IT- og Telestyrelsen
Ministeriet for Videnskab
Teknologi og Udvikling

Digital Signatur
Juridiske aspekter

IT- og Telestyrelsen
December 2002

Resumé

Borgernes retsstilling forringes ikke ved, at en aftale indgås elektronisk og signeres digitalt – aftaler indgået elektronisk har samme gyldighed som aftaler indgået på traditionel vis. Ved brug af digital signatur er det muligt at sikre dokumentationen for de enkelte delelementer i aftaleforløbet.

Med OCES-certifikatet er der ifølge Datatilsynet skabt den nødvendige garanti for, at alle almindelige transaktioner mellem myndighed og borgere kan foregå tilstrækkelig sikkert. Det vil sige, at de kommunikerende parter både kan være sikre på hinandens identitet og på, at deres meddelelser ikke ændres, uden at det efterfølgende kan konstateres eller – hvis de er krypterede - læses af andre undervejs. Dermed lever certifikatet også op til Persondatalovens krav om beskyttelse af personoplysninger, når disse blot overføres mellem to parter i krypteret form.

En myndighed, der indfører digital signatur, står imidlertid over for et meget vigtigt valg, nemlig hvordan de digitalt signerede meddelelser skal opbevares. Spørgsmålet er vigtigt, fordi det angår meddelelsernes juridiske bevisværdi – og netop bevisværdien er et af argumenterne for at indføre digital signatur.

Valget står kort sagt mellem at gemme meddelelsen med eller uden den originale digitale signatur. Gemmes den uden signaturen, skal myndigheden som bevis i stedet undersøge signaturens gyldighed og gemme dette resultat sammen med meddelelsen.

Denne vejledning anbefaler, at man vælger sidstnævnte løsning. Der findes ganske vist ingen retspraksis på området endnu, men det skønnes, at værdien af det såkaldte systembevis vil være tilstrækkelig. Det forudsætter dog, at myndighedens system og procedurer er bygget op, så ingen i praksis kan ændre i en signeret meddelelses indhold eller log.

Ved at vælge denne lagringsmodel opnår myndigheden flere andre fordele. Meddelelserne bevarer deres bevisværdi længere end de 5-6 år, der er holdbarheden[1], når man gemmer dem med den originale signatur. Dermed slipper myndigheden for at sortere meddelelserne efter, hvor længe de skal bevare deres bevisværdi. Og endelig er meddelelserne lagret i et format, der gør det lettere at aflevere dem til offentligt arkiv.

[1] Det vurderes, at de algoritmer, der ligger til grund for signeringen vil være kompromitterede efter 5-6 år. Signaturen er derfor reelt værdiløs som bevis.

Indholdsfortegnelse

1 Formål og målgruppe

Digital signatur er den digitale verdens pendant til en af aftalerettens grundpiller – den personlige underskrift.

Formålet med denne vejledning er at skabe øget klarhed om en række af de juridiske aspekter ved at anvende digital signatur i kommunikationen mellem myndigheder og borgere (eller virksomheder).

Vejledningen belyser blandt andet borgerens retsstilling og forskellene mellem OCES og kvalificerede certifikater samt Datatilsynets vurdering af OCES-certifikatet. Den sætter særlig fokus på spørgsmålet om, hvordan man bedst sikrer de signerede dokumenters bevisværdi. En kompleks udfordring, som myndigheden skal overveje grundigt, inden den vælger en bestemt lagringsmetode.

Målgruppen for denne vejledning er projektledere, jurister og andre, der har et særligt behov for at kende de retlige aspekter af brugen af digital signatur.

Denne vejledning er en blandt flere om digital signatur. De øvrige er:

- **Infrastrukturen til digital signatur**
  Målgruppe: IT-chefer, projektledere og andre, der aktivt skal være med til at implementere digital signatur i en offentlig myndighed

- **OCES – en fælles offentlig certifikat-standard**
  Målgruppe: IT-chefer, projektledere og andre, der skal beskæftige sig indgående med digital signatur og implementeringen af denne i myndigheden

- **Digital signatur – forudsætninger og fordele**
  Målgruppe: Beslutningstagere i offentlige institutioner, der skal afveje forudsætninger mod de økonomiske fordele og mulige serviceforbedringer, der ligger i at implementere digital signatur

- **Sikker brug af digital signatur**
  Målgruppe: Beslutningstagere og projektledere, der skal arbejde med digital signatur-projekter

Alle ovenstående vejledninger findes på IT- og Telestyrelsens/Signatursekretariatets hjemmeside (https://www.signatursekretariatet.dk).

2 Sikker indgåelse af aftaler

Aftaler indgået elektronisk har som udgangspunkt samme gyldighed som aftaler indgået på anden vis. Elektroniske aftaler indgås i dag som et naturligt led i en lang række forretningsmæssige dispositioner. Det kan være alt lige fra bestilling af vare på en hjemmeside til en aftale, der indgås via e-post.

De elektronisk indgåede aftaler har dog typisk rummet det problem, at det har været vanskeligt at eftervise, hvad de konkret indeholdt samt at dokumentere aftaleforløbet med 100 pct. sikkerhed. Det skyldes, at der ved elektronisk aftaleindgåelse ikke foreligger et traditionelt håndgribeligt bevis på den indgåede aftale - f.eks. i form af en kontrakt med begge parters underskrift.

Ved at knytte en elektronisk signatur til de afsendte meddelelser opnår man bl.a. en effektiv mulighed for efterfølgende at kunne dokumentere de enkelte elementer i en elektronisk aftaleindgåelse.

Brug af digital signatur har ingen betydning for den elektroniske erklærings formelle eller materielle gyldighed. Det er den underliggende viljeserklæring, der regulerer aftaleforholdet. Men den digitale signatur sikrer ligesom en almindelig underskrift, at selve aftaleindgåelsen kan foregå trygt, også selvom parterne ikke på forhånd kender hinanden. Hertil kommer muligheden for kryptering, der sikrer, at indholdet af aftalen kan holdes hemmeligt for en uvedkommende tredjemand.

Der foreligger ingen retspraksis, som kan give en konkret vurdering af digitale signaturers bevisværdi. Men det må formodes, at domstolene dels vil se på de konkrete omstændigheder ved certifikatets anvendelse (herunder f.eks. myndighedens procedurer), dels vil foretage en overordnet vurdering af certifikatets beskaffenhed. I denne kvalitetsvurdering må det forventes, at den bagvedliggende certifikatpolitik vil spille en central rolle.

I det følgende gennemgås en række juridiske aspekter af sikker elektronisk kommunikation og aftaleindgåelse mellem myndighed og borgere eller virksomheder.

2.1 Borgerens retsstilling

Når borgere skal kommunikere elektronisk med det offentlige, vil der især være behov for en sikker digital signatur (baseret på OCES-certifikatet), ved udfyldning af elektroniske blanketter og lignende .

I sådanne tilfælde vil borgerne kunne få en elektronisk bekræftelse på, at kommunikationen har fundet sted og en dokumentation for de oplysninger, der er afsendt. Det giver borgerne en større tryghed og en bedre bevismæssig stilling, end de normalt opnår gennem traditionel papirbaseret kommunikation.

I den forbindelse bør myndigheden nøje overveje, hvordan det elektroniske selvbetjeningssystem skal sættes op og anvendes, så det lever op til god forvaltningsskik. Det er f.eks. vigtigt, at borgerne præcist ved, hvad de forpligter sig til, når de benytter et elektronisk selvbetjeningssystem.

Afhængig af det konkrete selvbetjeningssystem hos myndigheden vil borgerne f.eks. have mulighed for at få indblik i sagens status hos myndigheden, herunder at få bekræftet, at sagen er modtaget af en sagsbehandler. Sådanne faciliteter vil også bidrage til at gøre borgeren mere tryg ved at anvende elektroniske systemer.

Overordnet kan det konkluderes, at borgeren i det mindste opnår den samme retsstilling ved brug af digital signatur sammenlignet med traditionel skriftlig kommunikation med myndigheden.

Det skal dog understreges, at der endnu ikke foreligger faste regler for den offentlige myndigheds elektroniske kommunikation med borgeren via f.eks. e-post eller ved lagrede beskeder på en webservice. Inden myndigheden sender elektroniske henvendelser til borgeren, skal myndigheden sikre sig, at borgeren har accepteret denne kommunikationsform. Myndigheden skal ligeledes være opmærksom på omfanget af borgerens accept. At en borgere i én sammenhæng har accepteret elektronisk kommunikation som kommunikationsform er ikke ensbetydende med, at accepten kan udstrækkes til at omfatte al efterfølgende kommunikation.

2.2 OCES-certifikat eller kvalificeret certifikat

Et OCES-certifikat til digital signatur er ikke et kvalificeret certifikat efter Lov om elektroniske signaturer. Loven kræver bl.a. personligt fremmøde for at få udstedt et kvalificeret certifikat, og det er udtrykkeligt ikke en forudsætning for at få et OCES-certifikat.

Teknologisk og organisatorisk er OCES-certifikaterne lige så sikre som kvalificerede certifikater. Sikkerhedsmæssigt er det alene metoden til at sikre brugerens identitet, der er forskellig. Som alternativ til kravet om personligt fremmøde, dobbelttjekker OCES-certificeringscentrene brugerens identitet via CPR-registeret og ved at sende udstedelsesinformation gennem to forskellige kanaler – certifikatmodtagerens registrerede bopælsadresse samt via e-post eller anden elektronisk kommunikation. Også ansvarsbestemmelserne i forbindelse med udstedelsen og anvendelsen af OCES-certifikaterne afviger fra kvalificerede certifikater. Det er således tilladt for OCES-certificeringscentrene at begrænse deres erstatningsansvar overfor myndigheder og erhvervsdrivende virksomheder, der køber OCES-certifikaterne eller anvender dem i deres egne løsninger. I forbindelse med kvalificerede certifikater, har certificeringscentrene ingen mulighed for at begrænse deres ansvar.

Ansvarsbestemmelserne for OCES-certifikaterne følger derfor, modsat kvalificerede certifikater, den model, der anvendes i forbindelse med Dankort. Her er den grundlæggende idé, at dem, der anvender og opnår fordele ved systemet, forretninger m.v., også bør bære en del af ansvaret.

Det skal dog fastslås, at OCES-certificeringscentrene ikke har mulighed for at begrænse deres ansvar overfor den almindelige forbruger.

2.3 Datatilsynets vurdering af OCES-certifikatet

Datatilsynet har vurderet sikkerhedsniveauet i OCES-certifikaterne og anført nedenstående retningslinier for brugen.

2.3.1 Borgeres indsendelse af oplysninger til myndigheder

Datatilsynet har vurderet OCES-certifikaterne med baggrund i certifikatetpolitikken og er kommet frem til følgende vurdering: "Det er …. Datatilsynets vurdering, at OCES certifikatet generelt vil kunne benyttes ved borgernes indsendelse af oplysninger til myndighederne. Datatilsynet er således af den opfattelse, at løsningen, som den nu foreligger beskrevet, og som er baseret på brug af folkeregisteradressen, i relation til databeskyttelsesmæssige krav må anses for tilstrækkelig sikker". Datatilsynet anfører dog tillige, at det som minimum kræves, at der anvendes kryptering. Se den fulde ordlyd af Datatilsynets vurdering her https://www.oio.dk/files/datatilsynssvar.PDF.

2.3.2 Borgernes adgang til offentlige myndigheders oplysninger

Datatilsynet har vurderet, at myndighederne kan give adgang til interne databaser med personfølsomme oplysninger på baggrund af OCES-certifikater. Tilsynet vurderer således,
"…at der på alle områder, hvor myndighederne i dag besvarer indsigtsbegæringer ved fremsendelse af almindelig post til den registrerede – eventuelt under anvendelse af

folkeregisteradressen – må siges at være tilstrækkelig sikkerhed ved brug af OCES-certifikatet".

Hovedreglen er altså, at data, som myndighederne i dag sender med almindelig post i forbindelse med begæringer om aktindsigt, også kan sendes elektronisk med brug af OCES.

Ved at anvende OCES-certifikater kan borgeren således modtage alle relevante oplysninger på sin computer, frem for som i dag at få dem sendt med almindelig post.

2.4 Sanering af forældede formkrav

Regeringen iværksatte i januar 2002 en lovmodernisering. Formålet er, at samtlige ministerier skal modernisere formkrav i deres lovgivning, der unødigt hindrer digital kommunikation.

Alle ministerier har indleveret en handlingsplan, hvor samtlige sådanne formkrav er identificeret. Handlingsplanerne skal beskrive, om formkravet ændres, og i givet fald hvordan og hvornår.

Samtlige handlingsplaner offentliggøres, så alle kan få indsigt i hvert ministeriums parathed til digital kommunikation.

I tråd hermed er forvaltningsloven ændret for at bemyndige ministrene til på hver deres område at ændre formkrav i love rent administrativt. Fristen for denne type lovmoderniseringer var sommeren 2002. Det betyder også, at muligheden for digital kommunikation nu kan skabes på bekendtgørelsesniveau.

Yderligere information om lovsaneringen fås på følgende hjemmeside: http://www.e.gov.dk/formkrav.

3 Sikring af signerede dokumenters bevisværdi

De offentlige myndigheders praktiske rutiner, når de kommunikerer med borgere, skal tilpasses brugen af elektronisk kommunikation og digitale signaturer. Især skal rutiner for registrering (logning) og journalisering (lagring) fastsættes på en sådan måde, at dokumenternes bevisværdi sikres.

Det tidligere IT-sikkerhedsråd har udarbejdet vejledninger om digitale dokumenters bevisværdi samt den praktiske brug af kryptering og digital signatur. Disse vejledninger giver en god gennemgang af problemstillingerne og kan downloades fra Ministeriet for

Videnskab, Teknologi og Udvikling's hjemmeside http://www.vtu.dk. En række af problemstillingerne behandles kort nedenfor.

3.1 To måder at lagre signerede dokumenter på

Alle myndigheder, der modtager meddelelser med digital signatur, kommer til at stå over for spørgsmålet: Hvordan skal vi lagre meddelelsen?

Der er flere måder at gøre dette på og flere hensyn, der skal tages. Det gælder først og fremmest:

- Sikring af bevisværdien
- Vurdering af de teknologiske muligheder
- Forberedelse til aflevering til offentligt arkiv

Med udgangspunkt i myndigheders praktiske erfaringer med at lagre meddelelser med signatur gennemgås i det følgende to generelle lagringsmetoder og deres fordele og ulemper:

- **Model 1: Den digitale signatur som bevis**
  I den første model gemmes meddelelsen **med** den digitale signatur. Dette sikrer, at forsøg på at ændre i meddelelsen kan spores, og afsenderens autenticitet kan kontrolleres ved at sammenholde signaturen med oplysninger, som certificeringscenteret ligger inde med. For at kunne eftervise, at man har modtaget meddelelsen på et tidspunkt, da signaturen var gyldig, er det nødvendigt også at logge tidspunktet for modtagelse af meddelelsen eller resultatet af en signatur-kontrol. I øjeblikket tilbyder markedet ikke uafhængige tidsstemplinger, men en sådan service vil kunne forenkle den beskrevne model

- **Model 2: Anvendelse af systembevis**
  I denne model vælger man at gemme meddelelsen **uden** den tilknyttede signatur – f.eks. i et dokumenthåndteringssystem. Samtidig logger man resultatet af den signaturkontrol, man foretog, og gemmer informationen i tilknytning til meddelelsen. Dokumentets bevisværdi er herefter knyttet til myndighedens evne til at bevise, at system og procedurer er bygget sådan op, at ingen i praksis har kunnet ændre i dokumentets indhold eller log

På baggrund af de hidtidige erfaringer anbefales det, at model 2 anvendes som lagringsmetode. Ved at vælge denne metode sikrer man bevisværdien og forbereder samtidig afleveringen af dokumenterne til offentligt arkiv. Anbefalingen understøttes af Statens Arkiver – se denne udtalelse på

(https://www.signatursekretariatet.dk/news/statens arkiv.pdf). Anbefalingen er dog givet med det forbehold, at der endnu ikke eksisterer en retspraksis på området.

Fordele og ulemper ved de to modeller uddybes i det følgende. I tekstboksen gengives erfaringerne fra to offentlige myndigheder, der har valgt hver sin model.

3.2 Fordele og ulemper ved de to modeller

3.2.1 Bevisværdien

Et af de vigtigste formål med at knytte en digital signatur på en meddelelse er at sikre bevisværdien. Model 1 medfører normalt, at myndigheden kan bevise

- hvem meddelelsen stammer fra
- hvornår den er modtaget
- at der ikke er ændret i meddelelsen siden signeringen

Fordelen ved at gemme meddelelser med digital signatur er, at man anvender den infrastruktur, der er bygget op omkring signaturer, certifikater og den tilhørende teknologi. Det betyder, at en tredjepart også efter lagringen garanterer for identiteten af afsender, og at teknologien ganske tydeligt viser, hvis der er gjort forsøg på at ændre indholdet.

I model 2 er anvendelsen af tredjepart mere indirekte. Myndigheden gemmer en log af, at afsenderens identitet har været kontrolleret hos tredjepart. Men det er ikke muligt at gentage denne kontrol senere.

Hensynet til bevisværdi er relevant i den periode, hvor myndigheden har "retligt og administrativt" brug for meddelelsen. Det vil sige indtil meddelelsen kan kasseres eller overgives til et historisk arkiv. Perioden kan variere meget fra meddelelse til meddelelse. Ved valg af lagringsform skal man være opmærksom på, at man er bedre stillet, jo længere bevisværdien holder.

Det tidligere IT-sikkerhedsråd har anbefalet, at myndigheder ikke anvender digital signatur, hvis der er behov for at anvende meddelelser bevismæssigt længere end en 5-6 år. Det skyldes flere forhold:

- Meddelelser med digital signatur kan ikke konverteres til et andet format, uden at signeringen går tabt
- Certificeringscentrene gemmer ikke informationer om certifikater længere end 5 år ved kvalificerede certifikater, mens de ved OCES-certifikater slet ikke behøver at gemme dem
- Algoritmerne, som signaturen er baseret på, må formodes at være blevet brudt

Disse forhold taler for at anvende model 2 – systembeviset – fordi det vil det være lettere at opbevare en log og en meddelelse i for eksempel TIFF-format i en længere periode end 5 år. Samtidig undgår organisationen at skulle sortere indkomne meddelelser, efter hvilke der skal gemmes på papir, fordi de skal bevares længere end 5 år til retlig og administrativ brug, og hvilke der kan gemmes elektronisk, fordi de ikke skal bevares så længe. Og anvendes der OCES-certifikater, vil organisationen under alle omstændigheder skulle logge resultatet af en signaturkontrol, da certifikaternes historik ikke opbevares i certificeringscenteret.

3.2.2 De teknologiske muligheder

Som myndighed vil man ofte ønske at kunne anvende den lagringsteknologi, man allerede har til rådighed. Digital signatur er kun implementeret sporadisk, og derfor har der ikke været en særlig stærk økonomisk tilskyndelse til at tilpasse ESDH-systemerne. Resultatet er, at nogle systemer er klar til at kunne gemme meddelelser med digital signatur, mens andre ikke er.

For myndigheder, der har investeret i et ESDH-system, der ikke kan håndtere digital signatur, vil der være en økonomisk tilskyndelse til at gemme meddelelser uden signatur og alene basere sig på systembeviser. Problemet må dog formodes at være midlertidigt, da evnen til at håndtere digital signatur i fremtiden vil være et af de uomgængelige krav til ESDH-systemer.

Bestyrelsen for Projekt digital forvaltning har i efteråret 2002 igangsat et projekt til etablering af en fælles ESDH-løsning, der tager hensyn til digital signatur. Styregruppen for projektet har repræsentanter fra statslige institutioner, Amtsrådsforeningen og KL, og 12 særligt udvalgte institutioner er i gang med at udarbejde en kravspecifikation, som derefter skal i udbud og implementeres i organisationerne.

3.2.3 Forberedelse til aflevering til offentligt arkiv

Aflevering til offentligt arkiv udgør et yderligere hensyn. Myndigheder, der skal aflevere elektroniske arkivalier til Statens Arkiver skal gøre dette i systemuafhængige arkiveringsversioner, og i de arkiveringsformater som Statens Arkiver kræver. For skriftlige dokumenter (modsat lyd og billede) er afleveringsformatet TIFF. Al information skal være dekrypteret i arkiveringsversionen. Da digital signatur er systemafhængigt og i sin oprindelige form er uløseligt bundet til det anvendte dokumentformat på underskrifttidspunktet, kan denne ikke medtages i sin oprindelige form, men indholdet af signaturen skal afleveres systemuafhængigt efter Statens Arkivers anvisninger. Det vil derfor være naturligt at overveje, hvordan denne konvertering kan ske så let og ubesværet så muligt.

For myndigheder, der anvender model 2, kan det være en yderligere fordel, at de ikke blot gemmer meddelelser uden signatur men også i et format, som Statens Arkiver vil modtage. I så fald vil en senere aflevering blive væsentligt lettere.

To myndigheder valgte hver sin model
I Nordjyllands Amt overvejer man at gemme meddelelser i et TIFF-format sammen med loggen fra et statustjek af den modtagne signatur. Altså en variant af model 2.

"For os har det været afgørende at have en bevisværdi, der strækker sig ud over de 5 år, Sikkerhedsrådet angiver. Vi ønsker ikke at skulle sortere alle meddelelser, efter hvor lang tid de skal gemmes, og så gemme alle "langtidsmeddelelserne" i papirformat. Og vi tror på, at de procedurer, vi har bygget op omkring vores dokumenthåndteringssystem, er så gode, at vi vil kunne overbevise en dommer om, at autenticitet og integritet er i orden. Også selv om der ikke er en digital signatur på selve meddelelsen," forklarer projektleder Kristian Alstrup Baden fra amtets IT-afdeling

I "din åbne kommune" (samarbejde mellem Skørping, Frederikshavn og Skagen Kommune og Dafolo) i Nordjylland har de valgt en anden strategi, der ligger tæt op ad model 1.

"Vi har valgt at gemme data og signatur flere steder i portal og fagsystem. Data gemmes i XML og som et dokument der indeholder signaturen. Vi er opmærksomme på, at der stadig ingen standard er for formatet, der gemmes i. Modtagne signaturer kan åbnes og verificeres. Derudover logges transaktioner, ligesom data sendes gennem dobbelt krypterede linier. Det har været vigtigt for os at vise, at det kan lade sig gøre at lave en sikkerhedsløsning, der overholder dansk lovgivning, og som ikke er baseret på dispensationer fra disse." udtaler tidligere projektchef Helle Foldager, Dafolo.