sektor, jf. ovenfor.