

Besl. O. nr. 53

Jf. Innst. O. nr. 41 (2000-2001) og Ot.prp. nr. 82 (1999-2000)

År 2000 den 14. desember holdtes Odelsting, hvor da ble gjort slikt

vedtak til lo v

om elektronisk signatur

Kapittel I Alminnelige regler

§ 1 Lovens formål

Formålet med denne loven er å legge til rette for en sikker og effektiv bruk av elektronisk signatur ved å fastsette krav til kvalifiserte sertifikater, til utstederne av disse sertifikatene og til sikre signaturfremstillingssystemer.

§ 2 Lovens virkeområde

Loven gjelder for sertifikatutstedere som er etablert i Norge. Loven regulerer rammebetingelsene for bruk av kvalifiserte elektroniske signaturer, med unntak av § 6 annet punktum og § 7 som gjelder alle elektroniske signaturer.

Kongen kan i forskrift bestemme at loven skal gjelde for Svalbard og Jan Mayen.

§ 3 Definisjoner

I denne loven menes med:

1. *elektronisk signatur*: data i elektronisk form som er knyttet til andre elektroniske data og som brukes til å kontrollere at disse stammer fra den som fremstår som undertegner,
2. *avansert elektronisk signatur*: en elektronisk signatur som
 - a) er entydig knyttet til undertegneren,
 - b) kan identifisere undertegneren,
 - c) er laget ved hjelp av midler som bare undertegneren har kontroll over, og
 - d) er knyttet til andre elektroniske data på en slik måte at det kan oppdages om disse har blitt endret etter signering,
3. *kvalifisert elektronisk signatur*: en avansert elektronisk signatur som er basert på et kvalifisert sertifikat og fremstilt av et godkjent sikkert signaturfremstillingssystem,

4. *undertegner*: den som disponerer et signaturfremstillingssystem og som handler på vegne av seg selv eller på vegne av en annen fysisk eller juridisk person,
5. *signaturfremstillingssdata*: unike data, som for eksempel koder eller private nøkler, som undertegneren benytter for å fremstille en elektronisk signatur,
6. *signaturfremstillingssystem*: programvare eller maskinvare som benyttes til å fremstille elektronisk signatur ved hjelp av signaturfremstillingsdata,
7. *signaturverifikasjonsdata*: unike data, som for eksempel koder eller offentlige nøkler, som benyttes til å verifisere en elektronisk signatur,
8. *signaturverifikasjonssystem*: programvare eller maskinvare som benyttes for å verifisere elektronisk signatur ved hjelp av signaturverifikasjonsdata,
9. *sertifikat*: en kopling mellom signaturverifikasjonsdata og undertegner som bekrefter undertegners identitet og er signert av sertifikatutsteder,
10. *sertifikatutsteder*: en fysisk eller juridisk person som utsteder sertifikater eller tilbyr andre tjenester relatert til elektronisk signatur.

§ 4 Kvalifisert sertifikat

Betegnelsen kvalifisert sertifikat skal kun brukes om sertifikater som oppfyller kravene i denne paragrafen og utstedes for en begrenset periode av en sertifikatutsteder som oppfyller kravene i §§ 10 - 15.

Et kvalifisert sertifikat skal inneholde følgende informasjon:

- a) en angivelse av at sertifikatet er utstedt som et kvalifisert sertifikat,
- b) sertifikatutstederens identitet og den stat den er etablert i,
- c) undertegnerens navn eller pseudonym med opplysning om at det er et pseudonym,

- d) eventuelt ytterligere opplysninger om undertegneren, dersom de er relevante for bruken av sertifikatet,
- e) de signaturverifikasjonsdata, som svarer til de signaturfremstillingsdata som er under undertegners kontroll,
- f) sertifikatets ikrafttredelses- og utløpsdato,
- g) sertifikatets identifikasjonskode,
- h) sertifikatutstederens avanserte elektroniske signatur,
- i) eventuelle begrensninger i sertifikatets anvendelsesområde, og
- j) eventuelle beløpsmessige begrensninger i sertifikatet med hensyn til hvilke transaksjoner sertifikatet kan brukes til.

Kongen kan i forskrift regulere hva det kvalifiserte sertifikatet nærmere skal inneholde.

§ 5 *Krav til kvalifiserte elektroniske signaturer brukt i kommunikasjon med og i offentlig sektor*

Kongen kan fastsette nærmere regler om hvilke krav som skal stilles til kvalifiserte elektroniske signaturer som skal brukes ved kommunikasjon med og i offentlig sektor.

§ 6 *Rettsvirkninger av elektronisk signatur*

Dersom det i lov, forskrift eller på annen måte er oppstilt krav om underskrift for å få en bestemt rettsvirkning og disposisjonen kan gjennomføres elektronisk, oppfylder en kvalifisert elektronisk signatur alltid et slikt krav. En elektronisk signatur som ikke er kvalifisert, kan oppfylle et slikt krav.

§ 7 *Innsamling og bruk av personopplysninger*

En sertifikatutsteder får kun innhente personopplysninger direkte fra den opplysningene gjelder, eller med dennes uttrykkelige samtykke og bare i den utstrekning som er nødvendig for å utstede eller opprettholde et sertifikat. Opplysningene må ikke samles inn eller behandles for andre formål, så fremt ikke den opplysningene gjelder har gitt sitt uttrykkelige samtykke til det.

Datatilsynet skal føre tilsyn med at denne bestemmelsen overholdes.

Kapittel II Sikre signaturfremstillingssystemer

§ 8 *Krav til sikre signaturfremstillingssystemer*

Et sikkert signaturfremstillingssystem skal sikre at signaturen er tilfredsstillende beskyttet mot forfalskning. Videre skal et sikkert signaturfremstillingssystem sikre at signaturfremstillingsdata:

- a) i praksis kun kan fremtre én gang og med rimelig grad av sikkerhet forblir hemmeligholdt,
- b) i rimelig utstrekning ikke kan utledes, og
- c) på pålitelig vis kan beskyttes av rette undertegner mot andres bruk.

Et sikkert signaturfremstillingssystem må ikke forandre data i elektronisk form som skal signeres, eller hindre at dataene vises for undertegner før det signeres.

§ 9 *Godkjenning av sikre signaturfremstillingssystem*

Godkjenning som et sikkert signaturfremstillingssystem, jf. § 8, gis av det organ som Kongen utpeker. Kongen kan i forskrift gi nærmere bestemmelser om organet og om krav til sikre signaturfremstillingssystem.

Likestilt med godkjenning etter første ledd er godkjenning fra et tilsvarende organ i en annen stat som er part i EØS-avtalen.

Kravene i § 8 skal anses oppfylt når den maskin- eller programvaren som benyttes, er i samsvar med de standarder for elektroniske signaturprodukter som Europakommisjonen fastsetter og som offentliggjøres i De Europeiske Fellelesskaps Tidende.

Kapittel III Krav til utstedere av kvalifiserte sertifikater

§ 10 *Krav til virksomheten*

Utstedere av kvalifiserte sertifikater skal utøve og administrere virksomheten på en forsvarlig måte slik at den kan tilby sikre, pålitelige og velfungerende sertifikattjenester.

Sertifikatutstederen skal til enhver tid ha tilstrekkelige økonomiske ressurser til å kunne drive virksomheten i henhold til kravene som er stilt i eller i medhold av denne lov.

§ 11 *Krav til produkter og systemer*

Utstedere av kvalifiserte sertifikater skal bruke pålitelige produkter og systemer som er beskyttet mot endringer, og som gir teknisk og kryptografisk sikkerhet i understøttende prosesser.

Kravene i første ledd skal anses oppfylte dersom sertifikatutsteder benytter seg av produkter og systemer som er godkjent av et organ i henhold til § 9 første og annet ledd, eller er i samsvar med standarder fastsatt av Europakommisjonen etter § 9 tredje ledd.

Sertifikatutsteder skal iverksette tiltak mot forfalskning av sertifikatene. Dersom sertifikatutsteder fremstiller signaturfremstillingsdata, skal utstederen garantere fortlørligheten av disse dataene under fremstillingssystemet.

§ 12 *Krav om katalog- og tilbaketrekkingsstjeneste*

Utstedere av kvalifiserte sertifikater skal sørge for en hurtig og sikker katalog- og tilbaketrekkingsstjeneste og skal sikre at det er mulig å fastslå dato og tidspunkt for ikrafttredelse eller tilbaketrekkning av et sertifikat.

§ 13 *Krav om kontroll av undertegners identitet*

Utstedere av kvalifiserte sertifikater er ansvarlige for at identiteten til undertegner og ytterligere relevante opplysninger om vedkommende blir kontrollert gjennom sikre rutiner.

Opplysninger om rutinene som nevnt i første ledd skal være offentlig tilgjengelige.

§ 14 *Krav til lagring av opplysninger*

Utstedere av kvalifiserte sertifikater skal lagre alle relevante opplysninger om kvalifiserte sertifikater i en rimelig periode, dog minst 10 år etter at sertifikatet er registrert i tilbaketrekkelingslisten.

Sertifikatutsteder skal benytte pålitelige systemer til oppbevaring av sertifikater i verifiserbar form, slik at

- opplysningens ekthet kan kontrolleres,
- sertifikatene kun er offentlig tilgjengelige i de tilfellene der innehaveren har gitt sitt samtykke, og
- eventuelle tekniske endringer, som bringer disse sikkerhetskravene i fare, er synlige for operatøren.

Utstedere av kvalifiserte sertifikater må ikke oppbevare eller kopiere undertegners signaturfremstillingsdata.

§ 15 *Krav om informasjon om vilkår, begrensninger og lignende*

Før en sertifikatutsteder inngår avtale om å utstede et kvalifisert sertifikat skal utstederen skriftlig informere motparten om

- vilkårene og begrensningene for bruken av sertifikatet,
- opplysninger om eventuelle frivillige akkrediterings- eller sertifiseringsordninger, og
- prosedyrer for klage og avgjørelse av tvister.

Opplysninger i henhold til første ledd kan sendes elektronisk, dersom det skjer i en for motparten umiddelbart lesbar form. Disse opplysningene skal også kunne kontrolleres av signaturmottakeren.

§ 16 *Utfyllende krav*

Kongen kan i forskrift fastsette nærmere regler om hvilke krav som kan stilles til utstedere av kvalifiserte sertifikater for å oppfylle bestemmelsene i §§ 10-15.

Kapittel IV Tilsyn og sanksjoner

§ 17 *Tilsyn med utstedere av kvalifiserte sertifikater*

Kongen kan utpeke et organ som skal føre tilsyn med at denne lov med forskrifter etterleves.

Tilsynet kan kreve de opplysninger og dokumenter som er nødvendige for å utføre sine oppgaver, og fastsette en tidsfrist for å sende dem inn.

Tilsynet kan gi påbud om at forhold som er i strid med bestemmelser som er gitt i eller i medhold av denne loven, skal opphøre og stille vilkår som må

oppfylles for at virksomheten skal være i samsvar med loven.

Tilsynet kan kreve at det gjennomføres IT-revisjon hos utstedere av kvalifiserte sertifikater og utpeke en revisor til å utføre IT-revisjonen. Sertifikatutsteder kan pålegges å betale for revisjonen.

Tilsynet kan frata en sertifikatutsteder retten til å anvende betegnelsen kvalifisert sertifikat, dersom sertifikatutstederen grovt eller gjentatte ganger ikke overholder lovens regler.

Kongen kan gi nærmere forskrifter om tilsynets virksomhet.

§ 18 *Registrering av utstedere av kvalifiserte sertifikater*

En sertifikatutsteder kan ikke utstede kvalifiserte sertifikater før registreringsmelding er sendt til tilsynet. Endringer i allerede registrerte opplysninger og nye opplysninger som skal registreres, skal meldes til tilsynet uten ugrunnet opphold.

§ 19 *Adgang til lokaler m.v.*

Tilsynet kan som ledd i sin kontroll, kreve adgang til steder der det drives virksomhet som står under tilsyn.

Tilsynet kan gjennomføre de kontroller det finner nødvendig, og kreve bistand fra personalet på stedet i den grad dette må til for å få utført kontrollen.

Lov av 10. februar 1967 om behandlingsmåten i forvaltningssaker § 15 om fremgangsmåten ved granskning, kommer til anvendelse.

§ 20 *Tvangsmulkt*

For å sikre at bestemmelser som er gitt i eller i medhold av denne lov overholdes, kan tilsynet bestemme at sertifikatutsteder skal betale en daglig løpende mulkt til staten inntil lovstridig virksomhet er opphørt eller pålegg og vilkår gitt med hjemmel i denne lov er etterkommet.

Mulkten løper ikke før klagefristen er ute. Påklages vedtaket om tvangsmulkt, løper ingen tvangsmulkt før klagesaken er avgjort med mindre klageorganet bestemmer annerledes.

Tilsynet kan frafalle påløpt tvangsmulkt.

§ 21 *Straff*

Med bøter straffes den som forsettlig eller grovt uaktsomt

- unnlater å registrere/sendte melding etter § 18,
- unnlater å gi opplysninger etter § 17,
- behandler personopplysninger i strid med §§ 7 og 14, eller
- gir uriktige eller villedende opplysninger til tilsynet.

Medvirkning straffes på samme måte.

§ 22 Erstatning

En sertifikatutsteder som utsteder sertifikater som utgis for å være kvalifiserte, eller som garanterer for slike sertifikater utgitt av en annen, er erstatningsansvarlig for tap hos en fysisk eller juridisk person som følge av at denne hadde hatt rimelig grunn til å ha tillit til at:

- a) informasjonen angitt i sertifikatet var korrekt på utstedelsestidspunktet,
- b) sertifikatet inneholder alle opplysninger som kreves i henhold til § 4,
- c) signaturfremstillingsdata og signaturverifikasjonsdata hører sammen på en unik måte dersom sertifikatutstederen fremstiller begge,
- d) undertegner disponerte korrekt signaturfremstillingsdata på tidspunktet da sertifikatet ble utstedt, eller
- e) sertifikatet blir registrert i tilbaketrekkingen, jf. § 12.

Sertifikatutsteder er ansvarlig etter første ledd medmindre han godtgjør at han, eller den han garanterer for, ikke handlet uaktsomt.

Sertifikatutsteder er ikke erstatningsansvarlig for skade som skyldes at sertifikatet har blitt brukt i strid med tydelige begrensninger i sertifikatets anvendelsesområde eller utover beløpsmessige begrensninger.

§ 23 Klageadgang

Tilsynets avgjørelser etter bestemmelser som er gitt i eller i medhold av denne loven, kan påklages til det organ Kongen utpeker.

§ 24 Gebyr

Kongen kan i forskrift bestemme at sertifikatutsteder som er registreringspliktige etter § 18, skal be-

tale gebyr. Gebyrene må ikke overstige kostnadene ved tilsynets virksomhet.

Kapittel V Internasjonale forhold

§ 25 Rettslig anerkjennelse av kvalifiserte sertifikater fra utstedere etablert utenfor Norge

Sertifikater fra sertifikatutstedere som er etablert innen EØS-området, anses som kvalifiserte sertifikater i henhold til denne lov dersom de oppfyller kravene til et kvalifisert sertifikat i det landet der utstederen er etablert.

Kvalifiserte sertifikater fra sertifikatutstedere som er etablert i land utenfor EØS-området, skal gis rettslig anerkjennelse på lik linje med kvalifiserte sertifikater fra sertifikatutstedere innen EØS-området dersom:

- a) utstederen oppfyller kravene i denne lov og har blitt godkjent iht. en frivillig godkjenningsordning i et medlemsland,
- b) en sertifikatutsteder som er etablert innen EØS-området, og som oppfyller kravene i denne loven, garanterer for utstederen, eller
- c) sertifikatet eller utstederen er anerkjent i henhold til multilaterale eller bilaterale avtaler med Norge, EU, tredjeland eller internasjonale organisasjoner.

Kapittel VI Ikrafttredelse og overgangsregler

§ 26 Ikrafttredelse

Loven trer i kraft fra den tid Kongen bestemmer.

§ 27 Overgangsregler

Utstedere av kvalifiserte sertifikater skal innen 6 måneder etter at loven har trådt i kraft registrere seg i henhold til § 18 eller innenfor samme frist opphøre med å kalle sertifikatene for kvalifiserte eller bruke betegnelse som gir inntrykk av at de er kvalifiserte.

Gunnar Skaug

president

Anita Apelthun Sæle

sekretær