Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

Forskrift om elektronisk kommunikasjon med og i forvaltningen

Fastsatt ved kgl. res. 25. juni 2004 med hjemmel i lov av 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven) § 15a og lov av 15. juni 2001 nr. 81 om elektronisk signatur § 5. Fremmet av Arbeids- og administrasjonsdepartementet. Endret ved forskrift 2. desember 2005 nr. 1398.

Kapittel 1. Innledende bestemmelser

§ 1 *Forskriftens formål og anvendelsesområde* [1]

(1) Forskriftens formål er å legge til rette for sikker og effektiv[2] bruk av elektronisk kommunikasjon[3] med og i forvaltningen. Den skal fremme forutsigbarhet og fleksibilitet[4] og legge til rette for samordning[5] 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.[6]

(2) Forskriften gjelder for elektronisk kommunikasjon[7] med forvaltningen og for elektronisk saksbehandling og kommunikasjon i forvaltningen[8] når ikke annet er bestemt i lov eller i medhold av lov.

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

---

[1] Se om forskriftens formål og anvendelsesområde i Veilederen del 1, kapittel 2.

[2] Sikker og effektiv bruk av elektronisk kommunikasjon oppnås ved å benytte tekniske, organisatoriske og rettslige virkemidler i samvirke. Det er ikke bare teknikken som må være til å stole på, men også det organisasjonsmessige rundt de tekniske løsningene, f eks organisering av loggfunksjoner, tilgangskontroll og revisjonsspor. Det kan også knyttes plikter til aktørene i kommunikasjonen, f eks plikt til å sende en klage på nytt hvis den som har sendt inn en klage ikke mottar kvittering.

[3] Se § 3(1) c.

[4] Det kan synes som en betydelig utfordring å skulle fremme forutsigbarhet samtidig som en skal fremme fleksibilitet. Tanken er imidlertid å kombinere behovstilpassede løsninger innenfor faste rammer, med krav om å informere brukerne om de valg som er gjort og de krav som er stilt.

[5] I forbindelse med tiltak for å fremme bruk av elektroniske tjenester og for å koordinere forvaltningens bruk av sikkerhetstjenester, er forvaltningsorganets valgfrihet begrenset hvis PKI baserte sikkerhetstjenesyer og –produkter skal benyttes. Alle statlige etater som skal ta i bruk tjenester for autentisering og elektronisk signatur er nå pålagt å benytte "Kravspesifikasjon for PKI i offentlig sektor", http://www.regjeringen.no/nb/dep/fad/dok/rapporter_planer/Rapporter/2004/Kravspesifikasjon-for-PKI-i-offentlig-se.html?id=106067 som er en forvaltningsstandard. I kravspesifikasjonen er det definert tre ulike sikkerhetsnivåer med tilhørende krav til sikkerhetstjenester. Dette forenkler vurderingene for forvaltningsorganene. De samme løsninger anbefales for kommunene. Fornyingsdepartementet arbeider også med planer for en ny portal for sikkerhetsfunksjonalitet, jf. pressemelding av 30.06.2006. Se også eForvaltningsforskriften § 27 med kommentarer.

[6] Se for øvrig regjeringens handlingsplan "eNorge 2009 - det digitale spranget", pkt. 1.1 *Digital deltakelse for alle*. http://www.regjeringen.no/nb/dep/fad/Tema/IT-politikk__eNorge/eNorge-2009.html?id=439499

[7] Se § 3(1)(c).

[8] Forskriften gjelder både publikums/borgernes kommunikasjon med forvaltningen og kommunikasjon mellom forvaltningsorganer.

[9] Lov av 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven). http://www.lovdata.no/all/nl-19670210-000.html

§ 2 *Begreper* [10]

(1) De begreper som er definert i lov om elektronisk signatur § 3[11] og forvaltningsloven § 2[12] benyttes på samme måte i forskriften her.

Kapittel 2. Alminnelige krav ved bruk av elektronisk kommunikasjon med forvaltningen

§ 3 *Bruk av elektronisk kommunikasjon ved henvendelser til et forvaltningsorgan*[13]

(1) Enhver[14] som henvender seg til et forvaltningsorgan[15] kan benytte elektronisk kommunikasjon, når det skjer i henhold til den form og fremgangsmåte og ved bruk av den elektroniske adressen, som forvaltningsorganet har anvist for den aktuelle type henvendelse.[16]

(a) Med *form* eller *fremgangsmåte* menes for eksempel bruk av spesielle skjema, bruk av en bestemt prosedyre eller lignende.[17]

(b) Med *elektronisk adresse* menes for eksempel en adresse til et nettsted, en e-postadresse, et nummer til en SMS-tjeneste eller lignende.[18]

---

[10] Forskriften benytter de samme begrepene som er brukt i de lovene som forskriften er forankret i. Dette gjelder bl.a. begreper som elektronisk signatur, sertifikat mv. Se mer om disse begrepene i lov om elektronisk signatur ("esl") § 3 og i forarbeidene til esignaturloven http://www.regjeringen.no/nb/dep/nhd/dok/regpubl/otprp/19992000/Otprp-nr-82-1999-2000-.html?id=162082 http://www.regjeringen.no/nb/dep/nhd/dok/regpubl/otprp/20012002/Otprp-nr-103-2001-2002-.html?id=169785.

[11] Lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3. http://www.lovdata.no/all/tl-20010615-081-001.html#3

[12] http://www.lovdata.no/all/tl-19670210-000-001.html#2

[13] Se Veilederen del 1, kapittel 3.1 *Fleksibilitet og behovstilpassede løsninger* og kapittel 3.2 *Valg av form og fremgangsmåte*.

[14] Bestemmelsen retter seg mot alle som vil kommunisere elektronisk med forvaltningen. Begrepet 'enhver' benyttes på samme måte som i offentlighetsloven § 2 annet ledd. http://www.lovdata.no/all/tl-19700619-069-0.html#2

[15] Se forvaltningsloven § 1. http://www.lovdata.no/all/tl-19670210-000-001.html#1

[16] Man har altså rett til å benytte elektronisk kommunikasjon når forvaltningsorganet har lagt til rette for det, og man gjør det slik forvaltningsorganet krever. Hvis det er opprettet egen nettside eller lenke for et bestemt formål må denne benyttes. Det er for eksempel opprettet en egen tjeneste for søknad om nytt skattekort. Slik søknad kan da ikke sendes til Skattedirektoratets generelle elektroniske adresse. Selv om forvaltningsorganet har lagt til rette for elektronisk kommunikasjon vil man alltid kunne henvende seg til organet muntlig eller ved ordinært brev, med mindre forvaltningsorganet kan påvise et særskilt grunnlag for å *kreve* at det benyttes elektronisk kommunikasjon. Se også Veilederen del 1, kapittel 3.2 *Valg av form og fremgangsmåte*, siste avsnitt.

[17] Det kan for eksempel være krav om bruk av web-skjema eller at man som bruker ledes gjennom en interaktiv prosess der man avgir opplysninger, gjør valg mv. og til slutt godkjenner resultatet av prosessen, for eksempel personlig selvangivelse på web.

[18] Eksempler på dette kan være en URI (URL) der en benytter web-skjema ved henvendelse til organet for å håndtere den økende elektroniske trafikken. Dette vil gi enklere og ryddigere håndtering, samt større muligheter til maskinell behandling av henvendelser. Se for eksempel enkelt kontaktskjema fra Fornyings- og administrasjonsdepartementet. http://www.regjeringen.no/nb/dep/fad/dep/Kontakt.html?id=347 .Ellers

(c) Med *elektronisk kommunikasjon* menes bruk av for eksempel internett, eller liknende kommunikasjonssystem, og bruk av talestyrte eller andre automatiske telefontjenester, men ikke bruk av taletelefon eller annen muntlig kommunikasjon.[19]

(2) Hvis det ikke er anvist noen egen elektronisk adresse, og det heller ikke er stilt noen særskilte krav til form eller fremgangsmåte, for den type henvendelse som er aktuell, kan den som vil henvende seg til forvaltningsorganet, bruke forvaltningsorganets generelle elektroniske adresse.[20]

(3) Når det benyttes elektronisk kommunikasjon ved henvendelse til et forvaltningsorgan, skal henvendelsen ikke rettes direkte til en enkeltperson[21],[22] med mindre forvaltningsorganet har lagt til rette for det,[23] eller det er avtalt i det enkelte tilfelle.[24]

(4) Forvaltningsorganet kan bestemme at henvendelser fra andre forvaltningsorganer kan sendes direkte til enkeltpersoner i forvaltningsorganet.[25]

---

vil den generelle elektroniske adressen for tiden være organets e-postadresse (eks. postmottak@fad.dep.no).

[19] Dette innebærer at for eksempel en kontofontjeneste vil være omfattet. Tradisjonell telefax omfattes ikke av forskriften.

[20] I tillegg til å opprette særskilte nettbaserte tjenester for bestemte saksområder eller brukere, bør forvaltningsorganet ha en generell side som gir publikum anledning til å ta kontakt med 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@oslo.kommune.no. Denne adressen kan brukes dersom publikum er usikre på hvilken måte henvendelser skal fremsettes eller til hvem de skal sendes.

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

[22] Det er klare ulemper ved å tillate at henvendelser sendes direkte til saksbehandler. For det første skaper det store utfordringer for arkiv og journalføring. Hvis for eksempel journalføringen svikter som følge av at henvendelsen er sendt direkte til saksbehandler, så glipper også grunnlaget for gjennomføringen av innsynsretten. Dessuten er det vanligvis 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.

[23] Det er altså en betingelse for å sende epost direkte til en saksbehandler at forvaltningsorganet har lagt til rette for det. Et eksempel på at det er lagt til rette for direkte henvendelser til saksbehandler kan være når forvaltningsorganet benytter elektronisk saksbehandling, arkiv- og journalsystem og det er 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 http://www.lovdata.no/for/sf/kk/tk-19981211-1193-007.html#3-1edd. Dette skal også være beskrevet i organets sikkerhetsstrategi, jf § 13 i eforvaltningsforskriften.

[24] 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 nedfelt i organets sikkerhetsstrategi jf § 13, for hvordan saksbehandlere skal håndtere direkte elektronisk kommunikasjon.

(5) Forvaltningsorganet bør legge til rette for at elektronisk kommunikasjon med forvaltningsorganet er brukervennlig og tilgjengelig for alle.[26]

§ 4 *Krav til bruk av sikkerhetstjenester og –produkter mv. ved henvendelser til et forvaltningsorgan*[27]

(1) Enhver[28] som henvender seg til et forvaltningsorgan ved bruk av elektronisk kommunikasjon i henhold til § 3, kan gjøre det uten bruk av sikkerhetstjenester eller -produkter, med mindre bruk av slike sikkerhetstjenester og -produkter er nødvendig for å oppfylle krav fastsatt i henhold til nr. (2)-(3) nedenfor eller følger av § 5, eller av krav fastsatt i annen lov eller i medhold av lov.[29]

(a) Med *sikkerhetstjenester og -produkter* menes 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), og andre løsninger, i henhold til forvaltningsorganets sikkerhetsstrategi, jf. § 13. Slike løsninger kan for eksempel være basert på bruk av elektronisk signatur og kryptering.[30]

---

[25] Dette forutsetter naturligvis at forvaltningsorganene har rutiner for journalføring av epost. Det er også grunn til å anta at forvaltningsorganene har bedre innsikt i hvem som er rette adressat, og i den aktuelle prosessen, enn en utenforstående bruker av forvaltningens tjenester.

[26] I dette ligger bl.a. en påminnelse om at løsninger for elektronisk kommunikasjon bør være lette å forstå og anvende og at de også bør være tilgjengelige for personer med nedsatt funksjonsevne. Tjenestene bør også være tilgjengelige fra ulike tekniske plattformer, for eksempel fra mindre bærbare enheter. I eNorge-planen 2009 fremheves det i pkt. 1.1 at elektroniske tjenester og verktøy skal tilrettelegges for alle. Se http://www.regjeringen.no/nb/dep/fad/Tema/IT-politikk__eNorge/eNorge-2009.html?id=439499

[27] Se Veilederen del 1, kapittel 3.4 *Krav til bruk av sikkerhetstjenester og –produkter*.

[28] Bestemmelsen retter seg mot alle som vil kommunisere elektronisk med forvaltningen. Begrepet benyttes på samme måte som i offentlighetsloven § 2 annet ledd. http://www.lovdata.no/all/tl-19700619-069-0.html#2

[29] Utgangspunktet er at henvendelser til et forvaltningsorgan kan skje uten bruk av sikkerhetstjenester og produkter. Forvaltningsorganet kan ikke sette krav om bruk av slike bare ”for sikkerhets skyld”. De krav som organet setter til kommunikasjonen skal reflektere relevante og legitime behov som er grunngitt i organets sikkerhetsstrategi, jf § 13. Sikkerhetsstrategien skal også omfatte relevante krav som er stilt i annet regelverk.

[30] I henhold til efvf § 4, kan forvaltningsorganet selv velge hvilke sikkerhetstjenester og -produkter de skal benytte. Valg av løsninger skal være forankret i forvaltningsorganets sikkerhetsstrategi, jf. § 13. I forbindelse med tiltak for å fremme bruk av elektroniske tjenester og for å koordinere forvaltningens bruk av sikkerhetstjenester, er forvaltningsorganets valgfrihet likevel begrenset.
Alle statlige etater som skal ta i bruk tjenester for autentisering og elektronisk signatur er nå pålagt å benytte ”Kravspesifikasjon for PKI i offentlig sektor” http://www.regjeringen.no/nb/dep/fad/dok/rapporter_planer/Rapporter/2004/Kravspesifikasjon-for-PKI-i-offentlig-se.html?id=106067 som er en forvaltningsstandard. De samme løsninger anbefales for kommunene. Se brev fra Moderniseringsdepartementet til samtlige statsetater 7. juni 2005 http://www.regjeringen.no/nb/dep/fad/aktuelt/nyheter/2006/Felles-sikkerhetsinfrastruktur-for-elekt.html?id=271154
Det er etablert en ordning for selvdeklarering av sertifikattjenester som oppfyller kravene i ”*Kravspesifikasjon for PKI i offentlig sektor*”, jf. forskrift 21. november 2005 nr. 1296

(b) Med *elektronisk signatur* menes løsninger som definert i lov om elektronisk signatur[31] § 3. Med *kryptering* menes omforming av data slik at de ikke er rekonstruerbare for uvedkommende. Krypterte data skal kunne rekonstrueres ved *dekryptering*.

(c) Med *krypteringsnøkkel* og *dekrypteringsnøkkel* menes data som benyttes for henholdsvis kryptering og dekryptering.[32]

(2) Forvaltningsorganet kan i det enkelte tilfelle[33] be om opplysninger som bekrefter avsenders identitet eller fullmakter, eller stille krav om at bestemte sikkerhetstjenester og -produkter skal tas i bruk, dersom dette er av betydning for håndtering av henvendelsen.

(3) Forvaltningsorganet kan bestemme at krav som nevnt i nr. (2) ovenfor skal gjelde generelt for nærmere angitte typer av henvendelser. Kravene skal være basert på forvaltningsorganets sikkerhetsstrategi, jf. § 13.[34]

(4) Forvaltningsorganet skal gjøre tilgjengelig sikkerhetstjenester og -produkter som oppfyller de krav forvaltningsorganet har stilt i henhold til nr. (2)-(3) ovenfor eller anvise hvilke løsninger som ellers kan benyttes.[35] Det samme gjelder for sikkerhetstjenester og -produkter som er nødvendig for å oppfylle kravene i § 5.

§ 5 *Formidling av taushetsbelagte opplysninger og personopplysninger til forvaltningen*[36]

(1) Når et forvaltningsorgan legger til rette for bruk av elektronisk kommunikasjon for mottak av opplysninger som på forvaltningens hånd kan være underlagt taushetsplikt, eller som kan være underlagt krav til sikring etter reglene om behandling av

---

http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20051121-1296.html]. Selvdeklarasjonen skal sendes til Post- og teletilsynet som er tilsynsorgan. Tilsynet publiserer en liste over tilsendte selvdeklarasjoner. Sertifikattjenester på denne listen ansees å tilfredstille kravene i kravspesifikasjonen. Selvdeklarasjonsordningen er forankret i eSignaturloven (esl.) § 16a http://www.lovdata.no/all/tl-20010615-081-004.html#16a . Denne bestemmelsen danner rammen for etablering av frivillige sertifiserings-, godkjennings- eller selvdeklareringsordninger. Slike ordninger gjør det enklere for brukerne å orientere seg blant de sikkerhetstjenester og –produkter som er tilgjengelige i markedet, og kan bidra til å etablere tillit til deres pålitelighet.

[31] Lov av 15. juni 2001 nr. 81 om elektronisk signatur. http://www.lovdata.no/all/nl-20010615-081.html

[32] Begrepene *"krypteringsnøkkel"* og *"dekrypteringsnøkkel"* er teknologiuavhengige begrep som brukes generelt innenfor sikring av elektronisk kommunikasjon. Formuleringene er ikke identiske (men i harmoni) med definisjoner i forskrift om informasjonssikkerhet (jf. sikkerhetsloven), fordi definisjonene der er mer omfattende enn det er behov for i denne forskriften. Begrepene er ikke brukt i lov om elektronisk signatur fordi loven ikke omhandler kryptering.

[33] 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.

[34] Forvaltningsorganets krav til bruk av sikkerhetsteknikker og –produkter skal være gjennomtenkte og grunnet i rettslige krav eller et reelt praktisk behov. Dette er søkt tydeliggjort i (3) ved å henvise til bestemmelsen i § 13, om sikkerhetsmål og sikkerhetsstrategi

[35] Forvaltningsorganet skal konkret angi hvorledes de krav de selv har stilt kan oppfylles. Dette kan gjøres ved enten selv å tilby relevante tjenester og produkter eller å navngi tjenesteytere og produkter som tilfredsstiller kravene.

[36] Se Veilederen del 1, kapittel 3.5 *Formidling av taushetsbelagte opplysninger og personopplysninger til forvaltningen*

personopplysninger eller tilsvarende regler, skal risiko for uberettiget innsyn i opplysningene være forebygget på tilfredsstillende måte.[37]

(2) Forvaltningsorgan som legger til rette for å motta opplysninger som nevnt i nr. (1), skal på hensiktsmessig måte informere[38] om eventuelle risikoer ved elektronisk overføring av slike opplysninger og om hva som er rette elektroniske adresse.[39]

(3) Forvaltningsorganet skal opplyse generelt[40] om hvordan taushetsbelagte opplysninger og personopplysninger sikres under behandling i forvaltningsorganet.

(4) Ved kryptering av melding til forvaltningen skal forvaltningsorganets krypteringsnøkkel eller krypteringsnøkkel til en nærmere angitt enhet ved forvaltningsorganet benyttes[41]. Hvis forvaltningsorganet benytter ekstern databehandler i henhold til personopplysningsloven § 15, kan databehandlerens krypteringsnøkkel benyttes hvis det godtgjøres, eller er alminnelig kjent, at databehandleren opptrer på vegne av forvaltningsorganet.[42]

(5) Kryptering med en enkeltpersons krypteringsnøkkel kan bare benyttes dersom forvaltningsorganet har lagt spesielt til rette for det.

§ 6 *Bekreftelse på at en henvendelse er mottatt* [43]

(1) Et forvaltningsorgan som mottar henvendelser i elektronisk form skal gi bekreftelse[44] til avsender om at en henvendelse er mottatt.

---

[37] Forvaltningen har en plikt til å sikre informasjon i henhold til regler om bl.a. taushetsplikt, personvern. Når forvaltningen inviterer publikum til å kommunisere elektronisk, må det også informeres om hvordan publikum skal gå frem for å gjøre dette på en trygg måte.

[38] Det er nødvendig å presisere forvaltningens veiledningsplikt på et område som for mange er nytt og ukjent. En "hensiktsmessig måte" å informere på kan være å legge informasjon om risikoer og nødvendige tiltak på hjemmesiden som publikum må besøke for å kunne kommunisere med organet.

[39] Se § 3 (1) b

[40] Ordet "*generelt*" er benyttet for å presisere at forvaltningsorganets opplysningsplikt ikke er så omfattende at det kan blottstille og derved true sikkerhetssystemene til forvaltningsorganet.

[41] Se Veilederen del 1, kapittel 3.5 og kapittel 4.5. Det er vanligvis forvaltningsorganets krypteringsnøkkel som skal benyttes; i praksis i form av et virksomhetssertifikat (som kan være et SSL-sertifikat).

[42] Skattetaten, Statens lånekasse og flere andre benytter f eks Altinn portalen, der det enkelte rettsubjekt registrerer sine opplysninger. Portaler som Altinn er jo ikke en del av forvaltningsorganet, men et subjekt som utfører nærmere bestemte oppgaver for et eller flere forvaltningsorgan. Etter alminnelig sikkerhetsoppfatning, skal hjelperen benytte egne krypteringsnøkler og ikke forvaltningsorganets nøkler. Dermed mister man den direkte knytningen mellom forvaltningsorganet og den enkelte avgiver av informasjonen. Det er derfor oppstilt et krav om å bekrefte fullmaktforholdet mellom forvaltningsorganet og databehandleren (portalen). Dette kan skje med både tekniske og organisatoriske løsninger. Se Veilederen del 1, kapittel 4.5.

[43] Se Veilederen del 1, kapittel 3.6 *Tilbakemeldinger på henvendelser som forvaltningsorganet mottar*.

[44] Bestemmelsen oppstiller et krav om kvittering på at en henvendelse er mottatt ved bruk av elektronisk kommunikasjon av forvaltningsorganet. Dersom forvaltningsorganet tilbyr Web-baserte søknadsskjemaer, kan IT-systemet som mottar en søknad kunne definere dette som et saksdokument og oppgi et referansenummer i dialogen med avsenderen av opplysningene. 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, for eksempel "spam", jf bestemmelsens (3) ledd. Det enkleste vil ofte være å legge opp til bekreftelse på alle mottatte henvendelser.

(2) Bekreftelse bør gis straks henvendelsen er mottatt. Den bør inneholde et referansenummer eller lignende og angi på hvilket tidspunkt henvendelsen ble mottatt.[45]

(3) Forvaltningsorganet kan unnlate å sende bekreftelse, hvis henvendelsen er av en slik art at den ikke utløser saksbehandling, eller mottaket fremgår på annen betryggende måte,[46] og ved bruk av automatiserte systemer der henvendelsen straks blir besvart. Forvaltningsorganet kan også inngå avtale med næringsdrivende og med andre forvaltningsorganer om ikke å sende egen bekreftelse etter denne bestemmelsen i forbindelse med rutinemessig eller periodisk rapportering.[47]

§ 7 *Henvendelser som ikke tilfredsstiller aktuelle krav*

(1) Henvender noen seg til urette myndighet eller benytter uriktig elektronisk adresse[48] 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 eller det av andre grunner finnes nødvendig. Organet bør samtidig gi frist til å rette opp feilen og gi veiledning om hvordan dette kan gjøres. [49]

(3) Forvaltningsorganet skal registrere tidspunkt for når det er sendt varsel etter nr. (1) og (2) ovenfor, og til hvem varselet ble sendt. Dersom feilen er av en slik art at det ikke er

---

[45] Når henvendelser sendes i strukturert form via Web-baserte skjemaer vil det være mulig å opprette saksnummer automatisk. Referansenummeret som oppgis i bekreftelsen kan da være det samme som saksnummeret. I tillegg skal bekreftelsen angi på hvilket tidspunkt henvendelsen er mottatt. Dette kan ha betydning bl.a. i forbindelse med avbrytelse eller beregning av frister mv. 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.

[46] F eks hvis brukeren får tilbakemelding på skjermen om at en overføring er vellykket.

[47] Det kreves her en særskilt avtale med organet. En forutsetter her at kommunikasjonen med forvaltningsorganet er betryggende løst på andre måter. Generelt bør en være forsiktig med å benytte unntaksregelen.

[48] 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.

[49] 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 nødvendige opplysninger. Det kan også foreligge feil som kan være av mindre betydning, for eksempel hvis feilen ikke har betydning for saksbehandlingen og ikke andre forhold taler mot det, eksempelvis fordi forvaltningsorganet sitter inne med andre opplysninger som bekrefter de aktuelle forhold.
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. Uansett skal avsender få veiledning og en rimelig frist til å rette feilen.

mulig å identifisere avsender, og varsel ikke kan sendes, skal det registreres opplysning om dette.

§ 8 *Underretning om enkeltvedtak og enkelte andre meddelelser fra forvaltningsorgan* [50]

(1) Underretning om enkeltvedtak[51] kan skje ved bruk av elektronisk kommunikasjon dersom parten[52] uttrykkelig[53] har godtatt dette og oppgitt den elektroniske adresse forvaltningsorganet skal benytte for å sende varsel[54] etter nr. (2) nedenfor.

(2) Forvaltningsorganet skal sende parten varsel[55] om at enkeltvedtak er fattet, om hvor og hvordan vedkommende kan skaffe seg kunnskap om innholdet, samt en frist[56] for når dette senest må skje.

---

[50] Se Veilederen del 1, kapittel 3.7 *Underretning om enkeltvedtak mv*.

[51] Se forvaltningsloven § 2 første ledd, bokstav b).

[52] Se forvaltningsloven § 2 første ledd, bokstav c).

[53] De fleste private og juridiske personer har nå e-postadresse, men de er ikke derfor nødvendigvis forberedt på at viktige meldinger kan komme inn på denne måten. For å unngå at noen skal lide rettstap fordi man har en annen holdning til sin elektroniske postkasse enn sin fysiske, er det bestemt at underretning om vedtak bare kan skje når mottakeren *uttrykkelig har godtatt* å motta meldinger på denne måten. Dette kravet følger direkte av fvl § 27 [lenke til lovdata fvl § 27], se også forarbeidene til bestemmelsen i Ot.prp. nr. 108 (2000-2001) pkt. 3.5.4.5 og pkt. 20.5, http://www.regjeringen.no/nb/dep/nhd/dok/regpubl/otprp/20002001/Otprp-nr-108-2000-2001-.html?id=166165
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. Forarbeidene (Ot.prp. nr. 108 (2000-2001) pkt. 20.5) uttaler at: *"Det sentrale er at uttrykket må forståes slik at det ikke skal foreligge rimelig tvil om at den private parten fullt ut har akseptert å motta elektronisk varsel etter fvl § 16 eller elektronisk underretning etter § 27*." Det må foreligge en erklæring om at man aksepterer å motta den type meldinger som samtykket omfatter. Tillegget *uttrykkelig* viser for det første at samtykket må være informert, dvs. at avgiver av samtykkeerklæringen må forstå innhold og omfang av samtykket, det ikke må være tvil om hva parten faktisk har godtatt, og at bevisbyrden for at det foreligger påhviler forvaltningsorganet.
Det oppstilles ikke noen formkrav, men det vil være naturlig å innhente samtykket i skriftlig form (på papir eller elektronisk). Dessuten 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. 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 § 8 (7).

[54] Begrepet *'varsel'* brukes gjerne om kortfattede beskjeder for å gjøre noen oppmerksom på noe, i dette tilfellet at det er fattet et enkeltvedtak.

[55] Underretning om enkeltvedtak skjer ved at det sendes et varsel om at vedtaket er truffet med en beskrivelse av hvor vedtaket kan hentes, for eksempel adresse til en nettside. Dette varselet kan sendes som ordinær e-post eller via SMS forutsatt at kravene i blant annet § 8 (4) kan ivaretas.

[56] Hvis det går mer enn en uke fra varselet er sendt, uten at parten skaffer seg tilgang til det, skal enkeltvedtaket iht § 8(7), ettersendes som vanlig brev i posten. Fristen må derfor være kortere enn en uke.

(3) Innholdet i enkeltvedtaket skal gjøres tilgjengelig fra egnet informasjonssystem,[57] jf. blant annet kravene i nr. (2), (4) og (5).

(4) Forvaltningsorganet skal forebygge risiko for uberettiget innsyn i enkeltvedtak på en tilfredsstillende måte.[58]

(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.[59]

(6) Underretning om enkeltvedtak anses å ha kommet frem på det tidspunktet parten skaffet seg tilgang til vedtaket fra forvaltningsorganets informasjonssystem.[60]

(7) Har parten ikke skaffet seg tilgang til enkeltvedtaket innen én uke fra det tidspunkt det ble sendt varsel 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.[61]

(8) Hvis det etter vedtakets art[62] ikke er tid til å gjennomføre ny underretning som beskrevet i nr. (7), bør forvaltningsorganet om mulig sende nytt varsel etter nr. (2). Når

---

[57] Et "egnet informasjonssystem" kan for eksempel være en adgangsbegrenset nettside hvor enkeltvedtaket er publisert. For å få tilgang til vedtaket, må parten gå frem slik det er bestemt i henhold til § 8(4), jf. noten nedenfor.

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.

[58] Enkeltvedtak vil vanligvis være omfattet av regler om taushetsplikt. Det er først og fremst partene og deres representanter som skal ha tilgang til enkeltvedtaket, jf fvl. § 18 og § 19, og forvaltningsorganet må sikre at de har kontroll med at ikke uvedkommende får tilgang. I forbindelse med tiltak for å fremme bruk av elektroniske tjenester og for å koordinere forvaltningens bruk av sikkerhetstjenester, ble det bestemt at alle statlige etater som skulle ta i bruk tjenester for autentisering og elektronisk signatur skal benytte "Kravspesifikasjon for PKI i offentlig sektor"
http://www.regjeringen.no/nb/dep/fad/dok/rapporter_planer/Rapporter/2004/Kravspesifikasjon-for-PKI-i-offentlig-se.html?id=106067
Løsningen er også anbefalt for kommunene. En slik løsning vil innebære at du kan identifisere og autentisere deg med din elektroniske signatur når du skal skaffe deg tilgang til vedtaket. Fornyingsdepartementet arbeider med en løsning for portal for sikkerhetsfunksjonalitet. Innholdet i den er ikke avklart pr 15. desember 2006.

[59] 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 er nødvendig med entydig og sikker identifisering av parten før enkeltvedtaket kan hentes frem fra informasjonssystemet. En sikkerhetsportal vil kunne tilby slik funksjonalitet.

[60] Det er det tidspunktet parten *faktisk skaffet seg tilgang*, ikke det tidligere tidspunkt da vedtaket ble tilgjengelig og det var opp til parten å skaffe seg tilgang til det.

[61] Hvis det går mer enn én uke før parten skaffer seg tilgang, skal enkeltvedtaket sendes som ordinært brev (papirpost). Forvaltningsorganet må derfor også ha 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, ved at de har oppgitt feil elektronisk adresse, er midlertidig avstengt fra sin nettforbindelse, 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. Systemet bør også sikre at vedtaket blir ettersendt som papirpost etter en uke, enten automatisk eller ved at saksbehandler får en melding om det.

[62] Det er altså vedtakets art som begrunner bruk av denne unntaksregelen og ikke forvaltningsorganets vurdering av hva som er mest hensiktsmessig. Et eksempel på hva som kan antas å være grunnet i

det sendes nytt varsel etter denne bestemmelse, begynner en eventuell klagefrist[63] å løpe fra den dag det nye varselet ble sendt.[64]

(9) Hvis vedtaket er av en slik art at det kan være aktuelt å benytte unntaksregelen i nr. (8), bør forvaltningsorganet etablere ordninger for å få bekreftet[65] den elektroniske adressen parten oppgir, før underretning skal finne sted. Forvaltningsorganet bør også vurdere å registrere en alternativ elektronisk adresse som kan benyttes i forbindelse med nytt varsel etter nr. (8).[66]

(10) 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.

(11) I forbindelse med underretning om enkeltvedtaket skal det informeres om forvaltningsorganet har lagt til rette for mottak av klage i elektronisk form og hva som er rette elektroniske adresse.[67] Det skal også informeres om at parten bør kontrollere at han mottar bekreftelse når klage leveres i elektronisk form, jf. § 9 (2).

§ 9 *Klage*

(1) Klage over enkeltvedtak kan fremsettes ved bruk av elektronisk kommunikasjon dersom det forvaltningsorganet som skal motta klagen har lagt til rette for det, jf. § 3 og § 4.[68]

(2) Hvis klager ikke mottar bekreftelse etter § 6, skal klagen sendes på nytt.

"vedtakets art" kan være situasjonen ved tildeling av studieplasser gjennom samordnet opptak. På grunn av den korte tiden det skal gjennomføres tildeling av studieplasser, vil det ikke være praktisk mulig å la søkerne få nyte godt av den tiden bestemmelsen i (2) gir.

[63] Se forvaltningsloven § 29. http://www.lovdata.no/all/tl-19670210-000-006.html#29

[64] Tidsfristen løper altså fra avsendelsen fra forvaltningsorganet og ikke tidspunktet i (6) som regulerer tidspunktet parten skaffet seg tilgang til vedtaket, se også Veilederen del 1, kapittel 3.7.

[65] Bekreftelse kan skje ved at organet sender en e-post eller en SMS til den oppgitte adressen, og at parten må bekrefte adressen ved å besvare henvendelsen.

[66] Når det er aktuelt å benytte unntaksregelen i (8) bør forvaltningsorganet forsikre seg om at den elektroniske adressen parten oppgir virkelig er den parten også senere kan treffes på når vedtaket skal sendes. Forvaltningsorganet bør også av samme grunn vurdere å registrere en alternativ adresse parten kan treffes på. Det er ikke krav om etablering av reserveløsninger dersom forhåndsvarselet ikke blir lest. På den annen side vil dette kunne føre til at forvaltningsorganet for eksempel ikke får inn de opplysningene de trenger, og derfor må kontakte parten på annen måte for å tilfredsstille kravene til sakens opplysning og forsvarlig saksbehandling. Det er tidsbesparende og mindre ressurskrevende for forvaltningsorganet å sikre seg med reserveløsning.

[67] Det er forvaltningsorganet som velger form eller fremgangsmåte, jf § 3 og § 4.

[68] Det er det forvaltningsorganet *"som skal motta klagen"* som må ha lagt til rette for elektronisk kommunikasjon. Dette vil regelmessig være instansen som fattet vedtaket som påklages og som skal forestå saksforberedelsen før oversendelse til klageorganet. Det vises her for øvrig til forvaltningsloven § 32 og § 33. http://www.lovdata.no/all/tl-19670210-000-006.html#32

§ 10 *Innsyn i opplysninger og dokumenter ved bruk av elektronisk kommunikasjon*

(1) Krav om innsyn i opplysninger eller dokumenter i en sak kan sendes forvaltningsorganet ved bruk av elektronisk kommunikasjon, jf. § 3 og § 4.[69]

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

(3) Innsyn etter § 10 (2) gis bare når det kan oppnås:

a) tilfredsstillende bekreftelse på at vedkommende har krav på innsyn,[70] og

b) at risiko for uberettiget[71] innsyn i opplysningene eller dokumentene er forebygget på en tilfredsstillende måte,

eller når innsyn kan kreves etter offentlighetsloven eller annen lovbestemt allmenn innsynsrett.[72]

(4) Hvis den som krever innsyn i dokumenter som er signert med avansert elektronisk signatur[73] ber om det, skal relevante sertifikater, og øvrige opplysninger som er nødvendige for å få bekreftet[74] signaturen, utleveres sammen med dokumentet.

---

[69] Begjæring om innsyn kan sendes elektronisk hvis forvaltningsorganet har lagt til rette for det, jf § 3 og § 4 .

[70] Hvis opplysningene det begjæres innsyn i er underlagt taushetsplikt eller innsynsretten på annen måte er begrenset, må forvaltningsorganet være tilstrekkelig sikker på at den som spør virkelig har krav på innsyn. Særlig praktisk er partenes innsynsrett etter reglene i forvaltningsloven § 18 flg http://www.lovdata.no/all/tl-19670210-000-004.html#18 . Den enkelte har også rett til innsyn i behandling av personopplysninger i henhold til personopplysningsloven § 18 http://www.lovdata.no/all/tl-19670210-000-004.html#18 . Videre har pasienter innsynsrett i sin journal etter reglene i pasientrettighetsloven § 5-1 og helsepersonelloven § 41. Dersom pasientjournalen føres elektronisk, kan også innsyn gis elektronisk så lenge kravene i bokstav a) og b) er oppfylt.

[71] I tillegg til å sikre at bare rette vedkommende får innsyn, kan det være behov for å sikre at ikke de opplysningene det er tale om kommer på avveie når innsynsretten utøves. Et tiltak vil være å sikre opplysningene under overføring ved kryptering (jf § 4(b)) ved for eksempel SSL-sesjon el. Risikoen for videresprednin av elektronisk lagrede dokumenter eller opplysninger er større enn ved papirbasert distribusjon. Hvorledes det elektronisk materialet det kreves innsyn i skal gjøres tilgjengelig, vil være opp til organet å håndtere ut fra hensynet til forsvarlig saksbehandling. En kan tenke seg at det kun skal gis lesetilgang og muligheter for utskrift på papir, men ikke at dataene overføres til den som har rett til innsyn. Videre finnes det teknisk muligheter for hindre kopiering av elektronisk lagrede dokumenter mv.

[72] Sikkerhetskrav er ikke nødvendig ved innsyn etter offentlighetsloven. Derfor har innsyn etter offentlighetsloven blitt plassert som alternativ, jf "*eller*". I den nye "lov om rett til innsyn i dokument i offentleg verksemd (offentleglova)" § 30, fremgår det at forvaltningsorganet ut fra hensynet til forsvarlig saksbehandling bestemmer hvordan dokumenter skal gjøres kjent, og det fremgår at det kan kreves papirkopi eller elektronisk kopi av dokumentet. Loven trer i kraft fra den tid Kongen bestemmer.

[73] Se lov om elektronisk signatur § 3 nr. 2. http://www.lovdata.no/all/tl-20010615-081-001.html#3

[74] 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.

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.

Alternativt kan forvaltningsorganet legge til rette for at verifisering kan skje i forbindelse med at det gis tilgang til dokumentet.

(5) Forvaltningsorganet skal også legge til rette for at den enkelte kan få tilgang til dokumentene i en form som gjør det mulig å dokumentere[75] innholdet overfor tredjepart. Dette kan om nødvendig skje i form av en papirutskrift av dokumentet som er bekreftet av forvaltningsorganet.

§ 11 *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.[76]

(2) Uttalelser til høringen kan avgis i elektronisk form, jf. § 3 og § 4.[77]

§ 12 *Forvaltningsorganets adgang til å nekte bruk av elektronisk kommunikasjon*[78]

(1) Hvis det er grunn til å anta at noen misbruker adgangen[79] til elektronisk kommunikasjon med forvaltningsorganet, kan vedkommende helt eller delvis nektes videre bruk av slik kommunikasjon med forvaltningsorganet.

(2) Før adgangen til å nekte bruk av elektronisk kommunikasjon med forvaltningsorganet iverksettes, skal forvaltningsorganet sende vedkommende varsel[80] om at det vurderer å

---

[75] 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.

[76] 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. 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.

[77] 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.

[78] Bestemmelsen gir adgang til helt eller delvis å sperre for elektronisk kommunikasjon *"hvis det er grunn til å anta"* at den elektroniske kommunikasjonskanalen misbrukes. Andre sanksjoner kan følge av annen lovgiving, for eksempel straffelovens regler om bedrageri og dokumentfalsk, jf spesialmotivene til § 15a. Se Veilederen del 1, kapittel 3.10 *Reaksjoner mot misbruk av elektronisk kommunikasjon.* Hjemmel for forvaltningsorganets sanksjonsmulighet er fvl. § 15a innledningen, samt litra (e) http://www.lovdata.no/all/tl-19670210-000-003.html#15a Se også Ot.prp. nr. 108 pkt. 3.5.4.7.2 (s. 42), samt 20.5 (s.180) om §15a.

[79] Forvaltningsorganet gis adgang til helt eller delvis å nekte videre bruk av elektronisk kommunikasjon når enten kommunikasjonsløsningen eller sikkerhetstjenester og –produkter som benyttes misbrukes. Vedkommende må da benytte tradisjonell kommunikasjon mot forvaltningsorganet.

[80] Regelen er et utslag av det kontradiktoriske prinsipp. Adressaten for varselet skal få anledning til å bli kjent med anførselen og eventuelt imøtegå den før sanksjonen iverksettes. Fristens lengde må settes slik at dette blir mulig å gjennomføre. Varselet må være skriftlig, jf. "sende". Det vil ikke uten videre være adgang til å benytte elektronisk kommunikasjon, jf. § 8(10).

nekte videre bruk av slik kommunikasjon og begrunnelsen for dette. Vedkommende skal oppfordres til å uttale seg om grunnlaget for avgjørelsen. Forvaltningsorganet skal sette en frist for slik uttalelse. Hvis det finnes nødvendig av sikkerhetsmessige årsaker kan forvaltningsorganet iverksette avgjørelsen straks.

(3) Den som blir nektet bruk av elektronisk kommunikasjon etter nr. (1) kan påklage avgjørelsen. Reglene i forvaltningsloven[81] kap. VI gjelder tilsvarende så langt de passer.

Kapittel 3. Forvaltningsorganets strategi for informasjonssikkerhet

§ 13 *Sikkerhetsmål og sikkerhetsstrategi* [82]

(1) Forvaltningsorgan som benytter elektronisk kommunikasjon[83] skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (*sikkerhetsmål* og *sikkerhetsstrategi*).[84] Sikkerhetsstrategien skal danne grunnlaget[85] for forvaltningsorganets beslutninger om innføring og bruk av sikkerhetstjenester og

---

I tilfeller der det er særlig alvorlige brudd, for eksempel når organets kommunikasjonsløsning er truet, kan forvaltningsorganet sperre kommunikasjonen samtidig som varselet sendes.

[81] Lov av 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven) kap. VI. http://www.lovdata.no/all/tl-19670210-000-006.html

[82] Se Veilederen del 1, kapittel 3.3 *Etablering av sikkerhetsstrategi.* Begrepene *"Sikkerhetsmål og sikkerhetsstrategi"* er også benyttet i personopplysningsforskriften § 2-3. http://www.lovdata.no/for/sf/fa/ta-20001215-1265-002.html#2-3

[83] http://www.regjeringen.no/nb/dep/fad/aktuelt/nyheter/2006/Felles-sikkerhetsinfrastruktur-for-elekt.html?id=271154 Se eForvaltningsforskriften § 3 (1) (c).

[84] Forvaltningsorganet har en *plikt* til å utarbeide sikkerhetsmål og sikkerhetsstrategi. Sikkerhetsstrategien skal være utarbeidet *før* man setter i gang med elektronisk kommunikasjon. I praksis betyr dette at en ikke kan utvikle og ta i bruk et nytt IKT-system, uten at mål og strategi for informasjonssikkerheten er utarbeidet. Forvaltningsorganer som allerede benytter elektronisk kommunikasjon uten å ha en slik strategi, må utarbeide en. Strategien kan medføre behov for endringer i virksomhetens løsninger. Virksomhetens mål for informasjonssikkerhet ved bruk av elektronisk kommunikasjon skal være formulert i sikkerhetsmål, og de nærmere valg og prioriteringer for å nå målene må være beskrevet i en sikkerhetsstrategi. Sikkerhetsmål og –strategi skal bidra til å legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon, på en samordnet og enkel måte, - både for de som skal kommunisere med forvaltningen (borgere og næringsliv), og for forvaltningen selv, jf. § 1.

[85] Sikkerhetsstrategien skal ikke bare danne grunnlag for valg av sikkerhetstjenester og det nærmere nivået på sikkerheten, men skal også danne grunnlag for eventuelt å velge *bort* sikkerhetstiltak der de ut fra nærmere vurderinger ikke anses nødvendige. Ofte tas elektroniske løsninger i bruk uten nærmere sikkerhetstenkning; for eksempel e-post. Dette er det ikke adgang til. Forskriften krever at dette i så fall skal være en bevisst og gjennomtenkt handling, med basis i sikkerhetsstrategien. Alle steder hvor forskriften gir adgang til å anvende sikkerhetstjenester og –produkter, skal eventuelle krav være basert på forvaltningsorganets sikkerhetsstrategi.

Sikkerhetsstrategien vil ha betydning for tilliten til forvaltningsorganenes tekniske løsninger og tilliten 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, som grunnlag for at borgere og næringsliv kan ha tillit til forvaltningen. Sikkerhetstenkningen skal være en integrert del av virksomhetens øvrige planarbeid (virksomhetsstrategi, inkludert strategi for IKT og informasjonssikkerhet), slik at styring av videre valg og bruk skjer ut fra en helhetlig tenkning.

-produkter på en helhetlig, planlagt, systematisk og dokumentert[86] måte. Sikkerhetsstrategien skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks[87].

(2) Sikkerhetsstrategien skal være utarbeidet i henhold til anerkjente prinsipper for informasjonssystemers sikkerhet.[88]

(3) I den utstrekning det er relevant skal sikkerhetsstrategien også adressere, og om nødvendig stille krav til, bl.a.:[89]

a) prosedyrer for anskaffelse, bruk, oppbevaring og sikring av

[86] Se tilsvarende krav i personopplysningslovens (pol) § 13, som krever planlagte og systematiske tiltak for informasjonssikkerhet for personopplysninger, med dokumentasjon. Se også pol § 14 om internkontroll med tilsvarende krav. http://www.lovdata.no/all/tl-20000414-031-002.html#13

[87] Krav til informasjonssikkerhet forekommer i flere lover, forskrifter og instrukser. Denne regelen peker på nødvendigheten av å se slike krav i sammenheng, og gjennomføre vurderinger og tiltak for informasjonssikkerhet på en helhetlig måte i den enkelte virksomhet, ut fra de regelverkene som stiller relevante krav. Slike krav vil av og til fremkomme direkte som krav til informasjonssikkerhet, og i andre tilfeller mer indirekte, for eksempel som bestemmelser om taushetsplikt eller som krav til tilfredsstillende autentisering eller lignende. I noen regelverk er kravene mer eller mindre harmonisert, men ikke alle. Se for eksempel krav til sikkerhet også i helseregisterloven (av 18. mai 2001, nr 24), §§ 16 og 17 http://www.lovdata.no/all/tl-20010518-024-003.html#16 , lov om Schengen informasjonssystem (SIS-loven av 16. juli 1999, nr 66) § 3 http://www.lovdata.no/all/tl-19990716-066-0.html#3 , samt tilhørende SIS-forskrift kapittel 7 http://www.lovdata.no/for/sf/jd/td-20001221-1365-007.html, som i stor grad gir politiet tilsvarende regler som i personopplysningsforskriftens kapittel 2 http://www.lovdata.no/all/tl-20000414-031-002.html . Et annet og kanskje mer praktisk eksempel kan være beskyttelsesinstruksen i statlig sektor som forvaltes av Statsministerens kontor (http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-19720317-3352.html). *Den stiller krav til forsvarlig behandling av opplysninger som må beskyttes mot uvedkommendes innsyn eller tilgang (konfidensialitet), jf de mange taushetsplikter i ulike regelverk, herunder i forvaltningslovens § 13 flg. Ved elektronisk behandling av slik informasjon skal laveste sikkerhetsnivå i forsvarets regler følges, jf forskrift om informasjonssikkerhet (av hensyn til rikets sikkerhet og selvstendighet og andre vitale nasjonale sikkerhetsinteresser) som er fastsatt med hjemmel i sikkerhetsloven. Dette er konsekvensrikt: hvis et forvaltningsorgan i staten følger beskyttelsesinstruksen, og skal gjøre bruk av elektronisk kommunikasjon for denne informasjonen, er det en lang rekke av de nevnte reglene som må oppdages og følges, blant annet om kryptering. Se instruksens § 12. Se nevnte forskrift om informasjonssikkerhet her: http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20010701-0744.html . Siden beskyttelsesinstruksen er en statlig instruks, gjelder den bare i departementer, direktorater og for fylkesmenn mv, men selvfølgelig ikke i fylkeskommunal eller kommunal sektor.*

[88] Anerkjente prinsipper er gjerne nedfelt i standarder. En viktig standard på dette området er Norsk Standard (NS 17799). Den ISO standard som NS 17799 implementerer, bygger på British Standard 7799, A Code of Practice for Information Security Management. Virksomheter kan derved utvikle, implementere og måle virksomhetens sikkerhetsarbeid og rutiner. Standarden kan kjøpes fra Standard Norge, se http://www.standard.no/ . NS 17799 er basert på den beste nåværende praksis innen arbeidet med informasjonssikkerhet både i England og i mange andre land. Datatilsynet anbefaler den på sin nettside; ved å følge den kommer man langt også i å følge personopplysningsforskriftens krav. Se http://www.datatilsynet.no/templates/article 888.aspx Standarden ligger også til grunn for en norsk ordning for frivillig sertifisering av informasjonssikkerheten i organisasjoner, forvaltet av Norsk Akkreditering.

[89] Oppregningen i tredje ledd, av krav til innhold i sikkerhetsstrategien, er tillegg og presiseringer til det sikkerhetsstrategien ellers skal omfatte. Disse kravene er omtalt i noter til de bestemmelsene det er henvist til i tredje ledd.

signaturfremstillingsdata[90], passord/PIN-koder og dekrypteringsnøkkel[91] knyttet til personlige sertifikat[92] eller sertifikat for ansatt i forvaltningen,[93] jf. § 15, § 17 og § 20;

b) prosedyrer for anskaffelse, bruk, oppbevaring og sikring av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsnøkkel knyttet til virksomhetssertifikat[94], jf. § 14 og § 21;

c) prosedyrer for å etablere og opprettholde et sikkert brukermiljø der det benyttes elektroniske signaturer[95], kryptering eller andre sikkerhetstjenester, jf. § 18;

d) prosedyrer for varsling og tilbaketrekking[96] av sertifikat og passord/PIN-koder ved mistanke om tap eller misbruk, jf. § 23;

e) prosedyrer for kontroll av sertifikater og tilbaketrekkingslister ved mottak av melding utstyrt med elektronisk signatur, herunder krav til hvor oppdatert informasjon om sertifikaters status bør være for de ulike formål sertifikatene benyttes for, jf. § 25;

f) prosedyrer for å nekte bruk av sertifikat mv. ved misbruk av elektronisk kommunikasjon med forvaltningen, jf. § 12;

g) prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon, jf. § 5 og § 24, se også personopplysningsloven[97] § 13 og personopplysningsforskriften[98] kap 2;[99]

---

[90] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 5. http://www.lovdata.no/all/hl-20010615-081.html I denne forskriftens sammenheng vil *signaturfremstillingsdata* vanligvis være den private nøkkelen i et nøkkelpar som benyttes for asymmetrisk kryptering (signering eller autentisering).

[91] Med *krypteringsnøkkel* og *dekrypteringsnøkkel* menes data som benyttes for henholdsvis kryptering og dekryptering. Se § 4(1)(c).

[92] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 9. http://www.lovdata.no/all/tl-20010615-081-001.html#3

[93] I veiledningen benytter vi fellesbetegnelsen "personsertifikater" for disse to typene (private personlige sertifikater og ansattsertifikater).

[94] Virksomhetssertifikatet identifiserer forvaltningsorganet (jf. § 14), i motsetning til personsertifikatene som identifiserer enkeltpersoner som brukere eller ansatte i forvaltningen. Se "Kravspesifikasjon for PKI i offentlig sektor" http://www.regjeringen.no/nb/dep/fad/dok/rapporter_planer/Rapporter/2004/Kravspesifikasjon-for-PKI-i-offentlig-se.html?id=106067.

[95] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3. http://www.lovdata.no/all/tl-20010615-081-001.html#3

[96] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 12. http://www.lovdata.no/all/tl-20010615-081-001.html#12

[97] Lov av 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven). http://www.lovdata.no/all/nl-20000414-031.html

[98] Forskrift av 15. desember 2000 nr. 1265 om behandling av personopplysninger (personopplysningsforskriften). http://www.lovdata.no/for/sf/fa/fa-20001215-1265.html

[99] Forvaltningsorganet skal beskrive sine prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon, se også personopplysningsloven §§ 13 og 14 med utfyllende forskrifter. http://www.lovdata.no/all/tl-20000414-031-002.html#13 , http://www.lovdata.no/for/sf/fa/fa-20001215-1265.html 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

h) prosedyrer for sikkerhetskopiering, oppbevaring og deponering av dekrypteringsnøkkel for opplysninger som angår forvaltningsorganet, jf. § 22.

Kapittel 4. Anskaffelse og bruk av sikkerhetstjenester mv

§ 14 *Sertifikat for forvaltningsorgan (virksomhetssertifikat)* [100]

(1) Forvaltningsorgan som benytter elektronisk signatur[101] kan benytte sertifikat som identifiserer forvaltningsorganet (*virksomhetssertifikat*).[102]

(2) Hvis det skal benyttes sertifikat ved underretning om enkeltvedtak og varsling etter § 8 og ved høringer etter § 11, bør det benyttes virksomhetssertifikat.[103]

---

behandlingsreglene gjelder normalt forvaltningsorganet som sådant. Den enkelte borger kan nok 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 gjør et "opplyst valg".

[100] Brukere av forvaltningens tjenester vil vanligvis ha større nytte av å kunne identifisere selve forvaltningsorganet enn å få bekreftet identiteten til den enkelte saksbehandler. Det er forvaltningsorganet som sådant, og ikke den enkelte saksbehandler, som er involvert i samhandlingen, av og til som part, av og til i en annen myndighetsrolle i en sak mellom to private parter. Se i Veilederen del 1, kapittel 4.2 *Sertifikat for forvaltningsorgan (virksomhetssertifikat)*. Når det benyttes sertifikat ved kommunikasjon utenfor forvaltningsorganet selv, bør det i størst mulig grad benyttes virksomhetssertifikat.

[101] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 1. http://www.lovdata.no/all/tl-20010615-081-001.html#3

[102] Det er utarbeidet en norsk profil for virksomhetssertifikater (en spesifikasjon der det bl.a. fremgår hvilke opplysninger et slikt sertifikat skal inneholde), se SEID-prosjektet; *"Anbefalte sertifikatprofiler for personsertifikater og virksomhetssertifikater"* versjon 1.02 (februar 2005), pkt. 6. http://www.npt.no/iKnowBase/Content/44961/SEID_Leveranse_1_v1.02.pdf] Sertifikatprofilene er gjort til del av *"Kravspesifikasjon for PKI i offentlig sektor*".

[103] I forbindelse med underretning om vedtak er det forvaltningsorganet som sådant som er avsender. Mottakerens behov er å få bekreftet at forvaltningsorganet står bak meddelelsen. Saksbehandlerens signatur og sertifikat er til liten hjelp i denne forbindelse. Hvis det benyttes sertifikat *bør* det derfor identifisere forvaltningsorganet. Når det benyttes virksomhetssertifikat kan naturligvis saksbehandlers identitet fremgå av vedtaket selv i den utstrekning det er relevant. Skulle det være behov for det kan man evt benytte både saksbehandlers og virksomhetens sertifikat i forbindelse med samme melding. Det samme gjelder høringsdokumenter, men disse vil det nok sjeldnere være behov for å utstyre med signatur.

§ 15 *Informasjon om bruk av sikkerhetstjenester mv* [104]

(1) Et forvaltningsorgan skal gi sine ansatte anvisning på hvilke sikkerhetstjenester og -produkter de skal benytte under tjeneste for organet, og hvorledes de skal gå frem for å anskaffe nødvendig utstyr og data, herunder signaturfremstillingsdata[105] og dekrypteringsnøkkel med tilhørende sertifikat[106] samt passord og PIN-koder mv. [107]

(2) Ved anskaffelse av utstyr og data som nevnt i nr. (1), plikter forvaltningsorganet å sørge for at den ansatte får informasjon om:

a) vedkommendes ansvar og plikter i forbindelse med oppbevaring og bruk av signaturfremstillingsdata og dekrypteringsnøkkel med tilhørende sertifikat samt passord og PIN-koder mv., jf. §§ 20 og 23,[108]

b) restriksjoner på bruk av data som nevnt i bokstav a),[109]

c) egen og andres mulighet for å trekke tilbake eller suspendere sertifikat,[110]

d) sertifikatets ikrafttredelses- og utløpsdato og virkningen av at sertifikatet løper ut eller blir trukket tilbake,[111]

---

[104] Aktsom og lojal bruk av sikkerhetstjenester og –produkter er viktig for sikkerheten i, og tilliten til, IT-systemene og til forvaltningens saksbehandling. En forutsetning for å oppnå dette er at arbeidstakerne får tilstrekkelig informasjon om disse forholdene. Det er viktig at slik informasjon er relevant og tilstrekkelig utfyllende, men like viktig er det at informasjonen er tilrettelagt på en måte som innebærer at arbeidstakeren faktisk setter seg inn i den. Et tykt hefte, som kanskje er vanskelig å forstå, og som arbeidstakerne ikke "orker" å lese, kan derfor gi falsk trygghet med hensyn til hva arbeidstakerne vet om forvaltningsorganets sikkerhetsbehov –prosedyrer. Og det er slett ikke sikkert det hjelper stort om man avkrever dem en skriftlig erklæring om at heftet er mottatt og lest. Men *sikkerhetsarbeidet er viktig*. Det er av stor betydning at arbeidstakerne er innforstått med forvaltningsorganets sikkerhetsstrategi. Det kan være en god investering å gi arbeidstakerne personlig veiledning om disse forholdene, for eksempel i form av kurs eller korte veiledningsmøter, i tillegg til det skriftlige informasjonsarbeidet.

[105] I denne forskriftens sammenheng omfatter signaturfremstillingsdata også privat nøkkel som benyttes for autentiseringsformål, det vil si for å bekrefte identiteten til en person eller en virksomhet, uten å knytte vedkommende til innholdet i en bestemt melding. Se for øvrig lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 5.

[106] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 9. http://www.lovdata.no/all/tl-20010615-081-001.html#3

[107] I dette ligger for det første det selvfølgelige, at en arbeidsgiver skal bistå arbeidstakeren med å skaffe de "verktøy" arbeidstakeren trenger i sitt arbeid. Men det er også en påminnelse om at arbeidstakeren ikke fritt kan velge hvilke sikkerhetstjenester og –produkter som skal benyttes i tjenesten, men må følge arbeidsgivers instrukser. Hvilke tjenester og produkter som skal benyttes, og prosedyrer for anskaffelse og bruk, skal være basert på de behov og krav som er beskrevet i forvaltningsorganets sikkerhetsstrategi, jf. § 13.

[108] Den enkelte skal informeres om kravene til forsvarlig oppbevaring og bruk av signaturfremstillingsdata, dekrypteringsnøkler, passord og koder, se nærmere om kravene i §§ 20 og 23.

[109] Hvis det er begrensninger i hva den enkelte kan bruke sine signaturfremstillingsdata og brukerrettigheter til, skal vedkommende informeres om dette. En slik begrensning kan for eksempel være at signaturfremstillingsdata med tilknyttet personsertifikat bare skal kunne benyttes i tjeneste for arbeidsgiver og ikke til privat bruk, jf. § 17. Et virksomhetssertifikat kan naturligvis aldri benyttes for private formål.

[110] Den enkelte vil være forpliktet til å gi varsel og begjære tilbaketrekking av sitt sertifikat dersom for eksempel signaturfremstillingsdata kommer på avveie eller det inntrer andre forhold som gjør at sertifikatet ikke lenger skal benyttes, for eksempel mistanke om misbruk, se § 23. Når det benyttes virksomhetssertifikat, eller personsertifikat som er beregnet for bruk i tjenesten, vil også forvaltningsorganet være berettiget til begjære sertifikatet trukket tilbake. Sertifikatinnehaveren skal informeres om dette.

e) hvilke opplysninger om den enkelte som vil fremgå av sertifikatet og sertifikatutsteders[112] behandling av personopplysninger,[113] jf. personopplysningsloven[114] § 19,[115] og

f) forvaltningsorganets sikkerhetsstrategi for øvrig, jf. § 13.[116]

§ 16 *Innhenting av samtykke ved bruk av elektronisk signatur*[117]

Når det benyttes elektroniske signaturer, skal forvaltningsorganet ha innhentet samtykke fra de ansatte i henhold til lov om elektronisk signatur[118] § 7 og § 14 annet ledd bokstav b om utstedelse og utlevering av sertifikat.[119]

§ 17 *Restriksjoner på bruk av sertifikat mv.*[120]

(1) Signaturfremstillingsdata[121], sertifikat[122] eller passord/PIN-koder som er ment for bruk i tjeneste for forvaltningen, skal ikke benyttes for andre formål.[123]

---

[111] Sertifikater har begrenset gyldighetstid (to til tre år er vanlig). Dette skyldes bl.a. administrative forhold. Etter at sertifikatet har løpt ut vil det vanligvis ikke være mulig å få vanlig statusopplysning om sertifikatet.

[112] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 10. http://www.lovdata.no/all/tl-20010615-081-001.html#3

[113] Dette vil avhenge av hvilken type sertifikat det er tale om, men for personsertifikater vil de personrelaterte opplysningene gjerne være begrenset til sertifikatinnehaverens navn og et løpenummer tildelt av sertifikatutstederen. På grunnlag av disse opplysningene kan sertifikatutstederen kople sertifikatet til for eksempel innehaverens fødselsnummer. Dette kan i visse tilfelle utleveres til sertifikatmottaker, men det forutsetter bl.a. at kravene i personopplysningsloven § 12 er oppfylt. http://www.lovdata.no/all/tl-20000414-031-002.html#12

[114] Lov av 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven). http://www.lovdata.no/all/nl-20000414-031.html

[115] Det er naturlig at slik informasjon gis i forbindelse med innhenting av samtykke etter efvf § 16.

[116] I tillegg til de forhold som er listet ovenfor, er det viktig at arbeidstakeren får informasjon om de alminnelige reglene om forsvarlig bruk av forvaltningsorganets informasjonssystem, se § 13(3)(c) og § 18. Se også de generelle merknadene til § 15 om betydningen av at slik informasjon gis på en måte som er effektiv.

[117] Personopplysningsloven kommer til anvendelse på behandling av personopplysninger i forbindelse med sertifikater og elektroniske signaturer. I tillegg finnes enkelte, delvis overlappende, særbestemmelser om behandling av personopplysninger i lov om elektronisk signatur.

[118] Lov av 15. juni 2001 nr. 81 om elektronisk signatur. http://www.lovdata.no/all/nl-20010615-081.html

[119] For *kvalifiserte sertifikater* gjelder det særvilkår at sertifikatene bare kan gjøres offentlig tilgjengelig når sertifikatinnehaveren har samtykket til det. Hvis forvaltningsorganets ansatte skal benytte personsertifikater i tjenesten, er det i praksis en forutsetning at slikt samtykke er gitt. For virksomhetssertifikat er det derimot ikke krav om slikt samtykke. Dette gjelder også om det disponeres av en enkeltperson (arbeidstaker i forvaltningen), jf. § 21(2). For *alle* sertifikater gjelder at opplysningene som samles inn til bruk i forbindelse med utstedelse og bruk av sertifikater, enten må samles inn direkte fra den opplysningene gjelder, eller med dennes uttrykkelige samtykke. Dette innebærer en begrensning i mulighetene for automatisk å tildele alle ansatte sertifikat. Opplysninger som er innsamlet for utstedelse og bruk av sertifikater, kan ikke benyttes for andre formål.

[120] Bestemmelsen fastlegger hovedreglene for når sertifikater kan benyttes i og utenfor tjeneste og for kommunikasjon med andre enn forvaltningsorganer. Bestemmelsens første og annet ledd gjelder den forvaltningsansattes bruk av sertifikat mv. Tredje ledd gjelder mulige restriksjoner rettet mot den enkelte bruker av forvaltningens tjenester.

(2) Personlige sertifikat skal ikke benyttes i tjeneste for forvaltningen med mindre det er utstedt eller godkjent for slik bruk.[124]

(3) Et forvaltningsorgan kan bestemme at et sertifikat som er utstedt spesielt for kommunikasjon med forvaltningen, eller med et bestemt forvaltningsorgan, ikke skal benyttes for andre formål. Slike begrensninger må fremgå av sertifikatet, og brukeren skal opplyses om begrensningene.[125]

§ 18 *Forvaltningsansattes bruk av forvaltningsorganets informasjonssystem*[126]

Forvaltningsansatte skal følge instruksene arbeidsgiver har fastsatt om bruk og sikring av virksomhetens informasjonssystemer, herunder om kontroll med materiale som skal lastes ned eller installeres på den ansattes arbeidsstasjon, og forvaltningsorganets sikkerhetsstrategi for øvrig, jf. § 13.[127]

---

[121] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 5. http://www.lovdata.no/all/tl-20010615-081-001.html#3

[122] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 9. http://www.lovdata.no/all/tl-20010615-081-001.html#3

[123] Virksomhetssertifikat skal naturligvis bare benyttes når det handles på vegne av forvaltningsorganet. Men også for personsertifikater som er utstedt for bruk i tjeneste for forvaltningsorganet skal bruken begrenses i henhold til dette formålet. Dette vil gjelde for bl.a. ansattsertifikater, der tilknytningsforholdet til forvaltningsorganet fremgår, men kan også gjelde andre personsertifikater som er utstedt for samme formål. Det vil nok sjeldnere forekomme at personsertifikater som bare identifisere innehaveren som enkeltperson kan sies å være utstedt til bruk i tjeneste for forvaltningsorganet. Sertifikatinnehaveren skal informeres om begrensningene, jf. § 15.

[124] Forvaltningsorganet har behov for å koordinere bruk av sertifikater, og personsertifikater som den enkelte ansatte selv har anskaffet kan bare benyttes i tjenesten dersom forvaltningsorganet har godkjent det. Også for forvaltningens brukere, som skal forholde seg til de aktuelle sertifikatene, kan ha behov for at forvaltningsorganet koordinerer og legger til rette for verifisering av meldinger og sertifikater dersom det benyttes personsertifikater ved meldinger fra forvaltningsorganet.

[125] Hvis et forvaltningsorgan utsteder, eller får utstedt, sertifikater til bruk ved kommunikasjon med forvaltningsorganet, og tilpasset den risikoprofil det representerer, kan det være aktuelt å begrense bruken av sertifikatet til dette formålet. Man kan for eksempel tenke seg at brukeren logger seg inn på en tjeneste med en tildelt engangskode, og at det deretter lastes ned "softsertifikater" som skal benyttes for videre kommunikasjon (nivå *"standard"* i henhold til *"Kravspesifikasjon for PKI i offentlig sektor"*). Bruk av engangskoden og de aktuelle sertifikatene kan være tilfredsstillende for kommunikasjon med forvaltningsorganet i en sammenheng der transaksjonstypene er kjent, men det er ikke dermed sagt at utsteder er parat til å anbefale sertifikatet for andre formål. En slik begrensning skal imidlertid fremgå av sertifikatet, og brukeren skal varsles om begrensningene, jf. §§ 15 og 19.

[126] Aktsom og lojal bruk av forvaltningsorganets informasjonssystemer er viktig for sikkerheten i, og tilliten til, IT-systemene og til forvaltningens saksbehandling. Bestemmelsen er en påminnelse om at de ansatte skal følge de instrukser arbeidsgiver har fastsatt når det gjelder bruk og sikring av virksomhetens informasjonssystemer. En forutsetning for å oppnå dette er at arbeidstakerne får tilstrekkelig informasjon om disse forholdene, jf. § 15. Det er av stor betydning at arbeidstakerne er innforstått med forvaltningsorganets sikkerhetsstrategi.

[127] I tillegg til de alminnelige tiltak for sikring av passord og andre tilgangskoder til IT-systemene, er det viktig at forvaltningsorganet har kontroll med at det ikke lastes ned programvare på brukernes datamaskiner som kan sette sikkerheten til systemene i fare. Slik risiko kan være knyttet til datavirus og "passordsniffere" mv, men også til skadelig kode som kan gripe inn i bruken av sikkerhetstjenester og -produkter og for eksempel endre data som skal signeres uten at brukeren kan oppdage det.

§ 19 *Informasjon*[128]

(1) Forvaltningsorganet skal sørge for at enhver, i den utstrekning det er nødvendig, får tilsvarende informasjon som nevnt i § 15 og § 17 (3) i forbindelse med anskaffelse av sertifikat eller, hvis det ikke er mulig, ved første gangs bruk av slike tjenester ved kommunikasjon med et forvaltningsorgan.[129] Forvaltningsorganet skal på samme måte informere publikum om at håndtering av signaturfremstillingsdata[130], passord/PIN-koder og dekrypteringsnøkkel skal skje i henhold til §§ 20 og 23.

Kapittel 5. Beskyttelse av signaturfremstillingsdata og dekrypteringsnøkkel mv

§ 20 *Krav til oppbevaring og bruk av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsnøkkel*[131]

(1) Innehaver av signaturfremstillingsdata[132] skal oppbevare og benytte disse på en slik måte at de ikke gjøres tilgjengelige for andre.[133]

(2) Innehaver skal aldri forlate arbeidsstasjon og lignende uten å sikre at signaturfremstillingsdata ikke er tilgjengelige for andre.[134] Innehaver skal sikre:

---

[128] Bestemmelsen pålegger forvaltningsorganet å gi forvaltningens brukere informasjon og veiledning om anskaffelse og forsvarlig bruk av sikkerhetstjenester og –produkter etter de samme linjer som gjelder for forvaltningsansatte, jf. § 15, og om eventuelle restriksjoner på bruk av den enkeltes sertifikat, jf. § 17(3).

[129] Hvis tjenestene leveres av tredjepart, må forvaltningsorganet enten sørge for at tilstrekkelig veiledning gis av tjenesteleverandøren, eller forvaltningsorganet må selv informere brukeren ved første henvendelse der det gjøres bruk av tjenestene. Veiledningen må være tilstrekkelig til at brukeren blir i stand til å benytte tjenestene på en effektiv og forsvarlig måte, og til at kravene i sikkerhetsstrategien blir realisert.

[130] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 5. http://www.lovdata.no/all/hl-20010615-081.html

[131] Bestemmelsen fastlegger kravene til aktsom og forsvarlig oppbevaring og bruk av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsnøkler. Kravene tilsvarer det som ellers må regnes som ”god skikk” på området. Kravene er rettet mot den enkelte bruker (også forvaltningsansatte).

[132] Se lov om elektronisk signatur § 3 nr. 5. http://www.lovdata.no/all/hl-20010615-081.html Når det benyttes digital signatur og sertifikater, er signaturfremstillingsdata ensbetydende med den ”private nøkkelen”.

[133] Ettersom signaturfremstillingsdataene er de ”hemmelige” dataene som gjør den elektroniske signaturen unik for innehaveren og den signerte meldingen, er det viktig at ikke signaturfremstillingsdataene kommer på avveie. Skulle en annen få kontroll over signaturfremstillingsdataene kan vedkommende opptre som den egentlige innehaverens ”elektroniske dobbeltgjenger”. Det er flere løsninger for oppbevaring av signaturfremstillingsdata. De kan være oppbevart i for eksempel et smartkort (eller SIM-kortet til mobiltelefonen), de kan ligge kryptert i programvare på brukerens datamaskin, eller de kan være lagret på en sentral server. Valg av løsning er avhengig av sikkerhetsprofil og bruksområde. Beskyttelsesmekanismene for signaturfremstillingsdata som er lagret sentralt eller i programvare har brukeren liten innflytelse over, men dersom brukeren selv kan velge passord eller kode som gir tilgang til dataene, er det viktig å velge passord og koder som er tilstrekkelig sikre (slik som for koder til bankkort og for passord til arbeidsgivers datasystem mv). Man bør typisk unngå bruk av for eksempel fødselsdato eller år, navn på familiemedlemmer og naturlige ord som man vil finne igjen i en ordbok. En utfordring med ”kompliserte” koder og passord er at man av og til vil ha behov for å notere dem ned. Kodene bør i så fall skjules, og ikke oppbevares sammen med kortet eller i naturlig tilknytning til datamaskinen.

[134] Brukeren skal sikre at ikke uvedkommende får tilgang til signaturfremstillingsdataene. Hvis de er oppbevart i smartkort eller lignende skal brukeren aldri etterlate kortet i kortleseren på datamaskinen, men

a) at signaturfremstillingsdata fjernes fra arbeidsstasjonen dersom dataene er lagret i smartkort eller i en annen enhet som lett kan fjernes, og

b) at den aktuelle arbeidsoperasjonen 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.[135]

(4) Bestemmelsene om oppbevaring og bruk av signaturfremstillingsdata gjelder tilsvarende for bruk av passord/PIN-koder o.l. og dekrypteringsnøkkel.[136]

§ 21 *Sikring av signaturfremstillingsdata og dekrypteringsnøkkel ved bruk av virksomhetssertifikat*[137]

(1) Ved bruk av virksomhetssertifikat skal forvaltningsorganet sikre at ikke uvedkommende får tilgang til eller kan benytte tilhørende signaturfremstillingsdata[138].[139] Organet skal også sikre tilfredsstillende kontroll med og registrering av personell og aktiviteter som benytter slike signaturfremstillingsdata.[140] Sikringstiltakene skal skje i henhold til organets sikkerhetsstrategi.[141]

---

ta det med seg, eller oppbevare det på et forsvarlig sted når vedkommende ikke er tilstede ved datamaskinen eller dataene ikke er i bruk (som for et bankkort).

[135] Signaturfremstillingsdata og personsertifikat skal ikke overlates til andre. Hvis en person skal signere på vegne av en annen, skal dette fremgå ved at underskriveren benytter sine egne signaturfremstillingsdata og sertifikat, med angivelse av at det signeres på vegne av en annen.

[136] For at bestemmelsen skal bli så enkel som mulig å lese, er bare signaturfremstillingsdata nevnt i teksten ovenfor, men de samme prinsippene gjelder for dekrypteringsnøkkel (som vanligvis også er en privat nøkkel) og for beskyttelse av passord og PIN-koder.

[137] Reglene om sikring av signaturfremstillingsdata i § 20 ovenfor, gjelder også når det benyttes virksomhetssertifikat. I tillegg kommer kravene i denne bestemmelsen om særlige forholdsregler ved bruk av virksomhetssertifikat. Bestemmelsen er rettet mot forvaltningsorganet. Se Veilederen del 1, kapittel 4.6 *Sikring av forvaltningsorganets krypteringsnøkler mv*.

[138] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 5. http://www.lovdata.no/all/tl-20010615-081-001.html#3

[139] Et virksomhetssertifikat kan disponeres av en eller flere ansatte i virksomheten, eller være koplet direkte til en server eller en bestemt systemaktivitet (for eksempel saksbehandlingssystemet). Virksomhetssertifikatet skal sikre at mottakeren kan verifisere at forvaltningsorganet er avsender eller kommunikasjonsmotpart, og det er naturligvis viktig at ikke uvedkommende kommer i posisjon til å opptre som om de var forvaltningsorganet. Det er forvaltningsorganets oppgave å legge til rette for at ikke uvedkommende får tilgang til signaturfremstillingsdataene. Hvis signaturfremstillingsdataene er lagret i smartkort gjelder de samme regler som for kort knyttet til personsertifikat, jf. § 20. Hvis signaturfremstillingsdataene er lagret sentralt i forvaltningsorganets datasystem, må tilgangskontroll og øvrige sikringstiltak sørge for at ikke uvedkommende får tilgang.

[140] Selv om virksomhetssertifikatet utad skal signalisere at det er forvaltningsorganet det kommuniseres med, må organet selv ha kontroll med hvilke personer eller systemaktiviteter (i et automatisert system) som utløser bruk av signaturfremstillingsdata knyttet til forvaltningsorganet. Praktisk sett betyr dette at systemet skal realisere tilfredsstillende tilgangskontroll og det skal logge hvilke personer og/eller systemaktiviteter

(2) Når flere personer hver for seg skal disponere virksomhetssertifikat, bør hver enkelt disponere eget virksomhetssertifikat med tilhørende signaturfremstillingsdata.[142]

(3) Ved bruk av virksomhetssertifikat 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.[143]

(4) Det skal vurderes om forvaltningsorganet bør være utstyrt med signaturfremstillingsdata og virksomhetssertifikat fra mer enn én sertifikatutsteder[144].

(5) Signaturfremstillingsdata og dekrypteringsnøkkel skal være sikret mot misbruk i henhold til forvaltningsorganets sikkerhetsstrategi, jf. § 13.[145]

§ 22 *Sikkerhetskopiering av dekrypteringsnøkkel mv.*[146]

(1) Forvaltningsorganet skal sikre at opplysninger og annet materiale som oppbevares av forvaltningsorganet i kryptert form, ikke blir utilgjengelige som følge av at

---

som utløser bruk av signaturfremstillingsdata som er knyttet til (den offentlige nøkkelen i) et virksomhetssertifikat.

[141] Sikkerhetsstrategien er nøkkelen til en helhetlig, planlagt og dokumentert gjennomføring av forvaltningsorganets sikringstiltak. Dette gjelder også sikring av virksomhetssertifikat som er kritisk i forhold til tilliten til å kunne kommunisere trygt med forvaltningsorganet.

[142] Selv om virksomhetssertifikatet identifiserer forvaltningsorganet, er hvert sertifikat unikt med eget serienummer og eget nøkkelpar. I de tilfellene der enkeltpersoner skal disponere slikt sertifikat på vegne av forvaltningsorganet, bør de ha hvert sitt (men i mange tilfeller vil det altså være lagret sentralt og styrt via tilgangskontroll mv). Når de aktuelle personer disponerer hvert sitt sertifikat (og nøkkelpar), kan forvaltningsorganet ved kontroll av signaturen se hvem av de ansatte som står bak meldingen. Dessuten behøver ikke alle få nytt sertifikat selv om et nøkkelpar skulle komme på avveie eller lignende. Dette kan lette administrasjonen av meldinger og sertifikater. Se også Veilederen del 1, kapittel 4.2 *Sertifikat for forvaltningsorgan (virksomhetssertifikat)*, tredje avsnitt.

[143] Når et forvaltningsorgan, eller en annen virksomhet for den delen, baserer mye av sin eksterne kommunikasjon på bruk av elektroniske kanaler, oppstår det risiko for avbrudd som er ny i forhold til tradisjonelle metoder. Dette gjelder for det første teknisk avbrudd i IT-systemene generelt, men i denne sammenheng gjelder det å forebygge stans i kommunikasjonen som følge av svikt i de sikkerhetsmekanismene som benyttes. Et forvaltningsorgan som overfor omverdenen identifiserer seg ved hjelp av virksomhetssertifikat, vil i en periode være avskåret fra å kommunisere dersom sertifikatet av en eller annen årsak må trekkes tilbake. Dette kan skje for eksempel fordi en mistenker at forvaltningsorganets egne nøkler er misbrukt, eller fordi sertifikatutstederens sertifikat av en eller annen grunn er trukket tilbake, eller er ute av drift. For å redusere risikoen for slike driftsavbrudd til et minimum, kan det være fornuftig for et forvaltningsorgan å disponere to virksomhetssertifikater, og forvaltningsorganet skal som et minimum ha beskrevet rutiner for hvordan man raskt kan ta nye signaturfremstillingsdata og sertifikater i bruk. Dette skal fremgå av sikkerhetsstrategien, jf. §13(3)(b). Det kan av de samme grunner være fornuftig å ha virksomhetssertifikat fra to forskjellige sertifikatutstedere, og forvaltningsorganet er pålagt å vurdere om det er behov for et slikt tiltak, jf. § 21(4).

[144] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 10. http://www.lovdata.no/all/hl-20010615-081.html

[145] Som for sikringstiltak ellers, skal signaturfremstillingsdata og dekrypteringsnøkler sikres i henhold til sikkerhetsstrategien.

[146] Det er viktig at forvaltningsorganets dokumenter mv alltid er tilgjengelige når det er behov for dem, og at man ikke risikerer at data går tapt som følge av at de ikke kan dekrypteres dersom dekrypteringsnøkler av en eller annen grunn bli utilgjengelige. Det skal derfor alltid finnes kopier av dekrypteringsnøkler som er knyttet til forvaltningsorganet. Bestemmelsen retter seg mot forvaltningsorganet. Se også § 24 nedenfor.

dekrypteringsnøkler går tapt. Forvaltningsorganet plikter å oppbevare kopi av dekrypteringsnøkler for slikt materiale.[147]

(2) Prosedyrer for sikkerhetskopiering, oppbevaring, deponering og utlevering av dekrypteringsnøkkel skal følge anerkjente prinsipper og skal fremgå av forvaltningsorganets sikkerhetsstrategi, jf. § 13.[148]

§ 23 *Varslingsplikt ved tap eller mistanke om misbruk av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsnøkkel*[149]

(1) Innehaver av signaturfremstillingsdata[150] skal straks varsle sertifikatutsteder[151] 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.[152] Det samme gjelder for bruk av passord/PIN-koder o.l. og dekrypteringsnøkkel.

---

[147] Det finnes motforestillinger av bl.a. personvernmessig art når det gjelder krav om sikkerhetskopiering og deponering av dekrypteringsnøkler generelt. Men ettersom det her dreier seg om dekrypteringsnøkler til data som gjelder *forvaltningsorganet* (og ikke til saksbehandler), utløser det ikke noe personvernmessig problem, jf. § 5(4).

[148] Både av sikkerhetsmessige grunner, og av effektivitetshensyn, er det viktig at rutiner for kopiering, oppbevaring, og utlevering (ved behov) av kopierte dekrypteringsnøkler er beskrevet i sikkerhetsstrategien. 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. Det er naturlig at retten til utlevering er knyttet til bestemte roller i forvaltningsorganet, for eksempel etatsjef eller den/de vedkommende bemyndiger, og at de det gjelder er kjent med rutinene.

[149] Varsling om tilbaketrekking av sertifikat ved mistanke om at signaturfremstillingsdata er kommet på avveie, og blir eller kan bli misbrukt, er en viktig del av sikkerheten rundt elektroniske signaturer og sertifikattjenester. Regler om dette vil regelmessig også foreligge som avtalevilkår mellom sertifikatinnehaveren og utstederen av sertifikatet. Bestemmelsen retter seg mot den enkelte bruker (og forvaltningsansatte).

[150] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 5. http://www.lovdata.no/all/tl-20010615-081-001.html#3

[151] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 10. http://www.lovdata.no/all/tl-20010615-081-001.html#3

[152] En viktig side ved sikkerheten rundt elektroniske signaturer og sertifikater er at potensielle mottakere blir varslet dersom det er mistanke om misbruk av signaturfremstillingsdata. Dette skjer gjerne ved at en statustjeneste vedlikeholder oversikt over sertifikater som av en eller annen grunn ikke lenger skal benyttes. Slik oversikt kan gjøres tilgjengelig som en såkalt "tilbaketrekkingsliste" (revokeringsliste), eller i form av en oppslagstjeneste der det i sanntid gis opplysning om sertifikatets status, se for eksempel lov om elektronisk signatur § 12. Den som disponerer signaturfremstillingsdata, enten de er knyttet til personsertifikat eller virksomhetssertifikat, skal alltid varsle (rette instans) hvis det er mistanke om misbruk eller signaturfremstillingsdataene har kommet på avveie. Det samme gjelder for dekrypteringsdata og passord/PIN-koder. Hvor varsel skal gis kan variere avhengig av løsning, men brukeren skal være gjort kjent med rutinene for dette, jf. § 15.

Kapittel 6. Forvaltningsorganets behandling av meldinger som er kryptert eller signert

§ 24 *Mottak av kryptert melding*[153]

(1) Melding som mottas av forvaltningsorganet i kryptert form, skal straks dekrypteres.[154]

(2) Hvis meldingen ikke lar seg dekryptere ved mottak, skal det straks sendes melding til avsender med beskjed om at forvaltningsorganet ikke får tilgang til meldingens innhold. § 7 gjelder tilsvarende.[155]

(3) Forvaltningsorganet skal sikre opplysningene under den videre behandling i organet i henhold til de regler som gjelder for de aktuelle opplysningene.[156]

§ 25 *Krav til kontroll av sertifikater og tilbaketrekkingslister*[157]

(1) Ved mottak av melding som er underlagt krav om bruk av avansert elektronisk signatur[158],[159] skal forvaltningsorganet kontrollere, i henhold til kravene fastsatt i organets sikkerhetsstrategi, jf. § 13:[160]

---

[153] Bestemmelsen stiller krav til håndtering av meldinger som er kryptert når de mottas av forvaltningsorganet. Bestemmelsen retter seg mot forvaltningsorganet.

[154] Når forvaltningsorganet mottar en kryptert melding skal den straks dekrypteres. Dette er for det første nødvendig for å kunne ta stilling til innholdet i meldingen, og eventuelt varsle avsenderen dersom noe viser seg ikke å være som det skal, jf. § 7. Men det vil også gjerne være slik at det benyttes andre mekanismer, eller i alle fall andre krypteringsnøkler, for å sikre dataene internt i forvaltningsorganet enn de som benyttes for å sikre kommunikasjonen med eksterne brukere. Når det benyttes offentlig-nøkkel kryptering med eksterne brukere, vil selve meldingen være kryptert med en engangsnøkkel, og denne engangsnøkkelen er kryptert med forvaltningsorganets offentlige nøkkel. Det er unødig krevende å administrere alle disse engangsnøklene over tid. Internt er det mer hensiktsmessig om alle data som skal krypteres (eller i alle fall alle data av en viss type eller tilhørende samme enhet) krypteres med en felles nøkkel, eller sikres etter de regler som ellers gjelder for de aktuelle dataene. Det er nok bare unntaksvis behov for å lagre dataene i kryptert form hos forvaltningsorganet. Hvis dataene er både signert og kryptert når de mottas, må forvaltningsorganet håndtere signaturene i henhold til §§ 25 og 26.

[155] Avsenderadressen er vanligvis ikke kryptert, så med mindre det er benyttet en annen avsenderadresse enn den avsenderen vanligvis treffes på, vil det i de fleste tilfelle være mulig å varsle vedkommende selv om selve meldingen ikke kan leses.

[156] Det kan foreligge særlige retningslinjer for den interne behandlingen av opplysningene.

[157] 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. Se mer om dette i Artikkelen. En portal for sikkerhetsløsning, slik som "Sikkerhetsportalen" var tenkt, vil kunne håndtere dette på vegne av de forvaltningsorganene som benytter den.
Kravene til sertifikatverifisering i § 25 er minimumsregler. Det kan være behov for å foreta tilsvarende kontroller også når det ikke er stilt krav om avansert elektronisk signatur, men det likevel benyttes sertifikater. For eksempel vil det vanligvis være nødvendig å kontrollere sertifikater som benyttes i forbindelse med innholdskryptering. Bestemmelsen retter seg først og fremst mot forvaltningsorganet som skal legge til rette for at de beskrevne kontroller kan gjennomføres.

[158] Se lov om elektronisk signatur § 3 nr. 2. http://www.lovdata.no/all/tl-20010615-081-001.html#3

[159] Bestemmelsen kommer til anvendelse i de tilfellene det er stilt krav om bruk av avansert elektronisk signatur. Når det først er stilt et slikt krav får man anta at det er behov for den sikkerheten en slik signatur representerer. For å oppnå dette er det nødvendig at signatur og sertifikat kontrolleres som angitt nedenfor.

a) at signaturen lar seg verifisere, herunder at meldingen ikke er endret,[161]

b) at tilknyttet sertifikat[162] fortsatt er gyldig og ikke suspendert eller trukket tilbake,[163] eller det dokumenteres at sertifikatet var gyldig på signeringstidspunktet,[164]

c) at sertifikatet er egnet for den aktuelle anvendelse, herunder sertifikatets sikkerhetsnivå og eventuelle begrensninger i sertifikatets anvendelsesområde,[165]

d) at sertifikatet er utstedt av en sertifikatutsteder som anbefales eller er anerkjent av koordineringsorganet, jf. § 27, eller som forvaltningsorganet kan akseptere i henhold til sin sikkerhetsstrategi.[166]

(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,[167] skal det sendes melding til avsender i henhold til reglene i § 7.

---

[160] Det kan variere fra område til område hvor strenge krav som skal stilles, eller i alle fall hvor oppdaterte statusopplysninger mv må være. Dette må forvaltningsorganet ta stilling til i sin sikkerhetsstrategi.

[161] Dette er en rent teknisk kontroll for å sjekke at meldingen er uendret, at signaturen hører til den aktuelle meldingen, og at signaturen kan verifiseres ved hjelp av et bestemt sertifikat (eller en offentlig nøkkel som forvaltningsorganet på annen måte kjenner).

[162] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 9. http://www.lovdata.no/all/tl-20010615-081-001.html#3

[163] Sikkerhetsstrategien fastsetter krav til hvor oppdatert slik statusinformasjon skal være, for eksempel om det kreves oppslag mot en kontinuerlig oppdatert tjeneste som leverer opplysninger om status på oppslagstidspunktet, eller om det er tilstrekkelig at det benyttes en tilbaketrekkingsliste med lavere ajourføringsfrekvens, for eksempel en liste som oppdateres daglig. Oppdateringskrav til statustjenestene fremgår av ”Kravspesifikasjon for PKI i offentlig sektor”, pkt. 5.1.

[164] For å sikre at ikke signaturen er avgitt av noen som misbruker signaturfremstillingsdataene, skal forvaltningsorganet kontrollere sertifikatets status (om det er trukket tilbake) når det mottar meldingen. Alternativt kan meldingen fra avsenders side for eksempel være utstyrt med en tidsstemplet statusopplysning som viser at sertifikatet var gyldig på signeringstidspunktet. En slik tilleggsopplysning vil også være nyttig ved arkivering av meldingen. Hvorvidt det er avsender eller mottaker som innhenter slik statusopplysning beror på partenes ”signaturpolicy”. Dersom statusopplysningen sendes med fra avsender, må man imidlertid være oppmerksom på muligheten for at en tilbaketrekkingserklæring ennå ikke var behandlet på det tidspunkt statusopplysningen ble avgitt.

[165] Ikke alle sertifikater er pålitelige eller beregnet for en hvilken som helst bruk. De kan være utstedt etter begrensede undersøkelser, eller utstederen kan ha hatt et helt bestemt formål med utstedelsen. Sertifikatmottaker må derfor kontrollere at sertifikatet er egnet for det formålet det benyttes for i det aktuelle tilfellet. Rent praktisk skjer dette gjerne ved at man på forhånd har godkjent visse typer sertifikater fra bestemte utstedere, eller sertifikater som er utstedt i henhold til en eller flere sertifikat policies (erklæringer som angir hvordan sertifikatene utstedes og behandles, og hvem som har ansvaret for dette, jf. forskrift om kvalifiserte sertifikater § 4). Eksempelvis var tidligere ”Sikkerhetsportalen” ment å skulle ivareta disse kontrollene på vegne av forvaltningsorganet. Ny løsning er under utarbeiding fra Fornyings- og administrasjonsdepartementet.

[166] Selv om sertifikatet etter sitt innhold og sin policy er anvendelig for det aktuelle formålet, er troverdigheten til sertifikatet avhengig av om forvaltningsorganet anser utstederen som pålitelig. Også denne vurderingen kan forvaltningsorganet ha overlatt til andre (typisk tidligere ”Sikkerhetsportalen”, jf. noten ovenfor). De sertifikatene som skal benyttes må være omfattet av selvdeklarasjons- eller tilsynsordninger som er etablert i henhold til esignaturloven § 16a. http://www.lovdata.no/all/tl-20010615-081-004.html

[167] Det er ikke alltid det spiller noen rolle om disse kravene er oppfylt. Hvis verifisering av signaturen er uten betydning for behandling av meldingen, for eksempel fordi signatur ikke er påkrevet, eller feilen er at sertifikatet har gått ut etter at meldingen ble signert, men uten at man har grunn til å mistenke at noe er galt,

§ 26 *Arkivering av avansert elektronisk signatur mv.*[168]

(1) Melding som er signert med en avansert elektronisk signatur[169], og som blir arkivert,[170] skal arkiveres sammen med de opplysninger som er nødvendige for å bekrefte signaturen.[171]

(2) For meldinger som skal konverteres til annet format,[172] skal arkivet ved mottak verifisere signaturen, og deretter på hensiktsmessig måte bekrefte tilknytningen mellom

---

eller at man har andre opplysninger som på tilfredsstillende måte reparerer feilen, er det ikke nødvendig å forsinke saksbehandlingen, eller påføre parten merarbeid, ved å returnere meldingen.

[168] 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. Arkivering av signaturer mv omfattes generelt av arkivloven og arkivforskriften. http://www.lovdata.no/all/nl-19921204-126.html, http://www.lovdata.no/for/sf/kk/kk-19981211-1193.html I tillegg kommer kravene i eForvaltningsforskriften og i "Kravspesifikasjon for elektroniske arkivsystemer i offentlig forvaltning", NOARK-4, som behandler arkivering av digitale signaturer i pkt. 10.2 http://www.riksarkivet.no/arkivverket/lover/elarkiv/noark-4/hva/del1.html . Se også Veilederen del 1, kapittel 4.4. SEID leveranse 3 gir krav til hva som skal lagres : http://www.npt.no/iKnowBase/FileServer/SEID_Leveranse_3_v1.0.pdf?documentID=44963

[169] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 2 http://www.lovdata.no/all/tl-20010615-081-001.html#3 .

[170] Det er ikke alle meldinger som er arkivverdige, jf. arkivloven og arkivforskriften.

[171] Hvilke opplysninger som er nødvendige er bl.a. avhengig av hvor lenge det er aktuelt å verifisere signaturen. I noen tilfeller har signaturen bare betydning i forbindelse med gjennomføring av transaksjonen, i andre tilfeller vil signaturen kunne være et viktig bevismiddel også flere år senere. Når det benyttes avansert elektronisk signatur får man anta at signaturens pålitelighet har betydning og at en del kontroller blir gjennomført ved mottak, jf. § 25. Som et minimum bør man i disse tilfellene arkivere kopi av meldingen, signaturen, sertifikatet og opplysning om at sertifikatet ble kontrollert og ikke var trukket tilbake på det tidspunkt den signerte meldingen ble mottatt (eller arkivert). Hvis sertifikatet etter sitt innhold kommer til å løpe ut i den perioden det kan være aktuelt å verifisere signaturen, kan det være aktuelt at opplysningene tidsstemples (dvs påføres dato og klokkeslett og signeres med en digital signatur med en beregnet levetid som er minst like lang som den tid det kan være behov for å verifisere signaturen på den aktuelle meldingen eller den type melding det er tale om), jf. § 26(2) nest siste setning. 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. Se også NOARK-4 pkt. 10.2.5, kravene K10.49-K10.53.
SEID leveranse 3 gir krav til hva som skal lagres : http://www.npt.no/iKnowBase/FileServer/SEID_Leveranse_3_v1.0.pdf?documentID=44963

[172] Det kan av tekniske og arkivfaglige grunner være nødvendig å konvertere (omgjøre) meldingen til et annet format for å kunne oppbevare den over tid. 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. Konvertering kan også skje fordi arkivet ønsker å lagre alle dokumenter/meldinger i et bestemt (NOARK-godkjent) format med én gang (Se NOARK-4, pkt. 5.3). Ved konvertering oppheves bindingen mellom meldingen/dokumentet og signaturen. Det vil ikke være mulig å verifisere den opprinnelige signaturen overfor meldingen i det nye formatet. Da må det iverksettes andre tiltak. 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 gjennomfører nødvendige verifiseringer, jf kommentarene til bestemmelsens første ledd. Deretter arkiveres meldingen sammen med arkivets bekreftelse på at korrekt verifisering fant sted på et

meldingen, meldingens signatur og relevante opplysninger fra sertifikatet[173] sammen med opplysning om tidspunktet for bekreftelsen.[174] Arkivet skal sikre at ikke meldingene, eller dataene som bekrefter de nevnte forholdene, utilsiktet eller urettmessig endres i oppbevaringsperioden.[175] Tilsvarende gjelder meldinger der tilhørende sertifikaters gyldighetsperiode er kortere enn den tiden det kan være behov for å bekrefte meldingens innhold, med mindre det benyttes tidsstempel[176] eller annen tjeneste som sikrer at signaturen ikke endres og at den også i ettertid kan verifiseres. Det enkelte forvaltningsorgan kan bestemme 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.

---

bestemt tidspunkt. Se også NOARK-4, 10.2. En fremtidig portal for sikkerhetsløsning vil kunne utføre denne funksjonen for forvaltningsorganet.

[173] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 9. http://www.lovdata.no/all/hl-20010615-081.html

[174] Dette er altså en alternativ fremgangsmåte til det som er beskrevet i § 26(1). Hvis meldingen skal konverteres til et annet format, *må* denne fremgangsmåten benyttes. I andre tilfeller *kan* den benyttes, se § 26(2) siste setning.

[175] Man overlater altså til arkivet å sikre meldingens integritet og troverdighet gjennom sine rutiner for sikker kontroll, lagring og oppbevaring. Tilliten til arkivfunksjonen og arkivets rutiner skal etablere den nødvendige bekreftelse på at knytningen 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 tidsstemple den konverterte meldingen og de aktuelle informasjonsuttrekk fra det tilknyttede opprinnelige sertifikatet. Se også § 10(4)-(5) om utlevering av materiale som er signert med avansert elektronisk signatur.

[176] Tidsstempling er en sikkerhetsfunksjonalitet som dokumenterer at et dokument eksisterte eller faktisk var i noens besittelse på et gitt tidspunkt. Tidsstempling kan foretas av arkivet selv eller av en uavhengig og tiltrodd tredjepart. Et forvaltningsorgan som mottar en signert melding, og som ønsker å få meldingen tidsstemplet, kan for eksempel videresende til tidsstemplingstjenesten hash-verdien av dokumentet (som er en matematisk representasjon av dokumentet som er signert) samt signaturen og avsenders sertifikat sammen med opplysning om sertifikatets status som er hentet fra statustjenesten. Tidsstemplingsfunksjonen legger så til opplysning om tidspunkt for mottak og påfører sin signatur på det hele og returnerer det.

Kapittel 7. Diverse bestemmelser

§ 27 *Koordinerende organ*[177]

(1) Kongen kan utpeke et organ som har koordineringsansvar for forvaltningens bruk av sikkerhetstjenester og -produkter ved elektronisk kommunikasjon med og i forvaltningen.[178]

(2) Koordineringsorganet skal utarbeide krav til sikkerhetstjenester og -produkter som anbefales brukt ved elektronisk kommunikasjon med og i forvaltningen.[179] Koordineringsorganet skal også vurdere om tilgjengelige sikkerhetstjenester eller -produkter tilfredsstiller kravene.[180]

(3) Koordineringsorganet kan bestemme at det under tjeneste for forvaltningsorganer kun skal benyttes sertifikater[181] fra sertifikatutstedere[182] som har inngått rammeavtale om levering av slike tjenester til forvaltningen eller som er anerkjent av koordineringsorganet.[183]

(4) Koordineringsorganet kan bestemme at det ved elektronisk kommunikasjon med og i forvaltningen bare skal benyttes sertifikater som er oppført på liste publisert i henhold til forskrift 21. november 2005 nr. 1296 om frivillige selvdeklarasjonsordninger for sertifikatutstedere § 11 første ledd.[184]

---

[177] Bestemmelsen fastlegger rammene for etablering av et koordineringsorgan for forvaltningens bruk av sikkerhetstjenester og –produkter ved elektronisk kommunikasjon. Se også Veilederen del 1, kapittel 4.8 *Koordinering av forvaltningens bruk av elektronisk kommunikasjon mv*.

[178] Fornyings- og administrasjonsdepartementet er oppnevnt som koordineringsorgan etter denne bestemmelsen, se forskrift 7. oktober 2005 nr. 1117.

[179] En slik ”anbefaling” foreligger nå, se *Kravspesifikasjon for PKI i offentlig sektor*, http://www.regjeringen.no/nb/dep/fad/dok/rapporter_planer/Rapporter/2004/Kravspesifikasjon-for-PKI-i-offentlig-se.html?id=106067. Regjeringen besluttet 28.02.2005, på bakgrunn av et strateginotat av 17.02.2005, http://www.regjeringen.no/nb/dep/fad/dok/rapporter_planer/Planer/2005/Strategi-for-utbredelse-av-PKI-anvendels.html?id=476736 at alle statlige etater som skal benytte PKI er pålagt å følge kravspesifikasjonen. Se også brev fra Fornyings- og administrasjonsdepartementet til samtlige statsetater av 20. september 2006. http://www.regjeringen.no/nb/dep/fad/aktuelt/nyheter/2006/Felles-sikkerhetsinfrastruktur-for-elekt.html?id=271154 Anbefalinger for sertifikatprofiler er utarbeidet av SEID-prosjektet og gjort til del av kravspesifikasjonen. Dette følger av kravspesifikasjonen, som henviser til SEID.

[180] Denne funksjonen ivaretas i dag i praksis gjennom selvdeklareringsordningen, se forskrift 21. november 2005 nr. 1296 med henvisning til ”Kravspesifikasjon for PKI i offentlig sektor”.

[181] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 9. http://www.lovdata.no/all/hl-20010615-081.html

[182] Se lov av 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 10. http://www.lovdata.no/all/hl-20010615-081.html

[183] Statlige etater som skal ta i bruk PKI er pålagt å benytte *Kravspesifikasjon for PKI i offentlig sektor* (som integrerer SEID sertifikatprofil). Kravspesifikasjonen definerer to sikkerhetsnivåer for personsertifikater og ett sikkerhetsnivå for virksomhetssertifikater.

[184] Det er truffet slikt vedtak, se brev fra Fornyings- og administrasjonsdepartementet til samtlige statsetater av 20. september 2006. http://www.regjeringen.no/nb/dep/fad/aktuelt/nyheter/2006/Felles-sikkerhetsinfrastruktur-for-elekt.html?id=271154

§ 28 *Ikrafttredelse*

(1) Forskriften trer i kraft 1. juli 2004.[185]

[185] Forskriften avløser en tidligere forskrift av 2002-06-28 nr. 656 med samme navn. I forhold til den tidligere forskriften er det gjort en del språklige og strukturelle endringer for å gjøre forskriften lettere å forstå. Også enkelte innholdsmessige endringer er gjennomført, men stort sett viderefører forskriften løsningene fra forskriften av 2002.