FOR 2004-06-25 nr 988: Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

DATO:	FOR-2004-06-25-988
DEPARTEMENT:	FAD (Fornyings- administrasjons, og kirkedepartementet)
AVD/DIR:	Avdeling for statlig forvaltning
PUBLISERT:	I 2004 hefte 10
IKRAFTTREDELSE:	2004-07-01
SIST-ENDRET:	FOR-2008-10-17-1119 fra 2009-01-01
ENDRER:	
GJELDER FOR:	Norge
HJEMMEL:	LOV-1967-02-10-§15a, LOV-2001-06-15-81-§5
SYS-KODE:	BF01, BG18, C12, C22, D02
NÆRINGSKODE:	91, *
KUNNGJORT:	29.06.2004
RETTET:	
KORTTITTEL:	eForvaltningsforskriften

INNHOLD

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

Kapittel 1. Innledende bestemmelser
§ 1. Forskriftens formål og anvendelsesområde
§ 2. Begreper

Kapittel 2. Alminnelige krav ved bruk av elektronisk kommunikasjon med forvaltningen
§ 3. Bruk av elektronisk kommunikasjon ved henvendelser til et forvaltningsorgan
§ 4. Krav til bruk av sikkerhetstjenester og -produkter mv. ved henvendelser til et forvaltningsorgan
§ 5. Formidling av taushetsbelagte opplysninger og personopplysninger til forvaltningen
§ 6. Bekreftelse på at en henvendelse er mottatt
§ 7. Henvendelser som ikke tilfredsstiller aktuelle krav
§ 8. Underretning om enkeltvedtak og enkelte andre meddelelser fra forvaltningsorgan
§ 9. Klage
§ 10. Innsyn i opplysninger og dokumenter ved bruk av elektronisk kommunikasjon
§ 11. Høring
§ 12. Forvaltningsorganets adgang til å nekte bruk av elektronisk kommunikasjon

Kapittel 3. Forvaltningsorganets strategi for informasjonssikkerhet
§ 13. Sikkerhetsmål og sikkerhetsstrategi

Kapittel 4. Anskaffelse og bruk av sikkerhetstjenester mv.
§ 14. Sertifikat for forvaltningsorgan (virksomhetssertifikat)
§ 15. Informasjon om bruk av sikkerhetstjenester mv.
§ 16. Innhenting av samtykke ved bruk av elektronisk signatur
§ 17. Restriksjoner på bruk av sertifikat mv.
§ 18. Forvaltningsansattes bruk av forvaltningsorganets informasjonssystem
§ 19. Informasjon

Kapittel 5. Beskyttelse av signaturfremstillingsdata og dekrypteringsnøkkel mv.
§ 20. Krav til oppbevaring og bruk av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsnøkkel
§ 21. Sikring av signaturfremstillingsdata og dekrypteringsnøkkel ved bruk av virksomhetssertifikat
§ 22. Sikkerhetskopiering av dekrypteringsnøkkel mv.
§ 23. Varslingsplikt ved tap eller mistanke om misbruk av signaturfremstillingsdata, passord/PIN-koder og dekrypteringsnøkkel

Kapittel 6. Forvaltningsorganets behandling av meldinger som er kryptert eller signert
§ 24. Mottak av kryptert melding
§ 25. Krav til kontroll av sertifikater og tilbaketrekkingslister
§ 26. Arkivering av avansert elektronisk signatur mv.

Kapittel 7. Diverse bestemmelser
§ 27. Koordinerende organ
§ 28. Ikrafttredelse

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

Hjemmel: Fastsatt ved kgl.res. 25. juni 2004 med hjemmel i lov 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven) § 15a og lov 15. juni 2001 nr. 81 om elektronisk signatur § 5. Fremmet av Arbeids- og administrasjonsdepartementet.
Endringer: Endret ved forskrifter 2 des 2005 nr. 1398, 17 okt 2008 nr. 1119.

Kapittel 1. Innledende bestemmelser

§ 1. *Forskriftens formål og anvendelsesområde*

(1) Forskriftens formål er å legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen. Den skal fremme forutsigbarhet og fleksibilitet og legge til rette for samordning av sikre og hensiktsmessige tekniske løsninger. Forskriften skal legge til rette for at enhver på en enkel måte kan utøve sine rettigheter og oppfylle sine plikter i forhold til det offentlige.

(2) Forskriften gjelder for elektronisk kommunikasjon med forvaltningen og for elektronisk saksbehandling og kommunikasjon i forvaltningen 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.[1]

1 Lov 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven).

§ 2. *Begreper*

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

1 Lov 15. juni 2001 nr. 81 om elektronisk signatur.

2 Lov 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven).

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

§ 3. *Bruk av elektronisk kommunikasjon ved henvendelser til et forvaltningsorgan*

(1) Enhver som henvender seg til et forvaltningsorgan 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.

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

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

(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.

(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.

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

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

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

§ 4. *Krav til bruk av sikkerhetstjenester og -produkter mv. ved henvendelser til et forvaltningsorgan*

(1) Enhver 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.

(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.

(b) Med *elektronisk signatur* menes løsninger som definert i lov om elektronisk signatur[1] § 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.

(2) Forvaltningsorganet kan i det enkelte tilfelle 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.

(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. Det samme gjelder for sikkerhetstjenester og -produkter som er nødvendig for å oppfylle kravene i § 5.

1 Lov 15. juni 2001 nr. 81 om elektronisk signatur.

§ 5. *Formidling av taushetsbelagte opplysninger og personopplysninger til forvaltningen*

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

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

(3) Forvaltningsorganet skal opplyse generelt 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. 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.

(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*

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

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

(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, 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.

§ 7. *Henvendelser som ikke tilfredsstiller aktuelle krav*

(1) Henvender noen seg til urette myndighet eller benytter uriktig elektronisk adresse 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.

(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 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*

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

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

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

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

(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.

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

(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.

(8) Hvis det etter vedtakets art ikke er tid til å gjennomføre ny underretning som beskrevet i nr. (7), bør forvaltningsorganet om mulig sende nytt varsel etter nr. (2). Når det sendes nytt varsel etter denne bestemmelse, begynner en eventuell klagefrist[3] å løpe fra den dag det nye varselet ble sendt.

(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 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).

(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. Det skal også informeres om at parten bør kontrollere at han mottar bekreftelse når klage leveres i elektronisk form, jf. § 9 (2).

1 Se forvaltningsloven § 2 første ledd, bokstav b).

2 Se forvaltningsloven § 2 første ledd, bokstav c).

3 Se forvaltningsloven § 29.

§ 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.

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

§ 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.

(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, og

b) at risiko for uberettiget innsyn i opplysningene eller dokumentene er forebygget på en tilfredsstillende måte, eller når innsyn kan kreves etter offentleglova eller annen lovbestemt allmenn innsynsrett.

(4) Hvis den som krever innsyn i dokumenter som er signert med avansert elektronisk signatur[1] ber om det, skal relevante sertifikater, og øvrige opplysninger som er nødvendige for å få bekreftet signaturen, utleveres sammen med dokumentet. 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 innholdet overfor tredjepart. Dette kan om nødvendig skje i form av en papirutskrift av dokumentet som er bekreftet av forvaltningsorganet.

0 Endret ved forskrift 17 okt 2008 nr. 1119 (i kraft 1 jan 2009).

1 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 2.

§ 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.

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

§ 12. *Forvaltningsorganets adgang til å nekte bruk av elektronisk kommunikasjon*

(1) Hvis det er grunn til å anta at noen misbruker adgangen 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 om at det vurderer å 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[1] kap. VI gjelder tilsvarende så langt de passer.

1 Lov 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven).

Kapittel 3. Forvaltningsorganets strategi for informasjonssikkerhet

§ 13. *Sikkerhetsmål og sikkerhetsstrategi*

(1) Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (*sikkerhetsmål* og *sikkerhetsstrategi*). Sikkerhetsstrategien skal danne grunnlaget for forvaltningsorganets beslutninger om innføring og bruk av sikkerhetstjenester og -produkter på en helhetlig, planlagt, systematisk og dokumentert måte. Sikkerhetsstrategien skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.

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

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

a) prosedyrer for anskaffelse, bruk, oppbevaring og sikring av signaturfremstillingsdata,[1] passord/PIN-koder og dekrypteringsnøkkel knyttet til personlige sertifikat[2] eller sertifikat for ansatt i forvaltningen, jf. § 15, § 17 og § 20;

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

c) prosedyrer for å etablere og opprettholde et sikkert brukermiljø der det benyttes elektroniske signaturer,[3] kryptering eller andre sikkerhetstjenester, jf. § 18;

d) prosedyrer for varsling og tilbaketrekking[4] 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[5] § 13 og personopplysningsforskriften[6] kap. 2;

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

1 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 5.

2 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 9.

3 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3.

4 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 12.

5 Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).

6 Forskrift 15. desember 2000 nr. 1265 om behandling av personopplysninger (personopplysningsforskriften).

Kapittel 4. Anskaffelse og bruk av sikkerhetstjenester mv.

§ 14. *Sertifikat for forvaltningsorgan (virksomhetssertifikat)*

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

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

1 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 1.

§ 15. *Informasjon om bruk av sikkerhetstjenester mv.*

(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[1] og dekrypteringsnøkkel med tilhørende sertifikat[2] samt passord og PIN-koder mv.

(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,

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

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

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

e) hvilke opplysninger om den enkelte som vil fremgå av sertifikatet og sertifikatutsteders[3] behandling av personopplysninger, jf. personopplysningsloven[4] § 19, og

f) forvaltningsorganets sikkerhetsstrategi for øvrig, jf. § 13.

1 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 5.

2 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 9.

3 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 10.

4 Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).

§ 16. *Innhenting av samtykke ved bruk av elektronisk signatur*

Når det benyttes elektroniske signaturer, skal forvaltningsorganet ha innhentet samtykke fra de ansatte i henhold til lov om elektronisk signatur[1] § 7 og § 14 annet ledd bokstav b om utstedelse og utlevering av sertifikat.

1 Lov 15. juni 2001 nr. 81 om elektronisk signatur.

§ 17. *Restriksjoner på bruk av sertifikat mv.*

(1) Signaturfremstillingsdata,[1] sertifikat[2] eller passord/PIN-koder som er ment for bruk i tjeneste for forvaltningen, skal ikke benyttes for andre formål.

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

(3) Et forvaltningsorgan kan bestemme at 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.

1 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 5.

2 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 9.

§ 18. *Forvaltningsansattes bruk av forvaltningsorganets informasjonssystem*

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.

§ 19. *Informasjon*

(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. Forvaltningsorganet skal på samme måte informere publikum om at håndtering av signaturfremstillingsdata,[1] passord/PIN-koder og dekrypteringsnøkkel skal skje i henhold til § 20 og § 23.

1 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 5.

Kapittel 5. Beskyttelse av signaturfremstillingsdata og dekrypteringsnøkkel mv.

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

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

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

a) at signaturfremstillingsdata fjernes fra arbeidsstasjonen dersom dataene er lagret i smartkort 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.

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

1 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 5.

§ 21. *Sikring av signaturfremstillingsdata og dekrypteringsnøkkel ved bruk av virksomhetssertifikat*

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

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

(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.

(4) Det skal vurderes om forvaltningsorganet bør være utstyrt med signaturfremstillingsdata og virksomhetssertifikat fra mer enn én sertifikatutsteder.[2]

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

1 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 5.

2 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 10.

§ 22. *Sikkerhetskopiering av dekrypteringsnøkkel mv.*

(1) Forvaltningsorganet skal sikre at opplysninger og annet materiale som oppbevares av forvaltningsorganet i kryptert form, ikke blir utilgjengelige som følge av at dekrypteringsnøkler går tapt. Forvaltningsorganet plikter å oppbevare kopi av dekrypteringsnøkler for slikt materiale.

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

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

(1) Innehaver av signaturfremstillingsdata[1] skal straks varsle sertifikatutsteder[2] 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. Det samme gjelder for bruk av passord/PIN-koder o.l. og dekrypteringsnøkkel.

1 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 5.

2 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 10.

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

§ 24. *Mottak av kryptert melding*

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

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

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

§ 25. *Krav til kontroll av sertifikater og tilbaketrekkingslister*

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

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

b) at tilknyttet sertifikat[2] fortsatt er gyldig og ikke suspendert eller trukket tilbake, eller det dokumenteres at sertifikatet var gyldig på signeringstidspunktet,

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

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

(2) Hvis en melding som er signert med avansert elektronisk signatur ikke tilfredsstiller kontrollene i første ledd, og dette har betydning for behandling av meldingen i forvaltningsorganet, skal det sendes melding til avsender i henhold til reglene i § 7.

1 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 2.

2 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 9.

§ 26. *Arkivering av avansert elektronisk signatur mv.*

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

(2) For meldinger som skal konverteres til annet format, skal arkivet ved mottak verifisere signaturen, og deretter på hensiktsmessig måte bekrefte tilknytningen mellom meldingen, meldingens signatur og relevante opplysninger fra sertifikatet[2] sammen med opplysning om tidspunktet for bekreftelsen. Arkivet skal sikre at ikke meldingene, eller dataene som bekrefter de nevnte forholdene, utilsiktet eller urettmessig endres i oppbevaringsperioden. 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 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.

1 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 2.

2 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 9.

Kapittel 7. Diverse bestemmelser

§ 27. *Koordinerende organ*

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

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

(3) Koordineringsorganet kan bestemme at det under tjeneste for forvaltningsorganer kun skal benyttes sertifikater[1] fra sertifikatutstedere[2] som har inngått rammeavtale om levering av slike tjenester til forvaltningen eller som er anerkjent av koordineringsorganet.

(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.

0 Endret ved forskrift 2 des 2005 nr. 1398 (i kraft 15 des 2005).

1 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 9.

2 Se lov 15. juni 2001 nr. 81 om elektronisk signatur § 3 nr. 10.

§ 28. *Ikrafttredelse*

(1) Forskriften trer i kraft 1. juli 2004.

Databasen sist oppdatert 8. juli 2011