



# Handling

## Signatur- og Systembevis

Teknisk vejledning i sikring af digitale signaturers bevisværdi



**IT- og Telestyrelsen**  
Ministeriet for Videnskab  
Teknologi og Udvikling



---

Signatur- og systembevis  
Teknisk vejledning i sikring af digitale  
signaturers bevisværdi  
Version 1.01

Udgivet af:  
IT- & Telestyrelsen

IT- & Telestyrelsen  
Holsteinsgade 63  
2100 København Ø

Telefon: 3545 0000  
Fax: 3545 0010

Publikationen kan også hentes  
på IT- & Telestyrelsens  
Hjemmeside: <http://www.itst.dk>  
ISBN (internet): 978-87-92311-06-1

---

>

---

---

## **Signatur- og systembevis**

Teknisk vejledning i sikring af digitale signaturers  
bevisværdi

Version 1.01

---

## Indhold

---

>

Introduktion	5
Målgruppe	5
Afgrænsninger og antagelser	5
Centrale begreber og terminologi	7
Modeller til sikring af bevisværdi	9
Kriterier for valg af model	9
Model 1: Kryptografisk Signaturbevis	10
Model 2: Systembevis	13
Indholdet af et signaturbevis	14
Model 3: Hybrid mellem kryptografisk signaturbevis og systembevis	15
Fremtidige modeller	16
Model 4: Systembevis genereret af tredjepart	16
Model 5: Tidsstempeling af tredjeparter	17
Sikring af logfilers integritet	19
Nøjagtige tidsangivelser	19
Beviskæder	19
Tilgængelighed	19
Anvendelse af ESDH System	20
Adgangskontrol på filniveau	20
Skrivning af log på WORM medier	20
Kryptografisk sikring af log	20
Intern notar	21
Ekstern notar	21
Appendix A: Logning af XML signaturer	23
Appendix B: Verifikation af en OCES signatur	24
Referencer	25

---

---

## Introduktion

>

---

Formålet med denne vejledning er at belyse, hvorledes bevisværdien af digitale signaturer kan sikres. Muligheden for at sikre digitalt signerede dokumenters bevisværdi er netop en af de centrale bevæggrunde for indførelse af digital signatur, og problemstillingen er helt central i forbindelse med digitalisering af den offentlige og private sektor.

Der er tidligere udgivet følgende publikationer på området: [eDag2Min], [JurAsp], [BevisVærdi] og [FESD]. I denne mere tekniske vejledning beskrives flere alternative metoder til sikring af bevisværdi, og en række kriterier for valg af metode diskuteres sammen med metodernes fordele og ulemper. Endvidere gives en række tekniske anvisninger på, hvorledes metoderne kan implementeres i praksis.

Vejledningen beskriver, hvad man som modtager af et signeret dokument kan gøre for at sikre bevisværdien af den digitale signatur, herunder hvorledes IT systemer til behandling af signaturer rent teknisk kan indrettes. I mange situationer har man som modtager en interesse i at sikre dokumentation for den digitale signaturs gyldighed, der kan fremlægges, hvis afsenderen på et senere tidspunkt ikke vil vedkende sig signaturen. Som eksempler kan nævnes elektronisk aftaleindgåelse, modtagelse af en signeret elektronisk ordre eller faktura, anmodning om en pengeoverførsel, tilmelding til et donorregister, accept af handelsbetingelser, elektronisk byggetilladelse etc.

Hensigten med vejledningen er at beskrive gængse metoder, som dog må forventes at ændre sig over tid i takt med den teknologiske udvikling og etablering af retspraksis på området. Udover eksisterende metoder peges på en række mere avancerede metoder og teknikker (f.eks. notarservices), der kan blive relevante i de kommende år, men som forudsætter etablering og drift af nye infrastruktureservices.

### Målgruppe

Vejledningen henvender sig primært til teknisk kyndige herunder IT ansvarlige, IT arkitekter, softwareudviklere og projektledere, der skal forholde sig til, hvorledes man ønsker at sikre bevisværdien af digitale signaturer i egne organisationer og systemer samt ønsker vejledning i, hvordan forskellige modeller kan realiseres i praksis. Endvidere kan indledende dele af vejledningen med fordel læses af forretningsansvarlige, da de overordnede beslutninger bør baseres på en konsekvens- og risikovurdering forankret i virksomhedens ledelse.

Det forudsættes, at læseren er bekendt med koncepterne for digital signatur og PKI infrastruktur. For en introduktion henvises til <http://www.digitalsignatur.dk/visArtikel.asp?artikelID=604> samt <http://sikkerhed.tdconline.dk/publish.php?id=978>

### Afgrænsninger og antagelser

Følgende emner ligger udenfor vejledningens sigte og behandles derfor ikke i det følgende:

- **OCES implementeringen af digital signatur**

Der tages afsæt i OCES infrastrukturen, hvor udstedelse af digital signatur er implementeret. Generelt vil sikkerheden omkring den indledende

---

---

>

---

identifikation af brugeren, generering og opbevaring af privat nøgle samt udstedelse af certifikat have betydning for signaturs efterfølgende bevisværdi. Dette er beskrevet i OCES CP'erne [OCES-CP].

- **Sikkerheden af det computersystem, hvor signaturen er afgivet.**

Denne vejledning tager udgangspunkt i en situation, hvor en part elektronisk modtager et digitalt signeret dokument og ønsker at sikre bevisværdien af den digitale signatur. Det antages derfor i det følgende, at det er signaturafgivers ansvar at sikre den private nøgle herunder den computer, hvor den private signeringsnøgle opbevares inklusive software, der anvender nøglen (f.eks. browsere og e-mail klienter).

Oftentimes ligger det udenfor signaturmodtagers muligheder at kontrollere miljøet, hvor signaturen blev afgivet, så dette behandles ikke nedenfor.

I nogle situationer vil signaturmodtager dog indhente signaturen via en web applikation, som signaturafgiver interagerer med via sin browser. Dette er f.eks. normalt i netbanker og offentlige portaler. Her vil signaturmodtager spille en mere aktiv rolle i signaturafgivelsesprocessen ved f.eks. at stille software til rådighed, der visuelt præsenterer dokumentet der underskrives og efterfølgende kalder signaturgenereringssoftware på signaturafgivers computer<sup>1</sup>. Måske installeres oven i købet software eller foretages sikkerhedsmæssige kontroller på signaturafgivers computer, inden signaturen kan afgives. Det ligger udenfor denne vejlednings sigte at diskutere sådanne teknikker og de bevismæssige implikationer af at anvende dem.

- **Hvorledes digitale beviser kan fremlægges i en retssal**

Nedenfor beskrives udelukkende handlinger, som foretages hos signaturmodtager (i dennes IT systemer) for at sikre bevisværdien af en digital signatur. Hvorledes digitale beviser kan overføres til og fremvises i en retssal behandles ikke.

---

<sup>1</sup> Eksempler på sådan signeringssoftware er Java Applets eller ActiveX kontroller, som hentes via signaturafgivers browser.

---

## Centrale begreber og terminologi

>

---

I dette kapitel beskrives en række centrale begreber samt terminologi, der anvendes i resten af dokumentet. Afvigelser i forhold til andre publikationer kan forekomme, da der så vidt vides ikke findes nogen alment accepteret terminologi for alle dele af området.

### **Digitalt Bevis**

Ved et *digitalt bevis* forstås en samling data, der kan fremlægges som dokumentation for et givet forhold i en retssag. I dette dokument opereres primært med digitale beviser, som dokumenterer at en part digitalt har underskrevet et givet dokument.

### **Kryptografisk signaturbevis**

Ved et *kryptografisk signaturbevis* forstås et digitalt bevis, der dokumenterer en digital signaturs gyldighed samt tilknytning til et dokument via signaturen selv - evt. suppleret med øvrig information som f.eks. et tidsstempel eller det tilhørende certifikat. Et kryptografisk signaturbevis rummer alle nødvendige data til brug for en senere genverifikation af signaturen og sikrer desuden, at man kan knytte signaturen til signaturafgiver.

### **Signaturbevis**

Et signaturbevis er et digitalt bevis, der dokumenterer valideringen af en digital signatur på modtagelsestidspunktet. I modsætningen til et kryptografisk signaturbevis indeholder det ikke signaturen, men derimod valideringsresultater som f.eks. om signaturen var gyldig, om dokumentet var ændret, certifikatet var spærret etc. samt tidspunktet for valideringen<sup>2</sup>. Signaturbeviser anvendes ofte som en del af et systembevis.

### **Konfigurationsbevis**

Ved et *konfigurationsbevis* forstås en beskrivelse, der dokumenterer et systems indhold og virkemåde på et givet tidspunkt eller i et tidsrum.

### **Systembevis**

Ved et *systembevis* forstås en beskrivelse, der dokumenterer, at et system er indrettet og sikret på en bestemt måde. I denne vejledning fokuseres på at dokumentere, at et system har gennemført en korrekt validering af en signatur samt opbevaret resultatet sikkert. Det er således ikke den kryptografiske signatur, der lægges til grund for systembeviset, men derimod dokumentation for det omgivende system, der har håndteret signaturen. I nogle situationer kan man dog vælge at lade et kryptografisk signaturbevis indgå i systembeviset.

Et systembevis for en digital signatur omfatter både tekniske og organisatoriske forhold, bl.a.:

- En logning af et signaturbevis indeholdende resultaterne af de udførte kontroller.

---

<sup>2</sup> Det detaljerede indhold af et systembevis beskrives senere.

---

>

---

- Dokumentation for bagvedliggende systemer, procedurer og politikker. Dette inkluderer bl.a. dokumentation for indhold og korrekthed af systemet, der var i drift, mens valideringen blev foretaget (et konfigurationsbevis), samt hvorledes logdata er sikret og opbevaret. Det kan også omfatte instrukser til personale vedr. forretningsgange mv.

### **Dokument**

I det følgende anvendes sprogbrogen, at en signatur påføres et *dokument*. Her skal *dokument* forstås i bredest mulige forstand som en samling data, der underskrives. Det kan f.eks. være et XML dokument, en e-mail etc. Der skeles ikke til, hvorledes dokumentet er modtaget - det kan være via et web service kald, i en e-mail eller ved interaktion med en browser. Det skal bemærkes, at en digital signatur er mere fleksibel end en sædvanlig underskrift og således kan underskrive dele af et dokument eller evt. flere dokumenter samtidig. For at holde fremstillingen enkel anvendes i det følgende den simple sprogbrug, at et dokument er underskrevet, men i praksis er det selvfølgelig vigtigt at skelne mellem f.eks. signerede og usignerede dele.

### **Signaturafgiver**

Signaturafgiver er den part, der har underskrevet et dokument med sin digitale signatur.

### **Signaturmodtager**

Signaturmodtager er den part, der modtager et signeret dokument fra en anden part (signaturafgiver), og som ønsker at sikre bevisværdien af signaturen ved at implementere nogle af mekanismerne beskrevet i denne vejledning.

### **Bevisværdi**

Ved *bevisværdi* forstås styrken af et digitalt bevis. En metode til sikring af bevisværdi vil have en række egenskaber, der generelt styrker eller svækker værdien af et bevis. Eksempler kan være hvorvidt uvildige tredjeparter kan attestere bevisets ægthed, eller hvorvidt det er muligt at forfalske data, der indgår i beviset. Bevisværdien vil i enhver sag altid skulle vurderes ud fra de konkrete omstændigheder.

### **Uafviselighed**

Ved begrebet *uafviselighed* forstås det forhold, at en afsender ikke senere kan påstå, at en meddelelse, som den foreligger, ikke stammer fra ham.

---

## Modeller til sikring af bevisværdi

>

---

Dette kapitel beskriver en række forskellige modeller til sikring af bevisværdien af en digital signatur. Beskrivelserne tager udgangspunkt i en situation, hvor en afsender digitalt har signeret et dokument og sendt dette til en modtager. Det antages videre, at modtageren har foretaget alle nødvendige sikkerhedsmæssige kontroller af signatur og certifikat og herefter ønsker at etablere et digitalt bevis i form af data, der kan fremlægges som dokumentation ved en eventuel tvist. De nødvendige sikkerhedskontroller på OCES signaturer og certifikater er beskrevet i detaljer i appendix B.

De centrale valg for signaturmodtager er, hvilke data der genereres som dokumentation, samt hvorledes disse data håndteres efterfølgende.

Nedenfor behandles en række modeller til sikring af bevisværdi:

1. Kryptografisk signaturbevis.
2. Systembevis baseret på logning af kontroller hos signaturmodtager.
3. Hybrider mellem de to første modeller.
4. Anvendelse af systembevis baseret på logning af kontroller hos tredjepart.
5. Anvendelse af kryptografisk signaturbevis kombineret med ekstra services leveret af tredjeparter som f.eks. tidsstempling, notarservices og arkiver.

I de følgende underafsnit belyses modellerne og deres fordele og ulemper diskuteres. Det skal understreges, at visse af dem forudsætter etablering af infrastrukturtjenester, som ikke findes tilgængelige pt. Disse er dog alligevel beskrevet, da øget anvendelse af digitale signaturer i de kommende år kan forstærke behovet for sådanne tjenester.

### Kriterier for valg af model

Den pt. mest anvendte model til sikring af bevisværdi er etablering af systembevis (model 2 ovenfor), da denne oprindeligt blev vurderet mest velegnet og anbefalet af IT & Telestyrelsen. Se f.eks. [JurAsp], [FESD] og [eDag2Min].

Imidlertid betyder udviklingen og diversiteten indenfor anvendelse af digital signatur, at andre modeller kan være mere relevante i nogle sammenhænge. *Man bør således analysere den enkelte virksomheds konkrete behov og anvendelse, når model til sikring af bevisværdi vælges.*

Flg. faktorer kan være udslagsgivende for valg af model:

- **Konsekvenserne ved utilstrækkelig sikring af bevisværdi** herunder økonomiske, strategiske, administrative, juridiske, omdømmemæssige, menneskelige og politiske konsekvenser. Disse bør afdækkes som led i en konsekvens- og risikoanalyse<sup>3</sup>, og en sådan analyse vil samtidig danne grundlaget for, hvor mange ressourcer der rationelt kan afsættes til modforanstaltninger.
- **Økonomiske omkostninger ved at implementere de forskellige modeller.**

---

<sup>3</sup> En sådan analyse kan eksempelvis foretages i henhold til DS-484.

- **Hvor langt et tidsrum bevisværdien skal sikres.** For nogle typer dokumenter og systemer er det ikke nødvendigt at håndhæve signaturen i mere end nogle få år (f.eks. mange former for ehandel), mens det i andre situationer er nødvendigt at kunne etablere dokumentation, der giver en stærk bevisværdi i en lang årrække (eksempelvis digitale dokumenter anvendt til elektronisk tinglysning, testamenter eller langvarige kontrakter).
- **Modenhed af drift, organisation og procedurer.** Det er vigtigt at overveje om organisationen, der genererer og opbevarer bevisdata, har etableret moden IT-drift, procedurer og politikker, der på betryggende vis kan sikre autenticitet, tilgængelighed og integritet af bevisdata. I nogle tilfælde er signaturmodtager borgere eller mindre virksomheder, der ikke kan antages at honorere sådanne krav.
- **Signaturmodtagers interesse i at sikre korrekte data.** Hvis den part, der genererer og opbevarer det digitale bevis, har en interesse i at manipulere data, kan dette udgøre et problem for bevisværdien. I borger-til-myndighed systemer, vil der typisk ikke være en interessekonflikt i at myndigheden genererer og opbevarer et elektronisk bevis, mens man i andre situationer (f.eks. elektronisk handel mellem to virksomheder) let kan forestille sig det modsatte.  
I sådanne tilfælde kan bevisværdien styrkes ved at inddrage uvildige tredjeparter i etablering af det digitale bevis.

På baggrund af den øgede anvendelse af digital signatur og udvikling af større modenhed i markedet, vil denne vejledning udbygge og differentiere tidligere anbefalinger i [JurAsp], idet forskellige metoder til sikring af bevisværdi kan være nødvendige i forskellige situationer.

### Model 1: Kryptografisk Signaturbevis

I denne model sikres bevisværdien ved at signaturmodtager gemmer originaldokumentet samt den digitale signatur med tilhørende certifikat. Umiddelbart er fremgangsmåden således analog til den papirbaserede verden, hvor man ville arkivere originaldokumentet med underskrift som bevis.

Metoden skal sikre, at man har alle nødvendige data til brug for en senere genverifikation af signaturen, samt at man kan knytte denne til signaturafgiver. I appendix A findes en række konkrete anbefalinger for logning af signaturer på XML dSig formatet.

#### Fordele

- Bevisdata (i form af signatur, certifikat, spærreliste samt OCSP svar) er kryptografisk forsegledet og kan derfor ikke indenfor en kortere årrække forfalskes eller ændres af modtageren, og dermed opnås en stærk bevisværdi.
- Signaturen vil på et senere tidspunkt kunne genverificeres - f.eks. i forbindelse med en tvist.

---

>

---

- Krav til systemer, der genererer og lagrer bevisdata er langt mindre end f.eks. ved anvendelse af systembeviser. Dette skyldes, at bevisværdien ikke afhænger af signatormodtageres evne til at godtgøre, at kun autoriseret adgang til bevisdata er mulig<sup>4</sup>. Populært kan man sige, at bevisdata er selvbeskyttende mod forfalskning eller modifikation. Dermed er modellen attraktiv for mindre virksomheder og borgere, der ikke har adgang til moden IT-drift med tilhørende procedurer og fuld sporbarhed, der kan honorere kravene til et systembevis.

### Ulemper

- På grund af en række tekniske forhold vil en afgivet signatur miste bevisværdi over tid<sup>5</sup>. På den baggrund har det tidligere IT-Sikkerhedsråd anbefalet [Praktisk], at man under normale omstændigheder ikke stoler på digitalt signerede dokumenter mere end seks år. Hvor lang en gyldighedsperiode, der kan opnås med kryptografiske signaturbeviser, bør vurderes i det enkelte tilfælde og vil afhænge af det tilhørende dokumentets forretningsmæssige værdi, styrken af de anvendte algoritmer, gyldighed af spærrelistesignatur og certifikat, samt hvor troværdig en tidsangivelse for spærrelistekontrol / OCSP svar, man kan fremlægge.

Som en overordnet tommelfingerregel kan man dog sige, at et kryptografisk signaturbevis ikke bør anvendes (isoleret), hvis der kræves en holdbarhed på mere end to år. Har man behov for længere holdbarhed kan flg. muligheder overvejes:

- Anvendelse af tidsstemplings- eller notarservices. Sådanne services vil kunne agere som uafhængige tredjeparter og underskrive bevisdata med meget lange signaturnøgler. Begge disse forhold vil give en bedre bevisværdi og holdbarhed. Det er dog umuligt at forudsige, hvor lang holdbarhed, man præcist opnår, da dette vil afhænge af den teknologiske udvikling samt videnskabelige fremskridt indenfor kryptologien. Dog vil alene det forhold, at to uafhængige og stærkt sikrede systemer kan fremlægge identiske beviser, øge bevisværdien betydeligt desuagtet længden af krypteringsnøgler.
- Anvendelse af systembeviser (beskrives særskilt).
- Bevisværdien kan forringes, hvis tidspunktet for signaturkontrollen ikke kan dokumenteres tilstrækkeligt. Et scenarie kunne være, at en signaturafgiver påstår, at en anden har misbrugt hans stjalne nøgle og tilbagedateret en signatur til et tidsrum, hvor den ikke var spærret. Dette kan for det første

---

<sup>4</sup> Det er naturligvis stadig nødvendigt at sikre tilgængeligheden af bevisdata f.eks. i form af backup og disaster-recovery procedurer.

<sup>5</sup> Dette skyldes, at udviklingen indenfor computeres regnekapacitet samt forskningen indenfor kryptologien til stadighed gør det muligt at "bryde" længere signaturnøgler. Dette giver signaturafgiver mulighed for at påstå, at signatormodtager har produceret en ny signatur med en beregnet nøgle. Enhver nøgle må derfor forventes at blive indhentet af udviklingen på et tidspunkt, så "holdbarheden" er begrænset. Det er vanskeligt at spå om takten, men 5-6 år er et konservativt bud.

---

>

---

imødegås ved anvendelse af tidsstemplings- og notarservices som beskrevet ovenfor. Desuden vil forudsætningen for scenariet i mange situationer være, at signatormodtager og misbrugeren af den stjalne nøgle vil skulle have indgået en sammensværgelse<sup>6</sup>, hvilket må formodes at stille signaturafgiver dårligt i en retssag.

- Bevisværdien af en signatur bortfalder, hvis signaturen er afgivet efter det tilhørende certifikat er spærret. Selvom signatormodtager foretager en spærrekontrol, inden signaturen accepteres, kan signaturafgiver i teorien hævde, at certifikatet var spærret før dette tidspunkt. Om dette reelt er et problem i praksis vil afhænge af situationen. Signatormodtager vil dog kunne træffe en række modforanstaltninger:
  - Det kan være, at tidspunktet for signaturafgivelsen fremgår af konteksten af systemet og kan dokumenteres på denne måde.
  - Signatormodtager kan inkludere en tidsangivelse i det dokument, signaturafsender skal signere, således at tidsstemplet er beskyttet af signaturen. I dette tilfælde bør signatormodtager sikre sig, at tidsangivelsen er korrekt.
  - Signatormodtager kan få dokumentet tidsstemplet hos en uvildig tredjepart, der tilbyder en sådan service (denne mulighed beskrives mere detaljeret nedenfor).

Ved anvendelse af den digitale signatur som bevisværdi, bør signatormodtager som minimum logge følgende data i sit system:

1. Tidspunkt for verifikation af signatur og kontrol af certifikat. Dette bør logges så troværdigt som muligt og f.eks. kunne korreleres med handlinger udført i forretningssystemer. Det er vigtigt at tidspunktet inkluderer angivelse af tidszone.
2. Originaldokument, hvis hash-værdi er signeret, eller entydig reference til dette. Dokumentet skal under alle omstændigheder senere kunne fremskaffes ved en tvist.
3. Den beregnede hash-værdi over originaldokumentet.
4. Signaturværdien.
5. Identifikation af anvendte algoritmer og parametre til signaturberegning (f.eks. hash-algoritme, signaturalgoritmer, kanoniseringer).
6. Signaturafgivers certifikat<sup>7</sup> eller entydig reference til dette.

Endvidere kan man overveje at logge flg. data:

- Identifikation af spærreliste (CRL), hvis en sådan er anvendt.

---

<sup>6</sup> Her tænkes f.eks. på situationer, hvor signaturen modtages og behandles af et on-line IT-system. Her ville forfalskeren både skulle tilbagedatere dokumentet eller transaktionen med den stjalne nøgle, **og** modtagersystemet vil skulle acceptere et tilbagedateret dokument eller transaktion, før svindlen kan lykkes. Hvis signatormodtager og svindler er én og samme bliver scenariet naturligvis mere sandsynligt.

<sup>7</sup> Man kan evt. klare sig med dele af certifikatet, men i praksis er det ofte lettest at gemme hele certifikatet (evt. base64 indkodet).

---

>

---

- Signeret svar på online-forespørgsler fra certifikatudsteder om certifikatets spærrestatus (OCSP).

Disse data kan anvendes til at godtgøre, at signaturafgivers certifikat ikke var spærret på underskriftstidspunktet og kan derfor være nødvendige at fremlægge i tilfælde af en tvist.

En væsentlig pointe er, at de ovennævnte logninger som signatur (inkl. tilknytning til dokument), certifikat, CRL / OCSP svar er kryptografisk forseglede (med signaturer). Dette gør det betydeligt nemmere (i et afgrænset tidsrum) at demonstrere loggens autenticitet og integritet i forhold til, hvis man havde anvendt logninger baseret på ikke-forseglede data, som det ofte er tilfældet med systembeviser (se nedenfor).

## **Model 2: Systembevis**

Ved anvendelse af systembeviser sikres bevisværdien af signaturen i udgangspunktet ved at logge resultatet af de kontroller, modtagerens IT-system har foretaget i forbindelse med verifikation af signatur og certifikat (et signaturbevis). Den digitale signatur gemmes således ikke, efter den er verificeret.

Logningen (signaturbeviset) er i sig selv kun dokumentation for, at systemet har gennemført valideringen af signaturen. Det er de bagvedliggende systemer, procedurer og politikker for at validering og logning bliver gennemført samt signaturbeviset gemt og opbevaret på en sikker og forsvarlig måde, som i den sidste ende bliver afgørende for bevisværdien.

Ved en eventuel tvist fremlægges systemets logs som dokumentation, og endvidere er det nødvendigt at redegøre for systemets virkemåde på det tidspunkt, hvor valideringen blev foretaget, samt øvrige relevante forhold herunder organisatoriske forhold. Det er således af afgørende betydning for bevisværdien, at man kan demonstrere at:

- Systemet har fungeret korrekt på det pågældende tidspunkt, således at kontroller og logninger var pålidelige. Dette indbefatter således et konfigurationsbevis.
- At det efterfølgende er usandsynligt, at manipulation med log eller system har kunnet finde sted. Dette kan eksempelvis omfatte dokumentation for sikkerhedsmæssige procedurer, adgangskontrol etc.

### **Fordele**

- Bevisværdien vil ikke direkte som følge af den teknologiske udvikling falde over tid, som det er tilfældet med kryptografiske nøgler. Metoden er derfor velegnet til dokumenter med lang levetid (>6 år). Dog kan man sige, at det i praksis bliver sværere over tid at godtgøre, hvordan et system så ud på valideringstidspunktet.

### **Ulemper**

- Bevisværdien vil afhænge af signaturmodtagers evne til at godtgøre integritet, korrekthed og adgang til systemet, der har genereret og opbevaret signaturbeviset. I store IT-installationer med hundredvis eller tusindvis af

softwarekomponenter kan det være omfangsrigt at dokumentere, hvad der var i drift på et givet tidspunkt, samt at valideringen fungerede korrekt.

- Alvorlige IT sikkerhedsbrister kan bringe bevisværdien i fare for samtlige opbevarede signaturbeviser genereret før dette tidspunkt. Hvis en person f.eks. har haft uautoriseret og uovervåget adgang til filen med logdata, er det således vanskeligt efterfølgende at vide, om de dokumenterede logninger er korrekte. Et andet eksempel kan være, at der opdages en fejl i den software, der har udført kontrollerne, der ligger til grund for logningerne. Dette kan kompromittere de logninger, der er genereret, mens fejlen har været til stede i systemet.
- Det er en afgørende forudsætning for bevisværdien, at organisationen har modne IT-processer - herunder skal sikkerhedsarbejdet være betryggende (f.eks. via en implementering af DS-484 standarden). Det kan være omkostningsfuldt for mindre virksomheder at honorere sådanne krav - og helt umuligt for privatpersoner.
- Hvis den part, der genererer systembeviset, har en klar interesse i at forfalske eller ændre en transaktion, kan systembevisets troværdighed blive draget i tvivl. Sådanne scenarier er f.eks. sandsynlige i forbindelse med elektronisk handel mellem to virksomheder.
- Kontrollen af signaturen kan ikke gennemføres på et senere tidspunkt (f.eks. ved en tvist), da nødvendige data ikke længere er tilgængelige.

### Indholdet af et signaturbevis

En række vejledninger har tidligere adresseret indholdet af et signaturbevis, der indgår som en del af et systembevis. I [eDag2Min], hvor minimumskrav til sikker e-post løsninger angives, fremgår det således, at et signaturbevis bør indeholde flg. data:

- Tidspunktet for signaturkontrollen
- Resultatet af signaturkontrollen
  - Angivelse af om signaturen er valid på modtagelsestidspunktet
  - Angivelse af om meddelelsen er uændret
- E-postens modtagelsestidspunkt
- Krypteringstilstanden<sup>8</sup>
- En entydig identifikation af signaturindehaveren i form af Subject Serialnumber.

I forbindelse med implementering af andre løsninger, hvor der ikke er tale om epost løsninger, henledes opmærksomheden på følgende:

- Det anbefales at logge resultatet af spærrecheck for at dokumentere, at certifikatet ikke var spærret ved genereringen af systembeviset.

---

<sup>8</sup> Denne rummer ingen bevisværdi i forhold til signaturen men kan bruges af en myndighed til at godtgøre, om man har efterlevet krav til fortrolighed i kommunikationen.

---

>

---

- For alle typer OCES certifikater er det Subject Serialnumber, der entydigt identificerer certifikatindehaveren. Dette forveksles ofte med certifikatets serienummer, der identificerer certifikatet entydigt hos en certifikatudsteder.
- Det er underforstået, at originaldokumentet selvfølgelig også lagres.
- I en fremtidig situation med potentielt flere udstedere af OCES signaturer kan det være relevant med en identifikation af udstederen.
- Da en person vil have flere certifikater over tid, er det relevant også med en logging af certifikatets serienummer, således at man kan identificere hvilket certifikat, der lå til grund for signaturen. Hvis en person f.eks. har haft spærret et certifikat, vil det være relevant at kunne dokumentere, at signaturen er afgivet og systembeviset genereret, mens det pågældende certifikat ikke var spærret.

Alternativt ser man ofte, at hele certifikatet logges, hvilket dog vil kræve lidt mere lagerplads.

I [FESD] afsnit 4.1.2 defineres indholdet af signaturbeviser i større detaljer og indeholder:

- En angivelse af om modtagen epost var krypteret
- Niveau af transportnøglekryptering
- Niveau af datakryptering
- Identifikation af certifikatudsteder
- Identifikation af certifikatindehaver. Her angiver teksten, at der er tale om certifikatets serienummer, mens de tilhørende eksempler stammer fra Subject serialnumber. Der byttes således rundt på identifikation af certifikatindehaver og certifikat. Man bør logge begge serienumre.
- Navnet på signaturafgiver (certifikatindehaver).
- Organisation som angivet i certifikatet.
- Navnet på den organisatoriske enhed fra certifikatet.
- CVR-nummer for medarbejder- og virksomhedscertifikater.
- Certifikatfingeraftryk.
- Om signaturen var gyldig.
- Dato og tidspunkt for verifikationen.
- CPR-nummer for personer.

Der opereres således med en række ekstra informationer i forhold til eDag2 anbefalingerne. I tilgift til ovenstående oplysninger tilrådes det at logge certifikatets serienummer for at få en entydig og søgbar reference til det anvendte certifikat.

Det bemærkes endvidere, at [FESD] definerer systembeviser både for ind- og udgående meddelelser samt logger dokumentation for, om en meddelelse var krypteret mellem afsender og modtager. I dette dokument behandles udelukkende indgående meddelelser.

### **Model 3: Hybrid mellem kryptografisk signaturbevis og systembevis**

---

---

>

---

I nogle tilfælde kan det give mening at etablere et kryptografisk signaturbevis og lade dette indgå i et systembevis (model 1 og 2 ovenfor).

De to metoder kan komplementere hinanden, således at den samlede bevisværdi øges. De konkrete fordele er:

- Det er muligt at opnå en lang levetid af bevisdata qua systembeviset.
- Ved kompromittering af systemet vil bevisværdien stadig kunne bevares via det kryptografiske signaturbevis.
- Den kryptografiske sikring giver en høj grad af troværdighed i en årrække, hvilket kan være relevant i situationer, hvor signaturmodtager kunne have en interesse i at manipulere med loggen.

Den primære ulempe er de øgede krav til lagerplads, der skal anvendes til at gemme begge typer bevisdata.

## Fremtidige modeller

### Model 4: Systembevis genereret af tredjepart

Blandt de primære ulemper ved systembeviser er de medfølgende krav til system, procedurer og politikker, der kan være svære at honorere for mindre virksomheder og borgere i særdeleshed.

En oplagt måde at undgå disse krav men samtidig opnå en stærk bevisværdi er at lade en tredjepart generere og opbevare systembeviset. Dermed out-sources forpligtelsen med at dokumentere, at log, systemer og procedurer er sikre og effektive, og det bliver vanskeligt at hævde at en tilbagedatering er sket efter signaturbeviset blev genereret. Dermed vil en uvildig tredjepart bidrage til tidsfastsættelse af signaturen.

Sådanne tjenester findes ikke på nuværende tidspunkt, men man kan forestille sig, at de etableres af private aktører på kommercielle vilkår, som fællesoffentlige services eller som en del af den nationale OCES infrastruktur.

Af udfordringer ved en sådan model kan nævnes:

- Hvis originaldokumenter er omfattet af logningen hos tredjeparten, etableres et centralt dokumentregister med meget følsomme oplysninger, hvilket kan stride mod forskellig lovgivning. Det vil derfor være fornuftigt, hvis kun hash-værdier af originaldokumenterne opbevares.
- Man kan risikere at etablere et "single point of failure". Dette kan dog håndteres ved strenge SLA-krav - f.eks. krav om to-center drift etc. Et alternativ til kravet om meget høj opetid er, at anvenderne af servicen etablerer en asynkron levering af bevisdata, således aflevering kan sættes i "kø" indtil servicen er oppe og forretningsapplikationerne fortsætte uden at vente.

Metoden kan desuden kombineres med en elektronisk arkiveringstjeneste, der anvendes til at sikre tilgængelighed og gyldighed af elektroniske dokumenter over en

---

---

>

---

lang tidsperiode. Krav til en sådan tjeneste findes i RFC 4810 "Long-term archive service requirements", som dog ikke udgør nogen form for standard pt. Der er tale om en række avancerede krav, som adresserer problemer som begrænset levetid af lagermedier, udviklingen indenfor teknologi og kryptografi, ændringer i teknologi som f.eks. dokumentformater, juridiske aspekter mv.

### **Model 5: Tidsstempling af tredjeparter**

En af de primære ulemper ved brug af kryptografiske signaturbeviser (model 1 ovenfor) er, at det kan være vanskeligt at dokumentere, at en signatur blev afgivet før certifikatet blev spærret.

Dette kan i en række situationer håndteres ved, at signaturen afgives over data, der indeholder en tidsangivelse. Her vil underskriveren således forsegle denne med sin signatur. Modtageren skal naturligvis kontrollere, at tidsangivelsen i dokumentet er korrekt indenfor en acceptabel tolerance, der kan skyldes usynkroniserede ure etc. Metoden forudsætter naturligvis, at underskriveren er i stand til at kontrollere den tidsangivelse, der signeres sammen med resten af dokumentet.

En mere generel løsning, der kan anvendes i alle situationer, er brug af troværdige tredjeparter til tidsstempling af signaturen. Med disse kan man etablere et stærkt, kryptografisk bevis for, hvornår signaturen blev afgivet. Hermed kan modtageren godtgøre, at signaturen blev afgivet, mens certifikatet ikke var spærret, da svindel med tilbagedatering således forhindres.

Internet standarden RFC 3161 - "Time Stamp Protocol" publiceret af IETF beskriver en protokol mellem en signatormodtager og en tidsstemplingservice. Basalt set fungerer protokollen ved, at modtager sender en hashværdi<sup>9</sup> til tjenesten, der herefter tilføjer en tidsangivelse og signerer over begge dele, hvorefter svaret returneres. Modtageren kan nu validere tidsstemplet og gemme svaret som kryptografisk forseglet bevisdata. Servicen får således ikke kendskab til originaldokumentet. Her skal man være opmærksom på, at også signaturen anvendt til tidsstemplingen har en begrænset holdbarhed, som dog ofte vil være længere idet tidsstemplingsservices normalt benytter lange nøgler.

Det skal endvidere nævnes, at ETSI har publiceret profiler [TS 101 861] og politikker [TS 102 023] for "Time Stamp Protocol". Profilen begrænser en række af de valg, protokollen muliggør, herunder valg af parametre, algoritmer, nøglelængder og transportprotokoller.

En ekstra gevinst ved tidsstemplingen er, at man kan opnå længere levetid af signaturen, hvis tidsstemplings servicen anvender lange signaturnøgler (f.eks. 2048 bit RSA nøgler eller signaturer baseret på elliptiske kurver). Som tidligere nævnt opnås i

---

<sup>9</sup> Hash-værdien skal i dette tilfælde være over signaturen af dokumentet og ikke over dokumentet direkte.

---

>

---

sig selv en øget bevisstyrke, når to uafhængige systemer kan bekræfte samme hændelse.

Der findes pt. ingen officielle services til tidsstempling i Danmark, men metoden kan dog blive en realistisk mulighed indenfor en relativ kort tidshorison, såfremt efterspørgslen øges<sup>10</sup>.

---

<sup>10</sup> På <http://security.polito.it/ts/> er listet en række offentligt tilgængelige services. Det er ikke undersøgt i forbindelse med udarbejdelsen af denne vejledning, om disse drives med en servicekvalitet, der gør dem egnede til sikring af bevisværdi i praksis.

---

## Sikring af logfilers integritet

>

---

Dette kapitel beskriver kort en række forskellige teknikker, der kan anvendes til sikring af logfilers integritet, da denne er afgørende i flere af de tidligere beskrevne metoder til sikring af signaturers bevisværdi. Ved anvendelse af systembeviser vil det eksempelvis være ødelæggende for bevisværdien, hvis det er muligt at manipulere med loggen indeholdende signaturbeviser.

De forskellige metoder har forskellige sikkerhedsmæssige-, driftsmæssige- og økonomiske konsekvenser, der må afvejes i hvert enkelt tilfælde. Det skal endvidere understreges, at det er udenfor rammerne af denne vejledning at gå i dybe tekniske detaljer.

Ved logdata tænkes i det følgende på de særlige data, der opsamles som en del af et digitalt bevis - og f.eks. ikke den almindelige logning, der finder sted til fejlsøgning (tracelog), statistikker, rapportering osv. Disse bør således holdes skarpt adskilt i systemet.

### Nøjagtige tidsangivelser

Hvis der kan rejses tvivl om rækkefølgen af hændelser dokumenteret ved logninger, kan bevisværdien let forringes eller i yderste konsekvens helt mistes. Derfor bør logninger altid forsynes med nøjagtige tidsangivelser. I miljøer hvor flere servere foretager logninger, som efterfølgende skal kunne sammenstilles til et hændelsesforløb, er det endvidere vigtigt at synkronisere disses ure indbyrdes. Dette kan eksempelvis gøres ved at anvende en NTP Server (Network Time Protocol). Se mere på <http://www.ntp.org>

### Beviskæder

I denne vejledning er der naturligt fokuseret på sikring af en signaturers bevisværdi som et isoleret fænomen. En signatur vil dog som regel indgå i en applikationskontekst, hvor det kan være relevant at logge et helt hændelsesforløb med henblik på at dokumentere, hvad der er foregået; dette kaldes typisk for en *beviskæde*. Således må det formodes at give anledning til øget troværdighed og bevisstyrke, hvis en hel beviskæde kan fremlægges i en retssag.

Man bør derfor for hvert enkelt system nøje kortlægge hvilke systemspecifikke hændelser, der kunne være relevante at inkludere i en beviskæde.

### Tilgængelighed

En log er ikke meget værd, hvis den ikke er tilgængelig ved en tvist. Derfor bør logdatas tilgængelighed sikres via backup-procedurer.

Et andet aspekt ved tilgængelighed er, at data som udgangspunkt bør logges i ukrypteret form, således at de kan fremvises uden senere dekryptering. Dermed mistes logdata ikke ved tab af dekrypteringsnøgler. Dog bør man være opmærksom på, at lovgivningsmæssige krav kan betyde, at f.eks. personfølsomme data skal være krypterede. Her kan man så overveje blot at kryptere disse samt sikre tilgængeligheden af den anvendte krypteringsnøgle.

### **Anvendelse af ESDH System**

Hvis man har indført et ESDH system, er det oplagt at anvende dette til at gemme vigtige logdata som f.eks. signaturbeviser. Et ESDH system vil nemlig ofte være indrettet således, at det er uhyre vanskeligt at slette eller manipulere med journaliserede dokumenter - populært sagt låses dokumentet ved journalisering. Endvidere vil der ofte i forvejen være etableret en række sikkerhedsprocedurer omkring systemet, der kan anvendes som yderligere dokumentation.

### **Adgangskontrol på filniveau**

Har man ikke et ESDH system, kan man sikre logfiler med de mekanismer til adgangskontrol, der allerede findes indbygget i operativsystemer, databasesystemer etc.

Der bør således oprettes en særskilt gruppe eller rolle i adgangskontrolsystemet, som er den eneste, der tildeles rettighed til at rette og slette logfiler. Rollen bør kun tildeles særligt udvalgt personale (f.eks. sikkerhedsadministratorer), som ikke er en del af det normale driftspersonale. En person bør således have et særligt arbejdsbetinget behov for at kunne få tildelt denne rolle/rettighed.

Hvis adgangskontrolsystemet giver mulighed for det, bør man sætte adgangen op, så én person ikke alene kan modificere eller slette data, men at to eller flere skal logge på systemet for at udføre disse kritiske handlinger. Dette mindsker kraftigt risikoen for svindel og øger troværdigheden af logdata. Endvidere bør man hvis muligt konfigurere systemet, så alle handlinger, der udføres med denne rolle aktiveret, bliver gemt i systemets revisionsspor (der igen skal sikres med nogle af de beskrevne metoder). Endelig bør man også gøre mulighederne for *tildeling* af denne specielle rolle til brugere så begrænset som mulig.

### **Skrivning af log på WORM medier**

En anden metode til sikring af integritet er løbende at skrive logdata på såkaldte "Write Once Read Many" (WORM) medier. Disse har den fysiske egenskab, at de ikke kan slettes eller ændres, når de først er skrevet.

Ved sådanne løsninger er det vigtigt at have omkringliggende procedurer, der sikrer at medier ikke kan fjernes, at falske medier ikke kan introduceres til samlingen med de gyldige, og at tilgængeligheden af medierne sikres. Her kan det eksempelvis være relevant at anvende fabriksnummererede medier.

### **Kryptografisk sikring af log**

En anden løsning er brug af kryptografiske teknikker til sikring af integritet og ægthed af logdata. Denne metode kan evt. kombineres med nogle af de ovennævnte.

Et eksempel kan være, at logdata tidsstemples og signeres med en digital signatur, inden de persisteres. Dette gør det umuligt at ændre ved logdata eller introducere falske logdata uden adgang til den private nøgle. Det er dog stadig muligt at fjerne enkelte hændelser, hvis hver logning signeres enkeltvist. Til at forhindre dette kan

---

>

---

man overveje i hvert enkelt log-element at inkludere en hash over forrige element i signaturen, så der foretages en kryptografisk sammenknytning af elementerne.

Et alternativ til at bruge signaturer er såkaldte "Message Authentication Code" (MAC) funktioner, der anvender symmetrisk kryptografi og således har væsentlig hurtigere køretid.

En afgørende forudsætning for værdien af de kryptografiske metoder er, at adgangen til den private nøgle (hhv. MAC-nøglen) er meget restriktiv, da uautoriseret adgang til nøglen vil kunne bruges til at forfalske logninger. Samtidig skal applikationer have nem adgang til at foretage logning. Dette dilemma kan evt. løses ved at udbyde en service til logning, hvis eksterne grænseflade ikke muliggør svindel, og som internt anvender en stærkt beskyttet kryptografisk nøgle. Eksempelvis kunne denne service modtage logdata via grænsefladen og herefter internt signere disse konkateneret med et tidsstempel, et løbenummer og hashværdien over sidste logning. En sådan service kunne eksempelvis udbydes som en intern notar (se nedenfor).

En ofte anvendt realisering er via et hardware security module (HSM), hvortil der etableres en rolleopdelt drift, som sikrer, at en enkelt privilegeret medarbejder ikke kan svindle med mekanismerne. Nogle HSM'er kan ydermere konfigureres, så en kryptografisk nøgle ikke kan udtrækkes fra hardwaren og kun kan anvendes til logningsoperationer, der som en integreret del vil påstemple enhedens tidsstempel. Dermed er forfalskning via adgang til nøglen i praksis umuligt.

Det skal endvidere bemærkes, at der findes en række kommercielle produkter på markedet, som tilbyder en sådan funktionalitet.

### **Intern notar**

Hvis en virksomhed har brug for at sikre bevisdata i en række forskellige sammenhænge, kan det være en god idé at udvikle en intern notarservice, som kan håndtere sikring af logninger med bevisdata på vegne af alle applikationer.

Udover en oplagt synergieffekt og konsistens bliver det også meget nemmere at skulle redegøre for, at bevisdata er håndteret betryggende i tilfælde af en tvist. Det er således et velafgrænset system / service med en simpel funktionalitet, der skal redegøres for / revideres, frem for et stort systemkompleks.

Det skal dog bemærkes, at løsningen nok primært er realistisk for virksomheder af en vis størrelse.

### **Ekstern notar**

Endelig kan man anvende en ekstern notar til at tidsstemple og lagre bevisdata. Det indebærer naturligt en højere grad af bevisstyrke, hvis en uafhængig og troværdig tredjepart indestår for logningens ægthed og integritet. Ulempen er naturligvis øgede omkostninger, og dette skal naturligvis afvejes mod de opnåede fordele og den forretningsmæssige risiko.

Der findes pt. ingen officielle notarservices på det danske marked.

---

-----

>

-----

---

## Appendix A: Logning af XML signaturer

>

---

Dette appendix rummer en række overvejelser til brug for logning af signaturer på XML dSig formatet, der er en standard under W3C organisationen [XMLdSig]. Overvejelserne knytter sig således til anvendelser af signaturbeviser (og ikke systembeviser, der i princippet er uafhængige af signaturformat).

Generelt er det lettest at logge hele XML dSig signaturen (<ds:Signature> elementet) samt evt. certifikater og eksternt refererede originaldokumenter. Hvis man af hensyn til lagerplads kun logger dele, bør man nøje sikre sig, at alle relevante informationer er medtaget, således at signaturen senere kan genverificeres:

- Parametre vedr. valg af algoritmer, kanonisering etc. er beskrevet som attributter i XML signaturformatet.
- Signaturværdien findes i <SignatureValue> elementet.
- Underskriverens certifikat befinder sig normalt i <X509Data> elementet, hvis det er inkluderet i XML dokumentet. I manglende fald, må det skaffes fra en anden kilde.
- Den signerede hash-værdi er beregnet over <SignedInfo> elementet.
- Originaldokumenterne hørende til signaturen er refereret via <Reference> elementer, som indlejres i <SignedInfo> elementet ved at inkludere deres hashværdi. Med andre ord signerer man reelt en hashværdi over nogle referencer, der igen indeholder hashværdier af originaldokumenterne.
- Originaldokumenterne kan være elementer i XML signaturen eller elementer i et omgivende XML dokument. Endvidere kan de være eksterne dokumenter refereret via en URI, hvilket er velegnet ved signering af ikke-XML dokumenter. For eksternt refererede dokumenter bør man overveje at logge en kopi af originaldokumentet, så dets tilgængelighed sikres.

---

## Appendix B: Verifikation af en OCES signatur

---

>

Dette kapitel beskriver specifikke kontroller, der bør foretages i forbindelse med verifikation af en digital signatur baseret på et OCES certifikat. Hvis en eller flere af disse udelades, vil resultatet højst sandsynligt være et usikkert system. Generelt må det frarådes at implementere disse kontroller selv, da selv en lille fejl kan bryde sikkerheden. I stedet anbefales at anvende velprøvet software til valideringen.

- **Kryptografisk verifikation af signatur med offentlig nøgle**  
I dette skridt verificeres signaturværdien med signaturafgivers offentlige nøgle. Dette gøres teknisk ved at dekryptere signaturen med den offentlige nøgle og herefter kontrollere, at den resulterende værdi er identisk med hashværdien på originaldokument.
- **Certifikatets gyldighed**  
Et certifikat må ikke anvendes udenfor dets gyldighedsperiode.
- **Kontrol af certifikatets spærrestatus**
  - En mulighed er opslag mod en spærreliste (CRL), der periodisk hentes fra certifikatudstederen. Ulempen ved denne metode er, at den lokale spærreliste aldrig er helt up-to-date.
  - En anden mulighed er on-line opslag hos certifikatudstederen (OCSP).

Bemærk at det normalt også er nødvendigt at foretage signaturkontrol på modtagne spærrelister og OCSP svar, som er signerede af certifikatudbyderen.

- **Kontrol af, at certifikatet er et ægte OCES certifikat**  
Dette skal foretages kryptografisk ved at verificere signaturen på klientcertifikatet med den offentlige nøgle fra det udstedende OCES CA. Det er således ikke nok blot at kontrollere "Issuer"-feltet i certifikatet eller inspicere CP feltet, da sådanne felter let kan inkluderes i falske certifikater. Det er endvidere essentielt, at man kun anvender ægte OCES CA certifikater. Typisk vil software til certifikatvalidering operere med et "trusted store", hvor disse CA certifikater kan indlægges til brug for efterfølgende validering.

Det er ydermere vigtigt at sikre sig, at underskriverens certifikat er direkte udstedt af et OCES CA. Dette vil modvirke angreb, hvor en person anvender et ægte OCES certifikat til at udstede nyt falsk OCES certifikat, der så forsøges anvendt til at afgive en falsk underskrift.

- **Kontrol af OCES certifikatets type**  
I nogle sammenhænge vil man ikke tillade alle typer OCES certifikater: medarbejder-, person-, virksomhedscertifikat. Typen af certifikat kan findes ved at se på OID feltet med referencen til certifikatpolitikken.

Det bemærkes, at generel validering af certifikatkæder omfatter en række ekstra kontroller, der ikke er beskrevet ovenfor. Der henvises i stedet til [X509]. Eksempler er kontrol af certifikatpolitik, "path constraints", "key usage", "policy constraints" mv. Disse bør derfor overvejes, hvis andre typer certifikater (end OCES) skal anvendes.

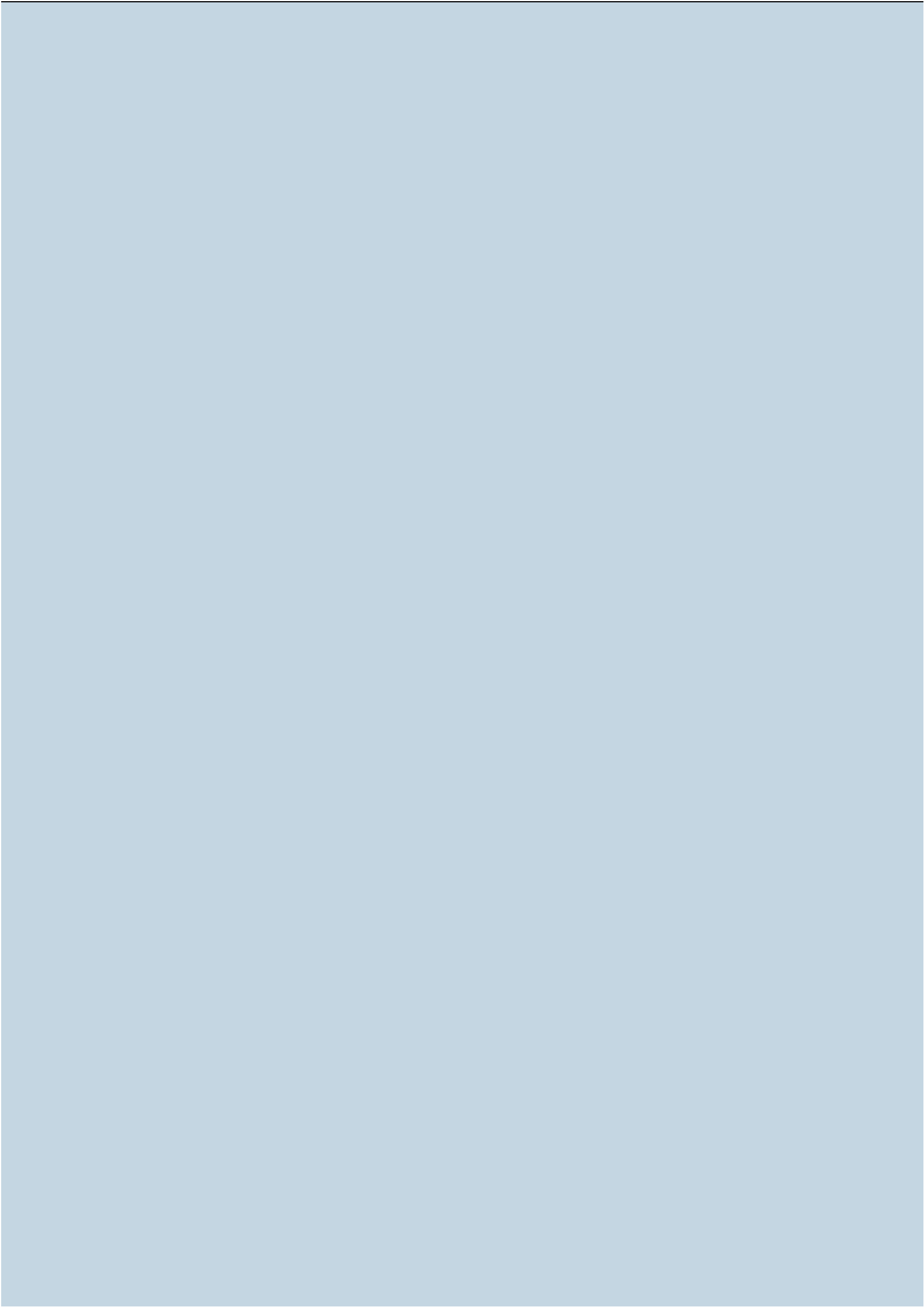
---

## Referencer

---

>

- [JurAsp]** IT- og Telestyrelsen: Digital Signatur Juridiske aspekter, december 2002,  
<http://www.signatursekretariatet.dk/pdf/vejledninger/juridisk.pdf>
- [BeisVærdi]** ”Digitale dokumenters bevisværdi - Introduktion og vejledning”.  
IT-Sikkerhedsrådet, December 1998.
- [FESD]** IT- og Telestyrelsen: FESD Sikker epostløsning, august 2006,  
[http://www.oio.dk/files/Sikker\\_epost\\_Godkendt\\_std.pdf](http://www.oio.dk/files/Sikker_epost_Godkendt_std.pdf)
- [eDag2Min]** Ministeriet for Videnskab, Teknologi og Udvikling:  
Minimumskrav til sikker e-post løsninger i forbindelse med  
eDag2, 16. juni 2004,  
<http://www.digitalsignatur.dk/db/filarkiv/4365/Minimumskrav.pdf>
- [Domst]** Arbejdsgruppe nedsat af Domstolsstyrelsen: Digital  
kommunikation med domstolene, København, oktober 2003,  
<http://www.domstol.dk/om/publikationer/Publikationer/Redeg%C3%B8relse%20-%20Digital%20kommunikation.pdf>
- [Praktisk]** IT-Sikkerhedsrådet: Praktisk brug af kryptering og digital  
signatur, maj 2000,  
<http://videnskabministeriet.dk/site/forside/publikationer/2000/praktisk-brug-af-kryptering-og-digital-signatur/html/index.html>
- [XMLdSig]** ”XML-Signature Syntax and Processing,  
W3C Recommendation 12 February 2002”.  
<http://www.w3.org/TR/xmlsig-core>
- [X509]** The X.509 standard, ITU-T.  
<http://www.itu.int/rec/T-REC-X.509/en>
- [OCES-CP]** <https://www.signatursekretariatet.dk/certifikatpolitikker.html>



---

<

---

## Center for Serviceorienteret Infrastruktur

Center for Serviceorienteret Infrastruktur (CSI) blev oprettet 1. december 2006 for en periode på tre år. Centret har til opgave at lede og facilitere opgaven med at producere en åben, national infrastruktur.

Centret har samlet en række af IT- og Telestyrelsens medarbejdere, der hidtil har arbejdet med forskellige aspekter af samme felt, herunder arbejdet med serviceorienteret arkitektur (SOA), brugerstyring og infrastruktur til e-handel.

---