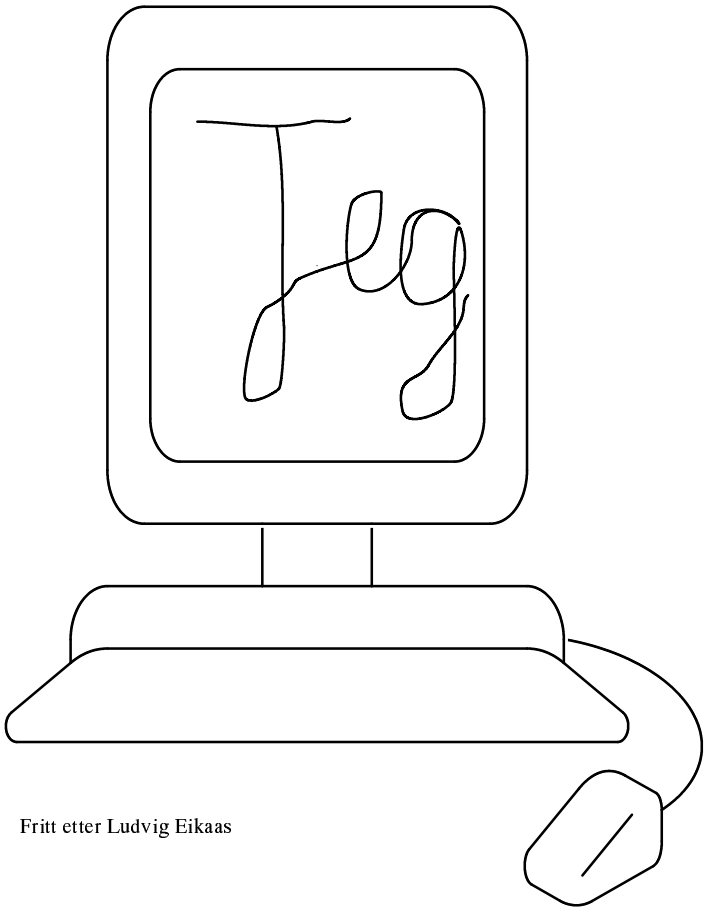


Fritt etter Ludvig Eikaas

UNIVERSITETET I OSLO

Institutt for informatikk

Langtidslagring av digitalt signerte dokumenter

Anne Karen Bonnevie Seip

Hovedfagsoppgave

8. november 1999

annikken@online.no

Forord

Oppgavens tema er autentisering og dataintegritet ved **langtidslagring** av digitalt signerte dokumenter. Jeg har fokusert på offentlige etaters bruk og behov, men resultatene kan også være til nytte i andre sammenhenger. Noen av konklusjonene mine er:

- Dersom digitalt signerte dokumenter skal lagres lenger enn anslagsvis 10 år, vil vedlikeholdsarbeidet for å opprettholde tilgang til dokumentene øke dramatisk,
- Ikke alle egenskaper eller karakteristika ved håndskrevne underskrifter lar seg realisere som digitale signaturer,
- Det offentlige har tatt i bruk digitale signaturer som ekvivalent med håndskrevne underskrifter uten å
  - Vurdere hvilke begrensninger som informasjonsteknologi setter,
  - Bestemme hvem som har ansvar for å definere sammenhengen mellom dem,
  - Vurdere ved testing om erstatningen er dekkende,
- I de nærmeste årene vil bruk av digitale signaturer og offentlig-nøkkel sertifikater medføre ekstra arbeid og utgifter i forhold til å underskrive papirdokumenter for privatpersoner. Det koster å anskaffe sertifikater og selv ta vare på elektroniske dokumenter, men saksbehandlingen kan gå raskere.

Jeg håper oppgaven vil påvirke det offentlige til å gå dypere i arbeidet med hvilke egenskaper ved underskrifter det er mulig å realisere ved bruk av informasjons-teknologi.

Det har vært en fryd å ta hovedfag i informatikk. Takk til Anne Berit Romsaas og Ragni Piene som endelig fikk meg til å starte.

En stor takk til mine to veiledere amanuensis Tone Bratteteig, Institutt for informatikk, UiO, og sjefsforsker Jon Ølnes, Norsk Regnesentral. De ble valgt med omhu. Tone og jeg har hatt fine diskusjoner om systemutvikling og objekt-orientering, og jeg fant ut at Jon og jeg har samme grunnsyn mht. datasikkerhet. Ettersom oppgaven spenner over mange fagfelt, har det vært inspirerende og utfordrende at de har trukket meg i hver sine retninger.

Tusen takk til mine foreldrene Ellen og Inge, til mine brødre Didrik og Børre, til svigerinne Anne-Marie og til niese Karen som har oppmuntret og støttet meg på alle måter for at jeg skulle få til dette.

Mange menneskers interesse for problemstillingen har båret meg fram. En spesiell takk for gode diskusjoner og for hjelp til Amund Eriksen, Rolf Riisnæs, Leif Nilsen, Jens Nørve, Maria Strøm, Trond Sirevåg, Arne Økstad, Odd Grønvold, Svein Solheim, Chris Mitchell, Tone Sandahl, Guri Verne, Kristin Skeide Fuglerud, Dag Wiese Schartum og alle andre som har gitt meg av sin tid og sine tanker, se listen i appendiks G på side 148. Takk til Knut Hegna og Berit Strange, biblioteket ved IFI. Og tusen takk til slekt, alle venninder, venner og kolleger for entusiasme og engasjement på mine vegne.

Takk for økonomisk støtte fra "Kommunikasjon: teknologi og kultur" ved Det historisk-filosofiske fakultet, Unversitetet i Oslo, fra Akershus fylkeskommune og fra UNIFOR (Forvaltningsstiftelsen for fond og legater ved Universitetet i Oslo).

Innhold:

Full innholdsfortegnelse:

Tabeller:

Figurer:

1 Innledning

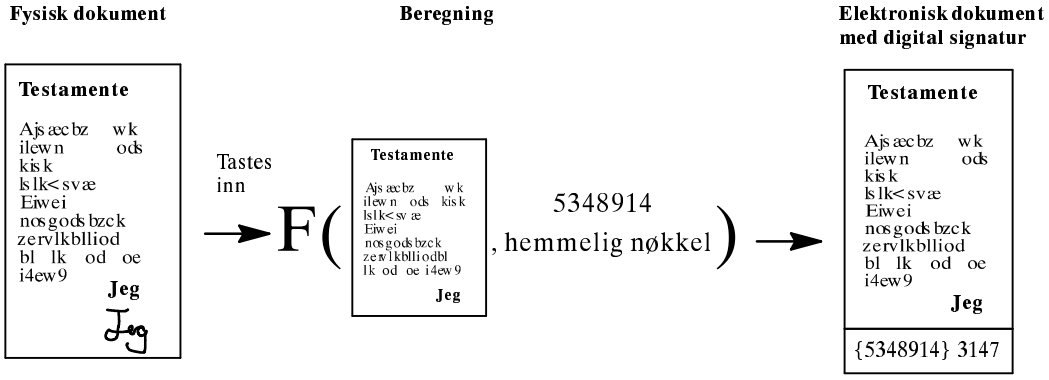
Incitamentet til denne oppgaven var et møte i Den norske dataforening i 1993. Der holdt Leif Nilsen (tidligere Alcatel) en forelesning om kryptering og digitale signaturer. Han forklarte så greit hvor elegant prinsippet for asymmetrisk kryptering er. Jeg ble skuffet og utfordret da jeg forsto at i den virkelige verden krever elegansen en kompleks infrastruktur.

1.1 Mål

Målet med oppgaven er å utdype og drøfte forskjeller og likheter mellom signerte fysiske dokumenter og digitalt signerte elektroniske dokumenter, og beskrive de spesielle utfordringene som opptrer i forbindelse med langtidslagring. Jeg skal undersøke sammenhengen mellom generelle krav til digitale signaturer, de krav aktuell juss stiller og de teknologiske mulighetene som fins.

1.2 Digitale signaturer

Man lager en digital signatur ved å beregne et tall ut fra dokumentet og en privat nøkkel som bare signataren (den som signerer) har tilgang til. Den offentlige nøkkelen, som hører matematisk sammen med den private, er tilgjengelig slik at alle mottakere av dokumentet kan verifisere dets ekthet.



Figur 1 En forenklet beskrivelse av håndskrevne og digital signaturer

En *digital signatur* er et dataelement som følger en elektronisk melding eller dokument, og som binder dokumentet til et individ eller en entitet (maskin, applikasjon eller menneske). Bindingen er slik at signaturener praktisk umulig å forfalske. Den kan verifiseres av en mottaker eller en uavhengig tredjepart. Hvis en bit endres, vil den digitale signaturen ikke godkjennes. Digitale signaturer støtter ikke-benekting, dvs. at eieren av den private nøkkelen ikke kan avvise å ha signert dokumentet [21].

1.3 Scenarier

Langtidslagring av digitalt signerte dokumenter åpner for problemstillinger som ikke fins i tilknytning til papirdokumenter. Jeg har laget senarier for å eksemplifisere noen utfordringer man står overfor.

1.3.1 Arkivere en sak

Året er 2001. Stortinget har ferdigbehandlet statsbudjettet. I Justisdepartementet skal saksdokumentene arkiveres elektronisk i original, lokalt på en server. Dokumentene er skrevet i Word 97 og digitalt signert av diverse ministre og saksbehandlere. Signatarene har sertifikater fra sentraladministrasjonens tiltrodde tredjepartstjeneste (TTP-tjeneste).

- Hvordan skal arkivaren i Justisdepartementet arkivere dokumentene?
- Kan de digitale signaturene beholdes eller skal de fjernes og erstattes med arkivarens digitale signatur?
- Er det viktigst å sikre dataintegritet (at data ikke endres) og bruke en arkivars digitale signatur eller å sikre autentisering av underskriverne og proof of origin ved å beholde signatarenes digitale signaturer?
- Lagres fjernede digitale signaturer for å sikre sporbarhet?
- Hva må ellers til for å sikre sporbarhet, og hvem har ansvar for det?

1.3.2 Verifisere et gammelt dokument

I år 2049 skal en forsker fra Rogalandsforskning se på saksgangen rundt budsjettbehandlingen i år 2001.

- Hvordan kan verifisering av dokumentene foregå?
- Hvem har satt opp reglene for verifisering?
- Er sporbarheten ivaretatt?
- Hva skjer med signaturer og ikke-benekting ved konvertering til nye formater eller nye medier?
- Hvis det er lesbart, hvordan skal man sjekke at reformateringen er riktig?
- Er det i det hele tatt mulig å se dokumentene på en skjerm?

1.3.3 Testamentet er forfalsket

Gerd Buer signerte sitt testamente digitalt med sin private nøkkel i 2005. Et vennepar så på og signerte etterpå med sine private nøkler. Hun lagret testamentet på sin PC sammen med informasjon om programvare, offentlige nøkler og sertifikater. Sønnedatteren Camilla og dattersønnen Johan hjalp henne vekselsvis med å flytte programmer og filer når hun kjøpte nye PCer. I løpet av 11 år byttet hun sertifikater og nøkkelpar 5 ganger.

Da Gerd døde i 2016, hadde hun ikke résignert siden 2005. Testamentet var lesbart og programvaren for verifikasjon virket. Camilla arvet så mye som det var mulig etter loven. Mens Johan ikke var nevnt. Han mente at testamentet var forfalsket, for mormor Gerd hadde alltid sagt at han skulle arve pianoet og Weide-

mannbildet hennes. Han henviste til at algoritmene som ble brukt i 2005, var knekt for lenge siden.

- Var testamentet gyldig?
- Kunne man bevise at testamentet var enten ekte eller forfalsket?
- Er det mulig å bevise at sertifikater og nøkler som ble brukt i 2005 var brukbare da?

1.3.4 Følge en saksgang bakover

I 2034 arbeider forsker Olivia Mortensen i Riksarkivet. Hun oppdager at referatet fra Stortingets avstemning om deltakelse i krigen i Kosovo i 1999 ble endret/editert i 2024.

- Hva skal til for å editere dokumenter lagret hos Riksarkivet?
- Hvilke muligheter er det for å oppdage at noe er endret og finne ut hvem som gjorde endringene?
- Var det autoriserte endringer?
- Har Riksarkivet et ansvar for at det ikke har skjedd en historieforfalskning?

1.3.5 Tillit og risiko

Rustad kommune godkjente Pål Hallskogs utbyggingsplan våren 2004 etter at den hadde vært til høring hos naboene. Da byggingen startet, protesterte naboen Kjell Pettersen. Han sa han umiddelbart hadde sendt et elektronisk brev med protest til utbyggingen. Da kommunen så over sakspapirene, fant de et brev fra Pettersen med 'ja' til utbygging. Den digitale signaturen på brevet var ikke sjekket ved mottak. Den viste seg å være falsk. Dette var i en tidsperiode i høsten 2003 da kommunen hadde få folk i IT-avdelingen og da de hadde dårlige backup-rutiner. Pettersens eget brev var vekk.

- Hvilken tillit bør/kan man ha til offentlige etater mht. riktig elektronisk saksbehandling?
- Trenger privatpersoner sertifikater?
- Hvilke retningslinjer og rettigheter har privatpersoner å forholde seg til?
- Bør Pettersen oppbevare en elektronisk kopi av det han skriver?

1.4 Problemstilling

1.4.1 Hovedspørsmål

I hvilken grad kan man bruke digitalt signerte dokumenter i stedet for håndsignerte dokumenter, og hvor lenge kan slike dokumenter lagres?

Oppgaven har et spesielt fokus på offentlige saksbehandling, men resultatene bør ha en langt mer generell gyldighet.

Elektroniske signaturer

OECD [79] påpeker at digital signatur, elektronisk signatur og elektronisk representasjon er tre relaterte, men distinkte begreper. Med en *digital signatur*

menes bruk av offentlig-nøkkel kryptografi[1]. En *elektronisk signatur* er et teknologinøytralt uttrykk. Det refererer i en bredere sammenheng til applikasjoner i elektroniske omgivelser og juridiske definisjoner av "signatur". En *elektronisk representasjon* er et enda mer generelt uttrykk som er ment å representere en eller annen form for en entitets identitet i det elektroniske miljøet. Det binder ikke nødvendigvis en part i form av en avtale slik en signatur gjør.

Begreper og teknikker er utdypet i appendikset punkt A.3 side 130. Jeg ser i hovedsak på digitale signaturer i denne oppgaven. Noen steder er det likevel naturlig å bruke begrepet elektronisk signatur.

En del sitater og definisjoner, som jeg refererer i oppgaven, syns jeg uttrykkes best på engelsk og har ikke oversatt dem til norsk.

1.4.2 Avledede spørsmål

Hovedspørsmålet har flere parallelle problemstillinger:

1 Hva gjør offentlige etater der elektroniske dokumenter trenger signatur?
2 Hva er det egentlig som skjer når man går fra den fysiske til den elektroniske verdenen?
3 Hva er det spesielle med langtidslagring?
4 Representeres ulike brukerkrav i systemspesifikasjon og programmer?
5 Klarer man å tilpasse lover, regler og standarder til den nye virkeligheten?

Hvor langt har offentlige etater kommet med å bruke digitale signaturer?

Statssekretærutvalget [134] skriver at "offentlig sektor er samlet sett den største IT-brukeren i Norge og kan spille en sentral rolle som pådriver for bruk av informasjonsteknologi i samfunnet". Når det offentlige samordner sine behov og tar i bruk digitale signaturer, f.eks. i Forvaltningsnettet, se punkt 1.6.1, legger de sterke føringer for alle som skal samhandle med dem. For eksempel beløp offentlige innkjøp seg i 1997 til totalt ca. 206 mrd. kroner [137]. Det kan gi grunnlag for mange elektroniske dokumenter og meldinger.

- Hvordan forsikrer etatene som tar i bruk digitale signaturer, seg om at det er samsvar mellom etatenes behov og det systemene gjør?
- Har forskjellige etater forskjellige arbeidsoppgaver som gjør at de vil forholde seg til digitale signaturer på ulike måter?
- Hvilke nye egenskaper får man ved digitale signaturer?

Overgang fra fysisk til elektronisk verden

Allerede i dag produseres det store mengder elektroniske dokumenter. Det er vanskelig å sikre arkivering av dem på tilsvarende måte som fysiske dokumenter arkiveres. Spesielt står offentlige etater foran store utfordringer. Den teknologiske utviklingen har ennå ikke løsninger på alle områder som skal tilsvare behandling av fysiske dokumenter. Lover og regler er ikke tilpasset den teknologiske utviklingen.

1. Det fins ingen god oversettelse av public key cryptograpy. Jeg velger denne skrivemåten.

- Hva er forskjellen på papirbasert og elektronisk dokumentbehandling der det er krav eller ønske om signatur?
- Hvilke egenskaper og funksjoner tilknyttet en håndskreven underskrift mister man ved å bruke digitale signaturer?

Langtidslagring

Hittil langtidslagres dokumenter på papir (pluss mikrofilm, fish osv.), bla. fordi all teknologien for elektronisk langtidslagring ikke er på plass. Sannsynligvis er det også fordi elektronisk langtidslagring viser seg å være en kompleks problemstilling, og at man faktisk ikke har definert de spesielle kravene til langtidslagring:

- Lagringsmedier og bestandighet
- Dokumentformater og framtidig lesbarhet.

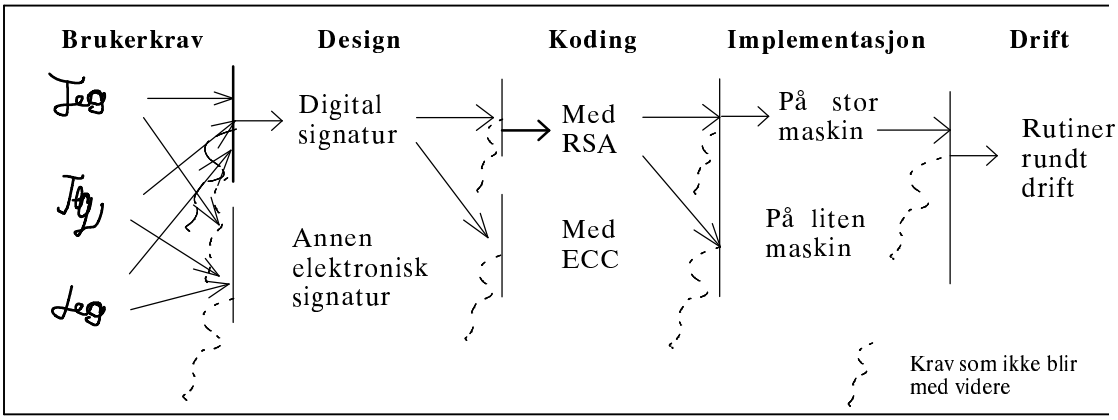
Noark-4, Norsk arkivsystem, addresserer en god del av dette [114]. Denne oppgaven ser på et tredje problem:

- Lagring og varighet av digitale signaturer.

Systemutvikling

Noen av brukerkravene forsvinner på vei mot et ferdig system. Ut fra mitt arbeid med systemutviklingsmetoder i Norges Bank, er jeg fascinert av den forvandlingsprosessen som skjer fra en brukers behov og ønsker til det som faktisk realiseres.

- Hvor i utviklingsprosessen er det man ofte mister vesentlige krav?
- Mister man vesentlige egenskaper når man går fra håndskreven underskrift til digital signatur?
- Er det bestemte grupper av brukere som ikke får det de trenger, og må forandre sine arbeidsrutiner?
- Dekker lovverket de nye verktøyene/metodene?
- Hva er ikke realisert lovmessig for å ta digitalt signerte dokumenter i bruk i stor skala?



Figur 2 Eksempel på steder i systemutviklingsfaser der man må ta avgjørelser om hvilke krav som skal være med videre

Det kan eksistere mange ulike brukerkrav fra ulike interessenter og ut fra hvem som får fremme dem. Et design vil vanligvis bare representere deler av bruker-

kravene. Noen av disse kravene kan designes på flere måter. Design kan realiseres på flere måter, f.eks. med ulike algoritmer. Valg av programmeringsspråk og måten man koder på, kan påvirke resultatet. Programmene kan implementeres på mange typer maskiner. Drift av maskiner og bruken av systemer med elektronisk signatur vil variere med bl.a. manuelle rutiner rundt systemet.

Det kan komme nye utfordringer til, i og med at informasjonsteknologien har helt andre egenskaper enn papir og håndskrift. Ett eksempel er at kopier av elektroniske dokumenter er umulig å skille fra en eller flere originaler.

Systemutviklere må sette seg inn i fagfeltene de skal lage datasystemer for. F.eks. gjelder det å forstå de lover og regler som skal danne grunnlag for en applikasjon. Som systemutvikler må man kunne formulere seg slik at jurister eller andre oppdragsgivere/brukere kan korrigere det man forstår. Det er ikke å forvente at ikke-teknologer skal forstå IT; systemutviklere må forstå brukernes fagfelt godt nok.

Lover, regler og standarder

Departementer og jurister som utformer lovverket, har stor påvirkningskraft overfor alle andre aktører. Deres bestemmelser får konsekvenser for samhandling mellom aktørene.

- Hvordan skal man få til den samme eller tilsvarende juridisk binding mellom en digital signatur og det elektroniske dokumentet som et underskrevet fysisk dokument representerer?
- Har ulike lover forskjellig forståelse av / forutsetning for hva en underskrift innebærer?
- Hvilke krav stiller lover og regler til langtidslagring av dokumenter i det offentlige?
- Hvem har ansvar for å definere og akseptere at de nye mekanismene virker etter hensikten?
- Hvilke standarder og mekanismer fins for å langtidslagre digitalt signerte dokumenter?
- Hva er det mekanismene ikke dekker av det lovene sier og det lovene bør si?
- Hvilke svakheter og risikoområder avdekkes?
- Er eksisterende krav til lagring dekkende, og er de mulig å implementere med dagens teknologi?
- Hva er det som er aktuelt ved integritet, uavviselighet, autentisering og tvister?

Mitt utgangspunkt er at lover kan endres når det oppstår nye behov.

1.5 Forskningstilnærming

1.5.1 Forskningsmetode

I arbeidet med oppgaven har jeg i hovedsak tenkt som en systemutvikler. Jeg har gått fra brukernes problemstillinger og krav, via begrensninger (og muligheter)

som teknologien og lovverket setter, til design og mot implementering. De fleste problemstillingene i punkt 1.4.2 *Avledede spørsmål* er aktuelle i alle system-utviklingsfasene.

Problemstillingen i oppgaven berører bla. feltene datasikkerhet, juss, system-utvikling, informasjonsteknologi generelt, offentlig saksbehandling og arkivering. Lagring av informasjon har man gjort nesten i all tid, så jeg har også sett på eldre materiale for å sette problemstillingen i perspektiv.

Jeg har brukt en kvalitativ tilnærming til stoffet. Jeg har analysert lovtekster som omhandler håndskrevne signaturer, elektroniske signaturer eller lagring av dokumenter, og standarder og guidelines for offentlig-nøkkel infrastruktur, innbefattet tiltrodde tredjepartstjenester, digitale signaturer, hash-funksjoner og generell kryptografi.

Tekstanalysen er supplert med intervjuer med fagpersoner, f.eks. jurister, datasikkerhetseksperter og arkivarer, der tekstene ikke er fullstendig, ikke går langt nok eller ikke er oppdatert.

I tillegg har jeg intervjuet ansatte i offentlige etater om pågående og mulig bruk av digitale signaturer. De har gitt meg informasjon om anvendelse og praktiske problemer ved gjennomføring av prosjekter.

Ved siden av dette har jeg gjort litteraturstudier innenfor fagområdene. Jeg har hatt nytte av tidligere arbeidserfaring fra Universitetet i Tromsø, Tobakks-skaderådet, Statistisk sentralbyrå og Norges Bank.

Tekstanalyser, supplerende intervjuer og intervjuer med brukere har bidratt til å se kontraster mellom teori og praksis, tolkningsmuligheter i lovverket og muligheter og svakheter ved dagens løsninger.

Liste over institusjoner og personer jeg har skaffet informasjon fra, fins i appendikset punkt G, side 148.

1.5.2 Avgrensning

I oppgaven konsentrerer jeg meg om dokumenter som skal ha underskrift i henhold til lov. Jeg går ikke inn på en juridisk vurdering av om dokumenter trenger underskrifter. Fokus er lagt på dokumenter som oppstår i eller sendes til offentlige etater. Det vil si at avsender og mottaker ikke nødvendigvis kjenner hverandre. Digitale signaturer er den eneste anerkjente metoden i åpne systemer. Jeg vurderer også andre typer elektroniske signaturer siden de til en viss grad er i bruk i samfunnet. I midlertid går jeg ikke i dypet av teknikker som brukes. Digitale signaturer står det en del om i appendikset. I forbindelse med langtidslagring vurderer og diskuterer jeg hvor klare definisjonene av eieres og brukeres krav er og hvem som har ansvar for definisjonene. Jeg ser på områder der definisjonene er uklare eller mangler, men jeg kommer ikke med egne definisjoner. I og med at bruk av digitale signaturer i åpne systemer medfører en kompleks infrastruktur, tar jeg opp spesielle utfordringer som langtidslagring skaper, f.eks. tidsstempling, ikke-benekting og formater. Begreper tilknyttet

infrastruktur og tiltrodde tredjepartstjenester er beskrevet i appendikset og regnes for kjent.

Jeg ser i liten grad på

- Konfidensialitet/hemmelighold,
- Overføring i nett,
- Generering, oppbevaring og sikkerhet ved private signeringsnøkler,
- Navngiving og identifikasjon,
- Lagring av annen informasjon enn tekst. Jeg går ikke inn på de spesielle utfordringene ved å lagre bilder, lyd, film eller pekere over lang tid,
- Ulike lovers forskjellig forståelse av / forutsetning for hva en underskrift innebærer,
- Dokumenter som utveksles med andre land.

Noen av problemstillingene i oppgaven har aspekter som kan tas i flere av kapitlene. For ikke å få for mange gjentakelser, har jeg måttet velge hvor de skal være.

Digitale signaturer er et område er i meget rask utvikling. Informasjonen kan fort bli uaktuell, og ny informasjon kommer til.

1.6 Initiativer i offentlige etater

For å få vite hvor langt det offentlige har kommet med praktisk bruk av digitale signaturer, startet jeg arbeidet med å intervjue ansatte i noen offentlige etater.

I hht. *Elektronisk samhandling med og i offentlig sektor* [131] er det en visjon at elektronisk samhandling skal bli en normal og anerkjent arbeidsform i det offentlige. Statskonsult foreslo bla. følgende strategier for å realisere en handlingsplan:

- Virksomhetene i staten og kommunesektoren utfordres til å vurdere prosjekter for elektronisk samhandling,
- Det arbeides for etablering av en tilstrekkelig nasjonal infrastruktur for informasjonssikkerhet. Forsøksvirksomhet med, ogetterhvert etablering av ordninger for digital signatur må prioriteres.

Justervesenet ble tildelt 0,9 millioner kr. og Forsvarets overkommando / sikkerhetsstaben (FOS) ble tildelt 4,1 millioner over statsbudsjettet for 1999 for å starte arbeidet med evaluering og akkreditering av hhv. IT-sikkerhetsløsninger for organisasjoner (tiltrodde tredjeparter) og produkter/systemer.

Offentlige etater har i stor grad klart å samordne arbeidet med digitale signaturer. Det er fruktbart og har satt fokus på flere utfordringer. I dette kapittelet presenterer jeg noen prosjekter og forsøk.

1.6.1 Forvaltningsnettsamarbeidet

Forvaltningsnettprosjektet (FNS) er et prosjekt i det pågående samarbeidet mellom Kommunesektoren og Staten på IT-området (KOSTIT). Arbeids- og

administrasjonsdepartementet (AAD) er ansvarlig på statlig side, og Kommunenes Sentralforbund (KS) på vegne av kommunesektoren [110]. Formålet er å bidra til enkel, sikker og kostnadseffektiv elektronisk informasjonsutveksling og -tilgang innad i offentlig forvaltning, og utad mot andre brukere.

Prosjektet har:

- Etablert rammeavtaler for offentlig forvaltning for utstedelse av offentlig-nøkkel sertifikater, programvare og utstyr for meldingskryptering, smartkort og kortlesere,
- Utviklet en sertifikatpolicy[2] som skal brukes ved utstedelse av sertifikater.

FNS vil vikre standardiserende uten å ha formell myndighet til å utvikle standarder. 15.9.99 ble det innenfor rammen av Forvaltningsnettsamarbeidet inngått en rammeavtale om kryssertifisering med Posten SDS, Telenor AS og Strålfors AS om leveranse av Tiltrodde Tredjepartstjenester og løsninger for digital signatur. Kryssertifisering er at to eller flere sertifiseringsautoriteter gir hverandre sertifikater for å stadfeste et tillitsforhold [116].

Forvaltningsnettprosjektet har foreløpig ikke stilt krav til sertifikater for privatpersoner eller virksomheter i privat sektor som vil samhandle med offentlige etater. Det har heller ikke tjenster for postmottak eller arkivtjenester i hht. Noark-4 [114]. I midlertid sier noen av leverandørene at de kan støtte Noark-4.

1.6.2 Personlige selvangivelser

I 1999 fikk deler av befolkningen tilsendt en delvis ferdig utfylt likning som en prøveordning. Den kunne endres før man godkjente den. Mottakerne fikk valget mellom å underskrive og sende inn likningen på vanlig måte som brev, eller å kommunisere med Skatteetaten via telefon eller Internett. Dersom man benyttet de to siste måtene, mistet man bindingen mellom mennesket og selve selvangivelsen. Via telefon oppga man en tilsendt PIN-kode (Personal Identification Number). Dette er bare en autentisering av at den som ringer har kjennskap til PIN-koden, j.fr. punkt 3.5. Det kan f.eks. være en annen i familien som har åpnet posten. Over Internett ble selvangivelsen SSL-kryptert (Secure Sockets Layer) som er kryptering mellom noder [109].

I ligningsloven står det at selvangivelser skal undertegnes. Men det er lagt til grunn i prøveforskriften av 16.12.97 at det er adgang til bruk av tastafon og Internett under prøveordningen [87]. Hvis prøveordningen vurderes som vellykket, regner man med at underskrifter ikke lenger blir nødvendige for selvangivelser som sendes, endres og godkjennes via telefon eller Internett.

Kommentar

Telefon og Internett må i denne sammenheng betraktes som åpne systemer der ingen av de som kommuniserer, har kontroll med det som gjøres. Metodene som

2. Det er vanskelig å finne et dekkende norsk ord for policy.

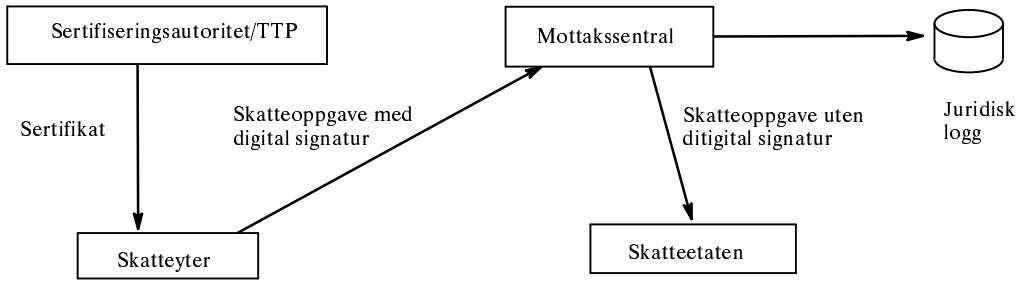
Skatteetaten har valgt, gir ikke autentisering av hvor data kommer fra. De gir verken uavviselighet, autentisering av personen eller en lenke mellom selvangivelsen og personen den gjelder. På den andre siden er det kanskje ikke så mange som vil sende inn andres selvangivelser.

Det er vanskelig å forstå at man signerer selvangivelsen når man taster en PIN. Det gir ikke mening å tenke seg å lagre en PIN-kode, som erstatning for signatur, sammen med likningen.

1.6.3 Årsoppgjørs- og ligningsoppgaver fra næringsdrivende

System for ligning av næringsdrivende (SLN-prosjektet) er en samordnet løsning for produksjon av årsoppgjørs- og ligningsoppgaver og en samordnet elektronisk overlevering av opplysninger fra næringsdrivende til Skatteetaten, Brønnøysund-registrene og Statistisk sentralbyrå. Jeg intervjuet prosjektledere i Skatte-direktoratet (SKD) i 1998 og i 1999. Målsettingen for SLN er at oppgaver som overleveres elektronisk, skal fullt ut kunne erstatte papirbaserte oppgaver [124]. Innrapportering skal undertegnes og lagres i 10 år.

Prosjektet vurderte i hovedsak digitale signaturer. Alternativene var PIN eller at mottaket printet ut hovedtall fra årsoppgaven som ble sendt til avsender for signering og retur. Det siste er reserveløsningen i dag i tilfelle ikke alt det formelle går i orden med digitale signaturer. Prosjektet har ikke formell kontakt med FNS, men følger deres retningslinjer og standarder.



Figur 3 Rapportering til Skattedirektoratet

En tiltrodd tredjepartstjeneste (TTP) som sertifiseringsautoritet for sertifikater og tilbakekallingslister, er satt ut til Posten SDS. De har ansvar for at skatteyterne legitimerer seg forsvarlig før de får et smartkort med sertifiserte nøkler. Legitimeringen følger samme prosedyrer som de bruker på Posten: Bankkort med bilde eller pass. Skattedirektoratet ønsker flere TTPer, men har ventet på opplegg for kryssertifisering.

Den årsoppgaveinformasjonen som skatteyteren ser på skjermen, trekkes ut og konverteres til en EDIFACT-melding. Deretter skjer signeringen. Dvs. signeringen utføres på noe annet enn det som sees på skjermen, selv om innholdet er det samme. Meldingen behandles med hash-algoritmen SHA-1, signeres med en 1024 bits nøkkel vha. RSA og krypteres med trippel DES 112 bits nøkkel.

Signerte oppgaver sendes til en mottakssentral. Skatteyterne har ansvaret inntil oppgaven er registrert i den juridiske loggen hos mottakssentralen. De får en EDIFACT-melding som kvittering. Seinere mottar de en kvittering om at oppgaven er logisk korrekt og godt nok grunnlag til ligning.

Posten SDS har også fått arbeidet som mottakssentral. Det er en annen rolle som de mener er godt adskilt fra rollen som TTP. Mottakssentralen verifiserer signaturen, fjerner den fra årsoppgaven og sender årsoppgaven, resultatet av signaturkontrollen, navn og fødselsnr. til Skattedirektoratet. Selv lagrer de alt som har hendt i en juridisk logg. Mottakssentralen skal kunne gjennfinne og autentisere årsoppgaven med signatur etter 10 år.

Det viktigste hittil er å få opplegget til å virke. Målet er å ha et landsdekkende tilbud i 2003. Det er også viktig for prosjektet at skatteyterne og regnskaps-kontorene ser at den elektroniske innrapporteringen er en rimelig løsning som de tjener på å bruke. SLN-prosjektet er ikke ferdig med den juridiske vurderingen om man fortsatt skal beholde kravet om håndskreven underskrift.

I hht. brukerkravspesifikasjonen til SLN [123] er det satt opp (uavhengig) kvalitetsgjennomgang for å få godtgjort at systemet, dokumentasjonen og tester er utført iht. standarder, regler og øvrige definerte krav. Dette utføres. På forespørsel om akseptansetest fra eierne, fikk jeg til svar at det er ikke gjennom-ført. Skattedirektoratet har foreløpig ikke lagt opp til akkreditering av TTPen, men er likevel opptatt av at skatteyterne også skal ha tillit til dem.

1.6.4 Dokumentutveksling mellom etater

EDNA

Elektronisk dokumentutveksling i norsk administrasjon (EDNA) er et pilotprosjekt mellom Kommunal- og regionaldepartementet (KRD) og Husbanken som startet formelt i 1995 [107]. Bakgunnen for prosjektet var de positive og negative sidene ved innføring av elektronisk post [147]. Prosjektets mål er "Å gjøre det mulig å benytte elektroniske verktøy på sikker og rask måte i saksbehandling, intern saksgang, arkivering og utveksling med eksterne parter". For å lykkes med det har de funnet det påkrevd å:

1 Bruke digitale signaturer,
2 Ha mulighet for kryptering,
3 Bruke TTP-tjeneste.

Prosjektet har sitt politiske legitimitetsgrunnlag i Statssekretærutvalgets rapport [134], Regjeringen Bondeviks tiltredelseserklæring 21.10.97 og i Nærings- og handelsdepartementets (NHD) IT-plan: "En utkant i forkant" (1998) [78].

EDNA startet med kommunikasjon mellom KRD og Husbanken. Informasjonen er i hovedsak ustrukturert. Teknologien i de to etatene var forskjellig og målet var at systemene deres skulle virke sammen.

Tabell 1 Systemer i KRD og Husbanken

Systemer	KRD	Husbanken
E-post	OnMail	(MS-Mail) - Notes
Tekstbehandling	Word 7.0 / 97 MS Office 97	Word (2.0/6.0) 97
Arkiv	OnFile / JASS	Cinet-Noark

Sett fra departementets side virker samhandlingen, og det er en leverandør-uavhengig, ikke-proprietær løsning. Sikkerhetsapplikasjonen, som kan signere og kryptere dokumenter, ligger 'utenpå' og er ikke knyttet til systemene for e-post eller tekstbehandling. Problemene brukerne har med kompatibilitet mellom ulike systemer, oppleves som helt overkommelige. Men de har ikke foretatt kontroller på at dokumentinnholdet er korrekt når dokumenter signert i ett tekstbehandlingsverktøy hentes fram i et annet.

Koplingen mot arkiv er ikke i bruk. Sikkerhetsapplikasjonen kan brukes med smartkort og nøkkellengden er 1024 bits. Posten SDS er TTP. Prosjektet har ca. 20 brukere. Hittil har alle dokumenter blitt arkivert som papirdokumenter.

Neste steg er å

- Avklare videre utvikling,
- Avklare juridiske uklarheter,
- Bestemme formater for langtidslagring,
- Ta i bruk et saksbehandlingssystem slik at det blir full integrasjon mellom tekstbehandlingssystem og arkivsystem.

Da kan mottatte elektroniske dokumenter verfiseres i postmottaket, lagres elektronisk og distribueres elektronisk for intern behandling. Saksdokumenter som sendes elektronisk, skal arkivregistreres og lagres elektronisk. Nye brukere ser ut til å kunne bli flere avdelinger og underliggende etater i KRD, Utenriks-departementet, Finansdepartementet og Justisdepartementet.

Erfaringer

Problemene med å komme igang har etter departementets mening vært:

- Psykologiske skranker,
- Intern elektronisk saksbehandling har hittil vært lite utnyttet,
- Gjennomsnittsbrukeren er ikke 'datafreak',
- Barnesykdommer ved uttestingen.

I KRD må signataren, den som signerer, selv aktivere applikasjonen for signering og kryptering. Den er meget rask. Da vet man at man signerer. Likevel ble prosjektlederne noe overrasket over medarbeidere som spurte etter hvor signaturen var, dvs. de savnet navnetrekket nederst på arket og noe ved den sosiale forståelsen ved å signere.

EDNA-prosjektet har hittil ikke tatt i bruk digitale signaturer internt.
Arne Økstad og Odd Grønvold, KRD, mener dét kan bli aktuelt når man tar i

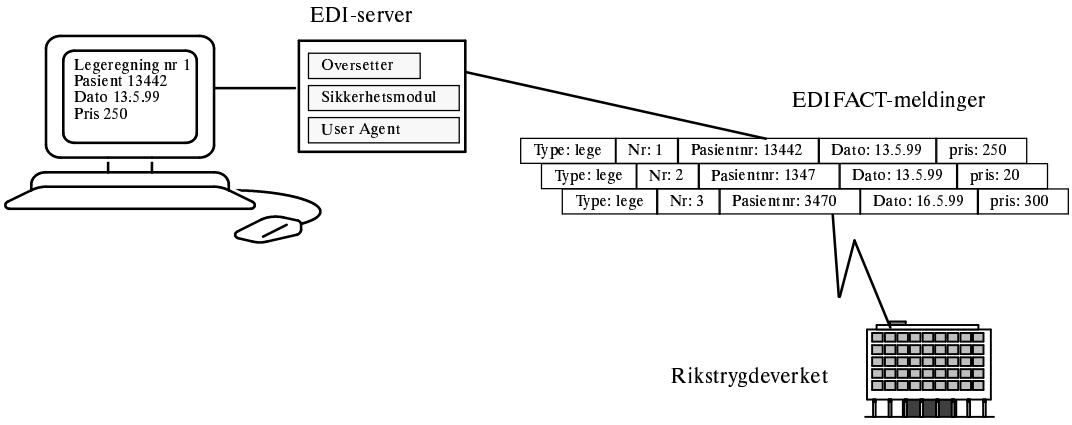
bruk saksbehandlingsverktøy integrert med arkivsystemer. Noark-4 [114] legger opp til at intern autentisering "ansees å bli tilfredsstillende ivaretatt ved Noarks automatiserte registrering av ansvarlige for utførte nøkkelaktiviteter og systemfunksjonenen for aktivitetslogging". Økstad og Grønvold mente at Noarks forslag om at arkivar kan fjerne den digitale signaturen på innkommen post og eventuelt erstatte den med arkivets signatur, vil redusere dokumentets autentisitet.

Prosjektet brukte lang tid på å analysere og samordne rutinene i departementet slik at det skulle bli mulig å ta i bruk elektroniske dokumenter og digitale signaturer. Etter min mening er det en vesentlig årsak til suksessen dette prosjektet har. EDNA-prosjektet har satt søkelyset på behovet for avklaringer på juridiske, formelle og arkivmessige problemstillinger.

1.6.5 Oversendelse av regninger til Rikstrygdeverket

Bakgrunn

Rikstrygdeverket (RTV) mottar regninger fra 250 leger og poliklinikker [84]. Det gjøres ved digitalt signerte samleforsendelser 1 - 2 ganger per måned.



Figur 4 EDIFACT-forsendelse til Rikstrygdeverket

RTV har satt ut samme utstyr til alle brukerne. Det viktigste er en EDI-server. Der blir hver regning oversatt til en EDIFACT-melding. Det lages en hash-kode over alle meldingene samlet (3 - 700 stk.) som så signeres digitalt. Dette vil si at avsender ikke signerer det som er på skjermen. Meldingene krypteres symmetrisk med en sesjonsnøkkel. Deretter sendes chifferteksten, den krypterte sesjons-nøkkelen og den digitale signaturen til Rikstrygdeverket. RTV sender en kontroll-melding tilbake om at forsendelsen er mottatt. Deretter 'pakkes' meldingen ut, men det sendes foreløpig ikke kvittering på at den videre behandlingen har gått bra. Noen leger har sine nøkler i et smartkort. Andre har det som en kryptert softwaremodul. RTV startet allerede i 1994 og fikk systemet opp i løpet av 2 år. De er sin egen TTP og har utgangspunkt i X.509 versjon 2-sertifikater. Men de har kryssertifisering mot versjon 3-sertifikater. Nye brukere kan kjøpe sine

sertifikater fra andre TTPer f.eks. Posten SDS eller Telenor. Etter pålegg fra Datatilsynet evaluerte Berdal Strømme opplegget i 1997.

Datatilsynet har godkjent den tekniske løsningen. Den skal utvides til hele landet. Sykehusene kommer til å kjøpe utstyret selv, mens det er uklart hvem som skal betale legenes utstyr. Rikstrygdeverket er i gang med kravspesifikasjon for apotekoppgjør, og de skal lage EDIFACT-meldinger for andre blanketter som er i bruk i helsesektoren.

Utfordringen er å få legene opp på et tilstrekkelig høyt sikkerhetsnivå slik at Datatilsynet godkjenner både den tekniske løsningen og den organisasjonsmessige sikkerhetspolitikken. Det kan komme EØS-krav om kryssertifisering mot utlandet. Det er Rikstrygdeverket forberedt på.

Erfaringer

Det har vært få problemer med systemet, bare 2 diskkræsj. Som Kommunal- og regionaldepartementet har de opplevd noen problemer med grensesnittet mellom kortleser og plattform. Legene er fornøyde. Oversendelsen tar fra 1 til 30 minutter avhengig av legenes maskinutstyr. Noen har 286-maskiner.

Det er krav om at regnskapsmeldinger skal lagres i 3 år. RTV lagrer meldingene i 10 år bla. for statistikk og forskning. Meldingene kopieres til nye lagringsformater hvert 3. år. De regner ikke med å ha problemer med lesbarhet eller verifisering i de 10 årene. EDIFACT-formatet har lang levetid. Ettersom det er RTV som bestemmer formater og lagrer versjoner av applikasjonene, regner de ikke med å ha problemer med å lese og verifisere forsendelsene.

1.6.6 Andre prosjekter

Det er mange offentlige etater som vurderer eller har startet arbeidet med å ta i bruk digitale signaturer. Jeg har kontaktet flere. De har ulike grunner for at bruk kan ta tid.

Løsøreregisteret

Løsøreregisteret har ikke startet med digitale signaturer. Det krever lovendring i hht. Kari Bjørkhaug, Brønnøysundreistrene [83].

Tinglysing

Justisdepartementet har ikke bestemt om de skal ta i bruk digitale signaturer i tilknytning til tinglysing [105].

Lagring av helseinformasjon

Som et ledd i programmet *Standardisering av informasjons- og kommunikasjons-systemer i helsevesenet* som ledes av Sosial- og helsedepartementet med KITH

(Kompetansesenteret for IT i helsesektoren) som sekretariat, er første del av prosjektet *Elektronisk pasientjournal (EPJ) standardisering* oversendt departementet etter at høringen er ferdig. Prosjektet startet i oktober 1998 [62].

Prosjektleder Torbjørn Nystadnes [93] påpekte ved første intervju at standarden, nå kaldt EPJark, er for langtidsarkivering der normal bruk av journalen er opphørt. De vil følge Noark og fjerne eventuelle digitale signaturer før arkivering. Men digitale signaturer på elektroniske pasientjournaler er ikke i bruk i Norge. Del 2 av prosjektet, som kommer i år 2000, vil ta opp mer rundt autorisasjon og tilgangskontroller. I hht. høringsnotatet om *Lov om helseregistre og elektronisk behandling av helseopplysninger* [126] vurderer Sosialdepartementet digitale signaturer, men trenger å avklare de juridiske problemene rundt overgangen fra papirbaserte journaler.

1.7 Oppgavens innhold

I **kapittel 2** ser jeg på egenskaper ved fysiske dokumenter og håndskrevne underskrifter som bakgrunn og utgangspunkt for hva en ny teknologi må forholde seg til. Deretter sammenlikner jeg med egenskaper ved elektroniske dokumenter og digitale signaturer, og vurderer hvordan ulik teknologi påvirker bruksmulighetene i **kapittel 3**. I **kapittel 4** går jeg gjennom lover og reglers krav i forbindelse med saksbehandling og langtidslagring, hva som fins og hva som ikke fins. I **kapittel 5** sammenlikner og diskuterer jeg hva som kreves generelt og ut fra lovverket, hvilke mekanismer som kan gi ulike løsningsalternativer, og hva det ikke er mulig å få til, spesielt relatert til langtidslagring.

Ettersom jeg tar opp mange problemstillinger, har det vært naturlig å kommentere funn underveis og trekke konklusjoner i hvert kapittel. Et sammendrag av mine viktigste konklusjoner kommer i **kapittel 6**. Noen av hovedbegrepene i oppgaven er utdypet i **Appendiks A**. **Referanselista** starter på side 150. I **Ordboka** har jeg definisjoner av ord, begreper og forkortelser. Til slutt er det et **stikkordregister**.

Under kirsebærtreet
i måneskin:
Ei kvinne
med eit brev i fanget

Blad frå ein austleg hage. 100 haiku dikt. 1965

2 Fysiske dokumenter og håndskrevne underskrifter

Papir har vært vår hovedmåte å lagre informasjon på gjennom mange hundre år. Underskrift har vært måten å vedkjenne seg innholdet på. I dette kapittelet prøver jeg å finne egenskaper som skal kunne leve videre når man tar i bruk ny teknologi. Det danner utgangspunkt for sammenliking med digitalt signerte dokumenter.

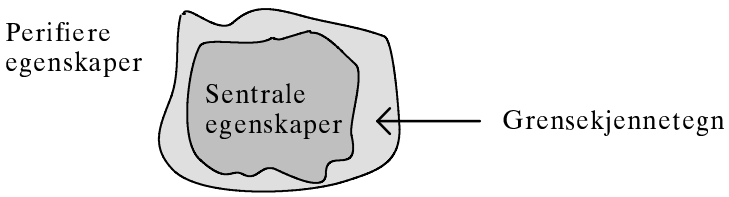
2.1 Egenskaper ved et fysisk dokument

Først ser jeg på egenskaper ved dokumenter som sådan. Jeg ønsker å finne ut hvilke av dem som er knyttet til den 'fysiske teknologien' som papir representerer og hvilke som er mer generelle. Noen egenskaper vil være mer relevante for oppgavens problemstilling enn andre. Derfor studerer jeg dokumenter i en kontekst: Hvem behandler dem og når er de tilgjengelige.

2.1.1 Sentrale, perifiere og grenseegenskaper

Hva slags egenskaper er bestemmende for likheter og forskjeller mellom fysiske og elektroniske dokumenter? For arvinger er det sentralt at testators underskrift er ekte og at testamentets innhold går i deres favør. For en jurist er det viktig at underskriften står nederst på arket, og derved forholder seg til hele innholdet, og mindre viktig hvordan arven fordeles. For en skriftekspert er det sentralt å kunne overbevise retten om at underskriften er ekte. Testamentets innhold er perifert. Grenseegenskaper ligger i den ofte uklare overgangen mellom sentrale og perifere egenkaper.

I artikkelen "Borderline Issues: Social and Material Aspects of Design" av Brown og Duguid [16] tar forfatterne opp at ulike interessenter kan ha ulikt syn på hva som er viktig ved et bestemt artefakt, et laget produkt.



Figur 5 Senter - periferi - grenser

Forfatterne påpeker at tekst, mer enn andre artefakter, kan vurderes uavhengig av hvilken kontekst den er del i. En tekst kan leses i badet eller i et fly. Men ofte er sammenhengen viktig. En flyvertinne på arbeid reagerer annerledes på en lapp der det står: "Dette er en flykapring", enn en som leser det samme i en bok hjemme.

Egenskaper ved et offisielt dokument kan være skrifttype, sideoppsett, institusjonens logo, farge og kvalitet på papiret, hvor dypt trykket og underskriften går i papiret. Dette er egenskaper som man ikke tenker på så ofte. De er med på å sikre at mottakeren av et dokument aksepterer det som ekte, når dokumentet har forflyttet seg fra avsender og/eller leses på et seinere tidspunkt.

Når teknologiutviklingen fjerner sentrale fysiske begrensninger/rammebetingelser ved et artefakt, kan den også fjerne aksepterte sosiale kjennetegn ved det. En begrensinng som ikke fins i særlig grad lenger, er vansker med å kopiere fysiske dokumenter. Etaters brevhoder kan kopieres. Aksepterte underskrifter kan kopieres. En leser av et dokument kan ikke lenger ha den samme tilliten til at dokumentet er ekte eller ikke endret.

Forfatterne setter opp 2 egenskaper ved grensekjennetegn som er nødvendige for at noe skal tilhøre grensen for et artefakt.

1 Et fysisk grensekjennetegn må bestå over tid. Hvis et sett av kjennetegn som løselig er med på å avgrense en genre, splittes eller brukes oppdelt over tid, kan det være uttrykk for at en ny genre oppstår. Det kan også være uttrykk for at kjennetegnene ikke lenger er essensielle for å definere genren.

Dette er problemstillingen vi opplever ved å gå fra fysiske dokumenter til elektroniske dokumenter.

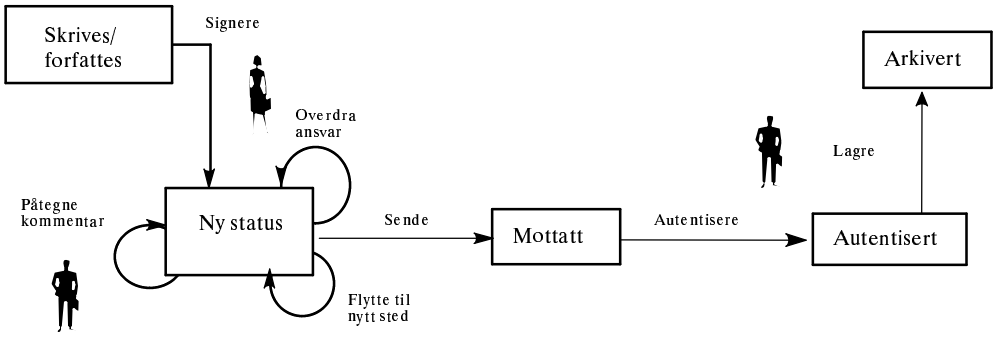
2 Den sosiale egenskapen ved et artefakts grense er at den forståes i en sosial sammenheng. Et artefakt, dets grense, dets genre og dets bruk og konvensjoner rundt bruk, må forstås i relasjon til de faktiske brukerne. Endringer i bruk behøver ikke nødvendigvis å være alvorlige, men de kan sende uforutsigbare bølger av konsekvenser også utenfor det samfunnet der artefaktet brukes.

De som utvikler SLN-systemet, System for ligning av næringsdrivende, se punkt 1.6.3, har egne ideer om framtidig bruk, men de vet lite om hvordan det faktisk kommer til å bli brukt. F.eks. kan innrapporteringen medføre endrete arbeidsrutiner i bedrifter som skal rapportere, i tillegg til at de går over til digitale signaturer. Arbeidsrutiner hos brukerne kan oppfattes som en grenseegenskap ved systemet av utviklerne.

2.1.2 Heterogene aktør-nettverk

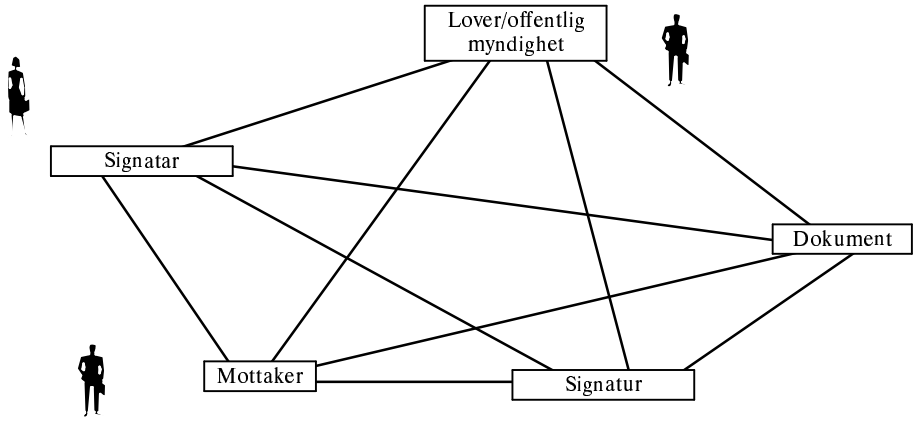
Tone Sandahl (USIT) skriver i sin doktoravhandling *From Paper to Digital Documents* [117] om arbeidspraksis som et heterogent aktør-nettverk. Med heterogent mener hun at både mennesker og artefakter inngår i nettverket. Arbeidspraksisen er forenklet og representert på en slik måte at det framhever hvordan aktantene, mennekskelige aktørerer og artefakter, er knyttet sammen for

å oppnå et bestemt mål. I *What do artifacts mean to us in work?* [66] skriver Sandahl og Lundberg at dokumenters fysiske beskaffenhet og synlige tilstedeværelse gjør dem til en aktant som koordinerer arbeidet ved å indikere 'hvem som holder dokumentet'. Dokumentet kan sees som en aktant når det får andre til å handle eller handler selv. Papiret opptrer som et tegn som skifter status avhengig av hvor det fysisk er plassert og hvem som har ansvaret for det.



Figur 6 Tilstandsdiagram for et fysisk dokument

Sett fra dokumentets side, får det en ny status og en kraftigere ladning [64] når det blir signert, når det får påtegning av en overordnet og når det autentiseres hos mottaker. Menneskene som utfører handlingene overfor dokumentet, skifter også status ettersom de er del av det heterogene nettverket. Den som signerer, blir signatar. Den som mottar dokumentet, blir ansvarlig for en videre behandligen av det.



Figur 7 Eksempel på aktanter rundt et signert dokument

I forbindelse med et signert fysisk dokument er det få aktanter og kjent interaksjon mellom dem, i motsetning til situasjonen rundt et signert elektronisk dokument, jf. Figur 14, s. 80. Selv om det fysiske dokumentet er skrevet på en PC, er PC'en uinteressant i denne sammenhengen. Juristen Peter Seipel [122] hevder at papir er en passiv informasjonsbærer. Dette ser ut til å stå i motstrid til dem som støtter aktør-nettverksteorien, f.eks. Sandahl [117].

2.1.3 Tilgjengelighet

Papir og blyant, eller tilsvarende, er lette å frakte med seg. Et fysisk dokument kan skrives og leses hvor som helst man vil. Det leses med øynene uten andre

hjelpemidler. Det er et tilgjengelig, direkte medium. Det er lett å lære hvordan man lager dokumentet og hvordan man bruker det.

Dokumentet kan oppbevares så lenge informasjonen på papiret er lesbar. (Imidlertid fins det nå mange dårlige papirkvaliteter som forkorter dokumenters levetid.) Det kan gjenfinnes, selv om det tar tid å finne det i store dokumentmengder. Ved lagring skaper arkivarer indekser og føyer nøkkelord til dokumentene for å lette gjenfinning. Alle disse egenskapene gir tillit til papir som medium for langtidslagring av dokumenters innhold.

2.1.4 Egenskaper ved en original

En original varer den tiden dokumentet eksisterer. Det er ikke noe man tenker særlig over. Det er bare sånn. Dvs. vanligvis vil tidsaspektet ved et fysisk dokument være en grenseegenskap. I hht. Seipel [122] er tid et begrep som i juridisk sammenheng brukes i forbindelse med bevisfunksjoner, og når rekkefølgen på transaksjoner, tidsavgrensninger og vilkår knyttet til tid er av interesse.

Ordet original nevnes lite i lovene. Det er nesten selvsagt når man har å gjøre med signerte dokumenter. Originalitet innebærer at dokumentet er ekte ved undertegningstidspunktet og at det er ekte og uendret i all ettertid. Papiret er bevismateriale per se [36].

Håndskrevne dokumenter er originaler. Utskrifter fra datamaskiner kan man ikke se om er originaler eller kopier. Juristen Rolf Riisnæs, Institutt for rettsinformatikk (IRI) påpeker at alle dokumentene som printes, er med på å svekke tilliten til papir som medium [98].

På kopier ser man vanligvis at underskriften er kopiert, eller det står at dokumentet er en kopi som også er signert. Et tredje alternativ er at alle undertegnede kopier regnes som originaler med samme bevisvekt.

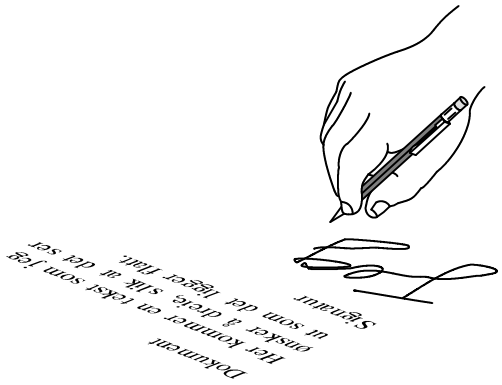
Latour [65] beskriver (*fysiske*) dokumenter som "uforanderlige mobiler". Mobilitet tillater dokumentene å være informasjonsformidlere mellom steder og i mange ulike situasjoner. Uforanderlighet tillater dem å overleve i både tid og rom.

2.2 Underskrifter

Underskrifter hører til personer. De brukes i ulike situasjoner, og man kan ha ulike roller og ansvar når man undertegner: saksbehandler, testator, dommer.

2.2.1 Egenskaper ved en signatur

En signatur identifiserer og er knyttet til en person. En signatur knytter seg til dokumentets innhold ved en kjemisk forbindelse mellom blekket og papiret [29]. Hvis man skal verifisere et fysisk dokument, må man vurdere både om dokumentets innhold er ekte og om signaturen er ekte.



Håndskrevne signaturer baseres på

- noe man er
- noe man kan (skrive signatur).

Juristen David Fillingham [28] påpeker at en håndskreven underskrift ikke har problemer med alder. Den er i sitt vesen biologisk knyttet til et bestemt individ for livstid og i all ettertid. Det samme påpekte juristen Roger Henriksen allerede i 1980 [36].

2.2.2 Signaturers juridiske funksjoner

Juristene Andreas Galtung og Rolf Riisnæs (IRI) skrev om rettslige aspekter ved digitale signaturer [31] i 1994, som del av prosjektrapporten om Meldingssikkerhet fra Norsk TEDIS.

De påpekte at det er delte meninger om hva ulike funksjoner kan innebære, men valgte å framheve de følgende:

a) I **identifiseringsfunksjon** ligger det at signaturen knytter et dokument til innehaveren av signaturen. De personlige elementene i den håndskrevne signaturen er med på å fastslå identiteten til underskriveren
b) I **bevisfunksjonene** ligger det at en underskrift på et dokument kan brukes som bevis i en rettssak.
c) En underskrift har **autentiseringsfunksjon** ved at den står under et dokuments innhold.
d) En signatur kan f.eks. understreke alvoret i en handling og har da mer av en **symbolfunksjon** enn en bevisfunksjon.
e) Underskrifter brukes til å avslutte prosesser, f.eks. forhandlinger og har da en **avslutningsfunksjon.**

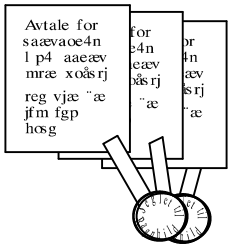
ISTEV (Istituto per lo Studio della Vulnerabilità delle Società Tecnologicamente Evolute) Italia, [52] har ført opp tilsvarende funksjoner. De knytter den sosiale verdien ved signering til punkt d), som de kaller en seremonifunksjon. De oppsummerer at en signatur attesterer det faktum at en person

- På et tidspunkt,
- Har vært på et gitt sted,
- Med intensjonen om å godkjenne/vedkjenne seg forfatterskapet av teksten,
- Med intensjonen om å knytte seg til en tekst skrevet av andre,
- Med intensjonen om at en part / et selskap er bundet av innholdet i en signert kontrakt.

2.2.3 Parafering

Å parafere er å medunderskrive et dokument som alt er underskrevet, en bekreftelse [12]. Flere personer kan signere samme dokument. De kan gjøre det samtidig, f.eks. ved en seremoni. I andre sammenhenger er rekkefølgen på signaturene viktig. En revisor skal signere regnskap etter at styremedlemmene har signert.

Signaturer avløste signeter da underskriverne lærte å skrive. Det fins gamle dokumenter der alle som inngikk avtale, signerte og festet sammen alle sakens dokumenter med snorer og alle signatarenes lakksegl [139].



2.2.4 Påtegning

Legen og filosofen Marc Berg skriver i sin artikkel *Medical Work and the Computer-Based Record: A Sociological Perspective* [9] om medisinsk arbeid som en kognitiv prosess der man samler 'observasjoner', der diagnostiske hypoteser testes og der avgjørelser om behandlingsmetoder tas. Pasientjournalen blir et verktøy og en informasjonsdatabase i den forbindelse. Alle helsearbeiderne påfører sine notater og resultater for å framskaffe et helhetlig bilde av pasientens situasjon.

På samme måte kan forarbeidene til et brev eller en utredning i det offentlige få påtegninger fra flere saksbehandlere og ledere før det endelige resultatet foreligger. Påtegningene plasseres fritt på dokumentene med ulike håndskrifter og muntlige formuleringer. Det gir den mottakende forfatteren en større informasjonsmengde enn om alt var skrevet på skrivemaskin på egne ark. Denne funksjonaliteten kan det foreløpig være vanskelig å gjenskape elektronisk.

2.3 Autentisering

Det som er autentisk, regnes som fullt ut ekte og pålitelig [12]. De som bruker dokumenter, trenger å vite at dokumentene er ekte og uforandret etter underskriving, at personen som undertegnet var klar over handlingen, at det fins måter å verifisere dokumenter på og at det fins instanser å henvende seg til i tilfelle en tvist om dokumentet oppstår.

2.3.1 Autentisere underskriver og kilde

Autentisering er prosessen med å bekrefte en oppgitt identitet. Det kan også beskrives som å bevitne, bekrefte ekthet, [139]. Identifisering har flere tolkninger, f.eks. fastslå hvem en person er, gjenkjenne, [139]. Begrepene står mer utførlig omtalt i appendikset s. 124.

Jurister setter begrepet autentisering inn i sín sammenheng. *The whole procedure of certifying the existence and modalities of the legal act can be described as "authentication",* ICRI (Faculty of Law, University of Leuven) [25]. Henriksen [36] definerer autentisering som "the act of referring", altså overføringen av en

fordring. Ved signering av en sjekk overdrar man en fordring fra egen bankkonto til den man utsteder sjekken til.

Henriksen skriver at de fysiske egenskapene ved et papir er irrelevante i internasjonal handel, hvis man ikke vet hvem som har satt fram fordringene i et dokument. Minimumskunnskapen man trenger er dokumentets opphav, hvor og hvem det kommer fra.

Det er vanskelig å autentisere et dokument som ikke er signert [25]. Det kan bare skje i sanntid ved direkte overlevering og visning av legitimasjon. Det er også vanskelig å autentisere et underskrevet dokument i ettertid. Signaturer sjekkes først når det oppstår en tvist. De færreste har en samling av andre folks signaturer for sammenlikning. Vi simpelthen antar at når vi mottar et dokument signert av en person, så tilhører signaturen personen [25].

Om en håndskreven underskrift ansees gyldig avhenger av og varier med hvem som autentiserer den: En mottaker av dokumentet eller en skriftekspert.

Et underskrevet brev med brevhode viser hvor dokumentet kommer fra: institusjonen, signaturen og eventuelt signatarens myndighet, rolle.

Entitetsautentisering er et begrep som brukes i sammenheng med informasjonssikkerhet. Det er en bekreftelse på at en entitet (en enhet, f.eks. et menneske, et dokument eller en maskin) er den den påstår å være på et gitt tidspunkt. For fysiske dokumenter gjelder en slik autentisering så lenge dokumentet eksisterer.

2.3.2 Ikke-benekting

Ved å signere et dokument manifesterer forfatteren sin intensjon om å forplikte seg til noe. Det er vanskelig å unndra seg en håndskreven underskrift, hvis man ikke kan bevise at den er forfalsket eller at dokumentet er endret i ettertid.

2.3.3 Dataintegritet

Dataintegritet er egenskapen at data ikke har blitt endret eller slettet på en uautorisert måte [41]. For å sikre informasjon mot uautorisert endring, brukes papir som informasjonsbærer. Selv om preging av informasjon på papir ikke garanterer dataintegritet, kan endringer oppdages [25]. En forfatter forsikrer om meldingens korrekthet ved å undertegne ved slutten av teksten. Består dokumentet av flere sider, kan alle sidene signeres. Endring av et papirdokument trenger likevel ikke være spesielt vanskelig uten at signaturen endres.

2.3.4 Forfalskning

Underskrifter ble brukt av romerne for å autentisere testamenter allerede i år 439 [28]. I år 539 laget de en lov om hvordan skrifteksperten skulle arbeide og uttale seg i tilknytning til forfalskning.

Tegn på falsk underskrift kan være: Signaturen er skrevet med en hastighet som er signifikant saktere enn den genuine underskriften, ofte skifting av grep mens man

skriver, stumpe begynnelser og ender, dårlig, ubesluttsom og skjelvende skriftkvalitet, overlappende skrift, skriften stopper på steder den skulle vært flytende.

En signatur på et dokument nyter tillit i vårt samfunn [132]. Det gir kanskje ikke så høy sikkerhet som ønskelig, men det er den enkleste og mest brukte måten. Dersom en person undertegner siste side i et 10 siders trykket dokument, kan andre lett forfalske de første 9 sidene.

Det er nokså lett å se endringer og forfalskninger ved et *håndskrevet* dokument. Beløpet på en sjekk må skrives både med tall og med bokstaver for å hindre forfalskning. Forfalskning kan også være å lage kopier av noe som skal være unikt. For sjekker brukes det spesielt papir som det ikke er så lett å få tak i. Det vanskeliggjør kopiering.

2.3.5 Sikker dato

Ved langtidslagring av dokumenter er det viktig å vite når dokumentet ble undertegnet. Det fins ikke spesielle verktøy for dette. Tekniske data ved papir, trykk etc. kan indikere tidsperiode for signering. Sakspapirer har vanligvis dato for signering. Det gir hjelp til å bestemme når noe ble avgjort dersom det oppstår en tvist. Dokumentet kan eventuelt datostemples og registreres hos Notarius Publicus. Det kan sendes rekommandert slik at man får kvittering for avsendingsdato. Mottatt dato kan journalføres av mottakende institusjon.

2.3.6 Verifisering

Å verifisere er å undersøke og fastslå riktigheten/ektheten av noe. Verifisering av fysiske dokumenter er ikke alltid enkelt. Man må ofte lete i gamle referater eller sakspapirer for å bestemme om en person hadde myndighet/autorisasjon til å signere en viss type dokumenter. Dvs. det kan ta tid å spore hva som har skjedd.

En underskrift ser "likedan" ut samme hvilken rolle man har som underskriver. Verifisering kan gjøres enklere og sterkere ved å sende et dokument til en Notarius Publicus og få det stemplet, eller f.eks. ved å ha en signeringsseremoni ved inngåelse av avtaler.

2.4 Egenskaper som blir synlige i bestemte sammenhenger

Dokumenter eksisterer i en eller flere sammenhenger, i kontekster. Hvorfor er noen dokumenter så viktige at de signeres? Både innholdet og situasjonen rundt dokumentet kan danne grunnlag for undertegningen. En signatur kan gi et dokument en avgrenset gyldighetsperiode (sertifikat) eller til 'evig' tid. Det kan danne grunnlag for uenighet. I en tvistesituasjon er det interessant å se hvilken rolle dommeren har i forhold til et signert dokuments ekthet og hvordan han løser tvisten.

2.4.1 Sosial forståelse for det å undertegne

Når man underskriver et dokument, er det en indikasjon på "endelighet" ved dokumentet. Man er klar over at man skriver sitt navnetrekk på noe. Man er

også innforstått med at man i visse situasjoner (f.eks. ved et salg) utfører en juridisk handling som binder teksten sammen med underskriften.

ICRI [25] påpeker at for at signaturen skal være juridisk bindende, må signataren forstå signeringsteknikken som en sosial seremoni der hun vet at hun binder seg juridisk ved å signere. Dette kaller de den sosiale meningen med å undertegne.

2.4.2 Påvirkning av underskrivingsprosessen

Noen ganger har man vitner ved undertegning av et dokument.

- En testator undertegner i vitners nærvær slik at de kan bekrefte at undertegningen skjedde av fri vilje og av rett person.
- Undertegning av traktater gir uttrykk for seremonier.

Håndskrift på et fysisk dokument gir en binding mellom pennen og papiret og hindrer klussing med underskrivingsprosessen. Man ser det man skriver under på og vet at det ikke fins skjult tekst eller liknende.

2.4.3 Gyldighetsperiode

I hht. ICRI [25] er god autentisering karakterisert ved at et undertegnet dokument er autentiserbart så lenge den juridiske handlingen dokumentet representerer, er av rettslig betydning. Dvs. den rettslige betydningen avhenger av at dokumentet er lesbart så lenge det trengs. Hvis det etter en tid ikke lenger er mulig å autentisere den juridiske handlingen, så vil man miste tillit til handlingen. Et flekket, brettet, gammelt sertifikat med svakt trykk kan man kan man tenke seg er forfalsket hvis føreren av bilen er ung.

2.4.4 Tiltro til forsvarlig lagring

Allmennheten bør kunne ha tiltro til at arkiver drives i samsvar med lover og regler, og de skal kunne ha tillit til at arkivene driftes på teknisk forsvarlig vis [6]. Mht. Riksarkivet og Statsarkivene så har nok de fleste den tiltroen. De fleste dokumenter som man vet er lagret i arkiver, finner man igjen.

2.4.5 Personvern

Selv om det lagres personinformasjon på papir, er den vanskelig å sammenstille hvis kildene er langt fra hverandre fysisk. Brev går oftest i lukket konvolutt. Det vil si at informasjonen vanligvis bare er tilgjengelig for dem som skal se den.

2.4.6 Tvister

Effekten av en underskrift vil variere med hvilken lov den vurderes mot. Henriksen [36] skriver at signaturen:

- Ofte betraktes som en bekreftelse på et dokuments autentisitet,
- Gir støtte til antakelsen om at den som signerte også er ansvarlig for at dokumentet er korrekt og/eller komplett.

Den som skal vurdere et dokument i et tvistemål, skal kunne forstå hva vurderingen går ut på. I Norge har vi fri bevisføring og bevisvurdering på fritt grunnlag. Det innebærer at de som skal overbevise dommerne, kan føre de bevis de ønsker. Men det innebærer også at resultatet er avhengig av at dommeren forstår hva det dreier seg om.

Dommere er vant med å forholde seg til papir. De vet at underskrifter binder underskriveren til dokumentets innhold.

2.5 Sammendrag

Fysiske dokumenter med håndskrevne underskrifter har innebygget at papiret binder underskriften både til dokumentets innhold og til signataren. Dokumentene er lette å bruke for de ulike interessentene: Forfatteren, leserne og eventuelt dommeren i en tvistesak. De er bestandige over tid og rom og kan leve i mange hundre år hvis papirkvaliteten er god. Det kan ta tid å finne dem igjen i store arkiver. Det er ikke så lett å verifisere ektheten av dem verken i sanntid eller i ettertid.

Tabell 2 Egenskaper ved håndsignerte fysiske dokumenter

Egenskap	**Fysisk dokument med signatur**
Autentisering av kilde	Signatur + f.eks. brevhode
Ikke-benekting	Signatur
Dataintegritet	Signatur på alle ark.
Lenke mellom verktøyet og dokumentet	Signere selv på dokumentet.
Vanskelig å forfalske	Nei
Gyldig så lenge den juridiske handlingen er viktig?	Papir og håndskrift varer over tid
Lett å verifisere?	Nokså lett ved personlig overlevering. Krever legitimasjon og skriftprøve. I ettertid er det vanskelig.
Autentisering av signataren	Krever legitimasjon og skriftprøve
Tidfesting	Ja. Dokumenter med dato kan sjekkes med en gang. I ettertid trenges det datostempel fra Notar i et åpent miljø.
Lesemåte	Med øyet
Forståelse for hva det vil si å undertegne	Ja, lett å forstå, innarbeidet 'kultur'.

2.6 Konklusjoner

Det er en utfordring å vurdere om egenskapene ved dokumenter og underskrifter kan tenkes avhengig eller uavhengig av den fysiske teknologien som papir og penn representerer.

2.6.1 Ønskete egenskaper ved elektroniske dokumenter

Dersom man skal langtidslagre signerte dokumenter elektronisk, mener jeg at man bør søke etter mekanismer for følgende egenskaper:

a) Et dokument skal kunne skrives og leses der man er og der man vil,
b) Et dokument skal kunne finnes igjen og leses så lenge det oppbevares,
c) Man skal når som helst kunne undersøke om innholdet er endret eller ikke,
d) Man skal når som helst kunne vurdere om endringer er utført i henhold til autorisasjon,
e) Alle endringer skal være sporbare,
f) Det skal når som helst være mulig å bestemme når dokumentet ble skrevet,
g) Det skal når som helst være mulig å bestemme hvem som signerte dokumentet,
h) Det skal ikke være mulig å benekte at man har undertegnet,
i) Den som signerte, skal være klar over at vedkommende faktisk signerte og bandt seg juridisk ved handlingen,
j) Ingen skal kunne påvirke underskrivingsprosessen,
k) Dokumentet skal være gyldig så lenge det er juridisk aktuelt at det er gyldig,
l) Allmennheten skal kunne ha tiltro til at lagring skjer på forsvarlig måte,
m) Den som skal vurdere et dokument i et tvistemål, skal kunne forstå hva vurderingen går ut på.

Noen av egenskapene gjelder informasjon generelt, men de fleste har å gjøre med informasjon som er koplet sammen med en underskriver/forfatter. Andre karakteristika ved egenskapene er tidsperspektivet og bevisstheten hos aktørene (underskriver, leser, dommer) om at de har et forhold til informasjonen. Dette er egenskaper som kommer i tillegg til dem man vanligvis tenker på i forbindelse med å underskrive dokumenter.

"It is certainly an idea you have there," said Poirot, with some interest. "Yes, yes, I play the part of the computer. One feed in the information ----".

"And supposing you come up with all the wrong answeres?" said Mrs. Oliver.

"That would be impossible," said Hercule Poirot. "Computers do not do that sort of a thing."

Agatha Christie: *Hallowe'en Party* 1969

3 Elektroniske dokumenter og elektroniske signaturer

I dette kapittelet ser jeg på karakteristika ved elektroniske dokumenter og sammenlikner med fysiske dokumenter. Jeg ser på om noen av egenskapene er spesielle for den elektroniske teknologien. Etterpå går jeg inn på ulike autentiseringsmetoder og vurderer egenskapene deres mot hverandre og mot ønsket funksjonalitet. Fordi teknologien er ulik for fysiske og elektroniske dokumenter, vil strukturen i dette kapittelet avvike noe fra det foregående.

3.1 Definisjon av elektroniske dokumenter

Det fins mange definisjoner, som kan forstås på ulike nivåer, f.eks.:

- "En avgrenset og sammenhengende informasjonsmengde, framstilt for et bestemt formål. Informasjonen kan bestå av av en kombinasjon av tekst, data, grafikk, bilder og multimedia. Et dokument kan også bestå av flere dokumenter (sammensatte dokumenter)" [130].
- "En speciel bitkombination i sammenhæng med et regelsæt, som muliggør læsning heraf" [59].
- "..a data carrier and the data recorded on it, that is generally permanent and that can be read by man or machine" (ISO 2382/4) [142].

ISTEV [52] beskriver et elektronisk dokument som informasjon preget (imprinted) på et magnetisk medium og at det når som helst kan fjernes, endres eller skrives om. Det er ikke alltid tilfelle. Man kan skrive filer til en CD-ROM-plate uten å kunne endre informasjonen på annen måte enn å ødelegge den ved å skrive over.

Ikke alt som skrives på datamaskiner, blir til elektroniske dokumenter. Informasjon som skrives på en datamaskin og deretter printes ut på et papir, regnes ikke som et elektronisk dokument. I den sammenhengen er datamaskinen å betrakte som en skrivemaskin.

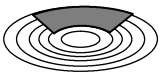
3.2 Egenskaper

Når papir og penn forsvinner, hva har man i steden? Hvilke nye egenskaper gir den nye teknologien? Hvilke egenskaper og karakteristika er felles for fysiske og elektroniske dokumenter?

3.2.1 Digitalisering

"A bit is a bit is a bit" skriver juristen David Masse fra Canada [67]. Digitalisering av informasjon er en enkel prosess. '0' og '1' er vanskelige og tidkrevende å lese, men lette å prosessere maskinelt. Informasjon i digital form kan lages, lagres, kopieres, skrives ut og overføres lett og raskt i store mengder. Dette gjelder ikke bare tekst, men også visuell og auditiv informasjon. '0' og '1' sier ingen ting i seg selv. De gir mindre informasjon visuelt enn 'a' og 'b'.

Rekkefølgen på bitene bestemmes av den som produserer informasjonen og har med intensjonen for bruk av informasjonen å gjøre. Voges skriver at intensjonen må deles av forfatter og leser. Det gjøres bl.a. ved at de bruker kompatible systemer for maskinvare, programvare og kommunikasjon [144]. Den faktiske representasjonen av hvert bit blir derfor vesentlig. Om man bruker ASCII i steden for EBCDIC, får konsekvenser for kommunikasjonen.



Et elektronisk dokument har ikke en fast fysisk tilknytning. Typer medier som bit-ene fins på, eller hvor på et medium de fins, er underordnet så lenge mediene ikke er flyktige, men kan holde på informasjonen en tid. Dette gjelder både lagringsmedier og medier for å vise/lese informasjonen, f.eks. skjermer. Dette er vesentlige forskjeller fra fysiske dokumenter og er det som gjør det lett å kopiere elektroniske dokumenter.

I boka *Hva datamaskiner ikke kan* [54] skrev forfatterne Jervell og Olsen i 1984 at data lagret på EDB-lesbar form kan *behandles* i langt større omfang og på en kvalitativt annen måte enn data lagret på papir. Elektroniske leksika kan ajourføres umiddelbart i motsetning til leksika i bokform. Andre egenskaper de nevner, er overføringen over store avstander av store datamengder på kort tid. Til forskjell fra papir, kan avsender og/eller mottaker også være maskiner.

Jervell og Olsen påpekte at informasjon og data ikke nødvendigvis er det samme. Forfatterne setter opp formelen $I = k \times D$. I er informasjon, D er data og k er en faktor mellom 0 og 1. Den avspeiler hvor personavhengig informasjonsinnholdet i dataene er. Teksten "En mikromaskin er en liten datamaskin, bygget opp omkring en mikroprosessor" gir lav k for fagfolk og en høyere k for ikke edb-kyndige. Dette er felles problemstillinger for fysiske og elektroniske dokumenter. Det spesielle inntreffer ved lagring og gjenfinning av informasjon. Siden man kan søke i fritekst i kjempestore datamengder, blir lagringsmåte og struktur viktigere enn for fysiske dokumenter. Ved søking i fritekst, f.eks. på Web, får man ofte for store datamengder som svar. Da blir det vanskelig å finne informasjonsinnholdet man søker. Man kan ønske seg en ekspert til å strukturere dataene for seg.

3.2.2 Dokumentet i tid og rom

Brown og Duguid [16] hevder at Bruno Latours definisjon [65] av dokumenter som "uforanderlige mobiler", j.fr. pkt. 2.1.4, ikke er interessant eller gyldig for elektroniske dokumenter. Elektroniske ordbøker og kataloger er frigjort fra bokinnbindingen som avgrenser de tilsvarende fysiske dokumentene. Er dermed

“uforanderlige mobiler” et unyttig begrep, eller gjelder det å finne mekanismer som gir tilsvarende egenskaper? Et digitalt signert dokument må være uforanderlig så lenge signaturen ’lever’. Dvs. bit-representasjonen må være uforanderlig. Men et slikt dokument flyttes ikke. Det er ikke mobilt slik fysiske dokumenter er. Informasjonsinnholdet og informasjonen om dokumentet sendes som pakker over nettet, og det framstilles et eksemplar, en kopi, hos mottakeren. Det vil si at dokumentet ikke flyttes, det kopieres.

Ved langtidslagring er det nyttig/nødvendig å lagre dokumentets tilstand eller status. Tilstanden tilkjennegis av dokumentets omgivelser. Dette er informasjon knyttet til produksjon, lagring og verifisering av dokumentet, f.eks. tekstbehandlingsverktøyet som ble brukt, algoritmen som ble brukt til signering og sertifikatet knyttet til den offentlige nøkkelen. Hvis sertifikatet fins på en tilbakekallingsliste, sier det at sertifikatet ble ugyldiggjort. Videre kan tidspunktet fortelle om signaturen var gyldig eller ugyldig ved signeringstidspunktet. Det at en såpass stor del av dokumentets statusinformasjon lagres utenfor dokumentet selv, er en vesentlig forskjell fra fysiske dokumenter.

Der man har tilgang til en datamaskin, kan man lage og lese elektroniske dokumenter. Dokumenter kan finnes og leses igjen relativt lett, selv om de lagres i lang tid, så sant man har formater som datamaskinene kan behandle, og kunnskaper om bruken av maskinene. Men man trenger maskiner i tillegg til øyne som ser. Det skaper helt andre utfordringer for langtidslagring enn de man har for fysiske dokumenter.

Et kjennetegn for elektroniske dokumenter er at de kan kopieres. Ut fra et eksemplar er det vanskelig å bestemme om dét er originalen, det intenderte, ekte dokumentet. Kopiene vil være jevngode med originalen hvis man ikke gjør noe spesielt med originalen. Når det gjelder programvare, har utviklerne begynt å signere sine programmer slik at kjøpere kan verifisere ektheten. Det er vanligvis umulig å bestemme tidspunktet for når et dokument ble laget. Det er ikke vanlig å logge hvert tastetrykk for å spore tidspunkt for endringer. Et digitalt signert elektronisk dokument kan si noe om når signaturen ble påført, j.fr. punkt 3.6.4, men ikke når dokumentet ble forfattet.

En elektronisk forsendelse er mer effektiv og koster mindre enn å bruke telefon, frimerker, og/eller tid ved bruk av overflatepost.

For fysiske dokumenter må alle som undertegner ved en seremoni, være tilstede samtidig for at symbolfunksjonen og avsluttningsfunksjonen skal ivaretas. For elektroniske dokumenter mener jeg dette er teknisk mulig vha. f.eks. en videokonferanse der alle har tilgang til det samme dokumentet fra egen maskin, og signerer etter tur. Men digitale signaturer støtter ikke alle formkrav (oppsett av dokumenter med felter som skal fylles ut, brevhoder, underskrift nederst på arket osv.). F.eks. er det ingen mening i å si at digitale signaturer skal plasses nederst på arket. En digital signatur er et tall beregnet ut fra dokumentet og en privat nøkkel, men tallet behøver ikke å plasseres på dokumentet. Det kan lagres separat.

3.2.3 Gjenfinning

Et dokument skal kunne finnes igjen så lenge det oppbevares. Det innebærer at arkivarer må kunne tilføye informasjon som gir mulighet for gjenfinning. Det må finnes mekanismer som finner og henter fram dokumenter. Dette kan være roboter for fysisk henting av lagringsmedia. Det kan være datamaskiner for lagring og søking. Dokumentene må eventuelt kunne konverteres til nye medier og nye formater når de gamle blir uaktuelle. Det må finnes mennesker med kunnskaper om å betjene mekanismene og maskinene.

Dokumenter som langtidslagres, skal ikke endres i innhold eller form (hvis formen er vesentlig). De må kunne gjenskapes via maskin til en skjerm e.l. slik at de kan leses også i ettertid. Dokumentene må være lagret i slike formater som de aktuelle maskinene kan bearbeide.

3.2.4 Originalitet

Henriksen [36] påpeker at det blir vanskelig å snakke om originalt datainnhold i et elektronisk dokument. Papirets egenskap som varig bærer av informasjon er ikke lenger til stede. Avsenderen har fortsatt sin kopi av det oversendte. En mottaker av et dokument vil ikke kunne vite om dataene på skjerm eller som utskrift er det som originalt ble skrevet, eller om innholdet er endret.

Elektroniske dokumenter eksisterer så lenge det fins en kopi. Det er forskjell på om noe er autentisk (ekte) eller om det er unikt (fins i ett eksemplar). For noen dokumenters vedkommende er det viktigste at de er ekte samtidig som de kan eksistere i flere eksemplarer, jf. 4.1.6. Negotiable dokumenter (f.eks. aksjer) og betalingstransaksjoner skal bare eksistere i én utgave. Å bestemme om et negotiabelt dokument er det dokumentet man handler ut fra, foreslår jeg kan gjøres i to trinn. I dokumentet setter man navnet og sertifikatet til den man overdrar dokumentet til. Deretter signerer man. Den som deretter har dokumentet, må kunne verifisere at vedkommende er den som navngis i teksten. Et annet alternativ er å registrere en tidsstemplet og serienummerert kopi hos en notar.

3.2.5 Forfatterskap

For fysiske dokumenter kan man presentere et dokument med underskrift og si "dette har jeg forfattet". Det gir ingen spesielt stor tillit. For elektroniske dokumenter gir det enda mindre grunn til tillit ettersom det er lett å framstille kopier på mange maskiner og servere. For å kunne si at dette elektronisk dokument er forfattet av A, bør vedkommende sannsynligvis registrere og tidsstemple et eksemplar hos en notar. I tillegg bør notaren autentisere innsenderen. Om forfatteren behøver å signere dokumentet, kan diskuteres siden en notar er en tiltrodd tredjepart. Men ettersom det fins et tilgjengelig opplegg med digitale signaturer og sertifikater, er det ikke ueffent å bruke det. Fotografer som ikke har tilgang til offentlig nøkkesertifikater, har tatt i bruk steganografi, skjult melding, et

bitmønster som de legger på sine fotografier. Det ser ut til å fungere bra for den profesjonen.

3.2.6 Signerte dokumenter i ulike kontekster

Personvern

Fysiske dokumenter sendes i lukket konvolutt. Det gir en viss grad av konfidensialitet og personvern. Man vil få det tilsvarende i den elektroniske verdenen ved hjelp av kryptering.

Personinformasjon som er lagret elektronisk, er lettere å sammenkople enn fysisk lagret informasjon. Generelt lagres det store mengder personinformasjon elektronisk. Pga. blant annet alle autentiserings- og tilgangsmekanismer som brukes, lagres den samme personinformasjonen flere steder. Men autentiserings-informasjon er sensitiv. Dette er en problemstilling man bør ha i mente, særlig i forbindelse med lagring av biometrisk informasjon. Det kan skape store problemer for den som informasjonen er knyttet til, hvis denne type informasjon ikke er korrekt eller hvis den korrumperes.

Tvister

Digitale signaturer er foreløpig ikke et særlig kjent begrep verken for framtidige signatarer eller for dommere. I en tvistesituasjon stiller det store krav til den som skal forklare for dommere hva digital signering er, om hvor det er likt og hvor det atskiller seg fra en håndskreven underskrift. Problemet kan være forbigående inntil folk venner seg til å signere digitalt.

Ved en tvist lang tid etter digital signering, må det være mulig å bekrefte at autorisasjonen for å signere gjaldt på signeringstidspunktet.

Teknisk perspektiv

Elektroniske dokumenter er avhengige av informasjonsteknologi. Der informasjonsteknologi er tilgjengelig, kan man raskt framskaffe kopier av dokumentene. Men de elektroniske dokumentene er foreløpig ikke like lett tilgjengelige andre steder slik papirdokumenter og penn er. Man er derfor avhengig av lett å kunne skrive ut dokumentene på papir og frakte dem videre til steder og personer som ikke har tilgang til IT. Ved utskrift "forsvinner" den digitale signaturen. I midlertid kan man autorisere ved en underskrift innholdet og at dokumentet har (hatt) en gyldig digital signatur i sin elektroniske form.

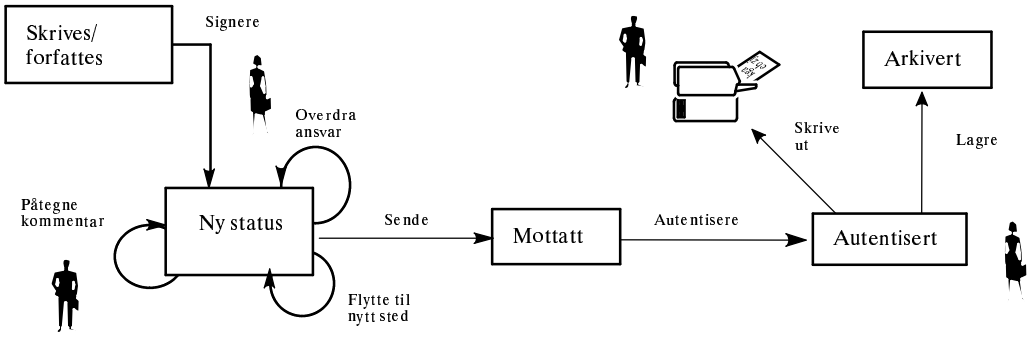
Tilgangen til elektroniske dokumenter kan bedre seg relativt raskt for privat-personer i industriland som Norge. Konvergensutvalget [76] ser for seg en utvikling i retning av et såkalt 'hjemmenett'. Det er tenkt som digitale sentraler som koordinerer et bredt spekter av digitaliserte funksjoner i hjemmene. Det kan omfatte tradisjonelle funksjoner som telefon, TV/radio, PC, video/DVD, CD-spillere, og dessuten et bredt spekter av mer utradisjonelle funksjoner som sentralisert energi- og temperaturstyring, alarmstyring osv. Det interessante er det at store deler av befolkningen etter hvert vil ha tilgang til en eller flere digitale terminaler med multifunksjonell karakter. De vil sannsynligvis gi tilgang over nett

til funksjoner som de er på stor fysisk avstand avstand fra, f.eks. vha. mer og mer avanserte mobiltelefoner. Dette er en vesentlig forskjell fra papir.

Organisasjonsperspektiv

Ettersom elektroniske dokumenter så lett lar seg kopierie, er det mer nødvendig å kunne verifisere autentisiteten til elektroniske dokumenter enn til fysiske dokumenter. Det gir avhengighet av en infrastruktur for informasjonsteknologi når man tar i bruk elektroniske dokumenter i stor skala.

Aktør-nettverkperspektiv



Figur 8 Tilstandsdiagram for et elektronisk dokument

I et aktør-nettverkperspektiv kan et fysisk dokument få ny status som er lett å observere, ved f.eks. å flytte det fra en innkurv til en utkurv. Dette kan gjøres tilsvarende for elektroniske dokumenter ved visuelt på en skjerm å flytte dem til nye steder eller nye personer. I en elektronisk verden kan det skapes nye aktanter ved at et elektronisk dokument kopieres eller skrives ut på papir.

For fysiske dokumenter er dokumentets status i hovedsak en iboende egenskap. Elektroniske dokumenter vil i stor grad måtte lagre statusen separat fra selve dokumentet. Når dokumentet sist ble endret, og hvem som har anvar for videre behandling, lagres ofte i separate filer, jf. datamodellen i Figur 11 på side 71 der strukturen er separat lagring av tilleggsinformasjon.

3.3 Trusler mot dokumenters autentisitet

IT-sikkerhet

Når man skal sikre elektronisk lagret informasjon, så trenger man oversikt over hva man vil sikre. Det er tre hovedområder innen sikkerhet:

- Fysisk sikring av bygninger, nettverk og maskiner
- Logisk sikring av programvare og data, bl.a. vha. tilgangskontroller og kryptering
- Administrativ sikring - arbeidsrutiner, prosedyrer etc.

Dette samles gjerne i en sikkerhetspolicy. For en offentlig-nøkkel infrastruktur er sikringen vesentlig for å opprettholde tilliten til og mellom alle aktørene.

Se punkt F.6 om gjeldende lovverk som redskap mot datakriminalitet.

Eksterne angripere

Mørketallsundersøkelsen fra 1998 [77] viser at eksterne angripere nå generelt er en større trussel enn interne når det gjelder datakriminalitet. Dette er en internasjonal trend. Ofte er det en kombinasjon av interne (som tilrettelegger for) og eksterne (som utfører) angrep. Tallene i Norge har hittil vært for små til å se omfanget av eventuelt samarbeid [85].

Interne angripere

Interne angripere er en meget viktig sikkerhetsrisiko. Ansatte trenger opplæring i hvilket ansvar de har for å ta vare på en institusjonens informasjon. Det må også finnes retningslinjer for arbeidet og arbeidsdeling slik at ingen blir fristet til å avgi eller endre informasjon på en uautorisert måte. I de nordiske riksarkivenes rapport om å bevare og tilby tilgang til elektroniske dokumenter [73] føres utro tjenere opp som et risikomoment.

Sammenlikning med papir

Datakriminalitet knyttet til elektroniske dokumenter er i sitt vesen ulik kriminalitet knyttet til papirdokumenter. Datakriminalitet beskrives som "..kriminalitet der utnyttelsen av datateknologi har vært vesentlig for overtredelsen." (Straffelovrådet NOU 1985:31).

Angrep på undertegnede papirdokumenter går på å:

- Stjele dokumentet,
- Forfalske dokumentet,
- Forfalske underskriften,
- Ødelegge dokumentet,
- Utnytte innholdet.

I tillegg til disse angrepene, kommer det teknologiavhengige angrep på elektroniske dokumenter, som f.eks.:

- Finne en privat nøkkel,
- Finne svakheter ved krypteringsalgoritmer,
- Finne svakheter ved annen programvare og maskinvare som kan utnyttes til egen vinning eller nekting av tjeneste,
- Korrumpere infrastrukturen for tiltrodde tredjepartstjenester.

Informasjonsteknologi har skapt en ny juridisk situasjon [95]:

- Angriperen kan være internasjonal,
- Typen kriminelle handlinger blir mer komplekse,
- Bevis skal hentes fra flere land,
- Det er flere lands lovgivninger som kan gjelde,
- Det tvinger seg fram en ny kompleksitet i lovgivningen.

3.4 Autentisering

Begreper som autentisitet og integritet blir satt inn i en til dels utvidet eller annen sammenheng i en elektronisk verden. Å verifisere ekthet må gjøres på en annen måte med den nye teknologien.

Fraværet av originalitet ved alle bits er en egenskap som representerer en betydelig utfordring når man skal etablere autentisitet, skriver Masse [67]. Det er en vanskelig/umulig og en tidkrevende oppgave å bestemme hvilken av eksisterende kopier som eventuelt var den første. Originalitet er dermed ikke umiddelbart brukbart som kjennetegn for å bestemme ekthet.

Elektroniske autentiseringsprosedyrer skal samle autentiseringsinformasjon fra en bruker (eller en annen fordringshaver f.eks. en server) [25]. De baseres på:

- Noe en person vet, f.eks. passord eller PIN,
- Noe en person har, f.eks. et smartkort,
- Noe en person er, f.eks. eget fingeravtrykk eller egen signatur,
- Kontekstinformasjon som fysisk plassering av en entitet eller et stykke informasjon [21] s. 321.

Noen autentiseringsmekanismer bestemmer bare entitetsautentisering (identifikasjon på et gitt tidspunkt), f. eks. PIN, og gir ikke andre egenskaper som er nødvendige for å trygge en juridisk handling. Entitetsautentisering, brukt alene, skaper ikke en lenke mellom autentiseringsverktøyet og den elektroniske informasjonen.

Autentisering av data- eller meldingskilde er forsikring om identiteten til meldingens opphav, en brukeridentitet, en maskin eller et system.

Dataintegritet er forsikringen om at data ikke har blitt endret på uautorisert måte [41]. En hashverdi beregnet over et elektronisk dokument er en integritetsmekanisme som kan verifiseres av en dommer hvis det oppstår tvist om innholdsintegritet.

Charles Pfleeger, Arca, [94] definerte integritet på sin forelesning på 22nd National Information Systemes Security Conference, Washington, på flere måter:

- Bare endret av autorisert person,
- Bare endret av autorisert system,
- Bare endret på autorisert vis,
- Ikke ending av det som lagres eller overføres,
- Internt konsistent,
- Presist, presist nok!
- Brukbart i en gitt situasjon.

Disse definisjonene kan kreve ulike mekanismer for å kunne realiseres.

Ikke-benekting er bindingen mellom en entitet (menneske eller maskin) og meldingen eller transaksjonen som den deltar i.

Henriksen [36] reiser spørsmålet om det er teknisk mulig å autentisere data med metoder som ikke er fysisk koplet til dokumentet selv, men som likevel sikrer de impliserte partene like mye som via en tradisjonell signatur, j.fr. kapittel 2.4.2. Ettersom teknikkene er ulike, kan man for elektroniske dokumenters del sende dem til en tiltrodd tredjepart for tidsstempling og eventuell registrering slik at man kan vise at dokumentet er avsendt.

Henriksen setter 3 krav til det han kaller en elektronisk signatur:

1 Den skal være personifisert slik at man kan bevise for andre at bare eieren kan ha laget signaturen. Han kaller det signataravhengighet.

2 Den elektroniske signaturen og meldingens datainnhold må høre sammen slik at man kan overbevise andre om at det ikke har skjedd endringer i datainnholdet. Dette kravet må man ha siden man ikke har papir. Han kaller det data-avhengighet.

3 En signatur må inneha visse juridiske egenskaper. I tillegg representerer den ofte en overgang fra planer til en endelig disposisjon. Derfor mener han det er nødvendig at signering framstår som en separat operasjon slik at personen som føyer til en signatur, forstår at han foretar en handling ved å signere.

3.5 Mulige signeringsmekanismer

Digitale signaturer, som diskuteres i punkt 3.6, er den eneste kjente mekanismen som gir høy nok tillit i åpne nettverk. Men de krever en utvidet infrastruktur for å kunne brukes mellom mennesker som ikke kjenner hverandre. Derfor er det viktig å vurdere om det fins enklere alternativer og hvilken tillit de eventuelt gir.

3.5.1 Passord og PIN

En av de mest brukte autentiseringsteknikker er passord. Passord omfatter også PIN, Personal Identification Number. Det er en betegnelse på et passord som består av en tallkode. PIN brukes f.eks. med bankkort mot minibanker, men vi ser også at det brukes mot banktjenester på Internett. Passord gir entitets-autentisering. I prinsippet er passord knyttet til innehaveren og bare kjent av vedkommende og av systemet det skal brukes mot. Ettersom ingen andre deler hemmeligheten, kan systemet anta at hvis passordet/koden er brukt, så er det av eieren [25].

PIN baserer seg på at både eieren av PIN-koden og den som verifiserer den, skal kjenne den og sammen holde kunnskapen hemmelig. Dette bryter med Henriksens første krav om signataravhengighet, j.fr. pkt. 3.4. ICRI [25] påpeker at denne teknikken ikke oppfyller alle egenskapene som kreves for autentisere juridiske handlinger og at det i tillegg er umulig å bruke teknikken mellom vilkårlige partnere. Passord må utveksles off-line på forhånd.

Integritet og ikke-benekting

Passord/PIN brukes for autentisering av handlinger, f.eks. Skattedirektoratets tjeneste for å bekrefte selvangivelsen på Internett eller telefon. Det fins ingen ubrytelig sammenheng mellom dataene som sendes/skrives, og passordet. Lagring av dokumenter med PIN gir ikke mening. Passord knyttes ikke til meldingen som autentiseres/autoriseres, og man løper derfor risiko for seinere endringer. Passord brukes mot systemet/programmet som brukeren skal kommunisere med. Både

professor Dorothy Denning, Georgetown University [21] og ICRI [25] påpeker at systemer hackes for å finne PIN og passord.

I et lukket system er det vanskelig for senderen av en melding å benekte forsendelsen hvis vedkommende ikke kan bevise at passordet er stjålet/korrumpert. Men det er ikke ikke-benektingen av den juridiske handlingen som kan garanteres, bare ikke-benektingen av aktiviteten å ha tatt i bruk et system og eventuelt laget en melding. I slike tilfeller kan logg skaffe sporbarhet om aktiviteten. Begge parter må i så fall ha grunn til å stole på loggen. Beviskraften ved en tvist er avhengig av tillit til dem som opererer systemet, til sikkerheten i systemene osv. For kyndige folk er det mulig å endre mange slags logger og skjule handlinger. Man løper også risiko for falske meldinger, j.fr. Dr. Ross Anderson [3] om innsideangrep i bank.

I et åpent system/nettverk mellom vilkårlige partnere har ikke mottakeren noen garanti for at avsenderen ikke vil benekte forsendelsen i ettertid. Selv om det fins en logg over det som foregikk, dekker bruk av passord bare oppkoplingen mot systemet, entitetsautentisering. Med en logg kan man kanskje se at en hemmelig kode har blitt tastet inn før oversendelse av et dokument. For en mottaker som skal langtidslagre dokumentet, gir logg liten trygghet, og det er vanskelig å definere hva man skal ta vare på for ettertida.

3.5.2 Biometriske metoder

Autentisering kan utføres ved å gjenkjenne biometriske karakteristika/kjennetegn. Bruk av biometriske egenskaper bygger på data som er unike for en person. Man kan skille mellom egenskaper man besitter (fingeravtrykk, iris, retinamønster) og egenskaper ved det man gjør (snakke, hastighet på tastatur, underskrive med penn). Hovedidéen er at disse egenskapene er det nesten umulig å forfalske. En fordel med biometri er at brukerne slipper å huske passord e.l., og biometri gir en sikrere autentisering enn passord. Men biometriske data kan stjeles. De kan brukes av en angriper på samme måte som et stålet passord med mindre den biometriske avlesningsmekanismen er helt fiklesikker og ikke avgir informasjon på uautorisert måte. De dekker bare delvis Henriksens første krav om signataravhengighet, se side 42, fordi det må være lagret en mal som autentiseringsinformasjonen skal sammenlikens med.

Biometri brukes vanligvis til personautentisering i øyeblikket. Fingeravtrykk, retinamønster etc. leses og sammenliknes med en lagret mal. Malen er vanligvis laget fra et antall tidligere avlesninger. Avlesningene varier med posisjon på avlesningsmatten, temperatur, skraper i huden osv. Et visst avvik fra malen godtas. Et fingeravtrykk er nokså likt hver gang man bruker det. Det innebærer at hvis en annen får tak i en elektronisk kopi av en avlesning, så kan vedkommende bruke den i andre sammenhenger. I en "kommende teknologi" bør bruker kunne autentisere seg overfor sitt eget smartkort vha. sitt fingeravtrykk og deretter la kortet autentisere seg overfor et system. Det er et eksempel på at biometri delvis erstatter passord/PIN.

3.5.3 Elektronisk underskrift

I banker blir kundene nå bedt om å skrive navnetrekket sitt på en pad i forbindelse med betalingstransaksjoner. Navnetrekket kommer fram på kassererens skjerm nederst på transaksjonen og kan sjekkes mot lagrete underskrifter [86]. Underskrifter som ikke er knyttet til dokumentet ved hjelp av kryptografi, kan lett kopieres ved klipp og lim til andre dokumenter, f.eks. av utro tjenere.

PenOp

En digital penn (PenOp, http://www.penop.com) registrerer en signatur skrevet for hånd. Den måler bl.a. bildet av autografen, hastigheten og rytmen. Deretter bindes informasjonen kryptografisk til dokumentet slik at hvis dokumentet endres, blir signaturen ugyldig. På denne måten etableres det en sammenheng mellom personen og vedkommendes signatur, og kryptografi skaper en sammenkopling med dokumentets innhold. Det er ikke signataren som er i besittelse av de kryptografiske nøklene. PenOp er tenkt som tilsvarende et fysisk dokument og at en underskrift bare verifiseres i en tvistesitussjon. Men signaturen finnes som en mal for sammenlikning hos den som eventuelt vil verifisere et dokument. En slik signatur er 'lik' for alle roller man har fordi den er knyttet til håndskriften.

Når et signert dokument skal konverteres til et nytt format, vil man miste underskriften eller måtte signere på nytt. Jeg har ikke funnet at denne problemstillingen er tatt opp av PenOp.

ICRI [25] påpeker at krypteringen i forbindelse med PenOp er symmetrisk. Det medfører at denne type applikasjoner bare kan brukes i lukkede systemer. Ben Wright, jurist tilknyttet PenOp, påpeker at løsningen for PenOp er proprietær [106]. Teknikken bak PenOp er utdypet i punkt C. Se side 132 om erfaring med bruk av PenOp hos Det norske Veritas.

Sosial forståelse av det å undertegne

Det har vært interessant å registrere mine egne følelser rundt at det fins et underskriftsprogram. Det å kunne se navnetrekket på skjermen ble plutselig meget vesentlig, ikke lenger bare et "borderline issue" [16]. Ettersom jeg forstår en del om hvordan digitale signaturer virker, så trodde jeg ikke at det å kunne se en underskrift ville bety så mye. Men det gjør det tydeligvis for meg også. Hva må det ikke da bety for dommere eller for folk som ikke har satt seg inn i teknologien, og som skal signere elektroniske dokumenter.

På den andre siden utfører de fleste av oss gjøremål som vi ikke forstår helt hva innebærer. Det er rimelig å forvente en tilvenning til bruk av digitale signaturer som erstatning for håndskreven underskrift. I midlertid har bankkunder fortalt meg om sin utrygghet første gang de ble bedt av kassereren i banken om å skrive navnetrekket sitt på en pad for å bekrefte en transaksjon. De lurte på hva som skjer i banken med noe så personlig som en underskrift.

Etter min mening er det forskjell på å lagre en persons offentlige nøkkel i en sertifiseringsautoritets database og å lagre en persons biometriske data slik PenOp gjør. Særlig i forbindelse med symmetriske metoder vil det kunne gi mye

dobbeltlagring. Biometriske kjennetegn, som et fingeravtrykk, kan lagres i eierens smartkort. Da kan autentiseringen skje i kortet som avtrykkets eier besitter, og ikke i flere eksterne databaser.

PenOps system for visuelle signaturer brukes i lukkete, avgrensete systemer. Det medfører at det etter hvert vil lagres databaser mange steder der det fins kopier av privatpersoners underskrift. Dersom man i steden bruker offentlig-nøkkel sertifikater, kan lagringen skje i én database og med kryssertifisering mot andre sertifikatautoriteter.

3.5.4 Symmetrisk kryptografi

Autentisering skjer ved å vise kjennskap til en delt hemmelig nøkkel. Metoden kan brukes mellom vilkårlige partnere hvis det fins tiltrodde autentiseringstjenere. Kerberos [135] er et eksempel på tiltrodd autentiseringstjener ved hjelp av symmetrisk kryptering.

Meldingsautentiseringsmekanismer beskrives i ISO-standard 9797 [41], [42]. Metoden kalles MAC, message authentication code. Vanligvis brukes blokkchiffer og ellers brukes hash-funksjoner. Formålet er å oppdage at data ikke er endret på uautorisert vis og å autentisere avsender. MACer kan gi økt tillit til at en melding kommer fra en entitet som er i besittelse av den hemmelige nøkkelen som er brukt. Styrken på autentiseringsmekanismen avhenger av:

- Nøkkelens lengde i bits og at den holdes hemmelig,
- Blokklengden i bits,
- Styrken på blokkchifferet,
- Lengden på meldingsautentiseringskoden og,
- Den metoden som brukes.

Meldingsautentisering vha. MAC gir sterk autentisering av datakilde. I og med at MAC-beregninger bruker symmetrisk kryptering, er det minst to parter, avsender og mottaker, som kjenner den hemmelige nøkkelen. Det medfører at Henriksens første krav om signataravhengighet, side 42, ikke er oppfylt . Å sende meldingen med en MAC via en TTP, kan gi økt beviskraft for avsender. Hvis det skal brukes ulike sesjonsnøkler for hver melding som sendes, må man holde orden på et stort antall av dem ved langtidslagring med MAC intakt. Dersom MACene fjernes ved lagring, slik det vanligvis gjøres, gir MAC bare entitetsautentisering og integritet.

3.5.5 Konklusjon

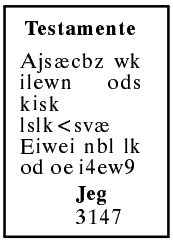
Det som kjennetegner de metodene jeg har gått gjennom her, er at man deler en hemmelighet eller informasjon om en egenskap med en annen (et system som noen andre har tilgang til). Det gir ikke samme tillit som en situasjon der man har eneansvaret for informasjonen. Noen av metodene gir heller ikke kopling mellom mennesket og dokumentet. Spesielt åpner metodene for innsideangrep hos mottakeren. Ingen av metodene ansees som tilfredsstillende i forhold til elektronisk signatur. Unntaket kan være PenOp, men det systemet har andre

svakheter, f.eks. personvern og at sikkerhetsmekanismene ikke er offentlig tilgjengelige.

3.6 Digital signatur

Den mest brukte metoden for å autentisere elektroniske dokumenter, er i dag digitale signaturer. Her følger en gjennomgang av egenskaper for å finne fram til likheter og forskjeller i forhold til håndskrevne signaturer.

3.6.1 Signering



En digital signatur kan knytte sammen personen som signerer og innholdet i det elektroniske dokumentet, se forklaring side 130. Sammenknytningen er en av de sentrale egenskapene for dokumenter med underskrift. Der man bruker offentlig-nøkkel kryptering, er den private nøkkelen bare kjent av signataren og den skal ikke sendes noen steder. Den tilsvarende offentlige nøkkelen er tilgjengelig for alle. Dette dekker Henriksens første krav til signataravhengighet, s. 42.

Link mellom data og hemmelig kode

En digital signatur beregnes på grunnlag av hele det elektroniske dokumentet. Det er dermed en sammenheng mellom innholdet i dokumentet og signaturen. Dette dekker Henriksens andre krav om dataavhengighet. Men det er få mennesker som kan verifisere at signeringsprogrammet ikke gjør andre ukjente ting i tillegg. Dette vanskeliggjøres ytterligere der det er proprietære løsninger, jfr. PenOp, punkt 3.5.2. Sjefsforsker Jon Ølnes, Norsk Regnesentral, påpeker i [148]: "En langt større trussel (enn sikkerheten målt ved nøkkellengden) er programmer som endrer informasjonen mellom det brukeren ser på skjermen og den representasjonen av dokumentet som faktisk blir signert. Brukeren tror hun signerer over skjermbildet, mens signaturen blir beregnet over manipulert informasjon." Et tekstbehandlingsverktøy kan f.eks. inneholde hvit tekst på hvit bunn.

Juristen David Fillingham [28] skriver at en digital signatur er knyttet til et menneske vha. individets private nøkkel, en kryptografisk algoritme og datamaskiner. Sammenhengen er avhengig av at den private nøkkelen holdes hemmelig. Det er en sterk matematisk sammenheng mellom personens private og offentlige nøkkel. Knyttingen mellom personen og vedkommendes offentlige nøkkel avhenger av sertifikatutsteders ærlighet og omhu ved utstedelse av sertifikater.

Man kan ha flere nøkkelpar for digitale signaturer, f.eks. avhengig av hvilken rolle eller myndighet man har ved signering. En håndskreven underskrift er lik for alle roller man har. Alle digitale signaturer er forskjellige. Dette er uavhengig av rollen. Det kommer som en følge av at dokumentene som signeres, er ulike og av egenskapene ved de kryptografiske algoritmene som brukes.

3.6.2 Offentlig-nøkkel infrastruktur

Fullingham påpeker at digitale signaturer generelt ikke kan verifisers uten sertifikater. Man kan sjekke dataintegritet ved å beregne dokumentets hashverdi i forhold til dekryptering av signaturen. Men man kan ikke ha tillit til hvem dokumentet kommer fra. Det kan man bare få ved å verifisere sertifikatet tilknyttet den offentlige nøkkelen.

Problemet oppstår ved skalering i store nettverk med kommunikasjon mellom "vilkårlige" parter. Der kan man ikke vite om den offentlige nøkkelen kommer fra riktig avsender eller fra en bedrager. Å tilbakekalle eller bytte egne nøkler er vanskelig: En bruker har ingen måte å få vite hvem eller hva som har referanse til den gamle nøkkelen [111]. Dette er problemer ved bruk av programmet PGP, Pretty Good Privacy [60]. PGP brukes blant kjente med sertifikater utstedt av folk som går gode for hverandre. Dette er bare brukbart i korte tillitskjeder (stole på "vennen til en venn"), og vil gi for lav sikkerhet i det offentlige rom.

Pga. mangel på tillit og tiltro mellom parter som ikke kjenner hverandre i et stort åpent nettverk, har man innført en offentlig-nøkkel infrastruktur (Public Key Infrastructure, PKI) med tiltrodde tredjeparter (TTPer). Se appendikset side 135 for mer informasjon om PKI og TTP. Behov for infrastrukturen kommer som en følge av skalering. Hvis partene har tillit til disse TTPene, vil de også ha tiltro til sertifikater som knytter en offentlig nøkkel til en bestemt person.

3.6.3 Autentisering

Et sertifikat som er digitalt signert av en sertifikatutsteder, løser mange autentiseringsproblemer. Sertifikatutsteders offentlige nøkkel fins tilgjengelig flere steder på nettet og kan lett verifiseres. På den måten trenger man ikke on-line tilgang til sertifikatutsteder.

Autentisering av kilde

Den offentlige nøkkelen som dekrypterer den digitale signaturen, er koplet til signatarens private nøkkel. Eierskapet til den offentlige, og dermed den private, nøkkelen aksepteres ved å verifisere det tilhørende sertifikatet.

Dataintegritet

Det vil umiddelbart gjenspeiles på den digitale signaturen hvis innholdet i et dokument er endret. Dersom en stor bokstav, *G*, ble endret til liten *g*, gir det en annen digital signatur, dvs. endringer oppdages.

Lett å verifisere?

Digitale signaturer er lettere å verifisere enn håndskrevne underskrifter tilhørende personer man ikke kjenner. Den offentlige nøkkelen er offentlig tilgjengelig og sertifisert av en sertifiseringsautoritet. Selve verifikasjonen skjer maskinelt i løpet av sekunder.

Ikke-benekting

Det fins flere handlinger man kan benekte i forbindelse med signering og forsendelse av et signert dokument [48]:

- avsendelse,
- mottak,
- signering
- mottak til en nettverksnode,
- videre sending fra en nettverksnode,
- flere gangers forsendelse av samme melding.

En signatar kan nekte å ha sendt en melding. En mottaker kan nekte å ha mottatt den. Men en signatar kan vanskeligere benekte å ha signert et elektronisk dokument der signaturen verifiseres med en offentlig nøkkel knyttet til et sertifikat signert med signatarens identitet. Men i og med at en privat nøkkel ikke er knyttet til en person på samme måte som en underskrift, kan eieren si at kortet med den private nøkkelen er stjålet eller korrumpert. En tjeneste for ikke-benekting er å sanke bevismateriale for at en hendelse, en forsendelse, har skjedd. Man kan bruke en TTP til en slik tjeneste. Noen, bl.a. Roe [115], reiser tvil om mulighetene for å få til uavviselighet ved hjelp av elektroniske teknikker i åpne systemer. Hvis avsender ønsker å benekte noe han mener han ikke har sendt, kan han vise til at han er utrygg på hva han faktisk signerer, det som han ser på skjermen eller noe annet. Mottakers tillit til signaturer blir avhengig av sikkerheten hos avsender. Hvis avsender ønsker å benekte en faktisk sending, kan han være tjent med å kunne skylde på dårlig sikkerhet.

3.6.4 Tidfesting

Tidfesting kan skje på flere måter. De gir ulik grad av sikkerhet og kan brukes i ulike situasjoner.

A Dato tastet i dokumentet

Vanligvis står det dato for undertegning i brev og dokumenter. Dersom mottaker mottar dokumentet innenfor en akseptabel/avtalt tidsperiode etter den påtegnete datoen, er det rimelig å akseptere tidspunktet for undertegning. Dette vil være en manuell arbeidsoppgave med mindre tidspunktet kan trekkes ut maskinelt fra meldingsformatet. Akseptabel tidsperiode vil variere med saksinnholdet. Tidsperioder for kjøp og salg av aksjer vil være korte, kanskje minutter. Tidsperioder for brev til et departement kan være timer eller dager.

Slike datoer kan forfalskes dersom avsender vet at mottaker ikke umiddelbart registrerer dokumentet som akseptert i en postjournal.

B Tidsstempel fra avsenders maskinklokke

Et tidsstempel fra avsenderens maskinklokke hjelper hvis mottaket registreres med en gang og er innenfor en avtalt tidsperiode. Dette kan gjøres maskinelt og automatisk ved mottak. Det er etter min mening en god utnyttelse av mulighetene ved den nye teknologien som ikke er mulig med papirbaserte systemer.

Men maskinklokka kan endres. Det blir dermed viktig for både avsender og mottaker å ha en felles forståelse eller en avtale om hva som er en akseptabel tidsperiode mellom påført tid og mottatt tid.

Risikomomenter

Kan man ha tillit til den datoen som signataren selv har satt i dokumentet hvis man har et gyldig sertifikat, men ikke tidsstempling? Kan en utro tjener i et

departement lage en ny utgave av dokumentet med dato satt f.eks. 2 uker tidligere? Det vil vises når dokumentet sist ble editert, eller hvor lang tid det tok før det ble journalført. Men hvis man flytter dokumentet mellom maskiner, mister man editeringsdato. En som sender inn selvangivelsen elektronisk eller sender innrapportering til Skatteetaten, kan tilbakedatere tidspunktet for avsendelse og påstå at e-posten ble sendt i tide, men at overføringen tok tid. I slike tilfeller bør man ha en avtale om når dokumentet må være mottaker i hende.

Tidfesting i ettertid løses ikke med en sertifisert digital signatur. Selv om sertifikatet er gyldig, behøver ikke mottaker å ha tillit til at datoen er riktig satt av avsender. Derimot vil en avsender skaffe seg økt beviskraft hvis mottaker returnerer en digitalt signert kvittering for mottak.

C Tidsstempel fra en tiltrodd tredjepart

Et digitalt signert dokument med tidsstempel fra en tiltrodd tredjepart gir sikker tidfesting av når et dokument eksisterte og når det ble mottatt av en TTP fra avsenderen. Hvis selve signeringstidspunktet er t_i, vil TTP'ens tidsstempel bli gitt i ettertid ved tidspunkt t_{i+x}. Hvor lang tid, x, i ettertid som er akseptabel, bør gjenspeile seg i en avtale mellom partene. Tidsstempel gir sporbarhet, dvs. muligheten for å logge at noe har skjedd.

Hvis avsender bare sender en signert hashkode av dokumentet til TTP for tidsstempling, sier stempelet bare at dokumentet eksisterte på det mottatte tidspunktet. Stempelet sier ikke noe om at dokumentet er sendt fra avsender til den intenderte mottakeren. Dette kan være en viktig distinksjon ved f.eks. anbudsrunder.

3.6.5 Sosial forståelse for det å undertegne

Det er få mennesker som forstår hvordan digitale signaturer virker, og det er ikke alle systemer som viser dokumentet som skal signeres, eller ber aktivt om en signatur fra signataren. Dette skaper avstand til den juridiske handlingen ved elektronisk signering. Det er et hinder for å ta i bruk ny teknologi. IT-folk har fått nok et område der de er modellsterke (å være rik på relevante begreper og forestillinger) overfor vanlige mennesker som skal ta teknologien i bruk [17].

Dagens løsninger virker fremmedgjørende. Ved signering skapes det et nytt dokument som det kan være vanskelig å finne etterpå. Det nye dokumentet har en lang streng for sertifikat og offentlig nøkkel. Det likner ikke på et fysisk dokument med underskrift. Etter min mening er dette et vesentlig minus ved bruk av digitale signaturer. På den andre siden bør det ikke være vanskelig å gjøre brukergrensesnittet litt mer brukervennlig, slik at terskelen blir lavere for folk som ikke signerer ofte. På samme måte som ved bruk av PenOp, kan man også gjøre underskriveren oppmerksom på at hun binder seg juridisk ved å signere.

Både mennesker, artefakter og konteksten de befinner seg i er aktanter i et samspill, Latour [64] s. 108-109. For å ta i bruk digitale signaturer i stor skala og på en effektiv måte, vil det måtte skje en endring hos flere aktanter:

- Måten man signerer på, vil måtte endres og bedres,
  - dataprogrammet som brukes, blir lettere å bruke,
  - dataprogrammet gir tydeligere melding om at nå utfører man en juridisk handling.
- Presentasjonene av en digital signatur overfor brukeren vil endres,
  - det vil stå med forståelig skrift:
    "Dette dokumentet er signert av Anne Seip.
    Den digitale signaturen har følgende verdi:....
    Dokumentet kan autentiseres ved å kjøre programmet X".

Bruksanvisning for å signere

1 Velg signering fra Sett inn menyen
2 Sett inn smartkortet
3 Tast PIN
4 Trykk OK for signering

- De ulike brukernes forståelse av at de signerer digitalt, blir bedre ved at de venner seg til systemet.

Jeg tolker Latour slik at om brukernes forståelse skal bli bedre, er avhengig av

1 Hvor godt man legger forholdene til rette for brukerne,

2 Hvor sterkt (i dette tilfellet) det offentlige ønsker bruk av digitale signaturer, og

3 Hvor dyktige brukerne er til å nyttiggjøre seg systemet.

3.6.6 Tvister

Forfalskning, kompromittering og feil

Man snakker om kompromittering av algoritmer og avsløring av nøkler i forbindelse med digitale signaturer. Anderson og Kuhn [4] beskriver diverse måter man kan 'klusse' med smartkort på. Dersom en signeringsnøkkel lagres i programvare på en PC, er den lett tilgjengelig for en kyndig inntrenger. I tillegg fins det mange steder der det kan oppstå programmeringsfeil og tilfeldige feil som kan skape problemer, når man skal generere og verifisere en privat nøkkel.

Bevisvekt

Bevisproblemer oppstår når det hersker tvil om hvorledes fakta forholder seg. Bevismateriale som sankes inn, er om hvorvidt en hendelse har funnet sted, når den i såfall inntraff, hvem (hvilke personer) som var involvert, og hva det resulterte i [53]. Avgjørelsen om en digital signatur er gyldig, avhenger i tillegg av at mange sikkerhetsprosesser og andre prosedyrer virker korrekt og av om en dommer forstår og aksepterer mekanismene som har vært i bruk, j.fr. Galtung og Riisnæs, [31].

3.6.7 Langtidslagring

Fillingham [28], peker på at det fins minst 4 problemer knyttet til langtidslagring:

- Lagringsmediene forringes over tid,
- Formatene foreldes,
- Kryptografiske algoritmer og relaterte standarder videreutvikles,

- Sertifikatenes livssyklus.

I tillegg kan det bli behov for

- kunnskap om å bruke gamle maskiner og gammelt utstyr.

Gyldighetstiden for en digital signatur kan altså bli kortere enn ønsket i forhold til den juridiske handlingen dokumentet representerer. Det vil bla. være avhengig av om formatet som ligger til grunn for den digitale signaturen, er lesbart.

Statusen til sertifikater utstedt av forlengst nedlagte sertifikatutstedere er ikke avklart. Fillingham mener det vil bli arbeidsomt og urealistisk å forvente at en offentlig-nøkkel infrastruktur skal tilby å avgjøre diskusjoner mellom motstridende interesser i det uendelige for hvert sertifikat som er utstedt. Han skriver at arkiver bør ha ansvaret for å iverksette prosedyrer som sikrer at innholdet i arkivet ikke forandres selv om formater endres.

Juridiske sider ved langtidslagring tas opp i kapittel og tekniske utfordringer tas opp i kapittel 5.

3.6.8 Sammendrag

Digitale signaturer, basert på asymmetrisk kryptering, er den mekanismen i den elektroniske verdenen som best tilsvarer egenskaper ved håndskrevne underskrifter. Det fins likevel en del problemer.

Tabell 3 Egenskaper ved digitalt signerte dokumenter

Egenskaper	**Digital signatur med sertifikat**
Autentisering av datakilde	Ja.
Ikke-benekting av signatur	Ja, i hovedsak.
Dataintegritet	Ja.
Link mellom data og signaturverktøy	Ja, men man vet ikke om man i tillegg signerer noe mer.
Lett å verifisere?	Ja.
Lett å forfalske	Nei.
Gyldig så lenge den juridiske handlingen er viktig?	Det vil variere og bare så lenge maskinene kan lese dokumentet og beregne signaturen.
Endringer gjort i hht. autorisasjon?	Ja, kan verifiseres i forhold til sertifikatpolicy der man definerer roller.
Klar over at signerer?	Avhengig av bl.a. applikasjonen.
Forstår dommeren hva det dreier seg om?	Kanskje. Det er komplisert fordi man også må vurdere tilstandsinformasjon som må lagres.
Tidfesting	Ja, hvis det sjekkes med en gang Bare med tiltrodd tidsstempel i ettertid.

3.7 Konklusjoner

Det tar tid å lære seg å tenke på elektroniske dokumenter uten først å tenke på papir og den teknologien papiret har tilgjengelig. Hvilke egenskaper vil man da overføre/ta med seg? Hvilke nye muligheter fins?

Det er mulig, i visse sammenhenger og med bestemte mekanismer, å knytte en elektronisk signatur til et elektronisk dokument på tilsvarende måte som en håndskreven signatur er knyttet til et fysisk dokument. Som tidligere vist i dette kapittelet, er den aktuelle teknologien for dette i dag digitale signaturer og offentlige nøkkelsertifikater.

3.7.1 Forskjeller og likheter

Hva slags egenskaper er bestemmende for likheter og forskjeller mellom fysiske og elektroniske dokumenter?

Likheten, og det fine, er at et elektronisk dokument laget med bits og bytes framstilles for mennesker og ser ut nesten som et tilsvarende fysisk dokument.

Hovedforskjellene er at:

- Et elektronisk dokument er avhengig av informasjonsteknologi og dermed ikke like tilgjengelig for alle. Man trenger maskiner og programvare både for å produsere, lese og vurdere om dokumentet er ekte, hvilket skaper økt kompleksitet og økt risiko for at man ikke får til det man vil.
- For å kunne verifisere digitale signaturer trenger man tilstandsinformasjon og opplysninger ut over dokumentet selv.
- Man trenger tillit til teknologien, ikke bare til mennesket som signerer.
- Teknologien gir muligheter for et uendelig antall kopier.
  - Noe man har (et smartkort) og
  - Noe man vet (PIN).
- Håndskreven underskrift er
  - Noe man er (biometri) og
  - Noe man kan (skrive).
- Bindingen mellom fysisk dokument og håndskreven underskrift er sterkere enn ved bruk av digitale signaturer.
- Digitale signaturer gir en meget sterk binding mellom dokumentinnhold og signatur, hvilket gir bedre beskyttelse mot forfalskning i etter tid enn håndskreven underskrift gir
- Man trenger en infrastruktur for offentlige nøkkelsertifikater.
- Digitale signaturer kan lettere verifiseres ved mottak ved hjelp av sertifikat. Håndskrevne signaturer må sjekkes enten ved personlig frammøte med legitimasjon eller mot skriftprøve, noe som sjelden gjøres.
- I større grad enn for fysiske dokumenter kan det være vanskeligere for en signatar å være innforstått med den juridiske og sosiale handligen ved å signere digitalt.
- Realiseringen av signerte dokumenter i en elektronisk verden kan ikke skje uavhengig av teknologi. Dvs. at teknologien setter begrensinger, selv om man kan designe og implementere ulike løsninger.

Tabell 4 Sammenlikning mellom ønskete egenskaper og muligheter ved elektroniske dokumenter med signaturer

Egenskaper kap. 2.6	**Ønskete egenskaper**	**Muligheter**
a	Skal være tilgjengelig hvor som helst	Trenger tilgang til datamaskin. IT kan gi tilgang til dokumenter som er langt unna.
b	Kan finnes igjen og leses med øyet	Trenger - strøm - maskiner, - riktige formater, - tekstbehandlingsverktøy, - krypteringsalgoritmer, og - kunnskap
c	Kunne undersøke om dokumentet er endret	Lett å se endringer hvis punktet over virker
d	Kan man se om endringene er utført ihht. autorisasjoner	Kan gjøres via sertifikatpolicy
e	Endringer er sporbare	Avhengig av lagring og logger/notar
f	Lett å tidfeste hvis dokumentet er datert	Lett å tidfeste når det fikk tidsstempel
g	Lett å bestemme hvem som signerte	Lett, hvis man har sertifikater og TTP'er.
g	Ikke-benekting	Mulig, men ikke-benekting er problematisk.
i	Signatar er klar over handlingen	Det er ikke sikkert at signataren er klar over handlingen
j	Ingen påvirker skriveprosessen	Vet ikke nok omhva skriveprosessen gjør
k	Dokumentet er gyldig så lenge det er juridisk aktuelt	Dokumentet er gyldig så lenge den digitale signaturen kan verfiseres
l	Allmennheten har tiltro til lagringen	Det er det ikke sikkert at man vil ha hvis arkivet ikke kan lese gamle formater
m	Dommere aksepterer dokumenter som bevis	Det er ikke sikkert at dommere vil akseptere og forstå elektroniske dokumenter som bevis. Kan være et forbigående problem som mest har med tilvending å gjøre

Man får mye ekstra arbeid i starten dersom man skal bruke digitale signaturer i åpne systemer/nettverk. Egenskaper som henger nøye sammen i et fysisk dokument, blir til flere prosesser inkludert tiltrodde tredjeparter for elektroniske dokumenter. Disse kan utføres av ulike instanser. Hver instans må vise seg tilliten verdig overfor brukerne. Privatpersoner får ekstra arbeid i forhold til å bruke fysiske dokumenter.

Ettersom ikke alle har tilgang til datamaskiner, vil man trenge å opprettholde rutinene rundt fysiske dokumenter i lang tid. Det vil si at i lang tid framover vil man mange steder ha parallelle systemer for papirdokumenter og elektroniske dokumenter.

3.7.2 Behov for designmekanismer

Utstrakt bruk av digitale signaturer vil etter min mening kreve en del forberedelser:

- Man trenger politiske/juridiske retningslinjer, og mekanismer for langtidslagring, som konvertering mellom maskiner og mellom formater.
- Man trenger å definere hvordan tiltrodde tredjeparter og annen infrastruktur skal fungere, og hvordan ansvar skal fordeles.
- Man må få til en binding mellom signeringsverktøyet og innholdet i det elektroniske dokumentet som hindrer innblanding fra utenforstående. Pga. den komplekse teknologien er det vanskelig å vite om man faktisk signerer over det man ser på skjermen. Fins det programmeringssetninger, makroer eller skjult tekst som gjør at man samtidig signerer på noe annet som man ikke vet noe om? Bruk av etterprøvbare standardløsninger vil sannsynligvis minske risikoen for uønskete sideeffekter.
- Det skal når som helst være mulig å bestemme når dokumentet ble skrevet. Det er et strengere krav enn man stiller til fysiske dokumenter. Men kravet er nødvendig i og med at elektroniske dokumenter kan kopieres i det uendelige. Det er en utfordring å skape tilsvarende mekanismer for å bestemme tidspunkter med tilsvarende tillit for elektroniske dokumenter. For fysiske dokumenter holder det å føre på dato. Vil en elektronisk verden gjøre at man trenger å påføre klokkeslett i tillegg?
- Man trenger opplæring av personell, brukere og dommere.

Life of the system should not require
a long list of rules
or mental strain.

Kerkhoff: *La Cryptographie militaire 1883*

4 Lover og regler for langtidslagring

I dette kapittelet eksemplifiserer jeg utfordringene ved bruk av digitale signaturer ved å se på hvilke krav og behov lover og regler setter. Alt er ikke nødvendigvis spesielt for det offentlige, men det eksemplifiserer problemstillinger samfunnet står over for.

4.1 Dokumentbegrepet

Det offentlige har lover og regler for behandling av dokumenter. I denne delen ser jeg om dét skaper spesielle situasjoner.

4.1.1 Definisjoner

Statens generelle kravspesifikasjon (SGK), Elektronisk saksbehandling [130] definerer dokument som en avgrenset og sammenhengende informasjonsmengde, framstilt for et bestemt formål. Informasjonen kan bestå av en kombinasjon av tekst, data, grafikk, bilder og multimedia. Et dokument kan også bestå av flere dokumenter (sammensatte dokumenter).

I *Juridiske problemstillinger ved elektronisk saksbehandling og dokumenthåndtering* [132] påpeker Statskonsult at offentlighetsloven ikke har noen definisjon av begrepet dokument. En kan heller ikke ta utgangspunkt i at begrepet betyr det samme i andre lover. Ved en lovendring i 1982 ble det gitt hjemmel for å gi forskrifter om at loven kommer til anvendelse på materiale som er "utarbeidet, overført eller lagret ved hjelp av elektronisk databehandling". Innsynsretten anvendes på den "naturlige enhet tekst eller opplysninger som på utskrift fra systemet framstår som ett dokument". Dvs. tankegangen i loven er fortsatt papirorientert. Ettersom dagens teknologi gir muligheter for å tilgjengeliggjøre andre typer informasjon, f.eks. lyd- og filmopptak, kan det skape problemer med innsynsretten siden disse ikke egner seg for utskrift på papir. Bruk av hyperlenker (deler av dokumentet kan befinne seg helt andre steder) kan på denne måten skape tvil om hvor et dokument ender og et annet begynner. Før forvaltningen har satt sammen informasjonen (f.eks. fra en database) ved et søk, kan det vanskelig sies å ha eksistert et dokument som inneholder opplysninger.

4.1.2 Kravet til skriftlighet

Lovverket inneholder en rekke bestemmelser som fastsetter at henvendelser til eller fra forvaltningen skal være skriftlige, f.eks. forvaltningsloven § 23. Statskonsult [132] påpeker at ved kravet til skriftlighet er det viktig å se på de hensynene som ligger til grunn for kravet. Kravet er satt ut fra bevishensyn. Man ønsker å sikre at det for ettertiden finnes dokumentasjon på hva som er besluttet, uttalt eller søkt om. Man ønsker å ha bevis for hvem som har stått bak en beslutning, søknad eller uttalelse. Bak dette igjen ligger f.eks. hensynet til orden, effektivisering gjennom standardisering (ligningsloven § 4-3) og hensynet til seremoni ved enkelte viktige disposisjoner, f.eks. inngåelse av ektepakt. Statskonsult antar at dersom en for bevishensynets vedkommende kan oppnå samme effekt ved bruk av elektroniske dokumenter som ved papir, vil andre hensyn bak skriftlighetskravene la seg imøtekomme på de fleste områder. Krav om skriftlighet forutsetter at det er mulig å hente fram dokumenter i sin opprinnelige form i lang tid etter arkivering

Det sentrale ved å kreve at en juridisk handling skal skje skriftlig, er at det skal finnes et fysisk uttrykk som til en viss grad er uavhengig av tid og rom. Det skal være mulig å få kjennskap til disposisjonens innhold fra andre kilder enn de personene som var til stede da disposisjonen ble foretatt. Når en disposisjon er dokumentert, er en mindre avhengig av nøytrale vitner. Samtidig vil et dokument ikke påvirkes av tiden på samme måte som vitners hukommelse.

ISTEV [52] skriver at tradisjonelt må et papirdokument med juridisk verdi tilfredsstille 4 basale krav:

- Et ark av papir som bærer (carrier),
- En fysisk representasjon av informasjonen,
- Navnet eller annen informasjon om skaperen av dokumentet,
- En håndskreven signatur som overdrar teksten.

Alle disse komponentene er del av det samme dokumentet og fysisk forenet i ett enkelt objekt. Det stadfester at papiret er dokumentet. Roger Henriksen [36] påpeker at papiret beholder sine vedvarende egenskaper mens dokumentet overdras fra en person til en annen, dvs. Latours uforanderlige mobiler [65].

I følge ISTEV foreslår de fleste nasjonale lover skrevne dokumenter. Noen av grunnene til det er:

a) Behovet for å sikre at det fins håndgripelige bevis for eksistensen av og naturen til partenes hensikt med å binde seg,

b) Ønsket om å hjelpe partene til å bli klar over konsekvensene ved å inngå en kontrakt,

c) Behovet for å forsyne alle med et leselig dokument og tillate reproduksjon av det slik at alle parter har tilgang til en kopi med det samme innholdet,

d) Kravet om å sørge for at dokumentet forblir uforandret over tid, og sørge for at det fins en varig vitnesbyrd om saken, som tillater en enkel lagring av data i en håndgripelig form,

e) Behovet for autentisering av data ved hjelp av en signatur, for å avslutte intensjonen til forfatteren av skrivet og for å frambringe et bevismateriale for intensjonen ved skrivet,

f) Kravet om å frambringe dokumentet i en slik form at det er akseptabelt for offentlige myndigheter og for retten,

g) Behovet for å lette/fremme kontroll og derigjennom muliggjøre revisjon

h) Kravet om å sette juridiske rettigheter og plikter ut i livet i de tilfellene der skriftlighet kreves for valideringsformål.

4.1.3 Må skriftlighet være knyttet til papir?

Statskonsult [132] skriver at ut fra en formålsbetraktning må en anta at skriftlighetskravet også forutsetter at disposisjonen fremkommer på et medium som muliggjør forflytning av dokumentasjonen, samtidig som den har varighet over tid. (Ikke skrift i sand.) Tekst som er lagret ved hjelp av edb, må etter en ren semantisk forståelse karakteriseres som skriftlig. Selv om et elektronisk dokument dypest sett er en rekke av elektriske impulser, mener de det er liten tvil om at et elektronisk tekstdokument slik det fremstår på en skjerm, dekkes av skriftlighetsbegrepet.

4.1.4 Formkrav

Formkrav gjelder som oftest dokumenter som gir uttrykk for viktige disposisjoner det er svært vesentlig å skaffe bevis for f.eks. testamente, arveloven [132]. Hvis lovgivningen setter krav om underskrift, er det spørsmål

- Om den digitale signaturen oppfyller lovens formkrav eller det bare er et vedtak man gjør,
- Om den digitale signaturen ivaretar de hensynene krav om underskrift er begrunnet i.

Hovedhensyn er som regel bevishensyn. Andre hensyn kan være at signering er en alvorlig handling (undertegning av ektepakt), eller at det reduserer mulighetene for tvang, svik e.l. (vitner med undertegning av ektepakt). Statskonsult skriver at i de tilfellene der dokumentets fysiske beskaffenhet har betydning, vil det være lite hensiktsmessig å lagre dokumentet elektronisk.

Lovkrav om underskrift kan være et hinder for å bruke elektroniske dokumenter. En klage skal være undertegnet. Loven skriver om telegrafisk klage, men ikke om klage via e-post. Ihendehavergjeldsbrev underskrives av interessentene etter tur. (Man må altså ha mekanismer for å vite rekkefølgen på underskriftene. Digitale signaturer viser rekkefølgen på underskriftene ved hva hver enkelt av dem beregnes ut fra.)

Statskonsult skriver at forutsetningen for å bruke digitale signaturer, er å gjennomgå lovverket for å avgjøre hvilke underskriftsbestemmelser som bør endres.

4.1.5 Grunner for å holde på fysiske dokumenter

Det kan finnes dokumenter som man trenger tilgang til, selv om strømmen går, f.eks. i ekstreme situasjoner som naturkatastrofer og krig. For noen typer dokumenter kan det være et avveiningsspørsmål. Hvis til en hver tid en stor andel av de fysiske pasientjournalene ved et sykehus er på avveie [1], bør det veies mot at ingen elektroniske journaler er tilgjengelige ved 0.02 % av tiden for en datamaskin.

I *Juridiske problemstillinger ved elektronisk saksbehandling og dokumenthåndtering* [132] står det at det på enkelte områder kan være meget gode grunner for å sondere mellom papir og andre medier. Maria Strøm, Statskonsult, som førte den første utgaven i pennen, sier at det er dype forestillinger i folk om at f.eks. testamenter skal være på papir [103]. For ihendehaverdokumenter er det juridiske systemet slik at det gir en viss beviskraft å være i besittelse av dokumentet [36].

Statskonsult påpeker at fysisk avstand vil spille en mindre rolle for faktisk tilgang til offentlige dokumenter. Det er ODIN på Internett et eksempel på. Men det er på det rene at innsyn via egen PC, ikke vil være et tilfredsstillende tilbud for alle. Derfor må forvaltningen opprettholde et system der krav om innsyn også kan imøtekommes ved utlevering av papirutskrifter.

4.1.6 Originaler og unike dokumenter

Det står lite om originale og/eller unike dokumenter i *Juridiske problemstillinger ved elektronisk saksbehandling og dokumenthåndtering* [132]. I hht. Statskonsult har man ikke opplegg for elektronisk å håndtere kravet om én original. Jeg mener at i enhver saksbehandling må det være en selvfølge å vite hvilken av diverse versjoner som gjelder.

UNCITRAL's modellov for elektronisk handel (United Nations Commission on International Trade Law) [141] definerer original på følgende måte:

> "(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:
>
> A there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and
> B where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented."

For meg ser det ut som UNCITRAL bruker ordet original om et uendret dokument. Rolf Riisnæs [97], Institutt for rettsinformatikk, Universitetet i Oslo, har funnet i hovedsak følgende områder som bruker begrepet original:

1 Original eller 'bekreftet kopi'. Dette endrer ikke informasjonsinnholdet, og stemmer nokså overens med UNCITRAL's definisjon.

2 Originalt bilag. For eksempel dokumentasjon av fradragsposter eller drosjeregninger skal bare legges fram én gang.

3 Originaleksemplar i forbindelse med opphavsrett. Man kan overdra et eksemplar fysisk, men ikke opphavsretten.

4 Originaltekster der man undertegner flere eksemplarer.

Det er bare punkt 2 som kan skape problemer i den elektroniske verdenen, hvis vi ser bort fra problemet med langtidslagring.

4.2 Underskrifter

Hvilke krav lovverket setter til underskrifter og hva det legger i det å underskrive, er vesentlig i et moderne samfunn. I denne delen ser jeg på hva lover, regelverk og rapporter tar opp av problemstillinger ved overgang til en elektronisk verden. Jeg sammenlikner med hva man har gjort i andre land og institusjoner.

4.2.1 Sammenheng med dokumentet

ISTEV [52] setter opp følgende punkter som bør vurderes for å avgjøre sammenhengen mellom håndskrevne underskrifter og digitale signaturer:

- Om en digital signatur kan tilfredsstille typiske funksjoner som en håndskreven underskrift har,
- Om et digitalt signert elektronisk dokument er en original eller en kopi,
- Om det er juridisk korrekt å "skape" et juridisk motstykke av en bekreftet digital signatur,
- Om et digitalt signert elektronisk dokument skal kunne betraktes som juridisk gyldig og virkningsfull.

Statskonsult [132] påpeker at den personlige underskriften har lang tradisjon som garantist for at dokumenter er ekte, selv om den vanligvis ikke sjekkes. Underskriften nyter stor tillit som autentisitetsbevis både hos det offentlige og i handelslivet, til tross for at det kan være vanskelig for en ufaglært å avsløre en falsk underskrift. At underskriften i praksis fungerer så godt som autentisitetsbevis, er nok hovedgrunnen til den tilliten den nyter.

Underskriften har minst to viktige funksjoner. I noen sammenhenger er det et rent bevismiddel for å knytte en person til en disposisjon, signataravhengighet. (Underskrive avtale om kjøp av PC.) I andre sammenhenger stiller lover krav om håndskrevet underskrift for at et dokument skal være gyldig. Som oftest er det også bevishensyn som ligger bak lovens krav (sjekkloven §1, arveloven § 49).

Den nye finansavtaleloven [80] har i sin § 8 at avtalen kan inngås ved hjelp av et elktronisk medium dersom kunden ønsker dette, og:

> "a) avtalens innhold i sin helhet er tilgjengelig for kunden ved avtaleinngåelsen, og
> b) det er benyttet en betryggende metode for å autentifisere inngåelsen av en avtale med det angitte innhold".

I hht. juristen Jens Nørve, Nærings- og handelsdepartementet, innebærer dette at det skal være samsvar mellom det man ser og det man signerer. I proposisjonenes alminnelige merknader kapittel 7.3 problematiseres de betryggende metodene for å autentifisere inngåelsen ved å diskutere i hvilke situasjoner man kan bruke en PIN-kode i steden for en elektronisk signatur. I midlertid problematiserer de ikke at en signatar, pga. teknologiens muligheter, kan komme til å autentifisere noe annet enn det vedkommende ser på skjermen.

4.2.2 Usignerte elektroniske dokumenter

Det er en rekke dokumenter som ikke er underlagt noe lovhjemlet underskrifts-krav, og som en ut fra bevishensyn ikke trenger å kreve underskrevet eller signert. Statskonsult [132] tenker seg andre autentiseringsmekanismer som ikke er like sikre som digitale signaturer, men som likevel er sikre nok. De foreslår f.eks. å bruke passord for en definert gruppe aktører. Dette autentiserer aktørene, men knytter dem ikke til selve dokumentene. Passord er det samme for alle dokumenter man skriver i et bestemt system der man bruker det passordet. Det skaper ikke en unik binding mellom signataren og det enkelte dokument, j.fr. pkt. 3.5.

Det er ikke gitt at det bør stilles like strenge krav til at autentiseringen skal kunne knyttes direkte til dokumentet i en søknad om parkeringsplass som i et vitnemål.

Når lovgivningen ikke setter krav til underskrift, må en vurdere om det ut fra bevishensyn er nødvendig at et dokument er signert.

- Et trygdekontor har originalen, hvis mottaker er i tvil om et vedtak.
- En begjæring om innsyn kan behandles etter en usignert e-post.
- En stillingssøknad behøver ikke være signert, så lenge vitnemål etc. er signerte og verifiserbare.

I hvilke tilfeller en godtar usignerte dokumenter, må avgjøres individuelt. For meg ser det ut til å være vesentlig om man vet at man behandler det intenderte, ekte dokumentet.

4.2.3 Signaturers juridiske funksjoner

Kan man sende et elektronisk dokument med en digital signatur hvis man ikke helt vet hva det er? Det er ikke så mange i dag som forstår hvordan en digital signatur virker og hva det er ved den som gjør at man binder seg juridisk, når et dokument påføres en digital signatur.

Juristene Andreas Galtung og Rolf Riisnæs har sett på hvilke funksjoner en hånd-skreven signatur fyller i *Rettslige aspekter ved digitale signaturer* [31]: identifiseringsfunksjon, bevisfunksjon, autentiseringsfunksjon, symbolfunksjon og avslutningsfunksjon. Deretter så de på for hvilke funksjoner en digital signatur

kan erstatte en manuell signatur, og om en digital signatur også fyller andre funksjoner som kan ha en rettslig betydning.

Digitale signaturer

Forfatterne har lagt følgende definisjon på digitale signaturer til grunn i betenkningen: "Data lagt til, eller en kryptografisk transformasjon som gjør det mulig for mottaker å bevise kilden/opphav og integritet av data og beskytte mot forfalskning". De sier at ut fra denne definisjonen fyller digitale signaturer langt på vei identifiserings-, bevis- og autentiseringsfunksjonen, samtidig som symbolfunksjonen og avslutningsfunksjonen ikke har slått rot. Forfatterne påpeker at i hvor stor grad funksjonene blir oppfylt, er avhengig av hva slags metoder og teknikker som brukes for å aktivisere den digitale signaturen (PIN, passord). Forfatterne forteller ikke hvilke krav som må stilles til digitale signaturer for at de skal fylle symbolfunksjoner og avslutningsfunksjoner. Etter min mening fyller en digital signatur avslutningsfunksjoner. Den står ikke nederst på arket, men den er beregnet ut fra hele dokumentet.

Jeg har ikke klart å finne at noen har skrevet om usikkerhet og risiko ved å gå fra håndskrevne signaturer til digitale.

Generelle rettslige spørsmål

Galtung og Riisnæs [31] tok for seg spørsmålene om bevis og erstatningsansvar. Med hensyn til bevis dreier det seg om i hvilken grad bruk av en digital signatur avgir godt nok bevis for det den er ment å bevise. Den frie bevisføringen i Norge innebærer at det er opp til dommeren i den enkelte sak etter en samvittighetsfull prøvelse, selv å ta stilling til i hvilken grad et aktuelt bevis godtas ført. Deretter skal dommerne fastslå hvilken vekt beviset skal ha, f.eks. i hvilken grad en digital signatur er et godt bevismiddel. Når de gjør dette, ser dommerne på hva slags øvrige mekanismer som i en bevissammenheng virker sammen med den digitale signaturen. Eksempel på slike mekanismer kan være sikkerhetsrutiner.

Mht. erstatningsansvar har den nye teknologien brakt nye aktører på banen. Forfatterne reiser som eksempel spørsmålene om hva slags ansvar som kan pålegges den som leverer programvare for generering av nøkler og hva slags ansvar en nøkkeladministrator har. Men dette drøfter de ikke videre. Forvaltningsnettsamarbeidets rammeavtale "Spesielle vilkår for kjøp av TTP-tjenester" har erstatningsbestemmelser - beløp per sertifikat ved uaktsomhet etc., altså TTPens ansvar.

Signaturbegrepet i norske lover og forskrifter

Forfatterne fant mellom 509 og 573 dokumenter (paragrafer) som inneholder bestemmelser om underskrifter. I 15 av dem dreier det seg om signaturer som kompetanse (myndighet til å utføre en handling eller foreta en beslutning). Den andre kategorien har de inndelt etter visse typer dokumenter som skal påføres en underskrift. Funnene viser at svært mange bestemmelser er knyttet til offentlig

virksomhet eller til utveksling av informasjon med offentlig virksomhet. Justisdepartementet [57] har initiert en kartlegging av mulige lovgivningsproblemer innen hvert departement og underliggende etater.

4.2.4 Autentisering av en juridisk handling

ICRI [25] definerer en juridisk handling som et uttrykk for en intensjon og en normal effekt som skal resultere i en lovlig endring i en legal posisjon for forfatteren (underskriveren). Både identiteten til personen og hans vilje til å la seg binde til handlingen bør fastsettes slik at signataren ikke kan avvise sitt forfatterskap. I noen tilfeller bør tidspunktet for signeringen fastsettes. Hele prosedyren med å forvisse seg om eksistensen av hendelsen og graden av visshet for at den inntraff, kan beskrives som autentisering.

Noark-4 [114], Norsk arkivsystem, som skal følges i hht. arkivforskriftens § 2-9 [5], sier i sitt pkt. 10.2.2 at for "å autentisere en *sending* (ut av virksomheten) antas det tilstrekkelig å bruke virksomhetens (arkivets) digitale signatur".

> "For å autorisere dokumentinnhold må det imidlertid være mulig å påføre en eller flere personlige digitale signaturer på det enkelte dokument som skal autoriseres. En personlig signatur vil også kunne brukes til å autentisere sendingen."

I Noarks pkt 10.2.2 står det at et sertifikat tilknyttet en mottatt digital signatur, bare kontrolleres ved behov mot vedkommende TTP-tjeneste. Videre står det

> "Måten verifisering foregår på, betraktes imidlertid som Noark-utenforliggende. Også de uavklarte spørsmålene som gjelder TTP-tjenesten(e)s evne til å langtidsverifisere sertifikater må regnes som Noark-utenforliggende."

Dette oppfatter jeg som en uklar ansvarsfordeling i og med at Noark på sin s. 64 skriver at det må finnes garantier for at dokumentene er ekte og autentiske (ikke forfalsket) og på s. 174, aksepterer at digitale signaturer har egenskapene å bekrefte avsenders autentisitet, opprettholder dokumentets integritet og autoriserer dokumenters innhold. Det står ikke noe om hvem som har ansvar for garantier eller for å sette standarder på området. Avdelingsdirektør Ivar Fonnes, Riksarkivaren [90], sier at det er den enkelte etat som bestemmer hvordan autentisering skal foregå. På den andre siden fremhever Jens Nørve, Nærings- og handelsdepartementet [89], at det er viktig at det opparbeides sentral kompetanse på dette komplekse området. Dette er viktig bl.a. for å sikre mest mulig enhetlige løsninger for lagring av signaturene i "kongerike". Han antar Riksarkivaren her har et ansvar, eventuelt i samarbeid med f.eks. Statskonsult.

I kartleggingsbrevet fra Justisdepartementet [57] står det at Justisdepartementet, Nærings- og handelsdepartementet og Arbeids- og administrasjonsdepartementet har et særlig ansvar for at bla. elektronisk kommunikasjon skal "bli like akseptert, tillitsvekkende og ha samme juridiske holdbarhet som tradisjonell skriftlig kommunikasjon og dokumentasjon". Kartleggingsprosjektet åpner for å finne alle hindringene for overgang til elektronisk signatur. Men departementet vurderer i

hovedsak at det er lovverket som er til hinder, ikke at teknologien setter grenser som gjør at digitale signaturer ikke kan likestilles med håndskrevne signaturer på enkelte områder. "Ny teknologi som f eks elektroniske signaturer vil etter alt å dømme gjøre det ønskelig og forsvarlig å vareta de hensynene som ligger bak underskriftskravet ved bruk av elektroniske meldinger." Det nevnes lite om hvilke generelle krav man skal stille til elektroniske signaturer for at de skal ha samme juridiske stilling som håndksrevne underskrifter. Langtidslagring av dokumenter nevnes ikke som problemstilling.

4.2.5 Andre land og organisasjoners arbeid med elektroniske signaturer

Signaturbegrepet er drøftet av bla. EU, j.fr. ISTEV [52] og ICRI, [25], FN, jfr. UNCITRAL [141], av American Bar Association [2] og MIT, USA [28].

EU

EUs utkast til direktiv for elektroniske signaturer [26] har følgende definisjon:

> "a signature in digital form in, or attached to, or logically associated with, data and used by a signatory to indicate that signatory's approval of the content of that data and which meets the following requirements:
>
> A is uniquely linked to the signatory
> B is capable of identifying the signatory
> C is created using means that the signatory can maintain under his sole control
> D is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable".

Målsettingen er å gi et forutsigbart sikkerhetsnivå for juridiske handlinger [61].

Tyskland

Tyskland har vedtatt en egen lov for digitale signaturer [18]. Loven har følgende sammenheng mellom en personlig signatur og lovverket:

> "Where a personal signature is demanded in acts or other statutory regulations, it is intended that in the future the digital signature under the Signatures Act be accepted as equivalent to the personal signature."

Med en digital signatur mener landet [18]:

> "a seal affixed to digital data which is generated by a private signature key and establishes the owner of the signature key and the integrity of the data with the help of an associated public key provided with a signature key certificate of a certification authority or the authority according to § 3 of this Act."

I motsetning til EU og til Galtung og Riisnæs, se s. 60, knytter altså Tyskland en elektronisk signatur direkte til teknologien, til offentlig nøkkelmekanismer.

UNCITRAL Model Law

UNCITRAL's modellov for elektronisk handel [141] har en teknologinøytral definisjon for signaturer.

"(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

A a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

B that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature."

I guiden til modelloven står det om den "funksjonelle-ekvivalent"-tilnærmingen som ble brukt ved utformingen av loven. Loven er basert på erkjennelsen av at der juridiske krav foreskriver tradisjonelle papirbaserte dokumenter, oppstår det et hinder for utvikling av nye måter å kommunisere på. Begreper som *skriftlig*, *signatur* og *original* måtte tilpasses maskinbaserte teknikker. Tilnærmingen ble å analysere hensikten og funksjonene til de tradisjonelle papirbaserte kravene, for så å bestemme hvilke av disse hensikter og funksjoner som kunne oppfylles elektronisk. Samtidig var forfatterne av loven klar over at informasjonsteknologi kan kreve nye regler. Papir er lesbart med øyet. Elektroniske dokumenter må reproduseres på papir eller framkalles på skjerm.

USA

American Bar Association (ABA) bruker bare begrepet digital signatur, og ikke begrepet elektronisk signatur i sin Guidelines for Digital Signatures [2]:

"A transformation of a message using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's public key kan accurately determine

1 whether the transformation was created using the private key that corresponds to the signer's public key, and

2 whether the initial message has been altered since the transformation was made."

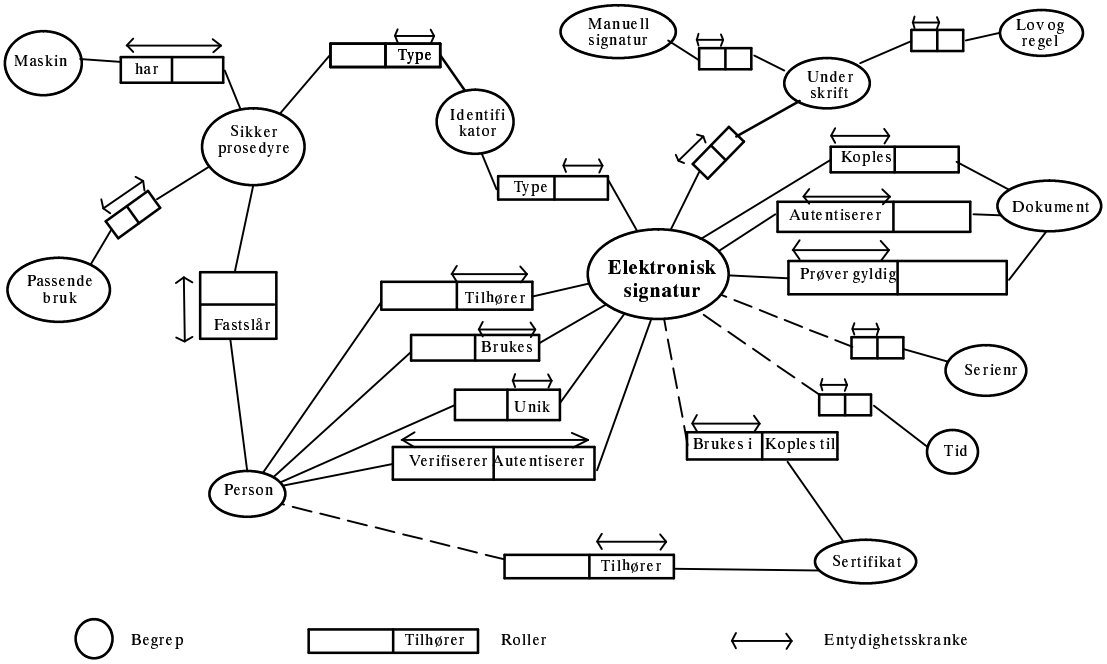
ABA påpeker at det er en del informasjon som må følge den digitale signaturen, inkludert

- algoritmen som brukes
- indikasjon på signatarens identitet eller på hvilken offentlig nøkkel som skal brukes for verifikasjon
- et tidsstempel
- et serienummer
- identifikasjon av sertifiseringsautoriteten, CA.

ABA nevner ellers nesten ikke serienummer eller tilsvarende mekanismer. (Serienummer er en nyttig mekanisme for å holde orden på rekkefølgen av oversendelser.)

USA har ikke føderalt regulerte lover for digitale signaturer. McBride Baker & Coles har listet definisjoner av begrepene elektronisk signatur og digital signatur

som brukes i ulike lover i de forskjellige amerikanske statene [68], [69]. Jeg har eksemplifisert dette i en Niammodell i Figur 9.



Figur 9 En Niammodell over amerikansk elektronisk signatur

Modellen leses slik at et sertifikat bare kan tilhøre én person, mens én person kan ha mange sertifikater og mange elektroniske signaturer. Begrepet *sertifikat* nevnes ikke i lovene, men kan ligge implisitt i en av egenskapene som nevnes i noen av lovene. Begrepet er sentralt hos ABA. Tid og serienummer står det ikke noe om i de amerikanske lovene. Modellen passer også for Norge. I midlertid er modellen avhengig av tidsperspektivet for å få med de fleste egenskapene jeg har definert i punkt 2.6.1 på s. 33.

4.2.6 Kvalifiserte sertifikater

Hensikten med utkastet til EUs direktiv for elektroniske signaturer er å tilrettelegge for bruk av elektroniske signaturer mellom medlemslandene og å bidra til deres legale aksept [26]. De forventes å bli behandlet på samme måte som håndskrevne signaturer, hvis de frambringes på en sikker måte og hvis de baseres på et 'kvalifisert sertifikat'. Sikre måter kan være at sertifikater baserer seg på fastsatte regler, f.eks. en policy, eller frivillige akkrediteringsordninger for sertifiseringsautoriteten.

Et kvalifisert sertifikat må i hht. direktivets Annex I inneholde:

a) An indication that the certificate is issued as a qualified certficate;

b) The identification of the certification service provider and the State in which it is established;

c) The name of the signatory or a pseudonym, which shall be identified as such;

d) Provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;

e) Signature-verification data which correspond to signature-creation data under the control of the signatory;

f) An indication of the beginning and end of the period of validity of the certificate;

g) The identity code of the certificate; (serienummeret)

h) The advanced electronic signature of the certification provider issuing it;

i) Limitations on the scope of use of the sertificate, if applicable; and

j) Limits on the value of transactions for which the certificate can be used, if applicable.

Det er ikke satt av plass til punktene a), i) eller j) i Versjon 3 av X.509 [38]. Det må eventuelt lages en utvidelse. Punkt d) oppfattes som uklart av dem som diskuterer egen tilpassning til kravene [108].

Internet-Draft IETF PKIX QC01 har laget en sertifikatprofil basert på RFC 2459 [112] som definerer underliggende sertifikatformater og semantikk for kvalifiserte sertifikater. Det legges opp til en samordning slik at det ikke skal bli konflikt med EU-direktivet. Kvalifiserte sertifikater utstedes bare til fysiske personer.

SEIS-SAT-prosjektet (Secure Electronic Information in Society, Self Assesment Test, Sverige) [8] har vurdert svenske og finske standarder opp mot i hovedsak RFC 2459. På noen områder skiller PKIX QC01 seg fra EUs krav. For noen krav er det uklart om de er obligatoriske eller ikke og om de er kritiske eller ikke. I hovedsak tilfredsstiller de svenske og finske standardene kravene til kvalifiserte sertifikater, med noen unntak. Sertifikatpolicyen som er utarbeidet for Forvaltningsnettsamarbeidet, FSP-HT [30], er basert på SEIS på de fleste områder. Arbeids- og administrasjonsdepartementet [108] vurderer at den holder kravene til kvalifiserte sertifikater på alle områdene unntatt punkt a).

Kvalifiserte sertifikater innbefatter visse krav til pålitelighet hos sertifiserings-autoriteten og dennes prosedyrer. Kravene stilles i direktevets Annex II (i stor grad i samsvar med ISO guidelines [49]) og i artikkel 3 punkt 4:

> "Member States may make the use of electronic signatures in public sector subject to additional requirements. Such requirements shall be objective, transparent, proportionate, and non-discriminatory, and shall only relate to the specific characteristics of the application concerned."

Begrepet kvalifisert sertifikat brukes til å beskrive vilkårene for å oppnå de rettsvirkninger som er beskrevet i direktivets artikkel 5 nr. 1: At medlemsstatene sikrer at en *elektronisk signatur* ikke nektes legal effekt, gyldighet eller gjennom-slagskraft bare fordi den er på en elektronisk form eller ikke baserer seg på et kvalifisert sertifikat eller basert på et sertifikat som er utstedt av en akkreditert sertifiseringsautoritet.

I Norge vil kvalifiserte sertifikater foreløpig måtte forholde seg til samlet norsk lov, og det vil sannsynligvis gi et diffust lovgrunnlag. I midlertid går Justis-

departementets kartleggingsprosjekt for tiden gjennom alle formkrav o.l. i norsk lovgivning for å identifisere bestemmelser som kan være til hinder for elektronisk kommunikasjon. Deretter kan man vurdere om det er mulig å finne fellestrekk som åpner for noen generelle regulatoriske grep (med visse unntak) eller om man må revidere hvert enkelt regelverk for seg for å få en presis regulering [97].

Etter min mening viser kravene til kvalifiserte sertifikater at:

- Det fins mange variasjoner som kan skape uklarheter,
- Det er vanskelig å definere hvordan infrastrukturen rundt digitale signaturer skal støtte den juridiske likestillingen mellom håndskrevne og digitale signaturer,
- EU, som andre land, har latt være å ta stilling til en rekke juridiske uklarheter ved overgang fra papirbaserte til elektroniske media før de setter likhetstegn mellom en håndskreven og en digital signatur,
- Det er et spørsmål om det er (teknisk) ønskelig/mulig å framstille elektroniske signaturer som ekvivalent med håndkrevne signaturer.

4.3 Egenskaper ved saksbehandling i det offentlige

Det offentlige skal ta i bruk digitale signaturer i stor skala. Det er en ny teknologi som kan få konsekvenser for organiseringen av arbeidet.

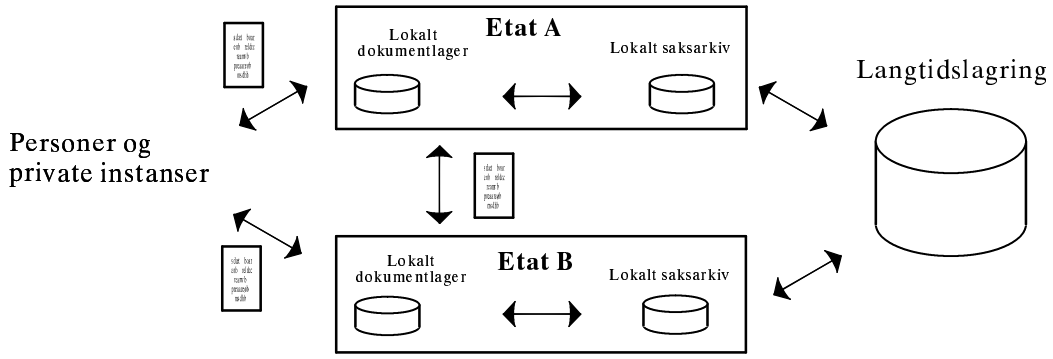
4.3.1 Saksgang

Et dokument oppstår i forbindelse med en saksgang i en etat. Det får kjennetegn som viser at det er ekte, og det deltar i en eller flere saksganger. Det arkiveres lokalt 25 - 30 år og sendes eventuelt til bevaring for framtida etter at saken dokumentet tilhører, er avsluttet.

Statens generelle kravspesifikasjon (SGK), Elektronisk saksbehandling [130], beskriver saksbehandling som:

- En prosess som utføres for å behandle saker på vegne av en virksomhet og som leder fram til en autorisert beslutning. Prosessen kan bestå av følgende aktiviteter: mottak og klargjøring av en sak, innsamling av informasjon, vurdering, avgjørelse/vedtak, ekspedering av vedtaksdokumenter.
- Saksbehandling er også å behandle informasjon og fakta, bruke lover og regler, følge prosedyrer, kommunisere med aktører som saken gjelder, og å treffe beslutninger.
- Saksbehandling kan gi andre resultater enn vedtak, for eksempel utredninger, uttalelser, prosjektplaner og nye regelverk.

Elektronisk saksbehandling innebærer at saksbehandlingen kan utføres med støtte av informasjonsteknologi.



Figur 10 Offentlig saksbehandling

I Norsk arkivsystem Versjon 4, Noark-4 [114], påpekes skillet mellom SGK's dokumentlager og et elektronisk arkiv. Dokumentlageret styres av saksbehandleren. Arkivet styres av Noark og er underlagt lov- og regelverk og strenge krav til kvalitetssikring.

4.3.2 Arkivloven

Etter den nye arkivloven § 6 [6] plikter alle offentlige organ å ha arkiv. Formålet er å trygge "arkiv som har monaleg kulturelt eller forskningsmessig verde eller som inneheld rettsleg eller viktig forvaltningsmessig dokumentasjon, slik at desse kan verta tekne vare på og gjorde tilgjengelege for ettertida." § 9 sier bl.a. at arkivmaterialet ikke kan "rettast på ein slik måte at tidlegare urette eller ufullstendige opplysningar vert sletta, dersom desse har hatt noko å seia for saksførebuinga, vedtak eller anna som etter føremålet med denne lova bør kunna dokumenterast."

Arkivforskriftens § 2-5 sier at "for databasar og anna elektronisk arkivmateriale skal det utarbeidast dokumentasjon som gjer det mogleg å nytte materialet også etter at den ordinære bruken er avslutta" [5].

Forskriftens § 2-13 gir Riksarkivaren ansvar for å godkjenne at det blir brukt bla. fullgode systemer og lagringsformat, se punkt 4.2.4 s. 62. I hht. §3-2 skal e-post, som etter form eller innhold må regnes som saksdokument, arkivmessig behandles som andre saksdokumenter. Men i Noark-4 [114] skriver de at "Tilfredsstillende løsninger som ivaretar den offentlige forvaltnings krav til dokumentformalisme, er imidlertid ikke innarbeidet i dagens e-postsystemer". Etter det jeg kan se, inneholder dette at det ikke er definert hvordan etatene skal forholde seg til innkommende, usignerte e-postdokumenter, som i henhold til lov krever underskrift.

Slik arkivloven og forskriften er formulert, vil ingen kunne sløyfe papir uten at statens arkivfaglige myndighetsorgan finner at det er forsvarlig. Kulturdepartementet skrev i brevet til høringsutkastene at det var to grunner til at de i

liten grad fant det formålstjenlig å tilpasse utkastene til elektronisk arkivmateriale [7]:

1 Papirdokumenter vil være det normale i mange år ennå,
2 Det er vanskelig å regulere noe som i svært liten grad er utprøvd.

Departementet mener det er mer naturlig å tilpasse og bygge ut regelverket etter hvert som en får mer praktisk erfaring med den nye teknologien. De påpekte at elektronisk baserte registre, spesialiserte fagsystemer og journalføringssystemer er langt mer sårbare enn papirbasert materiale.

4.3.3 Journalføring

I hht. arkivforskriften § 2-6 [5] skal alle offentlige organ ha en eller flere journaler for registrering av dokumenter i de sakene organet oppretter. Journaler skal føres elektronisk eller på papir. De skal bl.a. inneholde journalføringsdato, saks- og dokumentnummer, sender og/eller mottaker og dateringen på dokumentet.

I §2-10 står det at man skal legge opp til administrative rutiner som "sikrar at berre personale som leiinga har utpeikt til det, normalt arkivtenesta, kan utføre registrering og retting i journal- og arkivdatabasen." §2-14: "Systemene skal være godt nok dokumentert til at materialet kan nyttes også etter overføring til arkivdepot."

Der man ikke har elektronisk journalføring, skal dokumentene tas ut på papir. De skal påføres stempel som identifiserer dokumentet og knytter det til journalen. Arkivforskriftene henviser til Noark-standarden [114] for tilsvarende rutiner og dokumentidentifisering for elektronisk journalføring. I Noark-4 pkt. 2.1.4 står det at når saksdokumentene lagres elektronisk, må også alle opplysninger som merknader, kontrollinformasjon etc. i tilknytning til dokumentene lagres elektronisk for at man skal få et komplett elektronisk arkivsystem.

I Noraks pkt. 2.2.2 står det at når en saksbehandler henter et arkivdokument, skjer det ved en referanse til arkivdokumentet, ikke ved fysisk kopiering. Fra Noarks side er det et absolutt krav at arkivet er underlagt Noarks funksjoner for arkivstyring, tilgangskontroll og kvalitetssikring. Kvalitetssikring i arkivfunksjonen skjer ved å definere roller og aktører. Noark sikrer at saksbehandleren faktisk får tilgang til det korrekte dokumentet ved å sikre rutinene rundt dokumenthåndteringssystemet [90]. Men man kan likevel risikere at dokumentversjoner osv. ikke knyttes sammen. Programmeringsfeil i forbindelse med pekere er intet ukjent fenomen [3].

4.4 Arkivering

Langtidslagring av elektroniske dokumenter skaper nye utfordringer fordi man tar i bruk ny teknologi. Problemene blir påtrengende hvis man vil lagre dokumentene

med digitale signaturer. Dokumentet må kunne gjenskapes uendret hvis den digitale signaturen skal kunne autentisere dokumentet i ettertid.

4.4.1 Langtidslagring

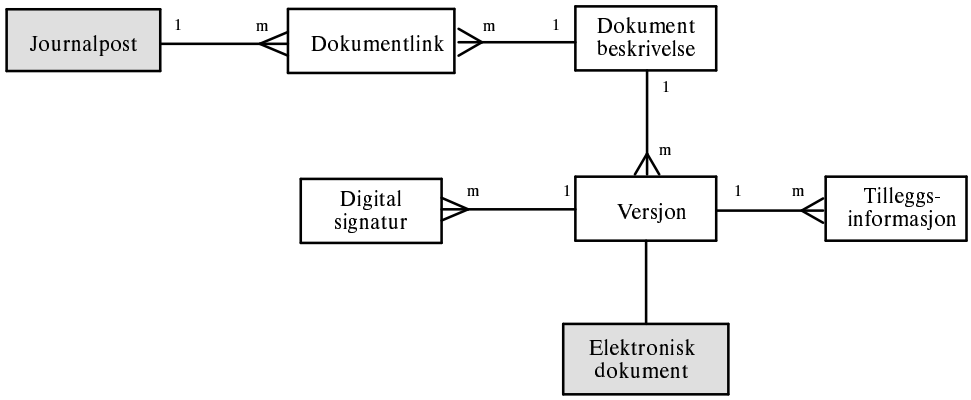
Etter arkivforskriftens § 5-2 kan arkivmateriale avleveres til Det statlige arkivverk (Riksarkivet og statsarkivene) etter 25 - 30 år. Ved avlevering overtar mottakende institusjon ansvaret for å opprettholde tilgjengeligheten til dokumentene (Noark-4 s. 72). For elektronisk arkivmateriale kan Riksarkivaren fastsette deponering av kopier på et tidligere tidspunkt. Etter forskriftens §2-13 kan Riksarkivaren fastsette om enten en elektronisk eller en papirbasert versjon av dokumentene, eller begge versjoner, skal avleveres til arkivdepot. Kulturdepartementet [7] påpeker at ingen kan sløyfe papiret uten at statens arkivfaglige myndighetsorgan finner det forsvarlig. I hht. § 5-8 "fastset Riksarkivaren spesifiserte krav til materiale som skal avleverast til Arkivverket". Kravene omfatter bla. ordning, dokumentasjon, merking, type og format.

Statskonsult [132] skriver at arbeidet med å holde edb-materiale tilgjengelig over tid, krever en viss spesialkompetanse, og at det derfor bør vurderes å endre reglene slik at edb-lagret materiale overføres til en sentral institusjon innen kortere tid. De er klar over at elektroniske dokumenter må konverteres til nye lagringsformater, men de tar ikke opp hvilke problemer det skaper i forhold til digitale signaturer.

Kulturdepartementet er i sitt høringsbrev [7] klar over at langtidslagring vil stille store krav til utvikling av teknologiske løsninger og til administrative rutiner. Det står mye i arkivforskriften om krav til arkivlokaler, men ingen ting om drift av edb-maskiner og opprettholdelse av nødvendig kompetanse. De skandinaviske riksarkivene [73] skriver utførlig om lagringsmåter, men heller ikke de nevner kompetansebehovet for å kunne drifte arkivene.

Noark [114] krever i sitt pkt. 5.1 at et elektronisk saksarkiv skal fylle den samme rollen som det tradisjonelle, papirbaserte arkivet. Et av problemene er at dokumentene må være lesbare og tilgjengelige også i framtiden. Noark påpeker at det må finnes garantier for at dokumentene er ekte og autentiske (ikke forfalsket). Det står ikke noe om hvordan det skal gjøres hvis den digitale signaturen er fjernet eller ikke kan verifiseres.

Dokumenter kan lagres i flere versjoner. På s. 65 i Noark-4 står det at dokumenter som er påført digitale signaturer, skal kunne lagres som egne utgaver, se Figur 11 som viser Noarks datamodell for elektronisk arkiv.



Figur 11 En forenklet datamodell for elektronisk arkiv i hht. Noark

Dette er utdypet i Noark-4 s. 70:

> *"Digitale signaturer*: Ved utveksling av e-post kan digitale signaturer brukes for å verifisere dokumenters *autentisitet* (at mottaker kan være sikker på avsenders identitet) og *integritet* (at innholdet ikke er endret). Digitale signaturer kan også brukes til autentitets-og integritetssikring av dokumenter som arkiveres i det elektroniske arkivet. Signaturen må da påføres dokumentet etter at det er konvertert til arkivformat."

Dette medfører enten at opprinnelig signatar må signere og avlevere i korrekt arkivformat eller at en annen enn opprinnelig signatar (f.eks. arkivar) signerer etter formatkonvertering.

> "I Noark skal det være mulig å arkivere dokumenter med digitale signaturer som en egen variant S. Slike dokumenter vil da fortsatt være verifiserbare. Signaturer og sertifikater skal dessuten kunne lagres separat i en egen tabell: *Digitale signaturer*. I denne tabellen skal det også lagres opplysninger om hvem som har verifisert signaturen og når det er gjort. På denne måten bevares spor etter signaturer og verifisering også i de tilfeller muligheten for fornyet verifisering har gått tapt. Mellom *Versjon* og *Digital signatur* er det et 1:M-forhold.
>
> *Tilleggsinformasjon:* Systemet skal automatisk logge en del informasjon i forbindelse med at dokumentet arkiveres elektronisk. Det gjelder tidspunktet for arkivering, og hvem som utførte arkiveringen. Likeledes skal det logges informasjon om når dokumentet ble konvertert til arkivformat og hvem som foretok konverteringen."

Statskonsult [132] skriver i forbindelse med lagring av digitale signaturer at det ofte ikke er nok for mottaker bare selv "å være sikker på at et dokument kommer fra A, han må også kunne bevise det for andre. Behovet for å kunne bevise det kan være til stede mange år etter at dokumentet ble utferdiget."

UNCITRAL's modellov [141] har følgende krav til bevaring av datameldinger:

> "Where the law requires that certain documents, records or information be retainted, that requirement is met by retaining data messages, provided that the following conditions are satisfied:
>
> A the information contained therein is accessible so as to be useable for subsequent reference, and

B the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
C such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received."

I midlertid beskriver heller ikke modelloven hvordan man kan demonstrere at informasjonen er intakt eller hvem som har ansvar for å definere hvordan det skal gjøres.

4.4.2 Digitale signaturer og langtidslagring

Statskonsult påpeker at det "kan være vanskelig å oppbevare en sikker digital signatur over lang tid. Har virksomheten dokumenter som må kunne autentiseres med stor sikkerhet etter lang tid, bør en vurdere andre autentiseringsmekanismer" [132]. De foreslår at virksomheten vurderer om den mottar henvendelser der autentisering av avsender ikke er av avgjørende betydning.

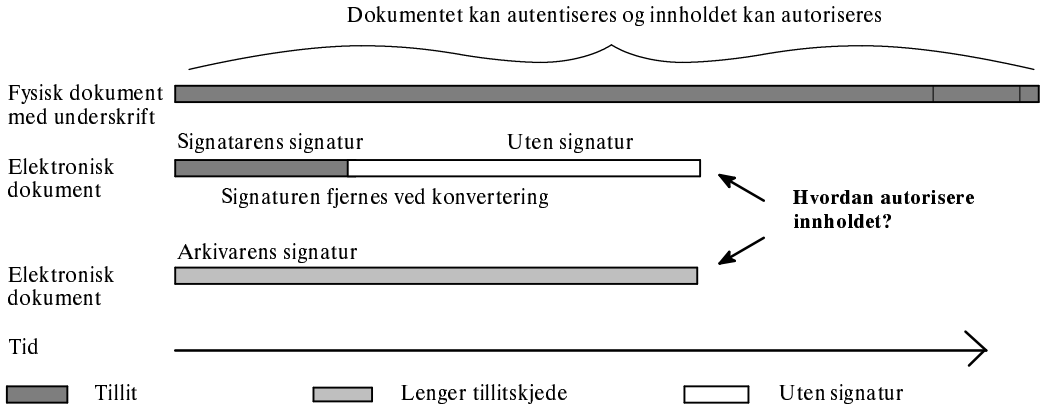
Noark er klar over at ved konvertering til annet format vil en digital signatur "knekkes" og ikke lenger være verifiserbar [114]. Grunnen til at den digitale signaturen ikke lenger kan verifiseres er bla. at tekstbehandlingsverktøyets format inngår i den digitale signaturen på tilsvarende måte som papir binder innhold og underskrift. Konvertering til arkivformat "opphever bindingen mellom dokumentet og signaturen. Etter dette kan ikke lenger den digitale signaturen brukes til å autentisere og integritetssikre det arkiverte dokumentet. I Noarks punkt 10.2.3 står det:

> "Ønskes bruk av digitale signaturer ved arkivering også etter en slik konvertering, må det påføres en ny signatur etter konverteringen. Man kan her enten signere med en hemmelig nøkkel knyttet til virksomhetens postmottak, eller velge å la den som foretar konverteringen påføre sin egen signatur. Det siste alternativet vil vanligvis være å foretrekke.
>
> En slik "arkivsignering" av et mottatt dokument ved konvertering til arkivformat bør først foretas etter at resultatet (innholdet) er kontrollert mot originalen. Ønskes spor bevart etter verifiseringen av de(n) opprinnelig påførte signatur(ene), kan man la den nye arkivsignaturen omfatte resultatet av verifiseringen av disse. Dokumentet kan i tillegg eventuelt lagres digitalt signert i den form det ble mottatt (det vil si i avsenderens produksjonsformat) slik at den konverterte arkivversjonen kan sammenholdes med originalen lå lenge denne er lesbar."

I Noarks krav K10.50 ser de på arkivsignaturen som et tegn på at det konverterte dokumentet er kontrollert mot produksjonsformatet og funnet innholdsmessig identisk. Men Noark tar ikke opp at de juridiske problemstillingene ved at et arkivert elektronisk dokument kan få en svekket stilling i forhold til et tilsvarenede fysisk dokument med underskrift.

Det at dokumentets ekthet/autentisitet etter en tid ikke kan verifiseres med den opprinnelige signaturen, skaper et skarpt skille mellom et elektronisk og fysisk

dokument. Universitet i Leuven, ICRI, [25] har tatt det opp, se punktet om gyldighetsperiode s. 31. Jeg har ikke fått svar på om de har sett nærmere på problemstillingen.



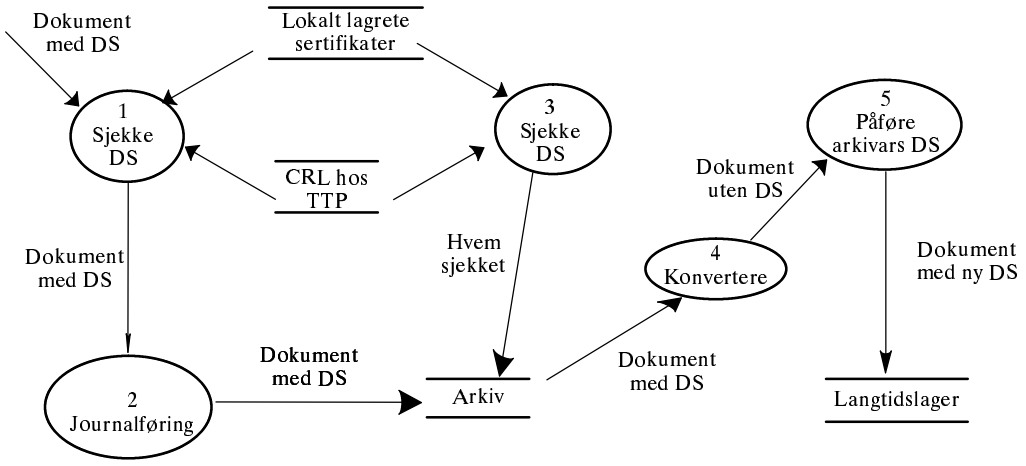
Figur 12 Arkiverte dokumenter med og uten signatur

Tillitskjeden blir lenger hvis arkivarens signatur kan erstatte signatarens. Dvs. en må stole ikke bare på den opprinnelige signaturen, men også på arkivarens. Jeg har ikke funnet problemstillingen rundt autorisasjon av tidligere signerte dokumenter omtalt verken i Justisdepartementet brev om kartlegging [57], i Det danske IT-sikkerhetsrådets rapport om Digitale dokumenters bevisverdi [53], eller i de danske Statens Arkivers krav til elektronisk arkivering [129].

I Noark-4 sitt pkt. 10.2.1 står det at Noark må ha opplegg for å utnytte og administrere digitale signaturer i to ulike sammenhenger:

1 Ved sending og mottak av (eksterne) dokumenter,
2 Ved arkivering.

Noark legges *ikke* opp til rutiner med bruk av digitale signaturer i intern saksgang. I brev til Kulturdepartementet skriver Riksarkivaren [113] at de ikke baserer seg på at digitale signaturer kan brukes til å verifisere dokumenter for langtidslagring. Selv om digitale signaturer har begrenset levetid, "så vil det ha verdi å bevare sporene som viser at de opprinnelig *ble* verifisert eller akseptert som autentiske". Personlige digitale signaturer fjernes før arkivering.



Figur 13 Mottak av digitalt signerte dokumenter

1 Signaturen sjekkes, ved behov verifiseres sertifikatet mot en TTP,

2 Journalføres som en versjon med digital signatur,

Forvaltnigsnettsamarbeidets FSP-1 policy påpeker at man alltid bør sjekke tilbakekallingslister [30].

Ved konvertering

3 Sjekkes den digitale signaturen,

4 Det registreres hvem som sjekket når. Dette lagres i journalen,

5 Eventuelt påføres arkivarens digitale signatur.

4.4.3 Tiltrodde tredjeparter

I hht. arkivforskriftens § 5-3 [5] skal offentlige organ som nedlegges, avlevere sine arkiv til arkivdepot eller til det organet som overtar saksområdet. En sertifikat-utsteder lagrer informasjon om knytningen mellom individer og deres offentlige nøkler, og de lagrer tilbakekallingslister. Begge deler skal kunne brukes i mange år i forbindelse med autentisering.

I dag ser det ikke ut til at en sertifikatutsteder er å betrakte som et offentlig organ, jf. FNS-avtaler med kommersielle aktører. Utsteding og administrasjon av sertifikater for digitale signaturer settes altså ut. I midlertid vil en slik TTP være et arkivskapende organ med verneverdig arkiv. Dersom arkivet betraktes som privat, skal Riksarkivaren holde oppsyn med det, § 13. Men i hht. § 14 er det bare hvis den private institusjonen mottar offentlig støtte at Riksarkivaren kan gi nærmere retningslinjer for arbeidet.

I Forvaltningsnettpolicien [30] står det i deres punkt 4.6.2 at registrering av alle viktige hendelser hos sertifiseringsautoriteter (SA) skal arkiveres i minst 15 år.

SAer skal revideres minst 1 gang per år (pkt. 2.7) og revisjonsloggen skal lagres i minst 7 år. Men jeg kan ikke se at revidering er det samme som at Riksarkivaren holder oppsyn med en TTPs arkiver.

Avdelingsdirektør Ivar Fonnes [90], Riksarkivaren, er enig i at bortsatte TTP-tjenester som sertifikatlister og tilbakekallingslister, vil være å betrakte som privat arkivmateriale. Men han kan ikke se at det er noe som Riksarkivaren skal ha oppsyn med. Han mener det er urealistisk, med den teknologien som fins, å arkivere sertifikater og tilbakekallingslister ut over tiden dokumentene er autentiserbare. Det vil bare være i ekstreme situasjoner at det vil være aktuelt å autentisere gamle dokumenter, og han tror ikke man vil bruke store ressurser på de få tilfellene.

4.5 Tvister

Grunnlaget for rettssikkerhet er forutberegnelighet og likhet. Der loven ikke dekker en problemstilling og de ulike aktørene blir uenige, kan tvisten komme opp for en domstol. Argumenter for å komme fram til beslutninger som er akseptable i hht. jussen, domstolene og rettssystemet, hentes fra rettskilder. Rettskilder er lover, forskrifter, instrukser og tilhørende forarbeider, rettspraksis og forvaltningspraksis, og "reale hensyn" [88].

4.5.1 Bevisvekt

Statskonsult [132] skriver at for dokumenter som ikke er undergitt formkrav, har underskriften betydning som bevismiddel. Retten avgjør på fritt grunnlag, og den er ikke bundet av om dokumentet er undertegnet. Når spørsmålet er hvorvidt dokumentet kan knyttes til utstederen, gir det liten mening å snakke om den digitale signaturens gyldighet. Men det gir mening å vurdere hvor stor sikkerhet den digitale signaturen gir for at ikke andre enn utstederen kan stå bak. Hvor stor bevisvekt man tillegger en digital signatur, må avgjøres i hvert tilfelle. Men kunnskap om virkemåten kan si noe generelt om hvor stor tillit en kan feste til den.

Statskonsult påpeker at sikkerheten i en digital signatur avhenger av to hovedfaktorer:

- Den tekniske sikkerheten avhenger av hvor avansert algoritmen er og hvor lang nøkkelen er,
- Hvor godt en kan hindre at uvedkommende får kjennskap til kodenøkkelen.

Man kan også få tilgang til å bruke en kodenøkkel uten å få kjennskap til selve verdien av den, f.eks. ved å besitte både smartkort og PIN [108]. Når koden blir kjent for andre, vurderes korteierens forhold opp mot en aktsomhetsstandard. Statskonsult skriver at det er likevel slik at digitale signaturer basert på moderne teknologi i de fleste tilfeller vil tilby større sikkerhet mot endringer og forfalskninger enn håndskrevne signaturer.

Her er det etter min mening viktig å ha klart for seg ulikhetene ved trusselbildene. For fysiske dokumenter kan man:

- Forfalske/endre innholdet i ettertid,
- Forfalske underskriften.

Disse to truslene - i ettertid - er langt på vei eliminert ved digitale signaturer så lenge algoritmer og nøkler holder. For elektroniske dokumenter er det i steden alvorlige trusler hvis programvaren for signering er korrupt, slik at man signerer noe annet enn det man tror.

Digitale signaturer i en bevisrettslig sammenheng

En del lovparagrafer sier noe om ulike typer dokumenters beviskraft. Ofte skrives det uttrykkelig om håndskrevne underskrifter. Galtung og Riisnæs [31] sier at dette i utgangspunktet ikke har noen praktisk konsekvens i forhold til adgangen til å føre digitale signaturer som bevis.

På forespørsel fra Nærings- og handelsdepartementet har Justisdepartementet utredet beviskraften av elektroniske dokumenter [56]:

> "I praksis vil partene i elektroniske avtaler antakelig normalt i sin bevisføring i første omgang legge frem utskrifter av de elektroniske dokumentene for domstolene. Dersom motparten ikke bestrider at utskriften gir uttrykk for et elektronisk dokument som har vært utvekslet mellom partene, er ytterligere bevisføring på dette punkt unødvendig. Dersom det skulle være behov for det, kan bevis for at tekniske sikkerhetsløsninger har vært benyttet, føres i form av f.eks. vitneutsagn eller muntlige eller skriftlige forklaringer fra sakkyndige som har foretatt en undersøkelse av dokumentet og systemet. Vi antar at utskrifter av elektroniske dokumenter i kombinasjon med sakkyndige erklæringer om at det er anvendt tekniske metoder med høy bevisverdi, vil ha stor overbevisningskraft."

Det er verd å merke seg at det ikke vil vises på en slik utskrift at dokumentet er digitalt signert, men man kan ta med en bekreftelse på korrekt utskrift.

Sikkerheten som bevis

Hvis partene i en sak vil legge en digital signatur til grunn, vil det bli et poeng å gjøre rede for hvorfor det er et godt bevismiddel. Galtung og Riisnæs [31] påpeker at da blir sikkerhet det viktige bevismiddelet. De henviser til bruken av digitale signaturer i det svenske Tulldatasystemet. Tollmyndigheten anser at man gjennom bruken av digitale signaturer (elektroniske segl) både sikrer meldingens integritet (sikring mot overføringsfeil) og ikke-benekting (at avsenderen ikke vil vinne fram med en påstand om at han ikke har sendt meldingen).

4.5.2 Rettigheter ved bruk av sertifikater

Hvilke rettigheter har en bruker av sertifikater (den som mottar og verifiserer en digital signatur)? En mottaker av et digitalt signert dokument må ha samme rettigheter som et håndsignert skriv gir. En underskrift på et fysisk dokument gir

mottakeren et forhold til den som undertegnet. Bruk av digitale signaturer gir brukeren ett forhold til avsenderen og ett til sertifikatutstederen. Brukeren må sjekke gyldigheten av sertifikatet mot siste tilbakekallingsliste [30]. En bruker kan inngå avtale med sertifikatutstederen, men jeg tror ikke det vil bli vanlig for enkeltpersoner. (Det vil bryte med hensikten for sertifikater å ha avtaler med alle sertifikatutstedere fordi man skal sjekke digitalt signert e-post fra mange land.) Vil brukeren kunne få tvister med både avsender og sertifikatutsteder?

Et sertifikat kan kanskje tilsvare et identifikasjonspapir. Men har en registreringsautoritet et større ansvar enn "Posten" når den aksepterer/godkjenner en persons identitet? Dette vil variere med sertifikatpolicien. Skattedirektoratet aksepterer samme identifisering som den Posten har ellers, se SLN-prosjektet punkt 1.6.3 s. 17. FNS-1 sertifikatpolicy [30] skriver ikke at sertifikater utstedt av en sertifiseringsautoritet er per definisjon ekte. I steden står det at sertifiseringsautoriteten ikke har ansvar ut over å sjekke informasjonen i sertifikatet etter vedtatte prosedyrer.

ABA sier i *Digital Signature Guidelines* [2], punkt 3.14 at sertifikatautoriteter ikke er ansvarlige for tap forårsaket av sertifikateier, eller som skyldes at man stoler på sertifikater utstedt av sertifikatautoriteten eller på informasjon som fins i et slikt sertifikat eller et repository.

4.6 Personvern og elektroniske spor

Formålet med utkast til ny personopplysningslov er *å beskytte enkeltindivider mot at deres personvern blir krenket gjennom behandling av personopplysninger* [81]. Lovutkastet er utviklet i hht. det vedtatte personverndirektivet fra EU (direktiv 95/46/EF). P*ersonopplysning* er opplysninger og vurderinger som kan knyttes til en enkeltperson. Elektroniske spor er ikke definert i lovutkastet. I hht. professor Dag Wiese Schartum, Avdeling for forvaltningsinformatikk (AFIN), Universitetet i Oslo, er det vanskelig å definere [101]. Begrepet knyttes særlig til opplysinger som generers ved kommunikasjon på nettet, opplysninger man ikke er klar over at legges igjen på ukjente steder. Det kan også legges igjen informasjon når man editerer et dokument eller behandler det i en applikasjon.

Lovutkastet skiller ikke mellom signerte og usignerte dokumenter. Det er det neppe grunn til å gjøre heller i og med at § 13 pålegger den behandlingsansvarlige å sørge for tilfredsstillende informasjonssikkerhet med hensyn til bla. integritet. Det kan tenkes at et signert dokument legger igjen flere spor i og med at dette dokumentet behandles av flere applikasjoner, bla. signeringsapplikasjon, verifiseringsapplikasjon og verifikasjonsprogrammer for sertifikater. Det kan bli vanskelig å etterkomme § 27 *Retting av mangelfulle personopplysninger* siden slike opplysninger lagres mange ukjente plasser. Den som samler inn personopplysninger må informere den registrerte (§ 19) og Datatilsynet (§ 31). § 28 gir forbud mot å lagre personopplysninger lenger det som er nødvendig for å gjennomføre formålet med behandlingen. Arkivloven [6] hjemler indirekte arkivering av personopplysninger.

Statskonsult [132] eksemplifiserer konflikten mellom personvernet og behovet for informasjon. Det vil f.eks. være mulig å lage et program som overvåker postjournaler og melder fra til eieren etter gitte kriterier, f.eks.:

- Laste ned alle dokumenter som sendes til eller fra noen i nabolaget,
- Laste ned til en advokat alle i et bestemt område som har kontakt med kommunens etat for byggesaker slik at vedkommende kan tilby sine tjenester,
- Laste ned alle henvendelser som berører en definert gruppe kjendiser.

Det fins ikke forbud mot å lage personprofiler som er ment å beskrive atferd, preferanser, evner eller behov, f.eks. i markedsføringsvirksomhet (§ 19). Men den behandlingsansvarlige skal informere den registrerte. Økt tilgjengelighet for offentlige dokumenter vil etter all sannsynlighet føre til nye bruksområder, særlig sett i sammenheng med den økte mulighet for selektering som elektroniske medier tilbyr og særlig hvis offentlige etaters postjournaler blir liggende on-line. Det vil føre til et mer gjennomsiktig samfunn, som reduserer den enkeltes mulighet til å ta kontakt med det offentlige uten at andre enn de som har en spesiell interesse, får kunnskap om dette. Dette kan føre til at enkelte vil vegre seg for å ta kontakt med det offentlige.

Dersom en TTP registrer hvilke nøkler som leveres ut til hvem, hvor ofte en enkeltperson har kontakt med trygdekontoret eller f.eks. hvem sine dokumenter som tidsstemples, vil TTPen etter hvert opparbeide seg et register med informasjon om hvem som har sendt meldinger til hvem og når dette har skjedd. Et omfattende register over kommunikasjon mellom enkeltmennesker eller mellom enkeltmennesker og forvaltningen vil kunne representere en trussel mot den personlige integritet.

Tatt i betraktning den betydelige trusselen mot den personlige integriteten denne typen opplysninger kan representere, påpeker Statskonsult at det bør vurderes om det er behov for å forskriftsregulere dette området for å sikre en betryggende behandling av denne type informasjon.

4.7 Krav til sikkerhet og kvalitet

Statskonsult skriver at når saker og dokumenter er papirbaserte, er det et problem at de kan komme bort, enten under saksbehandlingen eller ved transport [132]. I et elektronisk system vil truslene ha en annen karakter. De elektroniske dokumentene vil kunne endres, slettes eller være tilgjengelige for andre enn dem som er autoriserte brukere. De vil kunne være utilgjengelige for autoriserte brukere dersom strømmen går.

Statskonsult påpeker at bruk av elektroniske saksbehandlingssystemer vil medføre avhengighet av ekstern bistand til implementasjon og vedlikehold av systemene. "Det er ikke urimelig å anta at en datakonsulent under oppdrag vil kunne kopiere en hel database fra f.eks. et sosialkontor uten at dette vil bli oppdaget." De reiser

spørsmål om denne tilgangen er forenlig med forvaltningslovens § 13 b. Per i dag fins det ingen formelle krav til datakonsulenter. Tjenestemenn innenfor organet kan få tilgang i den utstrekning det er nødvendig for å oppnå en hensiktsmessig arbeidsordning. Der er det ingen forskjell på en arkivar og en system-administrator. Statskonsult utdyper ikke temaet om at autoriserte personer kan gå ut over sine fullmakter.

De skandinaviske riksarkivene [73] reiser problemstillingen om bevisvekt ved langtidslagring av elektroniske dokumenter og muligheten for utro tjenere.

> "Även om betonande av kravet på beviskraft tilsvidare uteslutande är en teoretisk fråga måste man medge att handlingar i elektronisk form som förvarats en längre tid inte har självklar beviskraft. Minimikravet är att en och samma person aldrig utan övervakning bör få komma åt depositions- og säkerhetskopian."

Det danske IT-Sikkerhetsrådet legger vekt på at man trenger organisatorisk adskillelse mellom funksjoner slik at en enkelt person ikke har kontroll over alle funksjoner i en prosess [53].

Personregisterlovens § 8 stiller krav til kvalitet på opplysninger og registre som brukes til å fatte avgjørelser. Regelen skal sikre korrekt avgjørelsesgrunnlag og pålegger korrigeringsplikt for uriktige eller ufullstendige opplysninger samt plikt til å begrense eventuell skade. Korrigering innebærer at opplysningene endres i form av retting, sletting eller supplering.

Et eksempel på saksbehandlingsregler som virker kvalitetssikrende, fins i *Reglement for departementenes organisasjon og saksbehandling*, § 9, 1984. Der står det at alle som deltar i behandlingen av en sak, skal påføre den sin signatur. Det er en regel som sikrer at en i ettertid kan kontrollere at blant annet kvalitetssikring virkelig er gjennomført. Statskonsult [132] påpeker at ved innføring av automatiserte prosesser er det viktig å være oppmerksom på at forvaltningsretten forutsetter en individuell behandling av saker. Ved elektronisk saksbehandling må man finne mekanismer for å få til den samme kvalitetssikringen og sporbarheten. Statskonsult tar ikke opp hvordan dette kan løses ved langtidslagring. Noark-4 løser dette ved automatisk registrering av ansvarlige for utførte nøkkelaktiviteter og ved systemfunksjonene for aktivitetslogging, deres pkt. 10.2.1, [114]. Som tidligere nevnt foreslår Noark å ikke bruke digitale signaturer ved intern saksgang.

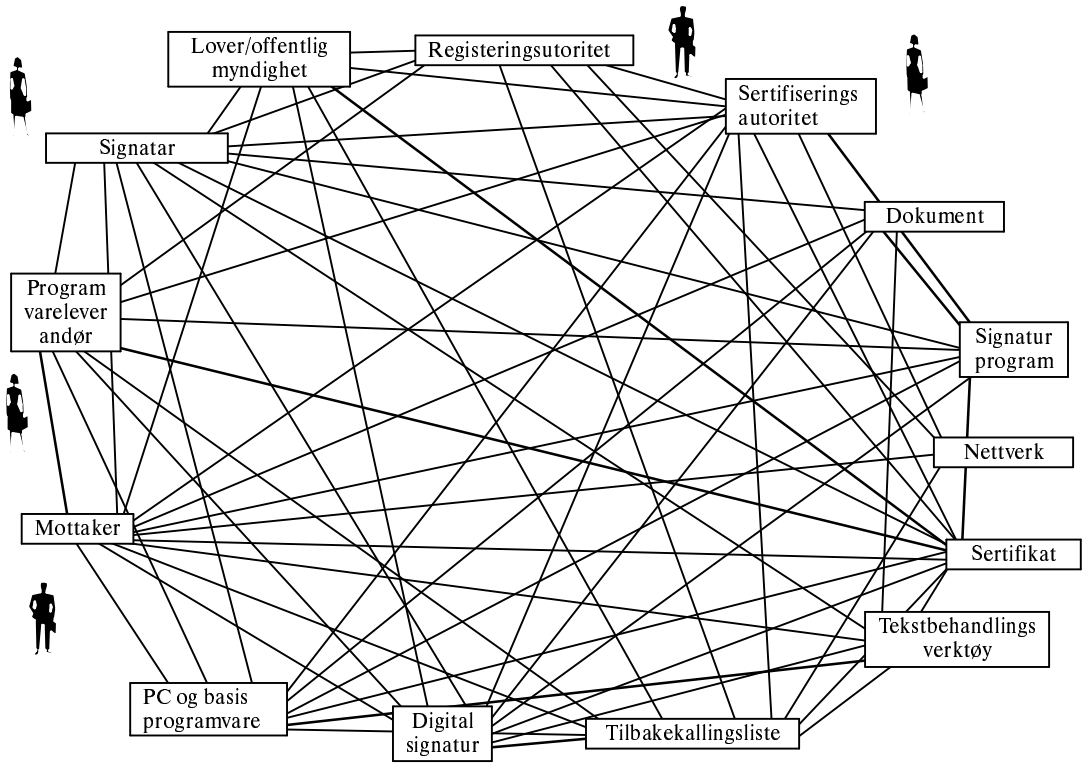
Det kan se ut som om bruk av digitale signaturer blir mer tungvint for mot-takeren enn en håndskreven underskrift er.

4.8 Diskusjon

4.8.1 Aktør-nettverkperspektiv

Ved overgang til bruk av digitale signaturer vil det opptre langt flere aktører/ aktanter fordi man tar i bruk en annen teknologi som grunnlag:

- Det elektroniske dokumentet
- Tekstbehandlingsverktøy
- PC og basis programvare
- Den digitale signaturen
- Sertifikateier/signatar
- Sertifikatbruker/mottaker
- Sertifiseringsautoriteter
- Nettverk
- Registreringsautoriteter
- Signaturprogrammer med programer for hashalgoritmer
- Tilbakekallingslister
- Programvareleverandører
- Lovverket og offentlige myndigheter
- osv.



Figur 14 Eksempel på aktanter rundt et digitalt signert dokument

Ettersom samhandlingen blir langt mer kompleks enn for fysiske dokumenter, vil lovverket og jurister bli viktige aktører for å øke rettssikkerheten. Ny teknologi ser ut til å kreve ikke bare en offentlig nøkkelinfrastruktur, men også en annen organisering av arbeidet i og med at det opptrer så mange nye aktører. Nettverk er f.eks. med på denne figuren fordi mottakeren trenger å sjekke tilbake-kallingslister. I midlertid har jeg ikke tatt med nettverk som overføringsmedium for her fins det flere alternativer. Sammenlikn forøvring med aktantene rundt håndskrevne signaturer på Figur 7 s. 25.

4.8.2 Autentisering

Fysiske dokumenter autentiseres bare hvis det er tvil, det oppstår en tvist eller ved innlevering med bruk av legitimasjon. Digitalt signerte dokumenter autentiseres i regelen alltid, men det kan være vanskeligere å autentisere dem i ettertid. I norske lover og regler er det ikke skrevet ned hva som menes med autentisering av en signatur. Det åpner for skjønn ved vurdering av fysiske dokumenter, som ikke fins ved bruk av digitale signaturer. Verken Statskonsult [132] eller Noark-4 [114] beskriver hva autentisering innebærer når man ser det uavhengig av teknologi. Statskonsult tar ikke høyde for at kopieringsegenskapen ved et elektronisk dokument gjør det nødvendig å sjekke dokumentets ekthet oftere, f.eks. sjekke den digital signaturen ved mottak av dokumenter. Det at man ikke har definert hva det innebærer å verifisere en digital signatur eller hvordan det skal gjøres, er en signaleffekt overfor framtidige brukere.

I arkivforskriftens § 2-13 står det at "en forutsetning for elektronisk lagring av saksdokumenter er at det blir nytta fullgode system, rutinar, dokumentlagrings-format og lagringsmedium som er godkjende av Riksarkivaren gjennom generelle føresegner eller enkeltvedtak." Så vidt jeg kan se, må dette innbefatte at Riksarkivaren godkjenner bruken av digitale signaturer. Ivar Fonnes, Riks-arkivaren [90], påpeker at heller ikke fysiske dokumenter autentiseres ved mottak til arkiv. Det er neppe fordi det ikke er ønskelig, men fordi det ikke er praktisk mulig å autentisere dem. Dersom man tar i bruk digitale signaturer, vil det være mulig å sjekke mange dokumenter. Da er det ingen grunn til å opprettholde "gammel praksis".

I hht Noark-4 [114] erstattes underskrivernes digitale signaturer med arkivarens ved langtidslagring. Det står at da mister man autorisasjonen i forhold til dokumentets innhold. Men det er samtidig et av kravene ved elektronisk arkivering. Regnes sporbarheten og autorisasjonen godt nok ivaretatt når denne informasjonen + en digitalt signert versjon lagres? Jeg har ikke funnet at de juridiske konsekvensene av manglende autorisasjon i forhold til innholdet er diskutert noe sted av jurister eller av Riksarkivaren. ICRI hevder at man vil miste mye av tilliten til den juridiske handlingen dokumentet tidligere representerte [25]. Det er Økstad og Grønvold, Kommunal- og regionaldepartementet, enige i [107].

Beskyttelse av data ved overføring mellom aktører er gjenstand for rettslige vurderinger f.eks. [59], og digitale signaturer regnes som en god beskyttelse i den forbindelse. Derfor er det interessant at det er ok å fjerne signaturene ved arkivering i etater eller riksarkiv. Det kan tyde på at man mener at tilliten til offentlige etater gjør at man ikke trenger autentisering internt. Så vidt jeg vet er dette ikke diskutert. Det er ikke i alle land at folk har samme tillit til de offentlige etatene.

Det er uklart for meg hvilket behov det skal dekke å lagre digitalt signerte versjoner. Når man har kopiert til nye formater, så er det ikke lenger mulig å verifisere signaturene mot de nye formatene. Gamle formater vil raskt bli foreldete. En annen sak er å lagre alle sporene.

4.8.3 Definere signaturers funksjonalitet

I forbindelse med digitale signaturer beskriver Galtung og Riisnæs signaturers funksjonalitet som om digitale signaturer dekker dem [31]. Men de skriver ikke om hva som skal gjøres med de egenskapene som ikke dekkes av en digital signatur, f.eks. hvilke krav som må stilles til digitale signaturer for at de skal fylle symbol- og avslutningsfunksjoner. Juristene legger vekt på at man må forstå at man signerer, men de har ingen løsning på problemet i den elektroniske verdenen. Som Statskonsult [132] og Riksarkivaren [114] går de rett over til å akseptere digitale signaturer som mekanismen som skal erstatte håndskrevne signaturer. Dette har, så vidt jeg kan se, en sterk påvirkningskraft overfor andre interessenter og framtidige brukere, etater, private organisasjoner og enkeltpersoner som ønsker å ta den nye teknologien i bruk. Jurister er viktige aktører ved overgangen fra håndskrevne til digitale signaturer. Det de mener om juridiske konsekvenser, får følger for alle brukere av digitale signaturer ved en konflikt.

Det at de viktige aktantene, jurister og lovmakere, har hoppet over det viktige systemutviklingssteget å definere hva sammenhengen er mellom håndskrevne og digitale signaturer, skaper ikke tillit hos de framtidige brukerne. Dette arbeidet er heller ikke nevnt eksplisitt i kartleggingsbrevet fra Justisdepartementet [57]. Denne 'unndragelsen' er ikke spesiell for Norge, j.fr. punktene 4.2.5 og 4.2.6 der jeg tar for meg andre lands og organisasjoners arbeider på området.

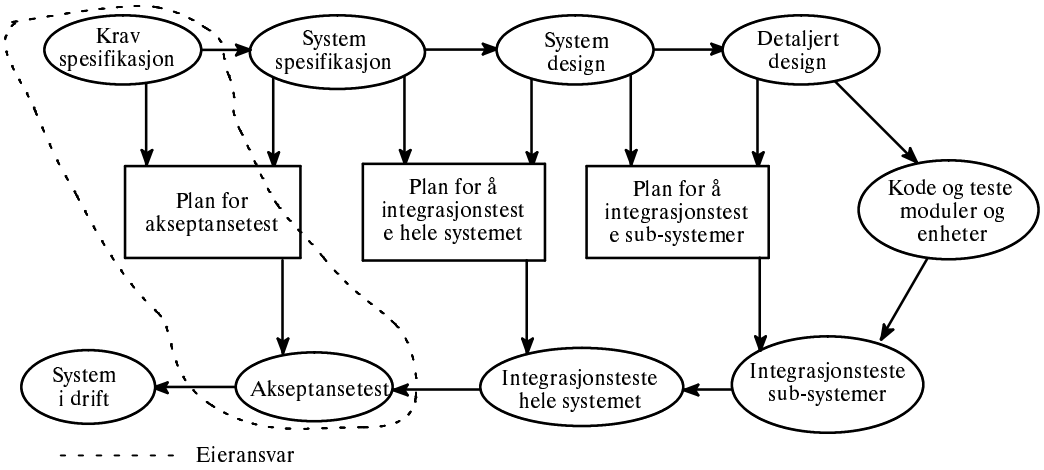
Det er derfor uklart for meg hvem som har ansvar for å definere signaturers funksjonalitet som grunnlag for hvilke krav man må sette til digitale signaturer.

4.8.4 Programmer for digitale signaturer

Dag Wiese Schartum skrev på s. 106 i sin doktoravhandling *Rettssikkerhet og systemutvikling i offentlig forvaltning* [118] at "Korrektheten av edb-programmer i forvaltningens saksbehandlingssystemer er åpenbart av avgjørende betydning ved vurderingen om i hvilken grad edb-basert saksbehandling kan sies å være rettssikker." På side 144 tar han opp at "instrukser og ikke skrevne normer i forvaltningen har dét fellestrekk at de begge tar sikte på å gi anvisninger på løsninger i rettsspørsmål". Etter min mening faller autentisering inn under denne problemstillingen. Her er det innarbeidet eller preferert (ikke-dokumentert) praksis som danner grunnlag for programmering. Schartum viser at det er mulig å knytte tvil til noen av de tolkningsvalg som treffes ved systemutviklingen. Han viser at i de programsekvensene han gikk igjennom, var det rom for uenighet om den regelforståelsen som var nedfelt i dem.

En underskrift oppfattes som gyldig selv om det kommer kaffeflekker på det fysiske dokumentet, selv om det er en ekstra blank et sted eller uthevet skrift manlger, men ikke hvis meningsinnholdet er endret [88].

Etter min oppfatning er det ikke-dokumentert praksis og skjønn som skal danne et utgangspunkt for programmer for digitale signaturer. Ved bruk av slike programmer får man langt mer faste og entydige svar enn juridisk praksis ellers vil gi. Det gir en avskalling fra diffuse brukerkrav til en bestemt produktspesifikasjon. Jeg opplever at verken Statskonsult, juristene eller Riksarkivaren helt vil vedkjenne seg problemstillingen. I hht. Tom Gilb produseres de fleste feil i produktspesifikasjonsfasen [33]. Barry Boehm oppsummerer aktiviteten *validering* som "Are we building the right product?" til forskjell fra *verfisering*: "Are we building the product right?" [11]. IT-personell kan intervjue framtidige eiere og brukere av et system om hvilke krav de har. Men det er bare eierne og brukerne som kan validere det ferdige resultatet, foreta akseptansetesten, j.fr. Figur 15 [125]. På den andre siden så kan de neppe ha ansvaret for kravspesifikasjon, opplegg for akseptansetest og akseptansetest/evalusering alene.



Figur 15 Testfaser i programutviklingsprosessen

ICRI [25] har sett mer utførlig på egenskaper ved håndskrevne og digitale signaturer, men de har heller ikke forslag til hvordan man skal evaluere resultatet.

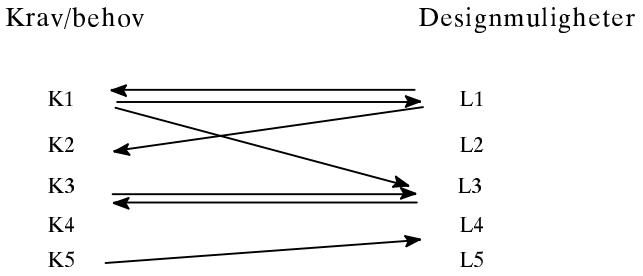
I *A Rational Design Process: How and Why to Fake It* [82] stiller David Parnas spørsmålet om hvem som bør skrive kravspesifikasjonen.

> "Ideally, the requirements documents would be written by the users or their representatives. In fact, users are rarely equipped to write such documents."

Jeg savner en avklaring av hvilke instanser som eier problemstillingen, en kravspesifikasjon og hvilke krav det offentlige stiller til å akseptere et datasystem for digitale signaturer. Departementene, underliggende etater og jurister bør være med på å definere behovene og hvordan man skal finne ut hvilke som nås.

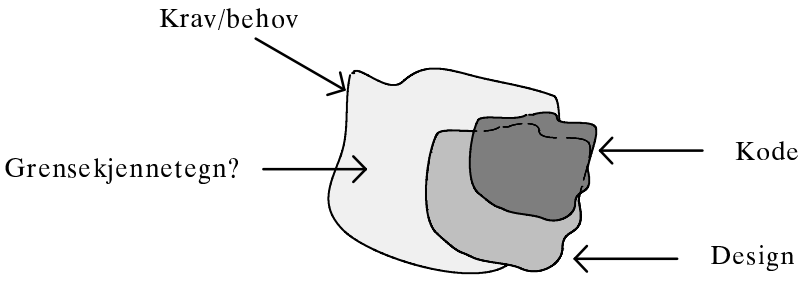
I midlertid har det blitt tydelig for meg at det er en særlig vanskelig oppgave. man skal beskrive de uhåndgripelige egenskapene ved en underskrift. Så skal det

skrives en kravspesifikasjon om hvordan egenskapene skal representeres ved hjelp av en teknologi som man heller ikke vet mye om. OECD [79] påpeker at det er viktigere å forstå hva en digital signatur kan gjøre, enn å forstå hvordan teknologien virker. Det er selvfølgelig riktig. Men hvis ikke teknologien virker på den intenderte måten, så får man et vesentlig hull i den logiske overgangen fra håndskrevne til digitale signaturer.



Figur 16 Mulig sammenheng mellom krav og tekniske løsninger

Jeg tror ikke det er en enkel sammenheng mellom krav og tekniske løsninger som Figur 16 gir inntrykk av, f.eks. at det fins et veldefinert krav som kan løses av en eller to bestemte designmuligheter. Ettersom egenskapene ved håndskrevne signaturer og autentiseringen av dem hører med til begrepet ikke-dokumentert praksis og skjønn, må kravene bli difuse og vanskelige å definere. Da må det også bli difust hvordan designet skal bli, og kodingen vil ikke alltid realisere alt som designes. Man kan heller ikke være sikker på at det som er utenfor designet, er uinteressante aspekter (grenseegenskaper) ved signaturfunksjonenene.



Figur 17 Sammenheng mellom krav, design og kode

4.8.5 Hvem trenger sertifikater?

Statskonsult [132] har ikke tatt sikte på å skrive en kravspesifikasjon for hva som trengs i forbindelse med bruk av digitale signaturer. Men de nevner i liten grad behovene som privatpersoner får, hvis de skal kommunisere elektronisk med offentlige etater. Her tenker jeg på at enkeltindivider kan trenge å oppbevare og autentisere mottatte dokumenter ettertid.

I Stortingsmelding nr. 41 om elektronisk handel [137] påpekes det at teknologiske løsninger i seg selv ikke er viktige, men dersom valg av teknologi medfører

organisatoriske endringer, vil disse endringene ha betydning for den rettslige reguleringen. Justisdepartementet har bedt departementene og deres etater vurdere behovet for lovendringer ved bruk av digitale signaturer. Jeg håper noen lager en risikoanalyse ved bruk av digitale signaturer. Den bør ha vurdering av:

- Hva taper man på å ikke ta i bruk digitalt signerte dokumenter,
- Hva taper man på å ta i bruk digitalt signerte dokumenter,
- Hva taper man på å ikke langtidslagre signaturen med dokumentene,
- Hvor er de største risikomomentene ved bruk av digitalt signerte dokumenter,
- Hva mangler av teknologiske løsninger,
- Risikoen ved å bruke enklere løsninger enn digitale signaturer og sertifikater,
- I hvilke situasjoner er tap av tillit og anseelse størst,
- Konsekvenser for privatpersoner dersom de velger å bruke digitale signaturer i kommunikasjon med offentlige etater.

Risikoer og verdier vil variere med situasjonenene som kan opptre. Det danske IT-Sikkerhetsrådet legger vekt på at man trenger å gjennomføre en risikoanalyse for å fastlegge hvor høy grad av sikkerhet man trenger [53].

Når det er pålegg om underskrift tilknyttet et dokument, vil offentlige etater ut fra egenskapene ved elektroniske dokumenter, ha behov for å verifisere at en digital signatur er ekte. Dvs. etatene trenger at privatpersoner har sertifikater tilknyttet sine offentlige nøkler.Det er foreløpig ikke stilt offentlige krav til privatpersoners sertifikater. Det offentlige må spesifisere hvilke sertifikater som godtas fra private personer og bedrifter, dvs. hvilke krav stilles til legitimasjon.

Sertifikater vil medføre ekstra utgifter og ekstra arbeid for privatpersoner. Jeg har ikke inntrykk av at privatpersoner i samme grad vil være opptatt av å verifisere ektheten av elektroniske brev som kommer fra en offentlig etat. Dersom det kommer til en tvistesak, kan personen alltids få en ny utskrift fra etaten og legge fram den. I hovedsak har vi tillit til offentlige etater i Norge. Privatpersoner trenger å vite at de tjener på å bruke sertifikater i sin kommunikasjon med det offentlige. De vil trenge sertifikater i forbindelse med betalingstransaksjoner, men disse sertifikatene utstedes i en lukket bankverden.

Det kan finnes situasjoner der en privatperson vil måtte stole på seg selv og sin PC. Dette gjelder f.eks. der vedkommende selv har ansvaret for et elektronisk dokument (originalen) eller hvis vedkommende kommer i konflikt med en offentlig etat. I noen tilfeller kan privatpersonen bruke en elektronisk notar. Det finnes ingen slik tjeneste i dag og det er heller ikke planer om det. I andre sammenhenger trenger vedkommende å ha en god PC, god programvare, gode konverteringsprogrammer ved migrering til nye plattformer osv.. Det kan bli dyrt og kreve gode kunnskaper f.eks. i en tvistesituasjon.

4.8.6 Tvister

Signaturprogrammer er på den ene siden skrevet slik at de realiserer en algoritme. Sikkerheten er avhengig av bla. hvor god algoritmen er, nøkkellengden og

sikkerhetsrutiner rundt programmet og nøkkelen. På den andre siden er programmet løsningen på en rettslig problemstilling, om digitale signaturer er juridisk likestilte med håndskrevne signaturer. Det siste er i hvertfall vanskelig.

Jeg har inntrykk av at jurister ønsker å overlate avklaringen av den siste problemstillingen til rettsapparatet. Statskonsult [132] skriver om den frie bevisbedømmelse. Jeg vurderer det slik at det kan stille store krav til dommere, hvis ikke problemstillingen blir mere utredet før en tvist, enn den er i dag.

Det fins et ansvarsforhold mellom sertifikatautoritet og sertifikateier. Kan en som skal verifisere en digital signatur, sertifikatbruker/mottaker, komme i konflikt med sertifiseringsautoriteten? NHD påpeker i et rammenotat i forbindelse med EU's forslag til dirketiv for elektroniske signaturer [27] at det kan oppstå et ansvar i forholdet mellom en sertifikattjenesteleverandør og en sertifikatbruker som stoler på innholdet i et sertifikat eller en katalog. Et tredje ansvarsspørsmål kan oppstå hvis en bruker uriktig er blitt innført i en katalog uten å være kunde hos tjeneste-leverandøren.

Hvis en etat ikke automatisk autentiserer en digital signatur ved mottak av et dokument, vil det styrke motparten i en tvist.

4.9 Oppsummering

4.9.1 Sammendrag

Digitalt signerte dokumenter trenger en langt mer komplisert infrastruktur enn håndsignerte papirdokumenter. Det ser ut til at lovverket bør avklare en del nye problemstillinger.

Skriftlighet

- Skriftlighetskravet er i hovedsak satt ut fra bevishensyn.
- Man ønsker å sikre dataintegritet, å vite hvem som signerte og signatar-avhengighet.
- Et fysisk uttrykk i form av papir er uavhengig av tid, rom og menneskene som forfattet dokumentet

Tilgjengelighet

- Problemer med dokumenters tilgjengelighet gir seg ulike uttrykk for fysiske og elektroniske dokumenter.
- Det fins ikke PC'er alle steder for alle mennesker, slik at tilgjengeligheten er vesentlig mindre for privatpersoner enn for det offentlige eller folk i arbeid.
- Hvis man har en PC med kommunikasjonsmuligheter og tilgangsrettigheter, er arkivene tilgjengelig samme hvor man befinner seg fysisk.

Autentisering

- Håndskrevne signaturer har tradisjon for å være garantist for dokumenters ekthet og gyldighet.

- De er et bevismiddel for knytningen mellom en person og en disposisjon.
- Det står ikke noe sted om hvordan man autentiserer håndskrevne underskrifter, bare at det gjøres ved tvister.
- Det er ikke obligatorisk i alle reglementer å sjekke sertifikatet knyttet til en offentlig nøkkel.
- Det står ikke klart at man bør autentisere en digital signatur med én gang, for å sikre autentisitet.

Digitale signaturer

- Det står lite om hvilke sider ved en håndskreven underskrift som dekkes av en digital signatur.
- Digitale signaturer forventes ikke av Noark å bli brukt internt i forvaltningen.
- Den digitale signaturen til en arkivar kan autentisere et dokument som sendes ut fra etaten (Noark).
- Skal innholdet autentiseres, må en eller flere saksbehandlere signere.

Langtidslagring

- Langtidslagring av elektroniske dokumenter skal ha samme egenskaper som lagring av fysiske dokumenter.
- Noark foreslår i hovedsak å erstatte eksterne signaturer med arkivsignaturer ved lagring.
- Informasjon om bl.a. sporbarhet, saksbehandlere osv. lagres med dokumentene.
- Digitalt signerte dokumenter lagres i egne versjoner.
- Arkivloven stiller ikke krav til sikring av maskin- og programvare.
- Arkivloven stiller ikke krav til sikring av kunnskaper om å behandle gammelt elektronisk materiale.

Tvister

- Nærings- og handelsdepartementet og Justisdepartementet godtar bruk av digitalt signaturte dokumenter som bevismateriale i en tvist.
- Mottakeren av et dokument kan få en tvist med sertifiseringsautoriteten.
- De første tvistesakene kan komme til å konkludere på et svakt rettsgrunnlag.

Konsekvensene av at elektroniske dokumenter er lette å kopiere

- Man må finne måter / bestemme regler for å tidfeste hvilken dokumentversjon som gjelder.
- Det er uklart når man kan godta andre måter enn digitale signaturer for å bestemme hvem som er signataren.

Tillit

- Det tas lite opp hvordan tiden påvirker tilliten til et elektronisk dokument. Riksarkivaren skriver at beviskraften kan bli mindre.
- Det er ikke skrevet mye om utro tjenere og deres nye muligheter for å gå utover egen autorisasjon.
- Det tas lite opp om utro tjenere kan bli et større problem ved bruk av elektroniske dokumenter.

- Det offentlige er klar over at elektronisk saksbehandling må støtte kvalitet på arbeidet og individuell behandling. Dette løses ved at informasjon om saksbehandlerne følger dokumentet.

Personvern vs. offentlighetsloven

- Teknologien gir økt tilgjengelighet og økt mulighet for sammenkopling av personinformasjon.
- Man må vurdere personvern opp mot offentlighetsloven og mot mulige nye bruksområder.

4.9.2 Vurdering av lover og regler mot ønskete egenskaper

Jeg har sett på lovverket opp mot ønskete egenskaper ved elektroniske dokumenter, j.fr. pkt. 2.6.1, side 33.

A Et dokument kan lages og leses alle steder

Statskonsult er klar over at ikke alle privatpersoner har tilgang til PC og baserer seg på å bruke papir i flere år framover. Kulturdepartementet er opptatt av det samme.

B Et dokument skal kunne finnes igjen og leses så lenge det oppbevares

Både Statskonsult og Riksarkivet er klar over problemstillingen. Riksarkivet har foreslått formater for langtidslagring. De dekker ikke helt behovet. Statskonsult har nevnt behovet for kunnskap for å kunne få tak i gamle elektroniske dokumenter.

C Man skal når som helst kunne undersøke om innholdet er endret eller ikke

I hovedsak er det mulig for langtidslagrete dokumentet uten digitale signaturer ved å hente lagret tilleggsinformasjon. Arkiverte dokumenter kan ha arkivarens digitale signatur. Man må ha tillit til oppbevaring og tiltrodd personell.

D Man skal når som helst kunne vurdere om endringer er utført i henhold til autorisasjon

Det stilles som et krav i Noark, men det er uklart hvordan de vil løse det.

E Alle endringer skal være sporbare

Historiske endringer lagres i hovedsak i tilknytning til dokumentene.

F Det skal når som helst være mulig å bestemme når dokumentet ble skrevet.

Dokumentets historie lagres.

G Det skal når som helst være mulig å bestemme hvem som signerte dokumentet

Slik informasjon lagres. Dette er viktigere for elektroniske enn fysiske dokumenter, som lettere lar seg kopier og endre, men det kommenteres ikke.

H Det skal ikke være mulig å benekte at man har undertegnet
Man må ha tillit til arkivsystemet og de ansatte.

I Den som signerte, skal være klar over at vedkommende faktisk signerte og bandt seg juridisk ved handlingen
Det nevnes som en problemstilling av Galtung og Riisnæs, Statskonsult og Noark.

J Ingen skal kunne påvirke underskrivingsprosessen
Det vet man ingen ting om. Riksarkivaren ser det ikke som sin oppgave å teste verifiseringen av den type systemer/applikasjoner.

K Dokumentet skal være gyldig så lenge det er juridisk aktuelt at det er gyldig
I og med at signatarens signatur fjernes ved arkivering, vil det ikke være tilfelle.

L Allmennheten skal kunne ha tiltro til at lagring skjer på forsvarlig måte
Det fins elektroniske dokumenter som ikke lenger er lesbare.

M Den som skal vurdere et dokument i et tvistemål, skal kunne forstå hva vurderingen går ut på
Det er ikke så mange som forstår det ennå.

4.10 Konklusjoner

Jeg mener følgende punkter er verd å merke seg:

- Det offentlige har i praksis akseptert å bruke digitale signaturer som erstatning for håndskrevne underskrifter. Imidlertid er det ingen som hittil har påtatt seg eller fått tildelt ansvaret for å definere underskrifters funksjonalitet.
- Verken Riksarkivaren eller jurister i departementene (som framtidige brukere og eiere av applikasjoner for digital signering) har tatt på seg ansvaret for å lage akseptansetester.
- Verken Riksarkivaren eller 'jurister' har tatt opp problemet med manglende autorisasjon av innholdet når dokumenter arkiveres uten signatarens signatur.
- Noark-4 har ikke definert hvordan man skal garantere for at langtidslagrete dokumenter er ekte og autentiske (ikke forfalsket).
- Dersom det offentlige ikke går dypere inn i sammenhengen mellom håndskrevne underskrifter og digitale signaturer, kan den første rettsaken om digitale signaturer konkludere på et svakt rettsgrunnlag.
- Databaser for sertifikater og tilbakekallingslister er arkivverdige. I midlertid er ansvarsforholdene i forhold til arkivloven uklare.
- Offentlige etater og bedrifter ser ut til å ha større behov for sertifikater enn privatpersoner.

- Det offentlige har ikke spesifisert hvilke typer sertifikater som kreves fra private personer ved bruk av digitale signaturer.
- Verken Riksarkivaren eller de nordiske riksarkivene nevner behovet for kompetanse innen informasjonsteknologi for å ta vare på elektroniske dokumenter.
- Det er ikke avklart hvordan etater skal autentisere innkommen elektronisk post som ikke er digitalt signert.
- Håndsignerte dokumenter gir mulighet for skjønn ved vurdering av autentisitet. Den formen for skjønn fins ikke for digitalt signerte dokumenter. Dvs. det er ønskelig å få en vurdering av hvilke positive juridiske virkninger ved digitale signaturer som kan brukes nå, samtidig som andre alternativer undersøkes.

How to construct a system
which can accept one level of description,
and produce the other.

Douglas R. Hofstadter: *Gödel, Esher, Bach* 1979

5 Mekanismer for design

I dette kapittelet tar jeg opp mekanismer tilknyttet langtidsbruk av digitale signaturer og tekniske utfordringer som har dukket fram i tidligere kapitler.

5.1 Tanker før design

Les Gasser viser i *Integration of Computing and Routine Work* [32] hvordan folk klarer å bruke datasystemer som er teknisk inadekvate. Uformell tilpassing, ekstraarbeid og omgåelser av arbeidsrutiner og systemer for å få gjort arbeidet, er vesentlig for å kunne bruke enkelte systemer/applikasjoner. Han påpeker at denne erfaringen har viktige implikasjoner for designere, de som implementerer systemer og for ledere. Erfaringen vil være relevant ved design av sikkerhets-systemer.

Kari Thoresen skriver i sin doktoravhandling *Computer Use* [140] om nød-vendigheten av å designe for heterogene brukergrupper. Det er essensielt for akseptanse av systemer at systemer takler uforutsigbar bruk. Under prøve-forelesningen anbefalte hun at man finner fram til en minimumsspesifikasjon som passer til vesentlige sider ved behovene. For mye spesialisering vil gjøre at enkelte brukere vil bruke systemene på egne, ikke-intenderte måter.

Ved design av systemer er det lett å henge seg opp i nåværende eller gammel teknologi og derved lage spesialløsninger som ikke varer så lenge. I 1980 designet juristen Roger Henriksen i Danmark [36] en elektronisk løsning for ihendehaver-dokumenter som ville blitt meget maskinavhengig. For at bare mottaker skulle ha et gyldig eksemplar av dokumentet, måtte avsenders maskin slette sin kopi automatisk. I dag er maskiner og programvare så komplekse at det er få som vil garantere at det lar seg gjøre. Henriksen var tidlig ute, så han så heller ikke store problemer med offentlige nøklers gyldighet eller distribusjonen av dem.

Noen design er mer generelle, mer teknologiuavhengige, enn andre. Men teknologien setter begrensninger, særlig når man kommer til realiseringen av systemer.

5.2 Standarder

Standard defineres som normal, vanlig [12]. Å standardisere er å fastsette, gjøre ensartet. Informasjonteknologi er et fagområde i rask utvikling. Det kommer

stadig nye standarder både for gamle og for nye mekanismer. Likefullt trenger man standarder for å kunne kommunisere og utvide egen handlefrihet. F.eks. vil det være en vesentlig innskrenkning i forhold til bruk av håndskrevne underskrifter hvis standard programvare gjør at man bare kan signere digitalt hjemme på egen PC.

Programvare som brukes for signering og verifisering, trenger å kunne benytte flere versjoner av algoritmer og standarder for kommunikasjon med ulike brukere. Så snart en implementert standard ikke lenger er tilgjengelig, mister man muligheten til å verifisere signerte dokumenter etter den standarden.

Standarder har ofte opsjoner, muligheter til å velge alternative løsninger. De må tilpasses, profileres, den aktuelle situasjonen. På noe områder fins det ikke standarder, eller de som fins, er gamle eller uaktuelle. På andre områder fins det flere standarder og de facto standarder som kiver om hegemoniet.

Programvare utviklet etter internasjonale standarder, gir brukerne og kjøperne mulighet til å etterprøve at varen virker etter spesifikasjonene. Internasjonale standarder er gjerne utprøvd over lengre tid av mange grupper fagfolk. Proprietære løsninger, der produsenten har laget egne standarder, går sjelden gjennom tilsvarende utvikling og utprøving. Det gir oftere sikkerhetshull. Brukere og kjøpere får sjelden anledning til å forstå hvordan varen er laget, sjelden mulighet til å teste/finne hull og bakdører som ikke er spesifisert.

5.3 Infrastruktur

Hvis man velger å ta i bruk sertifikater i tilknytning til digitale signaturer, trengs en offentlig nøkkelinfrastruktur.

5.3.1 Oppbygging av PKI

I følge Rådet for IT-sikkerhet [116] kan offentlig nøkkel infrastruktur, PKI, sees på som "et formelt samarbeid mellom ulike TTPer/sertifiseringsautoriteter (SAer) slik at nøkler signert og godkjent av en TTP blir godtatt av alle andre TTPer i en PKI". Roe [115] har gått til et finere deltaljeringsnivå:

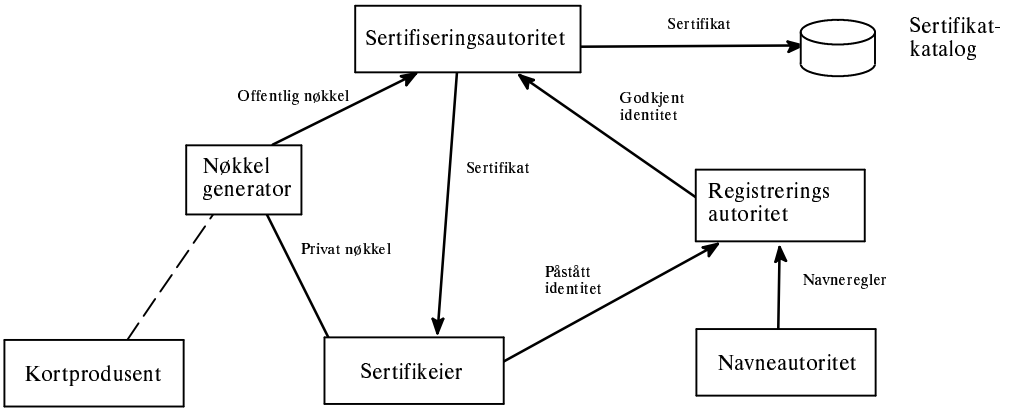
- Sertifiseringsautoriteter (SA),
- Globalt unike navn,
- En adressetjeneste (directory service) for å tilgang til sertifikater,
- En effektiv måte å tilbakekalle nøkler på,
- En avtale mellom brukerne om hvem som gir tillit til hva.

Jeg vil foreslå følgende beskrivelse av komponenter i en PKI:

- Aktører og roller,
  - Tiltrodde tredjeparter og deres tjenester,
  - Sertifikateiere og sertifikatbrukere,
  - Organisasjoner som kan evaluere og akkreditere TTPer,

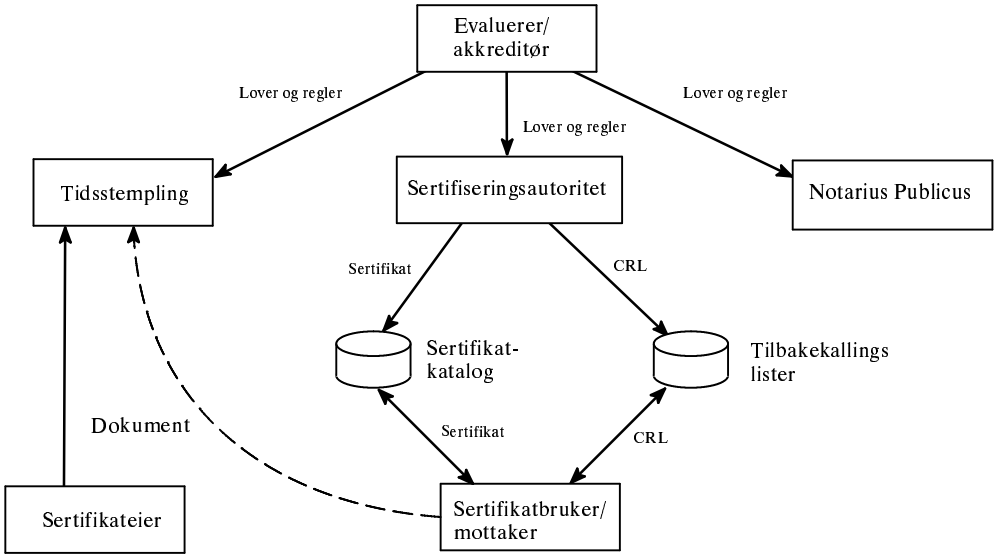
- Underleverandører,

- Tekniske komponenter,
  - Programvare,
  - Smartkort, maskiner og nettverk,
  - Standarder,
- Lovverk som regulerer infrastrukturen,
  - Avtaler mellom aktørene,
  - Evalueringskriterier.



Figur 18 Utsteding av sertifikat

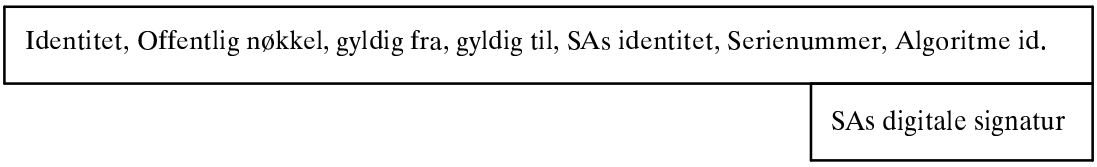
En framtidig sertifikateier går til en registreringsautoritet, RA, med sin påståtte indentitet. RA sjekker identiteten, tildeler et sertifikatnavn og gir melding til sertifiseringsautoriteten. Nøkkelgenerering kan utføres hos sertifiserings-autoriteten, hos en kortprodusent eller hos sertifikateier, avhengig av situasjonen. Standardene oppfordrer SA til å kreve av sertifikateier at den offentlige og den private nøkkelen henger sammen. Det kan f.eks. gjøres ved at sertifikateier signerer sin offentlige nøkkel med sin private nøkkel.



Figur 19 Roller og tiltrodde tjenester for digitale signaturer

Tiltrodde tredjepartstjenster kan være fordelt på flere aktører. Alle kan bli evaluert/akkreditert. En sertifikatbruker/mottaker av et dokument kan ønske å sjekke om en person har et sertifikat, og om sertifikatet fins på en tilbakekallingsliste (Certificate Revocation List, CRL). Både en sertifikateier og en mottaker av et signert dokument kan ønske å tidsstemple et dokument.

Sertifikater og tilbakekallingslister

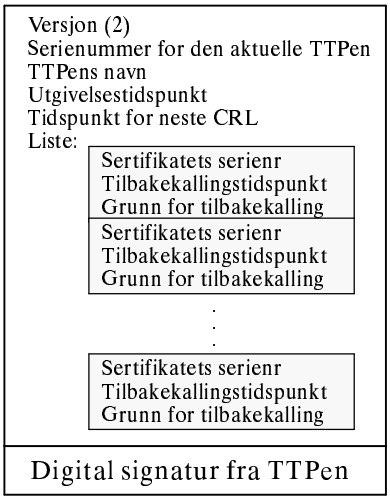


Figur 20 Strukturen på et X.509 sertifikat

Den mest brukte standarden for sertifikat er X.509 versjon 3 [38]. En sertifikateiers sertifikat kan se ut som Figur 20. Det signeres med sertifiseringsautoritetens digitale signatur.

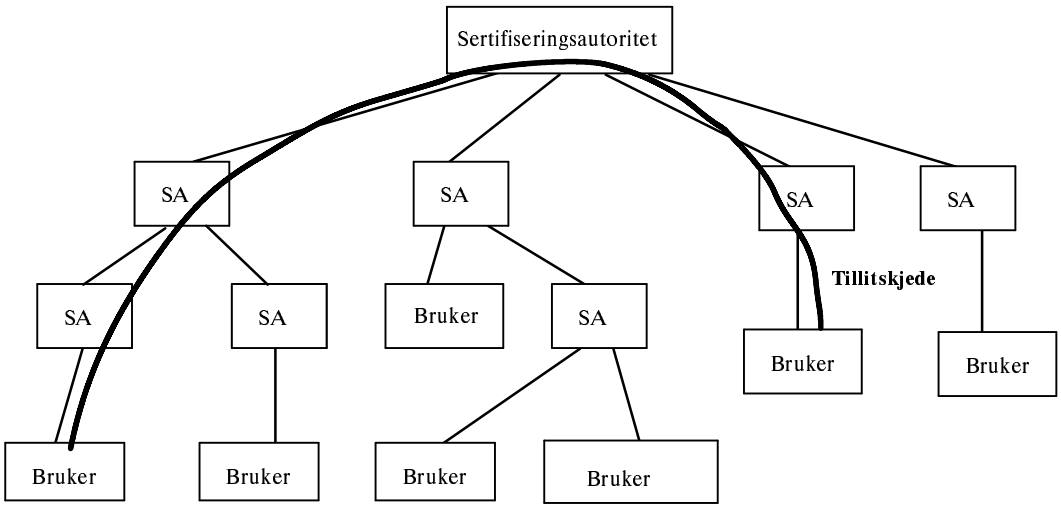
Verifiseringen av en sertifiseringsautoritets signatur gjøres med SAs offentlige nøkkel. Det betyr at en trenger å knytte denne nøkkelen sikkert til SAens identitet, på samme måte som brukernes offentlige nøkkel må knyttes til deres identitet gjennom sertifikater. SAs offentlige nøkkel spres via en rekke kanaler, slik at den skal være umulig å forfalske. Den legges normalt på brukernes smartkort, og beskyttes ved at SA signerer et sertifikat inneholdende SAs offentlige nøkkel med sin private nøkkel.

Når sertifikatets gyldighetsperiode er utgått, slettes sertifikatet normalt fra sertifiseringsautoritetens sertifikatdatabase. Hvis sertifikatet tilbakekalles før gyldighetsperioden er utgått, registereres sertifikatet på en tilbakekallingsliste.



Figur 21 Tilbakekallingsliste

Tilbakekallingslister kan bli lange, slik at det kan ta tid å laste dem ned til en PC. Men det er anleding for sertifiseringsautoriteten til å utstede 'delta'-lister som viser tilbakekalte sertifikater siden forrige tilbakekallingsliste. Ved sertifikatets utløpstidspunkt vil det normalt bli fjernet fra tilbakekallingslistene. Posten SDS sier de planlegger en on-line TTP-tjeneste der man sender forespørsel om et sertifikat var/er gyldig på et gitt tidspunkt og får det bekreftet/avkreftet[3] [96].



Figur 22 Sertifiseringshierarkier

En SA har et vanlig X.509 sertifikat som er utstedt av en SA 'på et høyere nivå' [148]. Det øverste nivået kalles ofte rot-SA og er en sertifiseringsautoritet man velger å ha tillit til. Denne typen sertifiseringshierarkier brukes per i dag bare i eksperimentelle systemer, men kan bli nødvendig på sikt i et internasjonalt perspektiv.

Brukere får utstedt sertifikater hos ulike sertifiseringsautoriteter. Det kan være fordi brukerne har tillit og/eller tilgang til en spesiell autoritet, fordi autoritetene dekker spesielle oppgaver eller fordi det ikke er optimalt å ha dem for store. For at brukere med sertifikater fra ulike utstedere skal kunne kommunisere, bør sertifiseringsautoritetene kryssertifisere hverandre. Det innebærer at to eller flere SAer utsteder sertifikater for hverandres offentlige nøkler for å stadfeste et tillitsforhold [116]. Kryssertifisering kan gjøres innenfor eller mellom sertifiseringshierarkier.

Som tidligere nevnt inngikk Arbeids- og administrasjonsdepartementet og Kommunenes Sentralforbund 15.9.99 innenfor rammen av Forvaltningsnett-samarbeidet en rammeavtale om SA-tjenster med Posten SDS, Telenor AS og Strålfors AS. Her har de tre leverandørene skrevet under en avtale om kryssertifisering.

3. RFC 2560 Internet X.509 Public Key Infrastructure On-line Certificate Status Protocol (OCSP), juni 1999.

5.3.2 Ikke-benekting

Ikke-benekting er beskrevet i to ISO-standarder: IS 10181-4 [46] og FDIS 13888-3 [48]. Hvis man trenger større beviskraft enn en digital signatur med tilhørende sertifikat gir, kan man samle bevismateriale vha. TTPer. Tjenesten er definert av begge standardene som

> "to collect, maintain, make available and validate irrefutable evidence concerning the occurrence or non-occurrence of a disputed event or action."

De vanligste tjenestene er innsamling av bevismateriale for hendelsene avsendelse, mottak, mottak til en nettverksnode, videresending fra en nettverksnode.

For å kunne bruke en slik tjeneste, må bla.:

- De utvekslende partene stole på den samme tiltrodde tredjeparten, som kan ha fordelt utførelsen av tjenesten på flere aktører,
- Den som sender en melding, må holde sin private nøkkel hemmelig,
- Den som skal generere bevismateriale, må vite hvilken ikke-benektingspolicy som gjelder og hvilket bevismateriale som skal genereres og tas vare på,
- Sikkerhetsmekanismene for digitale signaturer må tilfredsstille kravene i policien,
- Den som skal generere bevismateriale, må ha tilgang til tiltrodde tidsstempler og notarfunksjoner.

Ikke-benekting i praksis:

Jeg rapporterer at min nøkkel er kompromittert, og påstår at dette må ha skjedd før tidspunkt T. "Men jeg oppdaget det først nå...."

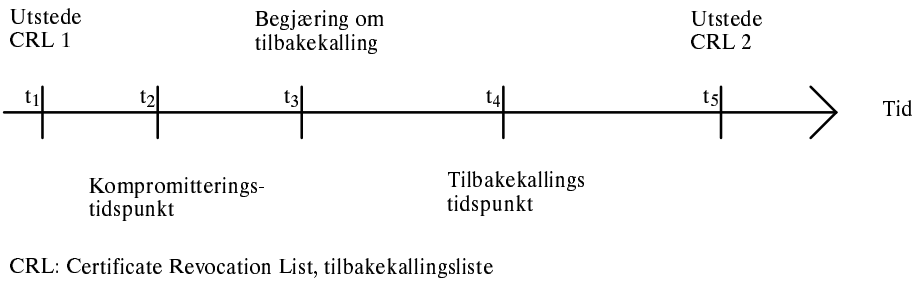
Digitale signaturer er ikke alene nok for å avgjøre tvister hvis sertifikatet er tilbakekalt. Den som vurderer bevismaterialet, må ha tilgang til tilbakekallingslister som viser at sertifikatet fortsatt var gyldig da signaturen ble generert. Hvis derimot signataren frivillig bruker uriktig tid, eller når en angriper kompromitterer den private nøkkelen, er det vanskelig å avgjøre en tvist. Da må man ha et tiltrodd tidsstempel i tillegg. Det kan vise at en melding ble signert før nøkkelen ble kompromittert og dermed at meldingen ikke var en forfalskning.

Hvis mottakeren benekter at en melding er mottatt og det ikke fins kvittering for mottak, er det vanskelig for avsenderen å bevise at den er sendt. Da vil en notartjeneste, som registrerer at en melding har vært innom der, være til nytte for avsenderen. Men det er avhengig av at begge aksepterer det TTPen framlegger av bevis.

Fordeling av risiko mellom aktørene

Siden elektroniske dokumenter trenger så mange mekanismer for å løse saker som er enkle for fysiske dokumenter, så må man fordele ansvar mellom mekanismene og mellom dem som har ansvar for mekanismene.

Warwick Ford og Michael S. Baum har tatt opp fordeling av risiko ved tilbakekalling av sertifikater i boka *Secure Electronic Commerce* [29].



Figur 23 Tidslinje for tilbakekalling

Rekkefølgen for hendelsene er vanligvis:

- t_1 Utstedelse av en tilbakekallingsliste, CRL 1, før den aktuelle tilbakekallingen.
- t_2 Kompromitteringstidspunkt. En hendelse inntreffer som gjør at sertifikatet skal trekkes tilbake. Det kan f.eks. være at nøkkelen stjeles.
- t_3 Begjæring om tilbakekalling. En autorisert person sender en anmodning om at sertifikatet tilbakekalles.
- t_4 Tilbakekallingstidspunkt. Sertfiseringsautoriteten aksepterer anmodningen om ugyldiggjøring
- t_5 Et ny tilbakekallingsliste utstedes og publiseres.

Forfatterne foreslår at den største risikoen skal bæres av den parten som har størst mulighet til å kontrollere den. Det er ikke sagt at det er lett å kontrollere risikoene.

Perioden (t_2 - t_3): Kompromitteringen har skjedd, men er ikke rapportert til sertifiseringsautoriteten. Brukere av sertifikatet kan ikke forventes å vite om kompromitteringen. Det kan være rimelig at sertifikateier bærer den største risikoen ved misbruk av den private nøkkelen i denne perioden.

Perioden (t_3 - t_4): Kompromitteringen er rapportert, men ikke publisert av sertifiseringsautoriteten. Brukere av sertifikatet kan ikke forventes å vite om kompromitteringen. Det kan være rimelig at sertifiseringsautoriteten bærer den største risikoen for denne perioden.

Perioden (t_4 - t_5): Anmodningen om ugyldiggjøring er akseptert av sertifiserings-autoriteten, men ikke publisert i en ny tilbakekallingsliste, CRL 2. Det innebærer at sertifikatbrukere ikke kan forventes å vite om tilbakekallingen. Risikoen vil være avhengig av hvilken mekanisme som brukes, og som man kan anta at partene er enige om. Hvis det er avtale om at tilbakekallingslister publiseres umiddelbart ved behov, er det rimelig å forvente at sertifikatbrukere sjekker siste CRL før et sertifikat verifiseres. Hvis tilbakekallingslistene publiseres med faste tidsintervall, kan det være i brukernes interesser å vente til CLR 2 publiseres.

Perioden etter t_5: Sertifiseringsautoriteten har oppfylt sine forpliktelser. Hvis en sertifikatbruker bruker et ugyldig sertifikat etter at tilbakekalling er publisert, er det rimelig at sertifikatbrukeren påtar seg det største ansvaret for konsekvensene.

Tvister vil i stor grad være avhengig av om man vet når hendelsene inntraff. Sertifiserte tidsstempler vil hjelpe på situasjonen. Ford og Baum påpeker at det ikke fins noen absolutt beste praksis på området.

5.3.3 Digitale signaturer

Levetiden og gyldighetstiden til en digital signatur kan påvirkes av teknologien på en helt annen måte enn håndskrevne underskrifter kan.

Nøkkellengder

"A cryptographic system is not acceptable if it is feasible for an opponent to make a chosen plaintext attack and find the key." [120]. Nøkkellengden er ett av elementene som bestemmer sikkerheten i et krypteringssystem. Hva som er rimelig sikker lengde, vil variere med hva slags algoritme som brukes. RSA-nøkler er lengre enn nøklene benyttet i elliptisk kurvesystemer. Jo lenger nøkkel som brukes i et system, jo lenger tid tar det å kryptere en melding.

I hht. Dorothy Denning [21] kan en gitt nøkkellengde bli for kort med en gitt rate i en gitt tidsperiode, hvor raten er $\log_{10}$ av antallet nøkler som kan testes per sekund. I de siste decenniene har antall transistorer som kan plasseres på en enkelt chip omtrent blitt doblet hver 18nde måned. Effekten har vært at prosseseringshastigheten i antall instruksjoner pr. sekund har forbedret seg med en faktor på 10 hvert 3.3 år og en faktor på 100 forbedringer hvert decennium (den såkalte Moore's lov, etter stifteren av Intel, Gordon Moore).

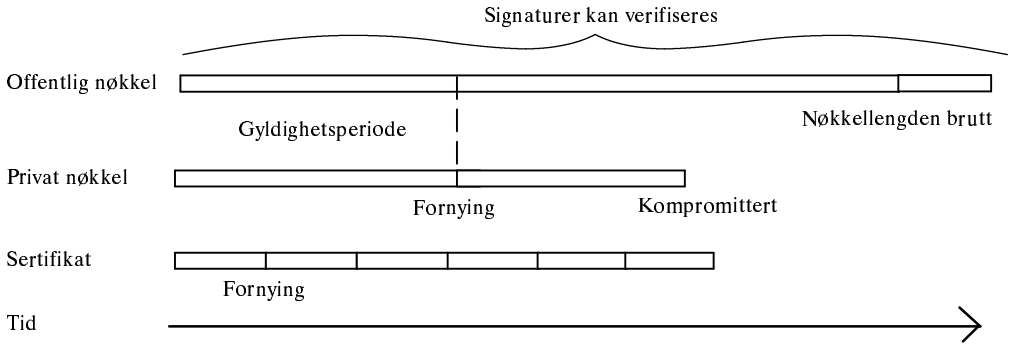
Petroleumsbransjens elektroniske arbeidsplass, SOIL, har i hht. [116] satt nøkkellengden ved bruk av RSA til 2048 bits. Det er forventet levetid for nøkkelen som er viktig. Den avhenger av

- Forventet utvikling på feltet,
  - Prosessorkraft,
  - Parallellisering,
- Uforutsigbare "kvantesprang",
  - I forståelsen for hvordan en algoritme virker,
  - Innen matematikken,
  - I den teknologiske utviklingen.

Kryptoalgoritmers styrke er utdypet i appendikset på s. 132.

Signaturers gyldighet

Signaturers gyldighet er bla. avhengig av nøkkelsertifikatet. Og det er forskjell på hvor lenge man kan bruke en privat nøkkel til å signere med og hvor lenge man kan verifisere signaturer.

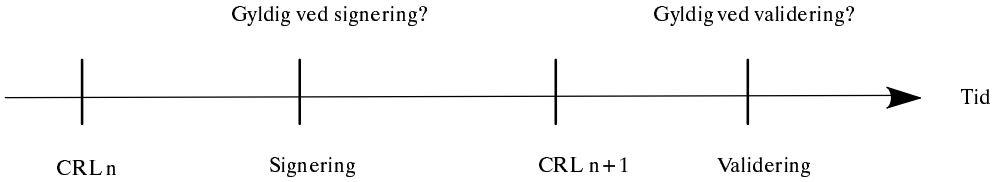


Figur 24 Bruk av digitale signaturer over tid

- Når et sett med en privat og en offentlig nøkkel er generert, koples den offentlige nøkkelen til et sertifikat. Punkt D.2 s. 138 utdyper nøkkelhåndtering.
- Sertifikater varer vanligvis kortere tid enn nøklene gjør. Ved gyldighets-periodens utløp kan det utstedes et nytt sertifikat for samme nøkkelpar. Det har en ny gyldighetsperiode og dermed blir sertifiseringsautoritetens digitale signatur på sertifikatet en annen.
- Nøklene er konstruert for å vare i mange år. Men de har relativt korte gyldighetsperioder som kan forlenges.
- Når/hvis den private nøkkelen kompromitteres eller f.eks. eieren slutter i jobben som nøkkelen var knyttet til, må sertifikatet tilbakekalles og den private nøkkelen ugyldiggjøres.
- Den offentlige nøkkelen kan fortsatt brukes til å verifisere tidligere signaturer.
- Når den teknologiske utviklingen gjør at nøkkellengden ikke lenger er tilstrekkelig, eller algoritmen brytes, kan signaturer fortsatt verifiseres hvis dokumentet har et tiltrodd tidsstempel som er satt tidligere.

Nøkler innen Forvaltningsnettsamarbeidet kan leve i inntil 5 år, men sertifikater utstedes for 1 - 2 år [30].

Historisk validering og sanntidsvalidering



Figur 25 Når er signaturen gyldig?

Ford og Baum tar opp to situasjoner som er interessante ved bruk av digitale signaturer for langtidslagring [29].

Validering ved signering. I noen situasjoner er sertifikatbrukeren (den som verifiserer) ikke opptatt av tilbakekallinger som kan opptre etter at signering er

foretatt. Eksempler på det er situasjoner med uavviselighet, f.eks. deponering av et testamente. I slike situasjoner er det nødvendig å sikre som bevis all sertifikat-informasjon som er knyttet til signaturen. Dvs. alle sertifikater i applikasjons-kjeden pluss alle tilbakekallingslister (Certificate Revocation List, CRL) eller annen tilbakekallingsinformasjon som gjaldt på signeringstidspunktet. I disse situasjonene er det bare nødvendig at signaturen er gyldig ved signerings-tidspunktet.

- Anta at et firma har sendt inn et digitalt signert årsregnskap til Skatteetaten. Ettersom slike regnskap *skal* sendes inn innen 1.mars, er det uinteressant om nøkkelen ble kompromittert uka etter. Det er mottakingstidspunktet som gjelder.
- I slike situasjoner stoler man på Skatteetaten og tror ikke at utro tjenere vil bruke den kompromittere nøkkelen til å endre regnskapet og signere på nytt.

Validering ved verifisering. I andre situasjoner er sertifikatbrukeren opptatt av om sertifikatene er tilbakekalt i tida fram til signaturverifikasjon, uavhengig av om signeringen har skjedd et bestemt tidspunkt i fortiden. Eksempel på denne situasjonen er:

- Å verifisere en programvareleverandørs signatur på en kopi av vedkommendes programvare som er distribuert elektronisk fra en internettserver,
- Å verifisere en sertifiseringsautoritets signatur på et offentlig nøkkelsertifikat,
- Å verifisere en tidsstemplende servers tidsstempel på en tredjeparts dokument.

I disse situasjonene ønsker den som verifiserer signaturen, generelt å sjekke at et gyldig, ikke tilbakekalt sertifikat eksisterer nå. I denne situasjonen går sertifikatets gyldighetsperiode generelt noe lenger (kanskje mye lenger) enn perioden som den offentlige nøkkelen brukes til signering.

5.4 Langtidslagring

Selv om dokumenter og databaser dannes/lages av ett eller flere individer, så vil de ofte være av interesse for mange flere mennesker enn først antatt. De kan bli brukt av personer som ikke har vært med på å lage dem. De vil ofte bli brukt sammen med andre dokumenter som forfatteren ikke visste om. Informasjonen i dokumentene kan være til nytte lenge etter at dokumentet er i aktiv bruk, f.eks. av juridiske eller historiske grunner.

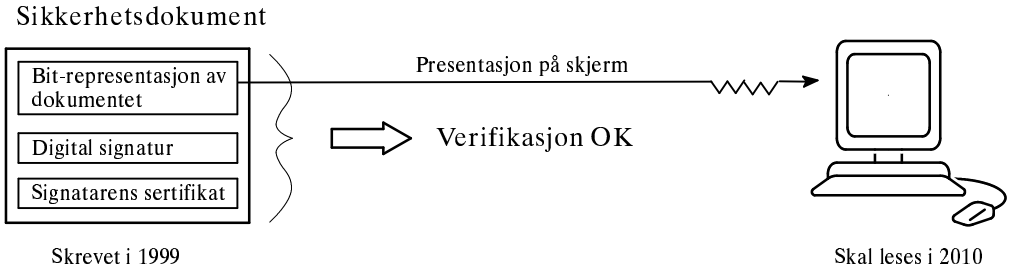
5.4.1 Elektronisk lagring

EUs DLM-Forum [24] påpeker at man må vurdere elektroniske dokumenter som komponenter i et større, videre informasjonssystem. De trekker fram særegen-heter ved elektroniske dokumenter:

- Det er ikke lagringsmediet som er dokumentet eller meldingen, slik et papirdokument kombinerer rollene som bærer og som selve informasjonen. Man trenger verktøy/maskiner for å lese elektronisk informasjonen.
- Elektroniske media har vanligvis kortere levetid enn papir eller mikrofilm.
- Den raske skiftningen i teknologi gjør det vanskelig å finne stabile og langtlevende formater.

DLM-Forum [24] definerer format som *datarepresentasjonen til kilden, slik som tekst/html, ASCII, Postscriptfiler osv*. Dette er å sette ulike nivåer i samme definisjon. Noark-4 [114] definerer format som *Struktur for lagring av et elektronsik dokument*. Definisjonene strekker seg fra måten å lagre bits på et fysisk lagringsmedium, via tegnsettet som brukes, f.eks. ASCII, til tekstbehandlingsformater. Alle disse definisjonene er aktuelle for langtidslagring av digitalt signerte dokumenter fordi signaturen kan være avhengig av dem alle. Ved konvertering fra ett format til et annet må man vurdere mulighet for tap av informasjon. Det er ikke alltid at to slike formater stemmer helt overens. Hvis man bytter fra ASCII til EBCDIC, vil presentasjonen av dokumentet endres. Hvis man går fra eldre til nyere versjoner av et tekstbehandlingsverktøy, kan man f.eks. miste fotnoteoppsettet. Ikke alle tekstbehandlingsvertøy er bakoverkompatible. Kopierer man data fra et gammelt lagringsmedium til et nytt, kan det skape problemer. Det fins ikke evalueringskriterier for hvordan man skal måle at felleskopiering av mange dokumenter har gått bra [100].

Et signert dokument må være konsistent og forbli det samme, bevare sin integritet. Det man leser på skjermen, skal ikke endre innhold og vanligvis heller ikke utseende i forhold til det signaturen beregnes over. Dvs. både må presentasjonen være korrekt og signaturen være gyldig for at en bruker av dokumentet skal kunne ha tillit til det.



Figur 26 Verifikasjon og presentasjon av et dokument

Ved bruk av digitale signaturer i forvaltningen er applikasjonen for beregning av den digitale signaturen "utenfor" tekstbehandlingsverktøyet. Ved overføring sendes et sikkerhetsdokument som inneholder en bit-representasjon av dokumentet (f.eks. i Word 1999) den digitale signaturen, og sertifikatet [96]. Applikasjonen som skal verifisere signaturen, leser og behandler de bitene den får uavhengig av tekstbehandlingsverktøyet [96]. Hvis verifikasjonsprogrammet som brukes i 2010, har opsjonene fra 1999, f.eks. riktig hash-algoritme, kan den verifisere signaturen. Problemet blir deretter hva "Word" i 2010 vil presentere på en skjerm for lesing. Mottakerens tekstbehandler kan ha andre maler for

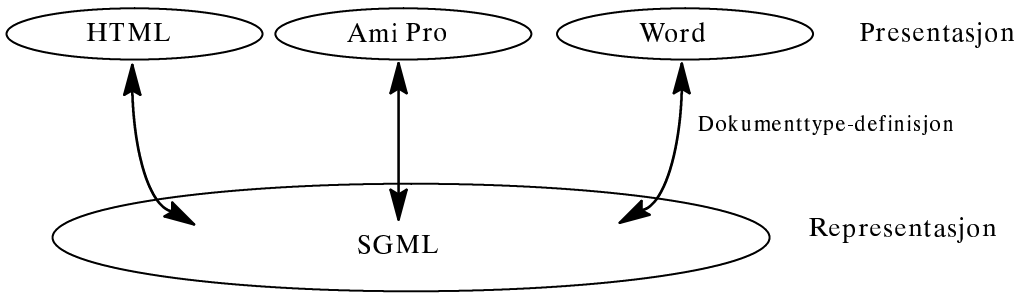
fontene, andre servicepakker (som MicroSoft sender ut for retting av feil) og f.eks. lese dokumentets redigeringshistiorie som følger med feil. Presentasjonen kan bli ganske anderledes.

Statskonsults rapport [133] viser at konvertering mellom tekstbehandlingsverktøy gir avvik. En italic font kan man kanskje klare seg uten, men det er umulig å si hva som vil være kritisk for et hvert dokument. Man vet ikke hvor bakover-kompatible tekstbehandlingsvertøy vil være i framtida. Dokumenter produsert med Norsk Datas Notis-program er f.eks. nå vanskelig lesbare [104]. Det norske Veritas konverterer for tiden DCF-dokumenter til SGML mm. [92]. Ved noen av konverteringene kan anslagsvis opp mot 20 % av konverteringen fungere feil. Alle dokumenter må korrekturleses. Det er særlig matematiske formler, tabeller og grafikk som skaper problemer.

Det kan se ut som et alternativ å signere et dokument i Word 97, som sendes til mottaker, og signere en kopi i ASCII for arkivering. Det blir alt for tungvint å skulle verifisere at man signerer det samme innholdet. DLM-Forum tar ikke opp juridiske problemer med langtidslagring av digitalt signerte dokumenter.

Det kan være vanskelig å kreve eierskapet/forfatterskapet til et dokument når man vet at presentasjonen i annet tekstbehandlingsverktøy enn det man opprinnelig skrev dokumentet i, kan gi avvik. Sannsynligvis vil avvikene ikke være store, men de kan likevel være vesentlige. I en tvistesituasjon der den frie bevisvurderingen gjelder, kan det styrke beviskraften å vise til å eie tidligere registrerte utgaver av et dokument. Selv om presentasjonen er ulik, så kan en gyldig signatur støtte ikke-benekting.

De aller fleste systemer som foretar en eller annen behandling av informasjon, benytter systemavhengige formater for å beskrive hensikten med innholdet. Tone Sandahl [99] påpeker at dokumentrepresentasjonen bør være plattformuavhengig for at digitalt signerte dokumenter skal kunne verifiseres i så lang tid som mulig etter signering. SGML (Standard Generalized Markup Language) [114] er et slikt format. Dokumenter som følger SGML, skal ikke inneholde koder som binder informasjonen til ett presentasjonsmedium (skrifttypedirektiver, fotnotehåndtering, layoutdirektiver til laserskriver, fotosetter osv.). Slike dokumenter lagrer strukturinformasjon separat i dokumenttypedefinisjoner (DTD). På den måten kan et dokument tas fram i f.eks. HTML, Word eller Ami Pro, avhengig av DTDen.



Figur 27 Presentasjon og representasjon av dokumenter

Hvis den digitale signaturen er beregnet ut fra representasjonsformatet, og representasjonen er maskinuavhengig, lik på alle maskiner og plattformer, vil den digitale signaturens livslengde bare være avhengig av at representasjonsformatet ikke er foreldet, at lagringsmediet ikke forringes, at kopiering til nye medier går bra, at kryptoalgoritmene er brukbare og at maskiner kan hente fram dataene. SGML er ment å skulle være maskinuavhengig og ha lang levetid. Men SGML er ikke utbredt. MicroSoft har annonsert at de planlegger å gå over til SGML som lagringsformat for Word.

Forsker Guri Verne, Norsk Regnesentral [104], reiser spørsmålet om dokumenttypedefinisjoner vil klare å gi samme representasjon i ulike tekstbehandlingsverktøy. Produsentene av de ulike verktøyene vil ønske å profilere sitt system ved å lage leverandørspesifikke tagger. Det vil presse brukerne til bare å bruke standardtagger. Alternativet kan være at offentlige etater har sín DTD som brukerne tvinges til å bruke ved kommunikasjon med det offentlige. Begge deler blir tvangstrøyer som bør vurderes.

Hvis et dokument har SGML som basis, kan man signere SGML-filen. Det problemet man da sitter igjen med, er om signataren har tillit til at det som presenteres på skjermen, er det samme som vedkommende signerer. Der vil DTDen være til hjelp i en tvistesitussjon. Dette er et reelt problem en del fagfolk har i forhold til f.eks. Word [108]. Word kan ha hvit tekst på hvit bunn, annen skjult tekst eller makroer som man ikke ser eller ikke vet om er med i beregningen ved signering.

En digital signatur basert på presentasjonsformatet vil forkorte signaturens levetid. Signaturen kan verifiseres, men det som presenteres i en nyere utgave av tekstbehandlingverktøyet, vil neppe garantere likt innhold.

DLM-Forum [24] foreslår at leverandører skal garantere bevaringen av data og tilgang til dem over lang tid. Dvs. at leverandører påtar seg å skaffe all maskin- og programvare og dokumentasjon som trengs for å gjenvinne data og for å eksportere dem til andre formater. Programvare er vanligvis mer maskinavhengig enn data. Hvis en applikasjon genererer data i et proprietært format, kan det bli nødvendig å arkivere hele systemet for å få tilgang til informasjonen. Dette inkluderer applikasjonen selv, plattformen, dokumentasjonen og kanskje de ansattes kunnskaper. NDs Notissystem eksemplifiserer dette i dag. Det er ingen vits i å arkivere informasjon hvis man ikke kan få tilgang til den når man ønsker det. I hht. Teknisk Ukeblad [143] har ikke Nasjonalbiblioteket ressurser nok til å migrere data på båndkassetter til nyere medier. Lagringsmedier forringes over tid. Dessuten fins det medier som ikke kan leses av nye maskiner. 5,25” disketter er et eksempel på dette i dag..

Dokumenter skal også fjernes. Det fins forskjellige nivåer for fjerning. Man kan slette et dokument fra en server og notere i den elektroniske journalen at det er slettet. Siden det ofte vil finnes flere kopier, kan man i andre situasjoner trenge å sende dokumentet til en Notarius Publicus og få registrert at dokumentet ikke lenger er gyldig.

5.4.2 Arkivformater

Arkivforskriftens §2-11 sier at "Materiale på elektronisk medium må kopierast eller konverterast til nye lagringseiningar i den grad det er nødvendig for å ta vare på og ha tilgang til dokumentinnhaldet" [5]. Pkt. 5.3.3 i Noark-4 [114] stiller følgende krav til et godt arkivformat:

- Formatet skal være åpent dokumentert,
- Det bør være en ISO-standard,
- Det må støttes av ferdiggjorte og godt etablerte produkter i markedet,
- Konvertering til arkivformatet må være enkelt å utføre,
- Det bør være mulig å konvertere til vedkommende arkivformat fra de fleste vanlige produksjonsformater, også fra grafikkformater (grafikkelementer bør inkluderes sammen med teksten),
- Det må være mulig å konvertere arkivformatet til nye formater senere.

Trond Sirevåg i Riksarkiet sier at de ikke har satt opp kriterier for vellykket migrering fra et format til et annet ennå [100]. Heller ikke EUs DLM-forum har noe om dette [24].

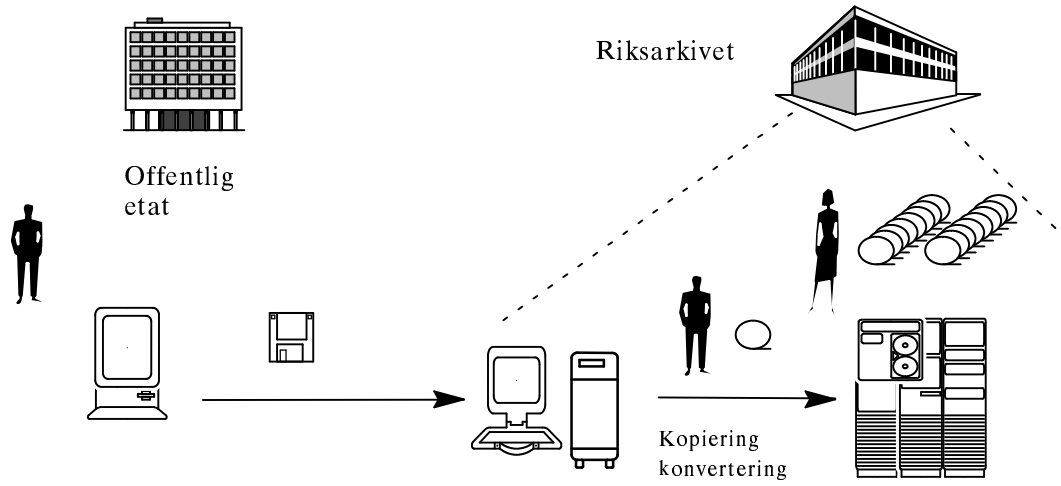
Noark aksepterer:

- Ren tekst: ISO Latin-1 8859-1:1987,
- SGML - ISO 8879: 1986, herunder subset-formatene HTML og XML,
- TIFF, versjon 6, (Tagged Image File Format, standardisert rastergrafikk-format),
- PDF (Portable Document Format, et ikke-redigert format, trykkformat, som både håndterer tekst og grafikk).

Noark påpeker at de generelle kravene til arkivformater medfører at arkivering av sammensatte dokumenter vil være forbundet med betydelige restriksjoner.

5.4.3 Arkivering

Riksarkivet overtar ansvaret for dokumenter de mottar, tar en kopi der de fjerner de personlige digitale signaturene, og signerer eventuelt med arkivarens signatur [114]. En digitalt signert versjon kan lagres med dokumentet, samt informasjon om sporbarhet se Figur 11 s. 71.



Figur 28 Langtidslagring

Ved langtidslagring må Riksarkivet med jevne mellomrom kopiere dokumentene til nye lagringsmedier og til nye formater.

For å få tilgang til og lese langtidslagrete, digitalt signerte, elektroniske dokumenter, trenger man:

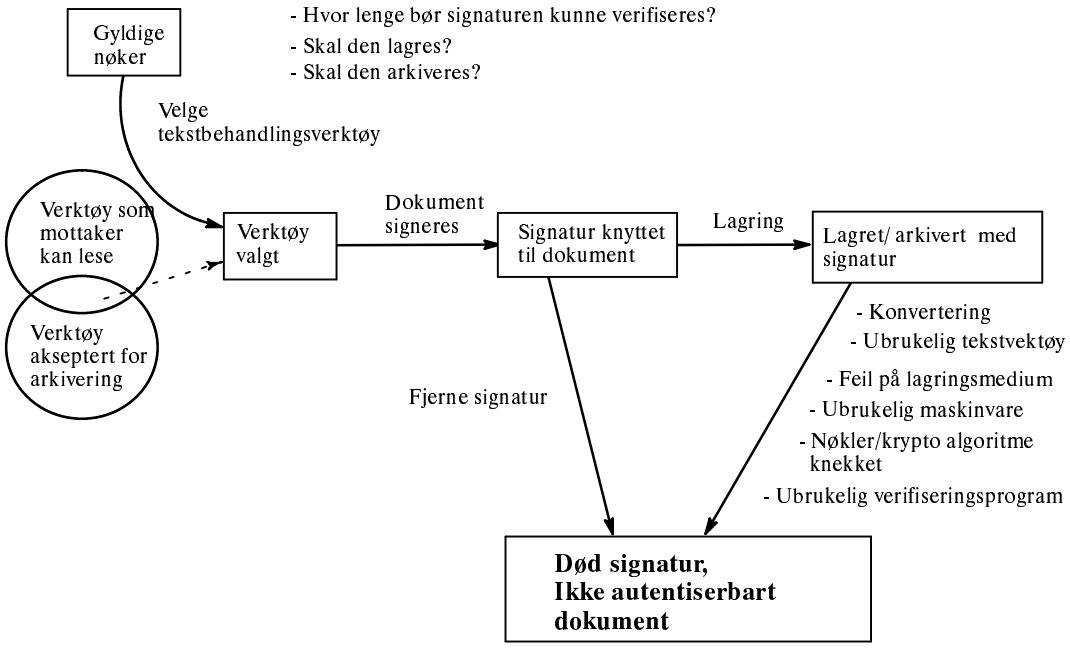
- Logikk og mekanismer for å lete fram dokumenter fra store mengder lagringsmedier,
- Stativer for å montere og lese fra det fysiske mediet,
- Maskinvare med riktig operativsystem for å kunne håndtere lagringsmediet, programvare, riktig basis programvare, riktig tekstbehandlingverktøy,
- Informasjon om egenskaper ved dokumentet, type, format, versjonsnr., identifikator osv.,
- Editorer for å lese dokumenter,
- Riktige versjoner av kryptoprogramvare o.l.,
- Tilgang til tilbakekallingslister og offentlige nøkler som klarer å vise om sertifikatene var gyldige ved signeringstidspunktet,
- Overføring av kompetanse til nye mennesker som skal utføre dette arbeidet.

Langtidslagring har med tid å gjøre. Når hendelser inntraff, er vesentlig for problemstillingen. Ved seinere tvister kan det være aktuelt å kunne avklare:

- Når dataene var intakte, ikke endret,
- Når data ble endret,
- Hvem som gjorde endringen på det tidspunktet,
- Om det var en autorisert endring på det tidspunktet.

Valg av lagringsmedier er kommentert i appendikset punkt E på side 140.

5.4.4 Langtidslagring av digitale signaturer



Figur 29 Tilstandsdiagram over signaturens levetid

Merk at sluttilstanden alltid er en "død signatur". Spørsmålet er hvor lang tid det tar før den havner der og hva som er konsekvensene av å havne der.

En saksbehandler som skal signere et dokument, må ta med i betraktningen:

- At mottakeren skal kunne lese og autentisere det elektroniske dokumentet ved mottak,
  - Hvilket tekstbehandlingsverktøy har mottakeren?
  - Hvilken autentiseringsmekanisme har mottakeren?
- Hvor lenge signaturen skal kunne være autentiserbar i etaten,
  - Skal signaturen være gyldig etter signeringstidspunktet?
  - Hvor lenge skal signaturen være verifiserbar?
  - Når signataren slutter, kan signaturen ikke fornyes i nytt format,
- Hvor lenge dokumentet skal lagres i etaten,
  - Hvordan skal man autentisere dokumentet etter at tekstbehandlingsverktøyet ikke brukes mer,
- Om det skal arkiveres med signatur,
  - Hvem bestemmer det?
  - Hva slags sak er det, hvilken lov det faller inn under?

Et dokumentet er ikke lenger autentisertbart hvis signaturen 'dør' med mindre et regelverk sier at verifikasjonsspor holder. Et slikt regelverk må spesifisere (strenge) krav til produksjonen av disse sporene. Det er ikke gjort noe sted.

Med en død digital signatur kan man ikke maskinelt autorisere at innholdet er signert av en bestemt person. Signaturen dør hvis én av følgende hendelser inntreffer:

- Signaturen fjernes før lagring/arkivering,
- Tekstbehandlingsverktøyet ikke lenger er brukbart eller tilgjengelig,
- Dokumentet konverteres til et nytt format,
- Verifiseringsprogrammet ikke er tilgjengelig lenger,
- Nøkler/algoritmer knekkes,
- Lagringsmediet forringes og det oppstår bitfeil
- Tiltro til sikker lagringen svekkes.

Dette syns jeg setter strenge rammer for bruk av digitale signaturer og hvor mye de kan sammenliknes med håndskrevne underskrifter. Hvis det er så at arkiver fjerner singatarens digitale signatur før arkivering, blir det ikke lange levetida. Word og liknende formater lever neppe særlig mer enn 5 år generelt. SGML, som kan påregnes å være en aktuell standard, kan kanskje leve i 15 år.

Hvis signatarens signatur arkiveres med dokumentet, hva skal til for at den skal leve lengst mulig?

- Dokumentet må kunne gjenfinnes og være lesbart,
- Tekstbehandlingsverktøyet må virke på en tilgjengelig maskin,
- Verifiseringsalgoritmen og hashalgoritmen må være brukbare.

Ved verifisering av et sertifikat, se sertifikatoppsett Figur 20 s. 94,:

- Verifiseres sertifiseringsautoritetens digitale signatur lokalt,
- Informasjon om sertifikatet med gyldighets periode fra og til leses og sendes til databasen for tilbakekallingslister,
- Hvis sertifikatet ikke står der, er sertifikatet gyldig.

Det riktige er å sjekke en tilbakekallingsliste *etter* signeringstidspunktet.

For å kunne gjennomføre verifiseringen;

- Må sertifikatet kunne presenteres på en skjerm,
- Må man ha tilgang til tilbakekallingslister,
- Må man ha et verifiseringsprogram som virker.

5.5 Risiko

En del risikomomenter knytter seg spesielt til mekanismene man benytter og tilliten man har til dem.

5.5.1 Sårbare områder

Datasikkerhet har vanligvis eksempler der Arne og Berit er de snille som utveksler informasjon og at det er en slem opponent, Carl, som prøver å ødelegge for dem. I noen situasjoner kan det være motsatt. Politiet kan ha lovhjemmel for å avsløre hva to mistenkte utveksler av informasjon.

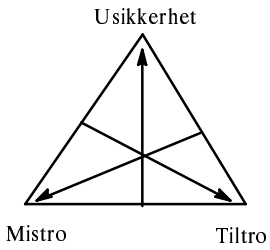
Tillit og risiko

“Sikkerheten i et system må utvikles med utgangspunkt i hva en velger å stole på. Det er teoretisk umulig å konstruere et sikkert system uten minst ett punkt som er

definert som ubetinget sikkert." [148]. På ett eller annet nivå må man ha noen man stoler på uten å kunne bevise det. PGP [60] har en tillitskjede mellom aktører som kjenner hverandre. Det offentlige rom i Norge innfører tiltrodde tredjeparter og sertifikater. Da stoler man på de tiltrodde tredjepartene og eventuelt dem som evaluerer dem. Det er likevel mange elementer innenfor systemet av tillit, PKI, som kan øke eller minske tilliten og risikoen for at noe galt kan skje. Eksempler på slike elementer utenfor TTPenes områder er

- Gjør datasystemet det det skal?
  - Signerer jeg bare dokumentet jeg ser på skjermen?
  - Gir det ikke-benekting på et akseptabelt nivå?
- Fins det utro tjenere?
- Er det vanskelig å bryte systemet?
- Er dette 10 år gamle dokumentet autentisk?

Audun Jøsang, Telenor, og Svein Johan Knapskog, NTNU, har satt opp en meningstrekant i artikkelen *A Metric for Trusted Systems* [58].



Figur 30 Meningstrekant

En persons mening om tiltro til et system blir en funksjon av tiltro (t), mistro (m) og uvisshet (u), ω{t, m, u}, der t, m og u alle er sannsynligheter mellom 0 og 1. ω = {1, 0, 0} uttrykker full tiltro til et system. ω = {0, 1, 0} uttrykker full mistro til et system og ω = {0, 0, 1} uttrykker full uvisshet om systemet.

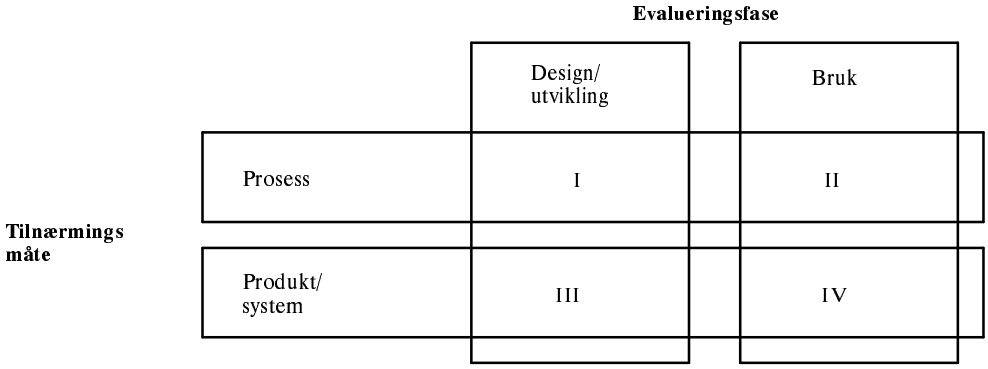
Hvis framtidige brukere, offentlige etater, bedrifter og privatpersoner, er i full uvisshet om sikkerheten ved bruk av digitale signaturer, så har de verken tiltro eller mistro til at mekanismene vil utføre de tjenestene man ønsker de skal utføre.

Hvilke mekanismer fins for å øke tilliten til et system? ISO/IEC JTC1/SC 27 arbeider med en teknisk rapport *A framework for IT security assurance* [51]. Arbeidet er i sin begynnelse. I rapportutkastet sliter arbeidsgruppen med begrepene assurance (*a measure of trust*, eller *grounds for confidence*) og confidence (*relates to a belief in the system to perform in the way intended and claimed*). *Overall confidence in a product or a system will usually require the application of more than one specific assurance method*. De påpeker at hvilken evalueringsmetode som er akseptabel, og hvilket nivå av tiltro som er godt nok, avhenger av organisasjonene og deres politikk/retningslinjer. De nevner først *systemeiers ansvar* for tiltro til et system i bruk. Deretter påpeker de at også andre instanser har ansvar:

- Standardiseringsorganer,
- Nasjonale og internasjonale lover og reguleringer,

- Spesielle instanser, f.eks. regjering eller banker,
- Autoriserte enheter innen en organisasjon,
- Policies,
- Systemakkreditører og
- Sluttbrukere.

Arbeidsgruppen har tentativt satt opp en kategorisering av evalueringsmetoder.



Figur 31 Kategorisering av eksisterende evalueringsmetoder

De har f.eks. plassert SSE-CMM[4] i kategori I og kategori II, BSI Code of Practice i kategori II og CC (Common Criteria), ITSEC og TCSEC i kategori III. Kategori IV er det området der man skal evaluere / skaffe seg tiltro til at et produkt eller et system gjør det det er ment å gjøre. Der har de foreløpig bare plassert Personnel Assurance som er ment å ta opp tiltroen til IT-eksperter, hvilket er på siden av det jeg leter etter i forbindelse med systemer for digitale signaturer. Arbeidsgruppa tar opp forholdet mellom verifisering og validering, j.fr. punkt 4.8.4 s. 82. De skriver at design av et system alltid starter med noen overordnete mål som ikke alltid lar seg oversette til presise krav, der implementasjon av dem kan vise til korrekt bruk ved verifisering. Hensikten med valideringsaktiviteter er å identifisere kritiske problemer. Det ser ikke ut til å eksistere egnete evalueringsmetoder for kategori IV, selv om sannsynligvis flere av de andre metodene kan ha brukbare elementer.

5.5.2 Trusler mot digitale signaturer

Det fins mange trusler mot tilliten til bruk av digitale signaturer:

- Det kan bli generert flere kopier av den private nøkkelen,
- Det kan bli generert 'svake' nøkler som er lette å knekke,
- PIN-koden knyttet til den private nøkkelen kan komme på avveie sammen med kortet som inneholder nøkkelen,
- Programvaren kan medvirke til at man signerer noe annet enn det man ser, f.eks. 1 000 000 kr. i steden for 10 000 kr., pga. feil i programmene eller ford de kan være 'klusset' med,
- Man får verifisert et annet sertifikat enn det man ber om å få verifisert,

4. System Security Engineering Capability Maturity Model, Model Description, V1.1, June 16, 1997.

- Verifiseringsprogrammet har en feil slik at man noen ganger får godkjent signaturer som ikke er gyldige,
- Tidsstemplingsprogrammet kan gi feil tid,
- Generatoren for randomiserte tall kan være svak,
- De tekniske komponentene i et system kan være dårlig testet,
- Dokumentet er ikke lesbart etter konvertering,
- Det fins ikke maskiner/programvare som kan lese gamle medier eller gamle dokumenter.

Det er en utfordring at brukere skal få en viss forståelse for mulige trusselbilder, slik at de kan lære om og vurdere den risikoen de løper ved å bruke digitale signaturer.

Svake algoritmer

Robert Morris, Sr., fra NSA, hadde i følge Steven Levy [22] to læresetninger på Crypto '95:

1 "Never underestimate the time, expense, and effort an opponent will spend to break a code. Beware of the frontal assault."
2 "Look to the plaintext. Exploit your opponent's mistakes."

Den første går på de som bruker store maskinressurser og knekker et krypto-system, slik entusiaster benytter maskiner på nettet for å knekke 40 bits nøkler. Den andre går på å finne svakheter i et system, slik andre entusiaster fant svak-heter i pseudorandom tallgeneratoren i Netscapes SSL-implemtasjon.

Det er en stor avstand mellom den matematiske algoritmen for sikkerhet og hver enkelt konkrete implementasjon i hardware og software [119]. Utviklingen har gjort at man må bruke lengre nøkler for å opprettholde nøklenes levetid og man vurderer å bruke kraftigere hash-algoritmer.

5.6 Diskusjon

5.6.1 Ikke-benekting og sertifikatstandarden X.509

I punkt 3.6.3 tar jeg opp at ikke-benekting av digitale signaturer ikke er like selvsagt som for håndskrevne underskrifter, selv om den digitale signaturen er knyttet til et sertifikat.

X.509 versjon 3 [38] er den mest brukte internasjonale sertifikatstandarden. Michael Roe [115] påpeker i sin doktorgradsavhandling at det i veiledningsmaterialet til X.509 står at den støtter tjenesten ikke-benekting, men at dette ikke nevnes i teksten. Det står heller ikke hvordan man skal løse konflikter rundt ikke-benekting. Han skriver at det er viktig å se på innsamlet materiale ikke som matematiske bevis, men som en samling observasjoner som skal overbevise oss om hvorvidt en hendelse inntraff eller ikke. Det kan få store konsekvenser hvis man konkluderer med at en hendelse inntraff, mens den faktisk ikke gjorde

det. Da kan det kreves stor overbevisningskraft for å vise at man ikke har gjort noe. Dersom det er lang tidsavstand mellom når en hendelse inntraff og når man trenger å bevise at den inntraff, kan det være andre enn aktørene som blir de involverte parter. Et eksempel på det er oversendelse av dokumenter der signataren og mottakeren begge har sluttet i jobbene sine, og der sjefene skal avgjøre hva som skjedde.

Det bør vurderes om det skal være en øvre ansvarsgrense for sertifikateier, på lik linje med ansvarsgrensen for bankkort. Ford og Baum foreslår at sertifikateier skal ta det største ansvaret i perioden etter kompromittering, se Figur 23 side 97. Hvis konsekvensene og ansvaret blir for stort kan det hindre folk i å ta i bruk offentlig nøkkel kryptografi. På den andre siden ønsker man ikke at en person skal kunne unndra seg sitt ansvar ved å lyve. Noe av dette avklares via sertifiseringspolicien som sertifieringsautoriteten arbeider ut fra.

Roe påpeker nødvendigheten av å ikke forvente for mye av tjenesten ikke-benekting. Feil i programvaren kan føre til stor forskjell mellom hva programmet gjør og hva det er ment å gjøre. Hvis noe uønsket hender, kan det være vanskelig å bestemme ansvaret for feilen. Utro tjenere kan forekomme. Det er viktig at det ikke er en fiende som genererer nøkkelparet og tar en kopi til eget bruk. Dette er vanskelig å verifisere. En sertifiseringsautoritet ønsker å være sikker på at det ikke genereres svake nøkler som er lette å knekke.

Validering av gamle elektroniske signaturer

I og med at tid er en naturlig egenskap ved et fysisk dokument, men ikke ved et elektronisk dokument, må det lages mekanismer som gjør at det elektroniske dokumentet kan bestemmes tidsmessig. Sertifiseringsautoriteten sletter normalt sertifikater fra katalogen når gyldighetsperioden er utløpt [30]. Men ved hjelp av sertifikatet som følger dokumentet kan man finne sertifiseringsautoritetens offentlige nøkkel i en sertifikatsti av SAs tidligere nøkler og bestemme tidsperioden for signering.

I åpne systemer der man ikke kan forvente at signatar og den som verifiserer et dokument har tillit til hverandre, kan det være et krav at tidsstempling påføres av en tiltrodd tredjepart hvis det kreves høy grad av sikkerhet.

Hans Nilsson, ID2 Technologies, og Denis Pinkas, BULL, har tatt for seg validering av gamle elektroniske signaturer [72] i forbindelse med ikke-benekting. Langtidsvalidering begynner når sertifikatet har utgått og en av følgende hendelser har inntrått:

- Sertifiseringsnøkkelen til sertifiseringsautoriteten, SA, som ble brukt til å godkjenne sertifikateiers nøkkel er byttet,
- Sertifiseringsnøkkelen til en rot-SA er utgått ved valideringstidspunktet,
- Ett eller flere kryssertifikater har utløpt.

Det er sertifikatautoritetens ansvar at all informasjon som er nødvendig for validering, fins tilgjengelig for den som skal validere. De bruker begrepet validere om prosessen som skal etablere at et sertifikat eller en 'sertifikatsti' (en historisk rekke av signerte sertifikater) er uskadd og korrekt.

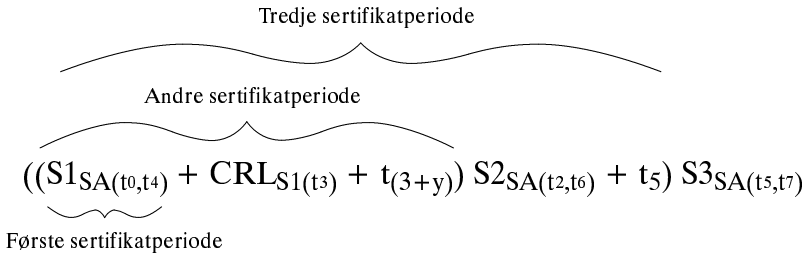
En viktig egenskap ved ikke-benekting er at hvis en signatur en gang har blitt validert, så kan det samme resultatet oppnås måneder og år seinere. Dette er tilfelle selv om sertifikatet tilbakekalles etter signering. Hvis sertifikatet tilbakekalles, må man vise at signering foregikk før tilbakekallingen. Det gjøres ved å få et tidsstempel fra en tidsstemplingsautoritet, TSA.

A → TSA:	h(M)	A er signatar og sender TSA en, hash h(M) av meldingen.
TSA → A:	$(h(M), id_{TSA}, t_1)DS_{TSA}$	TSA returnerer hash-koden signert til A, der id_{TSA} er identiteten til TSA. t_1 er tidspunktet for stempling og DS_{TSA} er TSAs digitale signatur.

Et slikt tidsstempel sier bare når dokumentet var innom TSA. Mottakeren av meldingen, B, trenger å vite når dokumentet ble signert og dermed erkjent av signataren. Dette gjøres ved å tidsstemple én gang til:

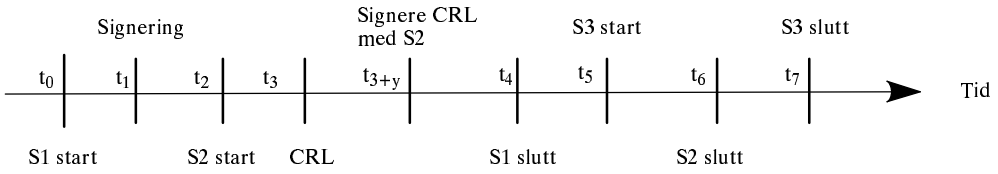
TSA → B: $((h(M),id_{TSA}, t_1)DS_{TSA}, t_{1+x})DS_{TSA}$ TSA sender hash-koden til B med et ekstra tidsstempel der x er en maksimum tidsperiode for å gi gyldighet til signaturen i henhold til autoritetens policy.

For å kunne validere gamle sertifikater lang tid etter signering, trenger mottaker en 'sertifikatsti'. Det er tidsstempling av alle tilbakekallingslister og sertifiseringsautoritetenes sertifikater. En slik 'sertifikatsti' kan ha følgende utseende:



S1	er sertifiseringssautoritetens sertifikat i tidsperioden t_0 - t_4
S2	er sertifiseringssautoritetens sertifikat i tidsperioden t_2 - t_6
S3	er sertifiseringssautoritetens sertifikat i tidsperioden t_5 - t_7
CRL_{t3}	er en tilbakekallingsliste for sertifikat S1 på tidspunkt t_3 tidsstemplet av SAen på tidspunkt t_{3+y}
t_5	er tidsstempling ved starten av S3's tidsperiode. $t_n < t_{n+1}$ $\forall$ n.

Alle sertifikatene overlapper hverandre i tid for at man skal kunne signere en 'sertifikatsti'. I den andre sertifikatperioden, fra t_2 til t_6, utstedes det en tilbakekallingsliste for S1 på tidspunkt t_3. Det tidsstemples med det nye sertifikatet S2 på tidspunt t_{3+y} . På denne måten kan man verifisere at et dokument signert på tidspunkt t_1 er gyldig, mens signering på tidspunkt t_{4+x} er ugyldig.



Figur 32 Tidsstempling av 'sertifikatstier'

5.6.2 Designmulighet

Levetid

Bæreren av informasjonen har en sentral posisjon. Bytte av teknologi viser dette. Papir er det eneste som trengs for å vise leseren den håndskrevne signaturen, og som gir den lang levetid. Ved bruk av informasjonsteknologi er det langt flere elementer som skal samvirke og bære informasjonen fram til leseren. Sammen og hver for seg påvirker de levetiden. I tillegg til det fysiske lagringsmediet påvirkes levetiden av formater, tekstbehandlingsverktøy og maskin- og programvare.

Levetiden til en digital signatur er avhengig av bla. hvor plattformuavhengig tekstbehandlingsformatet er. Ettersom signaturen beregnes bla. på grunnlag av tekstbehandlingsprogrammet dokumentet skrives i, og noen programmer er nærmere knyttet til maskinvaren [24], blir valg av tekstbehandlingsverktøy viktig. Dette er særegent for digitale signaturer. Men signaturenes levetid må holdes opp mot hvor sterke føringer offentlige etater vil legge på kommunikasjon med publikum. Hvis etatene velger et lite brukt tekstbehandlingsverktøy, vil dette kunne hindre elektronisk kommunikasjon.

Et vesentlig krav i forhold til design for lang tid er Noarks krav [114] om et ferdiggjort og godt etablert produkt i marketet. Word er f.eks. et godt etablert produkt, men det er proprietært og det kan inneholde skjult tekst, makroer mm.

Risikoområder

Man bør foreta risikoanalyse for å vite hvor lenge man kan satse på å langtidslagre digitalt signerte dokumenter. Ved risikoanalyse bør man spørre og svare på følgende spørsmål [55]:

- Hva er de tekniske svakhetene ved systemer og formater?
- Hva er de viktigste truslene?
- Hva er sannsynligheten for at en fiende eventuelt en utro tjener vil angripe en bestemt svakhet?
- Hvilken risiko løper man på hvert område?
  - Der man ikke får tilgang til det elektroniske dokumentet.
  - Signerer man bare det man ser?

Ingeniør og sikkerhetsarkitekt Jueneman og jurist Robertson [55] påpeker at proprietære algoritmer antas i langt større grad å inneholde fundamentale feil,

fordi de ikke utsettes for slike intense gjennomganger og granskninger som åpne spesifikasjoner og standarder blir. Man finner svakheter ved standardalgoritmer med ujevne mellomrom. Det invaliderer ikke tidligere digitale signaturer, men gjør dem noe mer suspekte.

Erfaring med den teknologien som er tilgjengelig i dag, tilsier at offentlige etater som skal arkivere dokumenter lenger enn 10 år, bør lagre dem som papirutgaver. Innenfor en tiårsperiode bør det være mulig å planlegge pålitelig tilgang til digitalt signerte dokumenter.

5.6.3 Heterogenitet

Hvis man først skal akseptere å ha noe ekvivalent med håndskrevne underskrifter, hvilke løsninger fins? For kommunikasjon mellom aktører som ikke kjenner hverandre, fins det ikke noe annet en digitale signaturer som binder signataren og dokumentet sammen. Etter min mening fins det store forskjeller i behov hos ulike brukere. Aktørene har ulike interesser. Mitt inntrykk er at privatpersoner i sin kommunikasjon med det offentlige i langt mindre grad har behov for sertifikater enn offentlige etater og private organisasjoner har.

Jurister har internalisert en forståelse for når underskrifter på papirdokumenter er gyldige [88] [89]. Det kan uttrykkes ved Pfleegers utvidete definisjon av integritet fra kapittel 3: *presist nok* og *brukbart i en gitt situasjon*. Det åpner for skjønn fra juristenes side som er viktig for å sikre kvalitet i saksbehandlingen, j.fr. punkt 4.7. Imidlertid snevrer valget av teknologi inn juristenes mulighet for skjønn når de aksepterer at digitale signaturer erstatter håndskrevne underskrifter. Det mener jeg det offentlige må ha i mente når de vurderer løsninger.

Minimumsløsninger

Pilotprosjektet EDNA i Kommunal- og regionaldepartementet brøytet nytt land og startet ut med en minimumsløsning for signering av ustrukturert tekst. De har fått til signering og kryptering av dokumentutveksling mellom to etater. Dokumentene tas ut på papir og lagres fysisk. Nå ser de behovet for å kunne lagre dem elektronisk. Samtidig viser en slik minimumsløsning nødvendigheten av å teste at man har fått det man ønsker seg. KRD har ikke foretatt den testen fullt ut. Da ville de sett at teknologien setter begrensninger selv for dem og at konvertering mellom tekstbehandlingsverktøy ikke gir god nok løsning i alle situasjoner. EDNA viser at full gjennomgang av rutier er nødvendig, selv for ganske enkle eksempler, ved innføring av denne type teknologi.

Når det offentlige skal vurdere standard tekstbehandlingsverktøy for digital signering, bør det vurderes om opsjoner som f.eks. hemmelig tekst, skal fjernes for å minske mistroen til verktøyet. Etatene kan signere en papirutskrift som bevis og for akrivering, og arbeide videre elektronisk med digitalt signerte utgaver. Det vil gi økt bruk av elektronisk saksbehandling og bedre meldingssikkerhet i noen ledd.

Stort apparat for Digitale signaturer

I det offentlige rom trenger man en offentlig-nøkkel infrastruktur. Det er et stort apparat og skaper mye arbeid, særlig for privatpersoner som skal kommunisere

med offentlige etater. De trenger PC og smartlkort. De trenger å være et bestemt sted eller i hvert fall finne fasilitetene, inkludert strøm og telefon, for å kunne signere. Dvs. det er viktig å avklare om man faktisk trenger den løsningen eller om man kan akseptere en enklere løsning. Dette er det vanskelig å ta stilling til før departementene har utredet behovet for lovendringer. Det kan tenkes at enkelte etater har datasystemer og kommunikasjonsbehov bare med en lukket brukergruppe. Da kan det være mulig å finne enklere løsninger, enten droppe sertifikatene eller ta i bruk f.eks. PenOp. Men offentlige etater vil trenge en PKI i sin samhandling med andre etater.

5.7 Konklusjoner

Valg av design for systemer og infrastruktur for digitale signaturer påvirker hvilke brukerkrav som realiseres, og brukernes tilit til å ta digitale signaturer i bruk.

- Den tilgjengelige teknologien legger begrensninger på hvilke egenskaper ved signaturer som kan realiseres elektronisk.
- Både presentasjonen av dokumentet på skjerm må være korrekt, og den digitale signaturen må være godkjent, for at dokumentet skal være autentisk.
- Enhver endring i et elektronisk dokument ugyldiggjør en tilhørende digital signatur. Det er en begrensing i forhold til signerte fysiske dokumenter og juristers virkelighet.
- Digitale signaturers levetid vil variere med hvor plattformavhengig tekstbehandlingsverktøyet er.
- Signaturene kan ikke i dag påregnes å ha en levetid på mer enn maksimalt maksimalt 10 - 15 år. Skal signerte dokumenter leve lenger, bør man bruke papir.
- Signerte dokumenters levetid må holdes opp mot hvor sterke føringer det offentlige vil legge på elektronisk kommunikasjon med allmennheten.
- Man skal ikke ha for store forventninger til ikke-benekting i en kompleks digital verden.
- Løsninger basert på anerkjente standarder testes vanligvis bedre enn proprietære løsninger.
- Sertifikatbruk vil kreve relativt mer av privatpersoner enn av offentlige etater.

6 Sammendrag og konklusjoner

Først gir jeg et sammendrag. Deretter presenterer jeg hovedkonklusjonene og andre funn. Til slutt svarer jeg på spørsmålene jeg stilte i innledningen og kommer med forslag til videre forskning og arbeid.

6.1 Sammendrag

Undertegnede fysiske dokumenter

Papir er bærer av nesten all informasjon knyttet til dokumentet. Det binder sammen dokumentets innhold og underskriveren, signataren. Den personlige underskriften har lang tradisjon som garantist for at dokumenter er ekte, selv om den vanligvis ikke sjekkes. Autentisering er vanskelig i ettertid, men mulig. Fysiske dokumenter kan lagres i mange hundre år. Den sosiale forståelsen for å undertegne er i hovedsak stor.

Overgang til en elektronisk verden

Det er vanskelig å definere hva en signatur er. Gjeldende lovverk har ikke definert hvordan man autentiserer et dokument og en underskrift. Det bygger på skjønn og en ikke-dokumentert praksis. Dette gjør det vanskelig å definere krav til et system for elektronisk signatur. Når man går fra noe difust til et elektronisk system, vil neppe det elektroniske systemet fange alle viktige aspekter fra en papirverden. Det skaper derfor usikkerhet hos meg som bruker at ingen har validert om man får det man er ute etter. Justisdepartementet skriver i sitt kartleggingsbrev av 15.3.99 [57] at NHD, AAD og JD har spesielt ansvar for å sikre at lovverket gir mulighet for å bruke digitale signaturer. Men brevet nevner ikke eksplisitt nødvendigheten av å vurdere om teknologien kan klare å dekke vesentlige funksjoner knyttet til håndskrevne underskrifter.

Elektroniske dokumenter kan lett kopieres. Det medfører at man trenger spesielle mekanismer for å binde signataren til dokumentets innhold. Den eneste mekanismen som dekker de difuse kravene, er offentlig-nøkkel kryptering, digitale signaturer og nøkkelsertifikater. Ved bruk av symmetrisk kryptering, er det minst to som deler en hemmelig nøkkel. Det gir ikke binding mellom signatar og dokumentets innhold på forsvarlig måte der partene ikke kjenner hverandre.

Elektroniske dokumenter vil ikke være tilgjengelig for alle. Det vil derfor være behov for papirutskrifter i flere år.

Digitalt signerte dokumenter

Digitale signaturer henger sammen med innholdet vha. bit-representasjonen og kryptering. Det er ikke en underskrift, men det gir en kopling mellom innholdet og signataren. Den nye teknologien gjør den sosiale forståelsen av å signere

vanskeligere å forstå i begynnelsen. Autentisering kan skje automatisk ved mottak av et dokument. Statusinformasjon om dokumentet lagres i stor grad separat fra dokumentet.

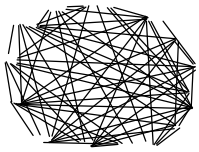
Digitale signaturers levetid

For at en digital signatur skal kunne leve over lenger tid, må både dokumentet kunne presenteres korrekt på en skjerm og signaturen må kunne verifiseres. Hvis bit-representasjonen er plattformavhengig, medfører det at den digitale signaturen blir ugyldig ved konvertering til ny plattform eller et annet tekstbehandlings-verktøy. De fleste systemer for digital signatur brukes mot proprietære løsninger, f.eks. Word. Det gjør dem platformavhengige og medfører at de neppe kan påregnes å forbli gyldige lenger enn 10 - 15 år. Dersom det representasjons-formatet som signeres er SGML, kna levetida kanskje vare i 15 år. Lagrings-medier, mangel på kompetanse, maskiner og programvare som brukes til å lese dokumentet, og levetida for kryptonøkler er variable som kan begrense signaturens gyldighetstid. Forventet levetida for nøkler kan forkortes ved uforutsigbare 'kvantesprang' i forståelsen av hvordan den tilhørende algoritmen virker, innen matematikken og innen den teknologiske utviklingen.

For papirdokumenter er underskriften tilgjengelig like lenge som papiret. Digitale signaturer vil vanligvis ikke være gyldige like lenge som resten av det elektroniske dokumentet. Men mange signerte dokumenter må kunne gi informasjon om hendelser knyttet til dokumentet i lang tid etter signeringen. Det vil derfor være ønskelig med en juridisk avklaring av i hvilke tilfeller det får konsekvenser at dokumentet ikke kan autentiseres, sjekkes for dataintegritet eller tidfesting av signaturen. Mulige problemer i forbindelse langtidslagring er ikke nevnt i kartleggingsbrevet fra Justisdepartementet [57].

Offentlig-nøkkel infrastruktur

Et system for digitale signaturer vil kreve en annen og mer kompleks infrastruktur enn den man har for fysiske dokumenter. Offentlige etater har behov for å kunne autentisere signataren på mottatte dokumenter. Det er de ikke sikret ved mottak av elektronisk post, selv om den likestilles med papirpost i forskriftene til arkivloven. Til det trenger avsenderne tiltrodde tredjepartstjenester og nøkkelsertifikater. Ved hjelp av sertifikatstier for sertifiseringsautoriteter kan man autentisere utgåtte sertifikater i ettertid. Databaser for sertifikater og tilbakekallingslister er arkivverdige. I midlertid er ansvarsforholdene i forhold til arkivloven uklare.



Man bør ikke forvente at ikke-benekting vil ha samme kraft i en elektronisk verden som ved bruk av papir. En privat nøkkel har en svakere binding til signataren enn håndskrift har. Det gir større mulighet for benekting. I tillegg er infrastrukturen kompleks med mange muligheter for svakheter.

Personvern

Hvem som syns det er viktig å kunne autentisere i ettertid, vil variere. Det vil kreve mye av enkeltpersoner å gå over til digtale signaturer hvis de selv må passe

på elektroniske dokumenter i ettertid. Hvis de ikke har forståelse for ansvaret ved å ta vare på dokumentene, er det lett å miste alt ved anskaffelse av ny PC. Eller de må ha forståelse for at de må lagre dokumentene hos en notar. Ettersom det er langt flere aktanter med i forbindelse med digitale signaturer enn med håndskrevne underskrifter, blir situasjonen langt mer kompleks. Å bevise at man har sendt eller å bevise at man ikke har sendt en påstått melding, blir en mye større, og en helt annen, utfordring for enkeltindivider som ikke bruker digitale signaturer ofte.

Den sosiale forståelsen kan bli bedre ved digital signering. Brukerne stilles overfor prosesser som virker fremmedgjørende og uvante i forhold til å underskrive for hånd.

6.2 Hovedkonklusjoner

6.2.1 De viktigste funnene

- Dersom digitalt signerte dokumenter skal lagres lenger enn anslagsvis 10 - 15 år, vil vedlikeholdsarbeidet for å opprettholde tilgang til dokumentene øke dramatisk,
- Ikke alle egenskaper eller karakteristika ved håndskrevne underskrifter lar seg realisere som digitale signaturer,
- Det offentlige har tatt i bruk digitale signaturer som ekvivalent med håndskrevne underskrifter uten å
  - Vurdere hvilke begrensninger som informasjonsteknologi setter,
  - Bestemme hvem som har ansvar for å definere sammenhengen mellom dem,
  - Vurdere ved testing om erstatningen er dekkende,
- I de nærmeste årene vil bruk av digitale signaturer og offentlig-nøkkel sertifikater medføre ekstra arbeid og utgifter i forhold til å underskrive papirdokumenter for privatpersoner. Det koster å anskaffe sertifikater og selv ta vare på elektroniske dokumenter, men saksbehandlingen kan gå raskere.

6.2.2 Andre funn

- Bindingen mellom fysisk dokument og håndskreven underskrift er sterkere enn bindingen mellom signatar og digital signatur.
- Håndskreven underskrift er
  - Noe man er (biometri) og
  - Noe man kan (skrive).
- Digitale signaturer er
  - Noe man har (et smartkort) og
  - Noe man vet (PIN).
- Informasjonsteknologi gir muligheter for et uendelig antall dokumentkopier.
- Man trenger tillit til teknologien, ikke bare til mennesket som signerer.
- Et elektronisk dokument er avhengig av informasjonsteknologi og er dermed ikke like tilgjengelig for alle der man måtte befinne seg. Man trenger

maskiner og programvare både for å produsere, lese og vurdere om dokumentet er ekte, hvilket skaper økt kompleksitet og økt risiko for at man ikke får til det man vil.

- I større grad enn for fysiske dokumenter kan det være vanskeligere for en signatar å være innforstått med den juridiske og sosiale handligen ved å signere digitalt.
- Det offentlige har ikke spesifisert hvilke typer sertifikater som kreves fra private personer ved bruk av digitale signaturer.
- Offentlige etater og bedrifter ser ut til å ha større behov for sertifikater enn privatpersoner.
- For å bruke digitale signaturer og offentlige-nøkkel sertifikater, trenger man en kompleks infrastruktur.
- Verken Riksarkivaren eller 'jurister' har tatt opp problemet med manglende autorisasjon av innholdet når dokumenter arkiveres uten signatarens signatur.
- Noark-4 har ikke definert hvordan man skal garantere for at langtidslagrete dokumenter er ekte og autentiske (ikke forfalsket).
- Dersom det offentlige ikke går dypere inn i sammenhengen mellom håndskrevne underskrifter og digitale signaturer, kan den første rettsaken om digitale signaturer konkludere på et svakt rettsgrunnlag.
- Det stilles strenge krav til digitale signaturer, men ikke kriterier for i hvilke situasjoner arkivaren kan signere eller hvordan verifikasjonsspor skal produseres.
- Databaser for sertifikater og tilbakekallingslister er arkivverdige. I midlertid er ansvarsforholdene i forhold til arkivloven uklare.
- Verken Riksarkivaren eller de nordiske riksarkivene nevner behovet for kompetanse innen informasjonsteknologi for å ta vare på elektroniske dokumenter.
- Signerte dokumenters levetid må holdes opp mot hvor sterke føringer det offentlige vil legge på elektronisk kommunikasjon med allmennheten.
- Man skal ikke ha for store forventninger til ikke-benekting i en kompleks digital verden.
- Både presentasjonen av dokumentet på skjerm må være korrekt, og den digitale signaturen må være godkjent for at dokumentet skal være autentisk.
- Enhver endring i et elektronisk dokument ugyldiggjør en tilhørende digital signatur. Det er en begrensing i forhold til signerte fysiske dokumenter og juristers virkelighet.
- Digitale signaturers levetid vil variere med hvor plattformavhengig tekstbehandlingsverktøyet er.
- Realiseringen av signerte dokumenter i en elektronisk verden kan ikke skje uavhengig av teknologi. Dvs. at teknologien setter begrensinger, selv om man kan designe og implementere ulike løsninger.
- For å kunne verifisere digitale signaturer trenger man tilstandsinformasjon og opplysninger ut over dokumentet selv.
- Løsninger basert på anerkjente standarder testes vanligvis bedre enn proprietære løsninger.
- Håndsignerte dokumenter gir mulighet for skjønn ved vurdering av autentisitet. Den formen for skjønn fins ikke for digitalt signerte

dokumenter. Dvs. det er ønskelig å få en vurdering av hvilke positive juridiske virkninger ved digitale signaturer som kan brukes nå, samtidig som andre alternativer undersøkes.

6.2.3 Svar på oppgavens problemstillinger

I hvilken grad kan man bruke digitalt signerte dokumenter i steden for håndsignerte dokumenter, og hvor lenge kan slike dokumenter lagres?

- Tidsperspektivet ved digital signering har vært lite påaktet.
- Digitale signaturer bør i hovedsak brukes der det ikke er behov for lagring av dokumentet over flere tiår.
- Digitalt signerte dokumenter kan ikke bevare sin signatur ved konvertering til nye formater. Signaturene vil neppe vare like lenge som selve dokumentet hvis dokumentet er ment å skulle arkiveres i mange år.

1 Hva gjør offentlige etater der elektroniske dokumenter trenger signatur?

- Kartlegging av behov for å endre lover er i gang. Men mandatet legger ikke spesiell vekt på problemene rundt langtidslagring eller at teknologien kan sette begrensninger.
- Noen etater har behov for å signere over strukturert informasjon, andre over ustrukturert. Dette gir behov for ulike løsninger.
- Noen etater har startet utprøving med digitale signaturer. De har ikke fullt ut testet om løsningene dekker behovene.

2 Hva er det egentlig som skjer når man går fra den fysiske til den elektroniske verdenen?

- Håndskreven underskrift er
  - noe man er (biometri) og
  - noe man kan (skrive).
- Digitale signaturer er
  - noe man har (et smartkort) og
  - noe man vet (PIN).
- Verifisering av en digital signatur med sertifikat kan utføres automatisk ved mottak og i ettertid hvis den nødvendige teknologien er tilgjengelig.
- En digital signatur er ikke knyttet til dokumentets innhold på samme måte som en håndskreven underskrift er. Signaturen er bla. knyttet til tekst-behandlingsformatet som kan være plattformavhengig.
- Teknologien gir muligheter for et uendelig antall kopier. Ved forflytning kan det lagres kopier på mange maskiner som derved kan bli tilgjengelige for andre enn autoriserte brukere.
- Man trenger maskiner og programvare både for å produsere, lese og vurdere om dokumentet er ekte, hvilket skaper økt kompleksitet og økt risiko for at man ikke får til det man vil.
- Man trenger tillit til teknologien, ikke bare til mennesket som signerer.
- For å kunne bruke digitale signaturer, trenger man tilstandsinformasjon og opplysninger ut over dokumentet selv.

- Elektroniske dokumenter lagrer tillstandsinformasjon separat fra dokumentet
- Man trenger en infrastruktur for offentlig-nøkkelsertifikater.

3 Hva er det spesielle med langtidslagring?

- Mange signerte dokumenter må kunne gi informasjon om hendelser knyttet til dokumentet lenge etter selve signeringen.
- Digital signatur på dokumenter gir ikke mening lenger når dokumentet har vært lagret så lenge at det må konverteres til et nytt format.
- Det fins få aktuelle formater som er i særlig bruk.
- IT ser ikke ut til å gi de samme mulighetene for langtidslagring som papir gir. For at signaturer skal kunne verifiseres i ettertid, må det finnes brukbar programvare, maskinvare og kunnskap om bruken.
- Den som ønsker at et dokument skal være autentiserbart i mange år, må ta mange forholdsregler.
- Langtidslagring av digitalt signerte dokumenter er et problem for privatpersoner som selv må ta vare på dokumentene.
- Egenskapen at en signatur varer like lenge som dokumentet skal leve, er neppe mulig foreløpig. Det er ikke påregnelig i dag å kunne lagre digitalt signerte dokumenter i mer enn 10 - 15 år med brukbar/verifiserbar signatur.

4 Representeres ulike brukerkrav i systemspesifikasjon og programmer?

- Det jeg har funnet av systemspesifikasjoner, ser i liten grad ut til å differensiere ulike brukergruppers behov.
- Et elektronisk dokument er avhengig av informasjonsteknologi og dermed ikke like tilgjengelig for alle.
- I større grad enn for fysiske dokumenter kan det være vanskeligere for en signatar å være innforstått med den juridiske og sosiale handlingen ved å signere digitalt.
- Privatpersoner ser ut til å få mer arbeid enn de har med fysiske papirer.
- Alle steder i prosessen med å utvikle systemer for digitale signaturer ser det ut til at krav kommer i konflikt med hverandre. Noen er ikke realiserbare rent teknisk sett.
- Offentlige etater og bedrifter ser ut til å ha større behov for sertifikater enn privatpersoner.
- Det offentlige har ikke spesifisert hvilke typer sertifikater som kreves fra private personer ved bruk av digitale signaturer.
- Det er ingen som har satt opp hvordan man skal teste at digitale signaturer gir det samme som håndskrevne signaturer.

5 Klarer lover, regler og standarder å tilpasse seg den nye virkeligheten?

- Det fins standarder og mekanismer for digitalt signerte dokumenter, men ikke for alt innen langtidslagring, f.eks. krav til formater og programvare.
- Den juridiske bindingen mellom signatar og den digitale signaturen er til stede, men ikke like sterk som til den håndskrevne underskriften.
- Noark-4 har ikke definert hvordan man skal garantere for at langtidslagrete dokumentene er ekte og autentiske (ikke forfalsket).

- De juridiske konsekvensene av at man ikke kan autorisere innholdet av elektroniske dokumenter etter konvertering til nye lagringsformater, er ikke utredet.
- De juridiske konsekvensene ved fravær av digitale signaturer ved arkivering er ikke utredet.
- Verken Riksarkivaren eller 'jurister' har tatt opp problemet med manglende autorisasjon av innholdet når dokumenter arkiveres uten signatarens signatur.
- Risikomomenter ved å ta i bruk digitale signaturer er ikke utredet.
- Verken Riksarkivaren eller de nordiske riksarkivene never behovet for kompetanse innen informasjonsteknologi for å ta vare på elektroniske dokumenter.

Justisdepartementet har sagt at dommerne kan se på digitalt signerte dokumenter på lik linje med fysiske dokumenter. Dermed har mye blitt overlatt til dem uten at de har forutsetning for å kunne vurdere likheter og forskjeller. Fordi jurister og offentlige myndigheter ikke tidligere har gjort nok utdypende arbeid om utfordringene ved å ta i bruk ny teknologi, kan dommerne få en stor oppgave. Det kan gi svakt funderte avgjørelser i de første tvistene på området.

Pga. fri bevisføring står rettssubjekter fritt til å bruke elektronisk kommunikasjon seg i mellom. Men det offentlige bør vise folk hvilken risiko de løper ved å bruke digitalt signerte dokumenter framfor papir.

Justisdepartementet [57] skriver at avklaring av rettslig usikkerhet i stor utstrekning finner sted ved at regelverksforvalterne endrer lover og forskrifter. Mht. autentisitet og integritet foreslår departementet at "det må gis egne regler med vilkår som de elektroniske meldingene må oppfylle". Jeg mener jeg har fått fram at elektroniske dokumenter ikke kan oppfylle alle krav. Spesielt gjelder dette autentisering ved langtidslagring. Kartleggingsbrevet nevner ikke det spesielle behovet for å vurdere utfordringer ved langtidslagring av digitalt signerte dokumenter.

6.3 Forslag til videre forskning og arbeid

Jeg foreslår at følgende saksområder avklares for å få bedre effekt ved bruk av digitale signaturer:

Juridiske problemstillinger

1 Man bør forske mer på egenskaper ved håndskrevne signaturer som man ønsker å utnytte ved langtidslagring i en digital verden,
   - Hvilke generelle og spesielle ønskete egenskaper ved en håndskreven underskrift lar seg ikke realisere med tilgjengelig teknologi?
   - I hvilke situasjoner vil det være akseptabelt å ha usignerte elektroniske dokumenter der man tidligere krevde underskrifter?
   - Hvilke risikoer løper samfunnet og enkeltpersoner når et signert dokument ikke lenger er gyldig?

- Får det konsekvenser at en digital signatur er snevrere i sin akseptanse av gyldighet og ekthet enn et håndsignert fysisk dokument?
- Hvilke konsekvenser får det at det kan være vanskeligere å få til ikke-benekting ved bruk av digitale signaturer?
- Hvordan skal man teste at digitale signaturer tilsvarer håndskrevne underskrifter på ønskete områder?
- Er det behov for å opprette en elektronisk notartjeneste? Hvem skal eventuelt ha ansvaret for den?
- En vurdering av hvilke positive juridiske virkninger ved digitale signaturer som kan brukes i samtiden, samtidig som andre alternativer undersøkes.

Elektronisk saksbehandling

2 Hvordan skal man utnytte digitale signaturer i saksbehandlingen selv om slike dokumenter er vanskelige å langtidslagre?
   - Regler for å beholde eller fjerne signatarens signatur,
   - Regler for utskrift av signerte dokumenter,
   - Regler for autentisering av dokumenter,
   - Regler for å bruke elektroniske dokumenter selv om signaturen har begrenset levetid,
   - Opplegg for å hjelpe privatpersoner som trenger å bevare på elektroniske dokumenter i sin samhandling med det offentlige,

3 Hvilke krav skal man stille til tekstbehandlingsverktøy?
   - Krav til formater for å få utført den saksbehandling som er nødvendig,
   - Krav til konvertering mellom tekstbehandlingsverktøy,
   - Krav som skaper tillit til at man signerer det man ser på skjermen?
   - Krav som letter bruken for privatpersoner,

4 Hvordan skal etatene forholde seg til usignert innkommen elektronisk post?

Teknologiske utfordringer

5 Hvordan påvirker formater av ulike slag livslengden til en digital signatur?

6 Fins det andre måter å knytte en signataren til dokumentet som gir større 'slingringsmonn' og 'presis nok' bruk slik den virkelige verden fungerer?

7 Hvor er de største teknologiske risikomomentene ved bruk av digitale signaturer?
   - Studier rundt nøkkellengder,
   - Er Moor's lov stabil nok som grunnlag for å bruke digitale signaturer?

8 Utdype hvor det mangler teknologi for langtidslagring.

A Identifisering og autentisering

Forskjellen mellom de to begrepene er aktuell i forbindelse med personer og ting, f.eks. dokumenter. Jeg syns det er uklart hva som er likt og hva som er forskjellig, og hva som trengs for å gå fra håndskrevne signaturer til elektroniske dokumenter. Her kommer min forståelse av problemstillingen.

A.1 Begrepene

A.1.1 Definisjoner

Autentisk fullt ut ekte og pålitelig [12]. Som virkelig har den opprinnelse el. hjemmel som oppgis; ekte [139].

Autentisering Å verifisere at noe er fullt ut ekte og pålitelig [12]. Prosessen med å bekrefte en oppgitt identitet. (fra datasikkerhetsdirektivet) [116]. Bevitne, bekrefte ekthet [139]. Man autentiserer både dokumenter, personer og datamaskiner (f.eks. noder).

- Dokumenter,
  - At det ikke er forandret (integritet),
  - At det hadde et bestemt innhold på et bestemt tidspunkt,
  - At en bestemt person har laget det,
- Personer,
  - At personen er den han gir seg ut for å være,
  - At en person, eller den som bruker en ident eller har en rolle, har autorisasjon til å utføre en oppgave,
- Utstyr,
  - At maskinen eller programvaren er den den sier å være (at DNB's maskin er DNB's maskin).

Autentifisering "give et dokument en form der garanterer dets ægthed" [20]

Identifisere 1) kjenne igjen, fastslå identiteten av; 2) regne seg som ett (med), ha samfølelse (med); 3) påvise identitet mellom (to eller flere ting) bringe under samme begrep [12]. Fastslå hvem en person er, gjenkjenne [139].

Identisk fullstendig lik, en og den samme, ensbetydende [12]. Sammenfallende [139].

Identitet 1) det å være identisk; 2) navn, stilling o l til en person [12].

A.1.2 Identifisere og autentisere

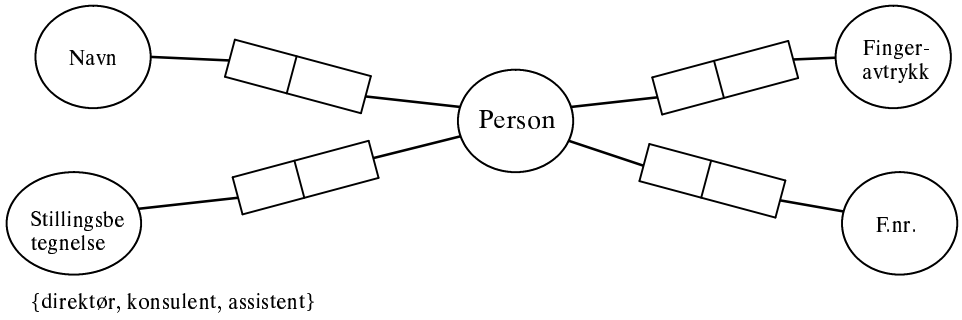
Identitet

Identitet har å gjøre med mer eller mindre særegne egenskaper ved en person eller en ting. De regnes som objektive.

1 Når man definerer noe som en art, eller tilhørende samme begrep, så setter man opp egenskaper og karakteristika som er spesielle for den arten.

2 "Noen" bestemmer gyldige verdier for ulike egenskaper ved den arten.

3 Når man gjenkjenner en entitet som tilhørende en art, ser man etter om alle egenskaper og karakteristika er tilstede og har verdier.



Figur 33 Niam-modell over et utvalg egenskaper som identifiserer en person

Tilordning av verdier til en bestemt utgave av arten kan gjøres av andre enn de som definerer arten eller den entiteten det gjelder.

Fornavn kan identifisere en person i en liten gruppe. Men det kan være to i en klasse som heter Turid. Da tar man med etternavnet for ytterligere å karakterisere/bestemme den man omtaler. Identitet er en eller flere egenskaper/kjennetegn man har (f.eks. fingeravtrykk) og noen egenskaper/ kjennetegn man får (navn, fødselsnummer). Noen egenskaper endrer seg over tid: høyde, hårfarge. Andre er mer stabile: fødselsnummer (innen et bestemt land). De kjennetegnene man får, får man tildelt av andre i bestemte sammenhenger: navn fra foreldre etter fødselen, stilling fra en arbeidsgiver ved tiltredelse.

Identifisering

4 Når man fastslår en persons eller en tings identitet, gjør man det i en viss sammenheng og på et bestemt tidspunkt. På et tidspunkt har en person rollen som hjemmeværende husmor. På et annet tidspunkt har personen rollen som underdirektør. Hvis situasjonen (rollen eller tidspunktet) er vesentlig, identifiserer man to ulike ting.

Å identifisere er å definere egenskaper/kjennetegn og vurdere om de til sammen er nok til å si at de bestemmer en person eller en ting.
$A = Pr(E_1,E_2,E_3,...E_n|S_i,t_i)$, sannsynligheten for at settet av egenskapene E karakteriserer A, gitt sammenhengen S_i på tidspunktet t_i. Identifisering skjer når man definerer hva som karakteriserer A. Det skjer også seinere når noen gjenkjenner A som seg selv, og ser, fastslår, at verdiene for de forskjellige egenskapene $(E_1,E_2,E_3,...E_n)$ er de som karakteriserer A.

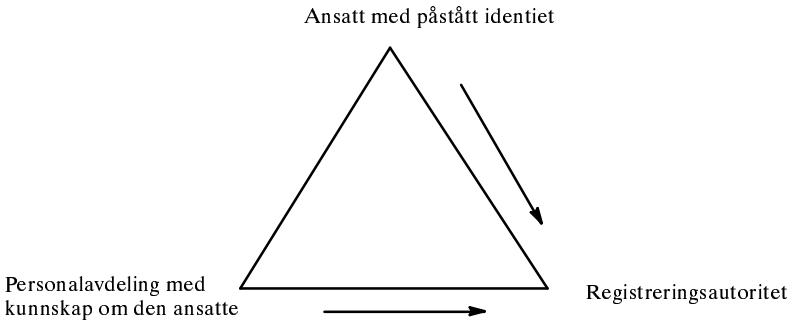
Eksempel: Et papirbrev om innvilget lån i 1999 fra DnB krakteriseres bla. ved E_1: brevhode, E_2: bankens adresse og telefonnr., E_3: lånesum, E_4: rentesats og undertegning av E_5: saksbehandler X. Hvis E_2: bankens adresse og telefonnummer mangler, så er ikke det bestemmende for å identefisere brevet. Men hvis brevhodet mangler, kan man bli mere usikker.

Autentisering

For å autentisere må man først ha slått fast, identifisert, at en entitet tilhører en art, et begrep. Bare på den måten vet man hva man skal vurdere egenskapene og deres verdier mot.

5 Å autentisere er å vurdere om egenskaper/kjennetegn som en person eller en ting presenterer, er ekte (ikke forfalsket), og om derved personen eller tingen er den den pretenderer å være. $F(Pr(E_1), P(E_2), ..P(E_n) \mid A_E, S_j, tj)$ er funksjonen å vurdere hvor ekte hver egenskap / hvert kjennetegn er, gitt en situasjon S_j på tidspunktet t_j ut fra hva som pleier å identifisere A. Autentisering er en subjektiv vurdering, selv om den gjøres maskinelt.

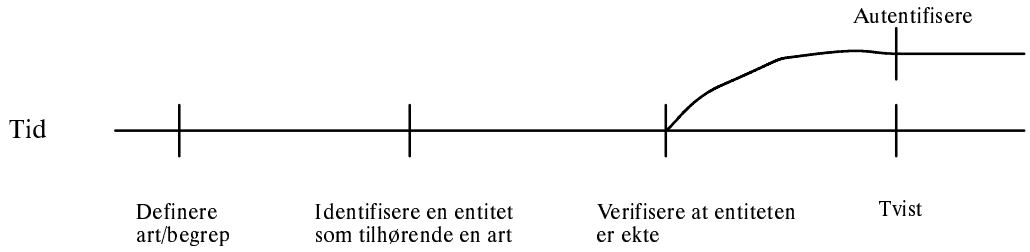
I autentiseringsprosessen setter man ofte påståtte egenskaper ved en entitet opp mot den kunnskapen en uavhengig, tiltrodd tredjepart har tilgjengelig. Når en ansatt møter fram hos en registreringsautoritet, ser registreringsautoriteten på den ansatte og på tjenestebeviset og vurderer dette opp mot bedriftens billedmatrikkel og annen informasjon fra personalavdelingen. Autentisering blir med andre ord ofte en trekantprosess.



Figur 34 Autentisering

Autentifisering

Autentifiserering står som et alternativ til autentisering i Store norske ordbok [139]. Men Tor Guttu, Institutt for nordistikk og lingvistikk, Universitetet i Oslo [91], har funnet en annen definisjon i Dansk Fremmedordbog [20]: ”give et dokument en form der garanterer dets ægthed”. Guttu utdyper det med å si ”at man ved å stemple et dokument ”gir det en form”, dvs. forandrer dets ytre på en eller annen relevant måte”. Jeg oppfatter dette til å være det arbeidet en notar eller en uavhengig ekspert gjør når de setter sitt stempel eller tilsvarende på dokumentet. Det arbeidet medfører at dokumentet får en annen status. j.fr. aktør-nettverksteori. Det vil også et elektronisk dokument få når det får et tidsstempel fra en notar.



Figur 35 Rekkefølgen for identifisering, autentisering og autentifisering

Å verifisere at entiteten er ekte, kan enten gjøres av en ekspert som autentifiserer, "stempler", entiteten og gir den en ny status som ekte, eller det kan avgjøres av en domstol som vurderer flere typer bevismateriale opp mot hverandre.

Tvister

Dersom det oppstår tvist om en identitet er ekte og hører til entiteten som påberoper seg den, kan det være en dommer som avgjør. I Norge har vi fri bevisføring. Dommere må forstå og vurdere tilgjengelige kjennetegn, verdier og det de skal brukes til.

A.1.3 Diskusjon

Man selv eller andre kan fastslå egen identitet ut fra mer eller mindre gitte kriterier. Men det er andre som vurderer om identiteten er ekte og tilhører / eies av A. Det er autentisering. Tidspunktet t_j for autentisering kommer oftest etter tidspunktet for identifisering t_i fordi man vurderer ektheten opp mot noe. Situasjonen S_j er ikke nødvendigvis helt lik S_i, der $i \neq j$.

Ved *identifisering* vurderer man om det er sannsynlig at summen av egenskaper identifiserer A. Hvis man finner at en egenskap E_i, ikke karakteriserer A, kan den fjernes og det blir de resterende kjennetegnene som karakteriserer A.

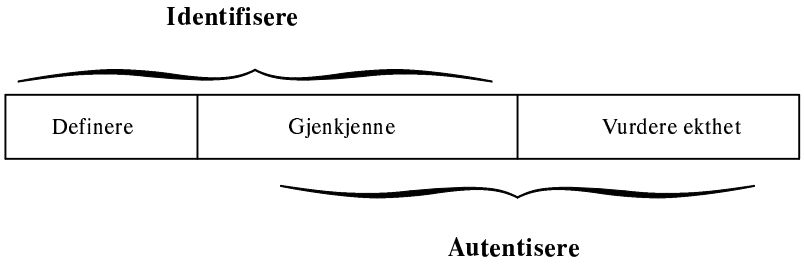
Ved *autentisering* vurderer man ektheten og beviskraften ved hver enkelt egenskap mot mer eller mindre veldefinerte kriterier for identifikasjon. Hvis én av de framsatte egenskapene ikke står til troende, kan A avvises som falsk.

På den andre siden sier man: 'Jeg identifiserer det der som min underskrift og jeg ser at dokumentet ikke er endret'. Da kjenner jeg igjen og vedkjenner meg underskriften min. Jeg kommer med en påstand om identitet. Jeg husker at jeg skrev under. Men kan jeg verifisere ektheten av underskriften? Må det vitner eller en skriftekspert til for verifiseringen? Skrifteksperten og jeg kan komme til forskjellig konklusjon. Da må de som skal akseptere underskriften og dokumentet, vurdere våre bevisføringer opp mot hverandre.

Det å gjenkjenne syns jeg er forskjellig fra å vurdere ekthet. Jeg kan gjenkjenne underskriften min på et papir. Men om den er kopiert eller ekte blir et ekstra stykke arbeid.

A.1.4 Konklusjon

Jeg tror at identifisering og autentisering brukes noe overlappende. Samtidig mener jeg at de består av to ulike funksjoner og utføres i rekkefølge. Identifisering kan skje uavhengig av autentisering, mens identifisering alltid må skje før autentisering.



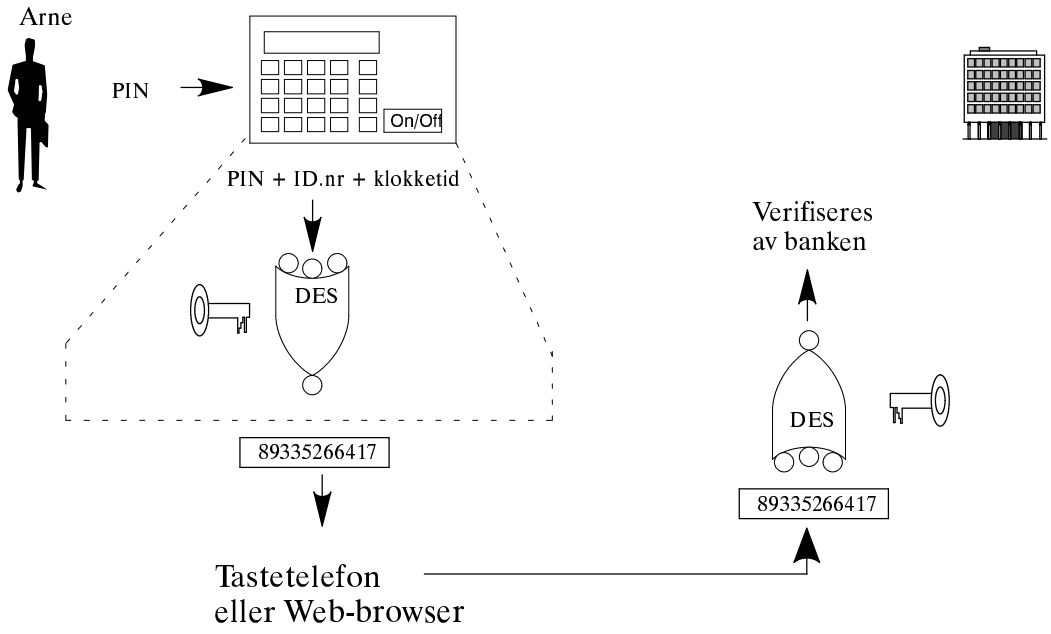
Figur 36 Aktiviteter for å identifisere og for å autentisere

A.2 Toveisautentisering av partene

Her er en autentiseringsmetode som brukes av en del banker. Det er sikrere enn vanlig passordbruk.

Autentisering med kort, symmetrisk metode

En person må autentisere seg overfor kortet han bruker. Kortet må autentisere seg overfor banken og banken kan autentisere seg overfor kortet.



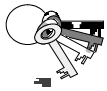
Figur 37 Autentisering ved hjelp av kort

Arne skal legitimere seg overfor banken og banken kan legitimere seg overfor Arne. Digipass ser ut som en liten kalkulator. Den har innebygd et identitetsnr., en klokke og en krypteringsalgoritme. Ved initiering av passet synkroniseres klokka med maskinklokken i banken. Maskinen beregner hvor store avvik passets klokke har til en hver tid. Arne autentiserer seg i forhold til passet ved å taste sin PIN. Den kan ligge lagret kryptert i kortet eller kortet verifiserer PIN ved en modulus 7 kontroll. Han kan deretter opprette forbindelse med bankens maskin via telefon, fax, PC e.l.. Han trenger ikke en spesiell leser til Digipass. Passet genererer et engangspassord på grunnlag av det innebygde identitetsnummeret og PIN + off-set ut fra en hemmelit algoritme. Engangspassordet oversendes banken f.eks. via en tastetelefon. Bankens maskin verifiserer at Digipass brukes av eieren. Arne kan be banken om et tilsvarende passord for å autentisere den. Det tallet Arne får, kan han taste inn i passet og få verifisert at det er den riktige banken som det kommuniseres med.

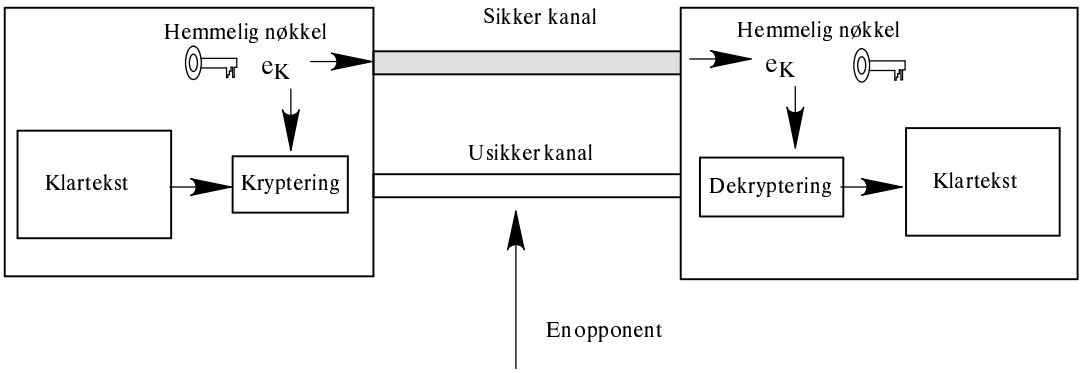
Autentiseringen bygger på bruk av engangspassord kombinert med en personlig PIN. Hvis man taster gal PIN og modulus 7 kontrollen likevel gir et riktig svar, vil banken ved sin beregning kunne se at PIN'en ikke er riktig. Engangspassordet sendes kryptert slik at ingen andre kan ha nytte av det. Et mistet Digipass kan ikke bruke av andre uten PIN. Det er fiklesikkert og ødelegger seg selv hvis noen prøver å bryte det opp.

Denne type engangspassord ser ut til å gi *ikke-benekting* av avsender. Men det eneste den sikrer er selve autentiseringen, hvis ikke det fins en utro tjener som har klart å ta i bruk nøkkelen for seg selv. Hvis det dreier seg om betaling av regninger, må hele sesjonen være on-line og den må logges for sporbarhet. Hvis betalingsinitieringen mellomlander hos en tredjepart uten tiltro, kan man ikke bevise noe.

- Banken må administrere 1 DES-nøkkel for hver bruker av Digipass



Det er verd å merke seg at det bare er passordet som sendes kryptert fra ende til ende. Resten av overføringene sendes vanligvis SSL-kryptert.



Figur 38 Sikker kanal for symmetrisk nøkkel

For at to parter skal kunne utveksle krypterte meldinger, f.eks. en DES-nøkkel eller et passord, over en usikker kanal som Internett, trenger de en sikker måte å

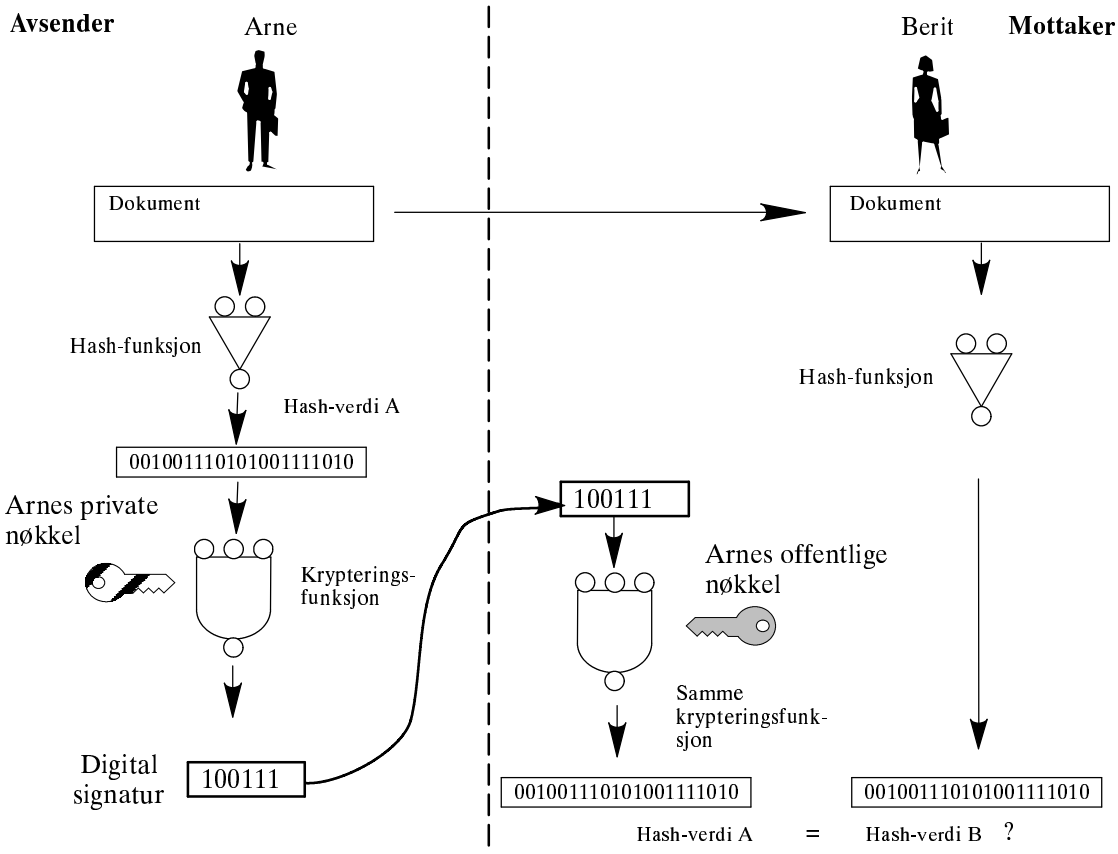
overføre den hemmelige nøkkelen. I dette tilfellet skjer det ved at betaler møter fram i banken, identifiserer seg og mottar Digipass.

A.3 Digitale signaturer

Offentlig nøkkel kryptografi ble oppfunnet i første omgang for å løse problemet med distribusjon av hemmelige nøkler [21] s. 336. Det er bassert på en asymmetrisk funksjon der hver bruker har 2 nøkler. Den ene er hemmelig, *privat*. Den andre er tilgjengelig for alle, *offentlig*. Man krypterer med den ene og dekrypterer med den andre. Den mest kjente funksjonen heter RSA etter oppfinnerne Rivest, Shamir og Adleman.

Eksempel

I steden for en sikker kanal til en hemmelig nøkkel, trenger Arne en 'autentisk kanal' til sin offentlige nøkkel. 'Kanalen' vil i dette tilfellet vanligvis være en tiltrodd tredjepart som går god for Arnes offentlige nøkkel. Det gjøres ved at TTPen utsteder et sertifikat der Arnes navn og offenlige nøkkel signeres med TTPens offentlige nøkkel. Berit henter sertifikatet et sted på nettet og verifiserer TTPen signatur. Når Berit har en autentisk offentlig nøkkel fra Arne, kan hun som mottaker av et dokument sjekke om det kommer fra Arne og sjekke om det er endret.

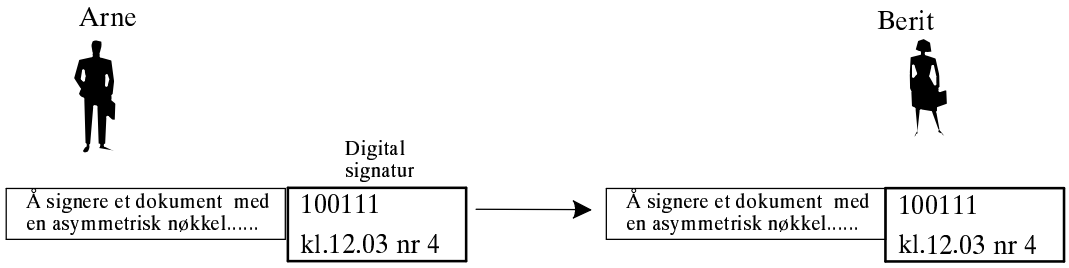


Figur 39 Digital signatur

Arne ønsker at Berit skal vite at meldingen hun får, kommer fra ham og at den ikke er endret. For å gjøre det sender Arne meldingen til Berit. I tillegg kjører han meldingen gjennom en enveis hash-funksjon hos seg. Det går relativt fort og gir et tall, en hash-verdi A, som er basert på meldingen og mye kortere enn den. Denne hash-verdien signerer han med sin private nøkkel og sender denne signaturen til Berit. Hvis Berit kan låse opp signaturen med Arnes offentlige nøkkel vet hun at signaturen kommer fra Arne. Opplåsingen gir hash-verdi A. Etterpå kan hun kjøre meldingen hun har fått gjennom den samme hash-funksjonen og få en hash-verdi B. Hvis hash-verdi A = hash-verdi B, har Berit verifisert at det er Arne har signert og sendt dokumentet og at dokumentet ikke er endret.

En **enveis hash-funksjon** er en funksjon der man ikke kan beregne startverdien ut fra resultatet. Dokument som kjøres gjennom funksjonen, blir til et tall av fast lengde. Ut fra det tallet kan man ikke gjenskape dokumentet selv om man kjenner funksjonen. Gitt en hash-verdi y, så skal det være beregningsmessig umulig å finne en annen melding x slik at f(x) = y ∀ x. Hash-funksjonen skal også være motstandsdyktig mot kollisjoner, bursdagsangrep, at to meldinger skal gi samme hash-verdi. Dvs. for hver x skal det være vanskelig å finne en x' slik at f(x) = f(x').

Det fins flere hash-algoritmer som er ISO-standarder i tillegg til de facto standarder. ISO-standardene er Information technology - Security Techniques - Hash-functions - Part 1 - 4. De har diverse opsjoner som kan kombineres. De mest kjente funksjoner er RIPMED-160, SHA-1 (160 bits, NISTs 'Secure Hash Algorithm'), [44], og MASH-1 og MASH-2 (brukes med RSA) [45]. En annen mye brukt funksjon er MD5 (128 bits, utviklet av Ron Rivest) [70]. Før brukte man hash-funksjoner med 128 bits. Nå brukes det mer og mer funksjoner som gir 160 bits resultater.



Figur 40 Digital signatur med tidsstempel

Hvis Berit trenger å vite at dokumentet er en bestemt betalingstransaksjon, som er sendt på et bestemt tidspunkt og som ikke er en kopi av en annen betalingstransaksjon, legger Arne et tidsstempel og et sekvensielt stigende nummer inn i den digitale signaturen. Signaturen hektes på transaksjonen. Berit hekter av signaturen og gjennomfører operasjonen i Figur 39.

Hvis Berit og Arne ikke kjenner hverandre (åpent system), sender Arne dokumentet til en tiltrodd tredjepart, TTP, som påfører tidsstempel, eventuelt serienummer og signerer.

Det fins to måter å beregne digitale signaturer og å gjenskape meldingen på:

1 Meldingen kan gjenskapes fra signaturen, digital signature without appendix
2 Meldingen må være et vedlegg til signaturen. digital signature with appendix.

Det fins mange standarder for digitale signaturer. Noen er basert på diskrete logaritmer [40], f.eks. DSA. Andre er basert på faktorisering [39]. RSA er et informativt appendiks til denne standarden.

B Kryptoalgoritmers styrke

Kryptomekanismer er en sterk metode for å beskytte data som sendes eller lagres på media som er utsatte for snusing eller stjeling [21]. Men de har to fundamentale begrensninger.

1 Data kan ikke beskyttes i maskinene mens de behandles. Da må de finnes i klartekst for å kunne manipuleres.
2 Mekanismene er ikke bedre enn det svakeste ledd.

Å måle styrken på kryptoalgoritmer er en upresis kunst [34]. Gollman har satt opp tre kategorier for styrke. En kryptografisk algoritme kan være

- Empirisk sikker. Ved lang tids analyse har man ikke funnet alvorlige svakeheter
- Beviselig sikker. Uttrykkes innen kompleksitetsteori. En algoritme er sikker, hvis det å knekke den er i hvertfall så vanskelig som et tilsvarende problem som regnes som matematisk vanskelig. Dette er et asymptotisk konsept som ikke sier noe om hvor hardt man må prøve.
- Ubetinget sikker. Algoritmen kan ikke knekkes selv med ubegrensede maskinressurser. One-time pad er det eneste eksempelet her, men det er nokså upraktisk i bruk.

Stinson [136] beskriver også

- Beregningsmessig sikker. “If the difficulty of an optimum attack exceeds the computational capability of the cryptoanalyst.”

“Brute Force” er metoden der man prøver alle nøklene etter tur. Jeg har også nevnt tidsavhengighet, forventet teknologiutvikling og “kvantesprang” i kapittel 5.

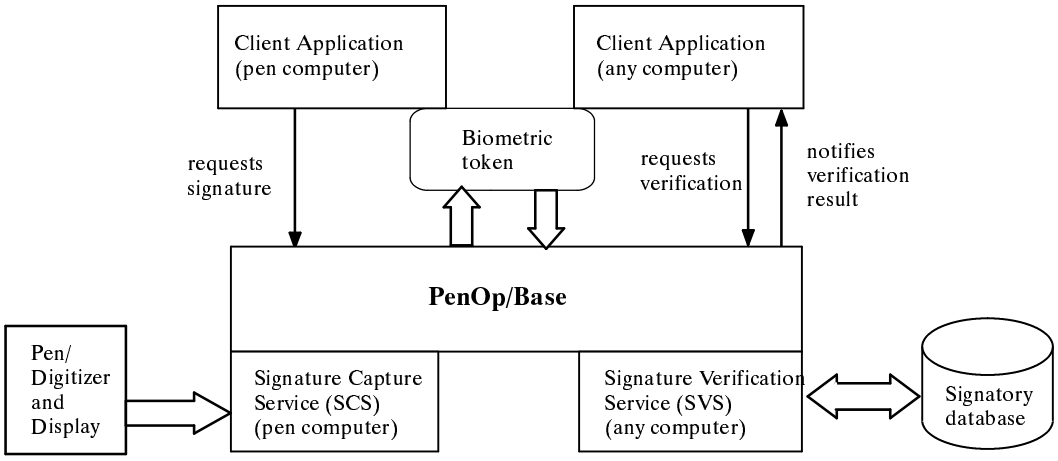
Offentlig nøkkelalgoritmer har følgende matematiske grunnlag:

- faktorisering (RSA)
- elliptisk kurve (ECC)
- diskrete algoritmer (ElGamal/DSA).

C Elektronisk signatur med PenOp

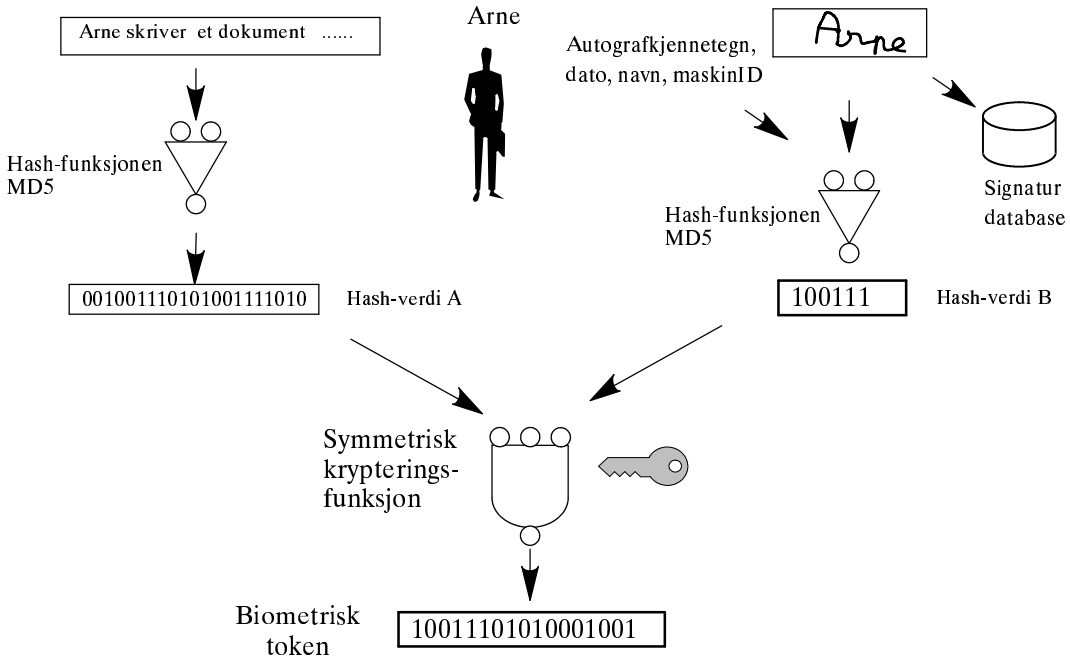
PenOp benytter biometrisk autentisering der signataren skriver navnet sitt på en pad. Maskinen registrer signaturen og krypterer den sammen med dokumentet. Løsningen er proprietær og benytter symmetrisk kryptering [106].

PenOp kan brukes i tilknytning til f.eks. Word eller PDF-dokumenter. Når signataren vil signere, kommer det spørsmål om bruker-ID eller et navn som vil vise hvem som signataren påstår seg å være. Deretter ber PenOp om selve signaturen. Den registreres sammen med informasjon som størrelse, form, løkker, linjer, prikker, hastighet osv. I tillegg ber PenOp om "Gravity Prompt" - en tekst som beskriver hvorfor dokumentet ble signert. Den skal lagres med dokumentet.



Figur 41 PenOp systemdiagram

Det er Signature Capture Service (SCS) som fanger signaturen som skrives på en pad eller en skjerm, pluss egenskapene assosiert med underskriften. Den krypterer og tillater lagring av informasjonen i en Biometric Token [146]. Signature Verification Service (SVS) kan ved verifikasjon rapportere sannsynligheten for at en bestemt signatur er autentisk.



Figur 42 Elektronisk signatur med PenOp

Her er min forståelse av hvordan signaturen genereres. PenOp har bare verifisert deler av dette. Løsningen er proprietær og delvis hemmelig. Jeg har inntrykk av at ved siden av dokumentet lagres autograf, autografkjennetegn, navn og maskin-Id i klartekst, pluss Biometrisk token som er kryptert. Signaturen og den tilhørende biometriske tokenen genereres i 4 steg:

1 H_1=MD5(M), der H1 er hashkoden fra dokument M ved bruk av hash-funksjon MD5.

2 $C_1=F_{KCA}(H_1,ID)$, der Fer en symmetrisk krypteringsalgoritme, KCA er en hemmelig nøkkel som hentes fra klient applikasjonen, ID er resten av informasjonen knyttet til underskriften og C1 er resultatet av krypteringen.

3 H_2=MD5(C_1), er den andre sjekksummen/hashkoden

4 Biometric Token = $G_X(ID, H_2)$, der G er den proprietære symmetriske algoritmen med hemmelig nøkkel X.

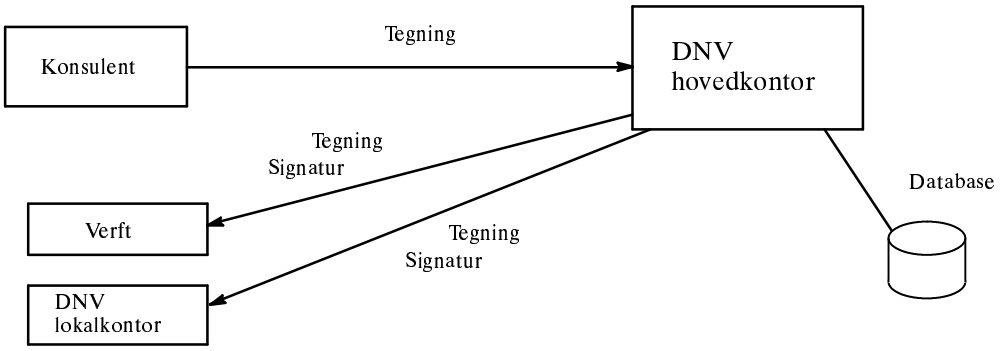
Ved verifisering dekrypteres den biometriske tokenen. Deretter:

- Hashes dokumentet for å få fram hashverdi A,
- Hashes autograf, autografkjennetegn, navn og maskinId i klartekst for å få fram hashverdi B.

PenOp kan brukes nokså likt underskrift på papirdokumenter. Signataren signerer og behøver ikke å ha PC eller huske PIN. Men signataren må gå f.eks. til etaten eller banken for å signere. Signeringen er knyttet til en bestemt PC. Signataren har ikke selv kontroll med hvor signaturene hans lagres og hvor trygt de lagres. PenOp sier de har lagt vekt på å spre risikoen for sikkerhetsbrudd, men det kan ikke verifiseres. Dersom PenOp tas i bruk på mange avgrensete områder, vil det eksistere mange databaser med de samme underskriftene. Databaseeierne vil ikke være tiltrodde tredjeparter og vil neppe kunne pålegges krav om oppetid for eksterne brukere. Denne formen for signatur vil ha samme problemer med langtidslagring som digital signerte dokumenter har, siden signaturen beregnes på grunnlag av tekstbehandlingsverktøyet dokumentet er skrevet i.

Eksempel

Det norske Veritas prøver ut PenOp på et avgrenset område [102]. De ønsker å kunne bevise for kunder hva de selv har godkjent i tilfelle det kommer til en tvist. De har ikke behov for signaturer fra sine motparter. DNV mottar skipstegninger fra konsulenter, legger på egne kommentarer og signerer med PenOp. Deretter sendes tegningene til verft der skipene bygges. Verftene har ikke PenOp, men ser en signatur på tegningen. Tegningen skrives så ut. Den lokale DNV-representanten kan, i tilfelle tvil få den verifisert ved hovedkontoret.



Figur 43 DNV og PenOp

Papirtegninger får stempler av ulike slag og de skrives ut på spesialpapir fra Veritas. Foreløpig er det ikke mulig å få stemplene med på de elektroniske tegningene. Det opplever de ansatte som et draw back i forhold til papirtegninger. Alle tegninger tas ut og lagres fysisk på papir i 30 år.

DNV har også kommunikasjon med offentlige etater. De har ikke diskutert hva de skal gjøre med det elektronisk.

D Offentlig nøkkelinfrastruktur, PKI

D.1 Tiltrodde tredjeparter

I hht. *Guidelines on the use and management of TTP services* [49] letter en tiltrodd tredjepart en trygg utveksling av informasjon samtidig som informasjonen beholder sin integritet. TTPens rolle er å øke tiltroen til at meldinger og transaksjoner overføres til den tilsiktede mottaker til rett sted og på en korrekt måte. I tilfelle tvister skal det finnes metoder for å generere bevis for hendelsesforløpet. De typer beskyttelse og graden av sikkerhet på tjenestene en TTP tilbyr, vil variere bl.a. med hvilken sammenheng applikasjonene operer i.

De viktigste tjenestene TTPer tilbyr er:

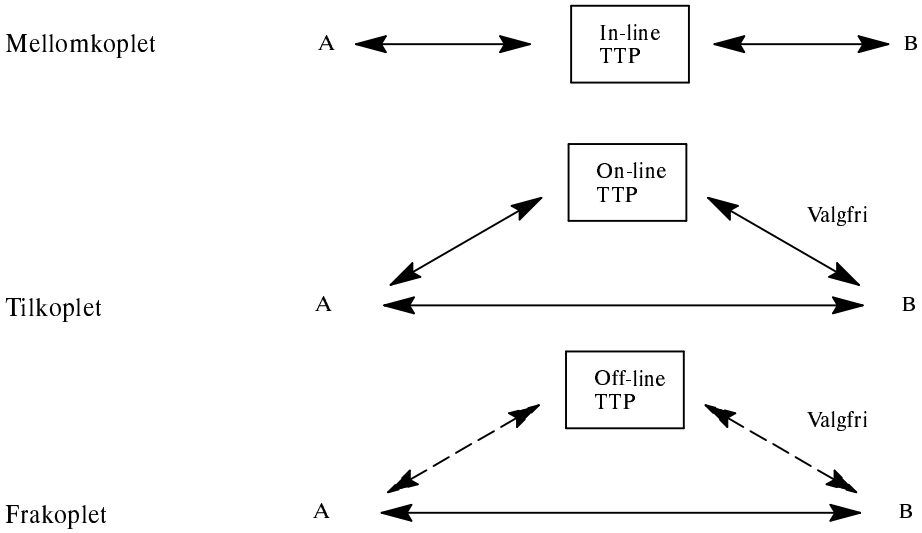
- Nøkkeladministrasjon,
- Utsteding og administrasjon av sertifikater,
- Tidsstempling,
- Innsamling av bevis for ikke-benekting,
- Elektronisk notarius publicus,
- Elektronisk arkivering.

Andre tjenester kan være:

- Katalogtjenester,
- Identifisering og autentisering,
- In-line oversettelsestjenster,
- Gjenoppretting av nøkler og data,

- Personalisering av smartkort,
- Tilgangskontroller,
- Hendelsesrapportering og alarmadministrasjon.

TTP-tjenester kan være mellomkoplet, tilkoplet eller frakoplet [148], [70]. Mellomkoplet tjeneste, in-line, virker i sanntid og all kommunikasjon går via TTPen. f.eks. autentisering hvis partene er i ulike sikkerhetsdomener, eller for tidsstempling. Tilkoplet tjeneste, on-line, brukes i sanntid der en eller begge parter er avhengige av å kunne kontakte TTPen underveis eller i hvert fall ved starten, f.eks. bruke TTP utveksling av autentiseringsmekanismer. Ved frakoplet tjeneste, off-line, deltar ikke TTPen i kommunikasjonen, men partene er avhengige av at TTPen har produsert sine bevis på forhånd.



Figur 44 TTP-tjenester: in-line, on-line og off-line

For å være effektiv bør en TTP:

- Operere sikkert,
- Operere innenfor et legalt rammeverk som er konsistent for alle deltakende parter,
- Tilby en rekke tjenester der minimumstjenestene er godt definert,
- Tilpasse seg nasjonale og internasjonale standarder der det er aktuelt,
- Følge en akseptert 'best code of practice',
- Tillate uavhengig voldgift,
- Følges av en type administrativ myndighet som overvåker at utførelsen av oppgavene er i hht. akkrediterte regler,
- Utføre tjenestene på en uavhengig og upartisk måte,
- Ha offentlig tilgjengelige regler for avslag på å utføre visse tjenester,
- Påta seg ansvar innenfor definerte grenser for tilgjengelighet og tjenestekvalitet.

Bruk av tiltrodde tredjeparter baserer seg på den fundamentale observasjonen at tjenestene bare vil bli akseptert av entiteter som har tillit til dem. Denne tilliten kan bare opprettholdes gjennom godtgjøring for at:

- Det er implementert en passende sikkerhetspolicy: en generell politikk med vanlig språk mot brukere og en politikk om tekniske aspekter,
- Sikkerhetsproblemer blir tatt hånd om ved korrekt implementerte sikkerhetsprosedyrer og -mekanismer,
- Tjenestene blir utført korrekt og i samsvar med klart definerte sett av roller og ansvar,
- Grensesnitt og prosedyrer for kommunikasjon med brukere er passende for funksjonene som skal utføres og at de blir brukt korrekt,
- Regler og forordninger er i samsvar med målene for pålitelighetsnivået og følges av ledelse og ansatte,
- Kvaliteten på prosesser, operasjoner og arbeidspraksis har blitt passende akkreditert,
- TTPen oppfyller forpliktelser som er oppført i en formell kontrakt inngått med brukerne,
- Det er en klar forståelse og aksept av det juridiske ansvaret,
- Overensstemmelse med lover og regler opprettholdes og revideres,
- Kjente trusler og vernetiltak er klart identifisert,
- Trussel- og risikoanalyse gjøres regelmessig for å sikre at krav til konfidensialitet, integritet, tilgjengelighet og pålitelighet tilfredsstilles,
- Riktig organisering og pesonaltiltak er i drift,

Oppsummeringsmessig at man kan stole på en TTPs pålitelighet og at den kan sjekkes og verifiseres.

En tjenesteyter bør vurdere følgende juridiske problemstillinger:

- Ansvar. Tilfeldige eller overlagte feil fra en TTP kan føre til stor skade for en bruker. For at brukeren skal ha tilstrekkelig tillit til å bruke tjenestene, bør ansvar mellom partene avtales formelt. Dette innebærer også avgrensing av ansvar.
- Personvern. Brukere skal kunne være forvisset om at informasjonen de gir til en TTP er fullstendig beskyttet mot innsyn hvis ikke annet er avtalt.
- Juridisk binding vha. f.eks. digitale signaturer.
- Personvernlovgivning,
- Anonymitet,
- Retten til å undersøke f.eks. akkreditiver,
- Framtidige lover og reguleringer.

En eventuell akkreditering av en TTP innebærer en godkjenning av tjenestene som tilsvarer oppgitte definisjoner, og tillit til sikkerhetsnivået. Avhengig av de tjenestene som tilbys, bør akkrediteringsprosessen inkludere gjennomgang av:

- Samsvar med relevante nasjonale og internasjonale lover og regler,
- Samsvar med tekniske standarder,
- Samsvar med sikkerhetspolitikken,
- Samsvar med veldefinerte, spesifikke profesjonelle regler,
- Samsvar med 'best code of practice',
- Om sikkerhetstiltakene er passe i forhold til trusler, risikoer og sikkerhetspolitikken.

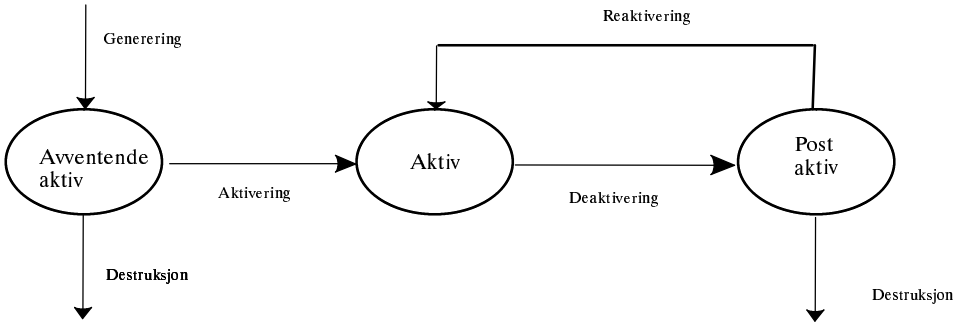
Evalueringsstandarder

Det fins flere evalueringsstandarder innenfor sikkerhet. De mest kjente er

- Orange Book [23] fra DoD, USA, behandler tiltrodde systemer.
- ITSEC fra EU, behandler både produkter og systemer.
- ISO-arbeidet Common Criteria [50], behandler både produkter og systemer.
- *Code of Practice* [15] fra BSI, UK, behandler i hovedsak organisasjoner.

D.2 Nøkkelhåndtering

I hht. ISO/IEC 11700-1 *Key management* [47] er nøkkelhåndtering administrasjonen og bruken av tjenestene generering, registrering, sertifisering, deregistrering, distribusjon, installasjon, lagring, arkivering, tilbakekalling, nøkkelavledning og destruksjon av nøkkelmateriale.



Figur 45 Generell livssyklus for kryptografiske nøkler

En TTP trenger å generere flere typer nøkler for å kunne utføre sine tjenester. Nøkler genereres og kommer i en avventende tilstand, f.eks. før personalisering av et smartkort. Noen nøkler kommer aldri i aktiv bruk og destrueres. Andre aktiveres og blir dermed gyldige for kryptografiske operasjoner. Deaktivering eller blokkering begrenser nøkkelens bruk. Det kan skje ved at feil PIN er tastet for mange ganger, nøkkelens gyldighetsperiode er utløpt eller at nøkkelen er tilbakekalt. En postaktiv nøkkel skal bare brukes for dechiffrering og verifisering. Reaktivering tillater en postaktiv nøkkel å brukes igjen. Det kan skje hvis en nøkkel har vært suspendert.

Trusler mot nøkkelhåndtering inneholder bla.:

- Avdekking av nøkkelmateriale. Det kan være i klartekst, ikke beskyttet og kan aksesseres, eller det er kryptert og kan dekrypteres,
- Modifisering av nøkkelmateriale. Endre nøkkelmateriale slik at det ikke kan brukes som intendert,
- Uautorisert fjerning av nøkkelmateriale,
- Ufullstendig destruksjon av nøkkelmateriale. Det kan føre til kompromittering av gyldige eller framtidige nøkler,
- Uautorisert tilbakekalling av nøkler,
- Maskerade. Å utgi seg for å være en autorisert bruker eller entitet,
- Forsinket utøvelse av nøkkelhåndteringsfunksjoner,
- Misbruk av nøkler,
  - Å bruke en nøkkel for en oppgave den ikke er autorisert for, f.eks. bruke en nøkkelkrypteringsnøkkel for datakryptering,

- Å bruke en nøkkelhåndteringsfunksjon for noe den ikke er autorisert til å gjøre, f.eks. uautorisert kryptering eller dekryptering av data,
- Bruke en nøkkel etter at gyldighetsperioden er utløpt,
- Overdreven bruk av en nøkkel,
- Utlevering av nøkler til en uautorisert mottaker.

D.3 Sertifikattjenester

Hensikten med sertifikater er å gi tilgang til en persons offentlige nøkkel uten at man behøver å treffe vedkommende personlig [115].

De facto standard for offentlig nøkkel sertifikater er X.509 V3, også i hht. [49]. De mest aktuelle sertifikattjenestene i forbindelse med denne oppgaven er:

- Sertifikatutsteding,
- Kryssertifisering,
- Notarius Publicus.

Sertifikatutsteding

En sertifiseringsautoritet (SA, CA - Certificate Authority) er en TTP som utsteder sertifikater der en offentlig nøkkel er knyttet til en unik identitet. Dette oppnås ved å:

- Identifisere entitetenhvis offentlige nøkkel presenteres for sertifisering,
- Forsikre seg om kvaliteten på det asymmetriske nøkkelparet som brukes til å produsere sertifikater,
- Sikre sertifiseringsprosessen og den private nøkkelen som brukes til å signere offentlig nøkkelinformasjon,
- Administrere de systemspesifikke dataene som inkluderes i den offentlige nøkkelinformasjonen, slik som sertifikatets serienr., sertifiseringsautoritetens identifikasjon osv.,
- Tilordne og sjekke gyldighetsperioder,
- Gi informasjon til den som skal ha sertifikatet at det er utstedt,
- Sikre at to ulike brukere ikke får tildelt samme identitet,
- Vedlikeholde og utstede tilbakekallingslister,
- Logge alle steg som inngår i generering av sertifikater.

Det å registrere og identifisere brukere settes ofte bort til en registreringsautoritet, RA. Men det er sertifiseringautoriteten som har det fulle ansvaret for sertifikatene.

D.4 Tidsstempling

En klient kan ønske å få sine egne data tidsstemplet, dvs. bevis for deres eksistems på et gitt tidspunkt. Han kan også ønske bevis for at han eier et dokument på et gitt tidspunkt. Det første tilfellet gjøres ved å legge til et tidsstempel til dokumentet eller dokumentets hash-verdi og signere over dette. I det andre tilfellet må tidsstemplingsautoriteten, TSA, også signere over klientens signatur.

D.5 Notarius Publicus

En notarius publicus stempler og lagrer dokumenter. En tilsvarende elektronisk tjeneste vil bestå av å føye en digital signatur med tidskode til et elektronisk dokument og lagre dette i en stor database.

E Egenskaper ved lagringsmedier

Hva er det som er viktig for å kunne lagre lengst mulig? Ved langtidslagring av digitalt signert informasjon er det av interesse å se på egenskaper ved eksterne/ frittstående lagringsmedier og dokumentformater. Dokuementformater diskuteres i kapittel 5.4.1 på side 100. Informasjon er hentet fra "To Preserve and Provide Access to Electronic Records" fra de skandinaviske nasjonalarkivene [73], "Filesystemer. Lagring og behandling av store datamengder" av Kjell Bratbergsengen [13] og "Multimedia" av Erling Maartmann-Moe [71].

Jeg ser på digital lagring, ikke nedfotografering eller scanning.

Generelle egenskaper

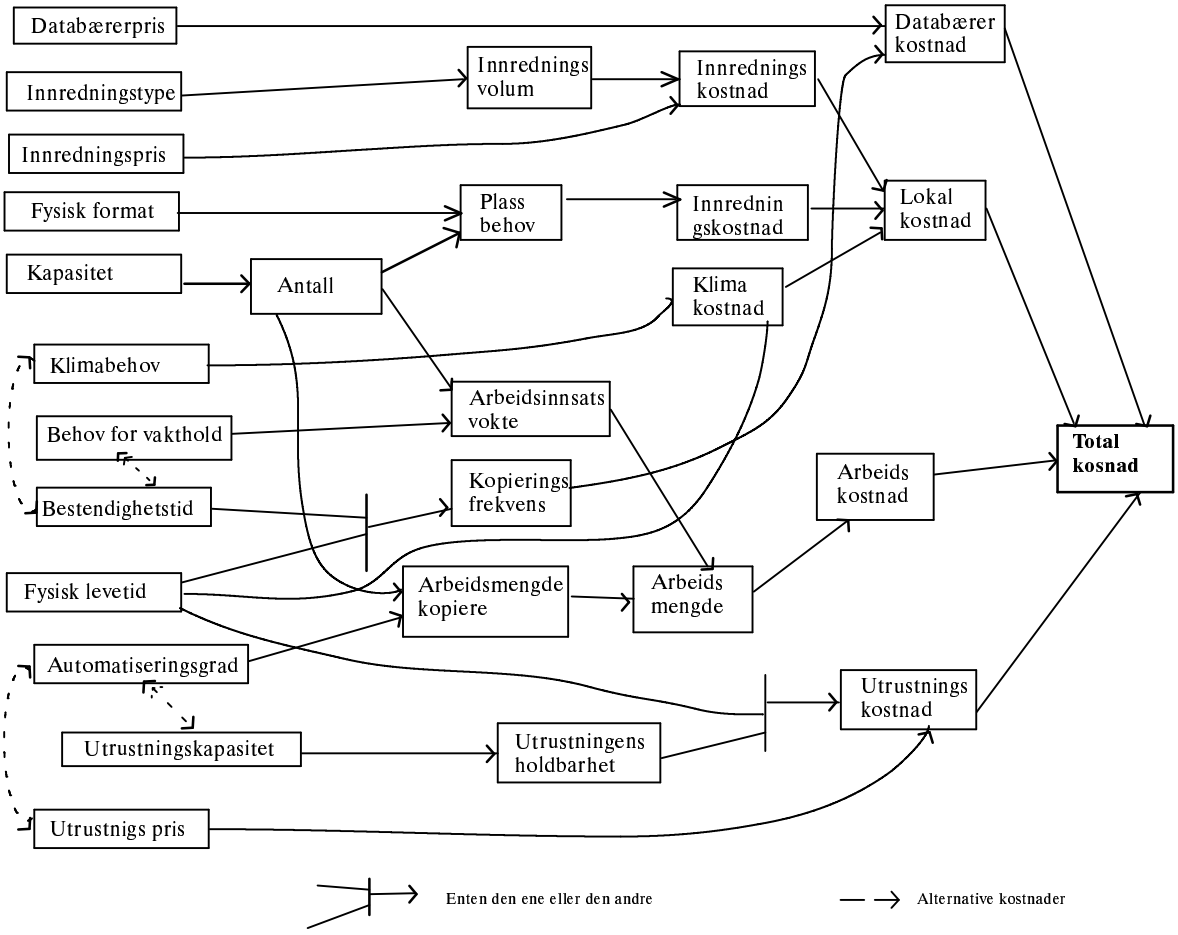
Levetiden for arkivmateriale er avhengig av periodisk kopiering og konvertering til nye datamedier. Det er mange aspekter som må vurderes opp mot hverandre og optimaliseres når arkiver skal langtidslagre elektroniske dokumenter:

- Aksesstid,
- Anskaffelsespris,
- Autentisering. Ved arkivering blir hvor sikkert dokumentene lagres og hvordan bedømming av autentisitet foregår, viktige spørsmål både fra et teknisk og et arkivsynspunkt. Det kan handle om f.eks. fysisk tilgang, om det er umulig å overskrive eller umulig å omskrive,
- Automatiseringsgrad. Automatisering av behandling av disker og taper, er dyrt. Det må veies opp mot mennesker til å hente dem fram, montere og sette på plass,
- Behov for påpassing. Hvor ofte bør man spole igjennom magnetbånd for å sjekke at de er ok og ikke har klistret seg sammen?
- Driftssikkerhet for lese- og skrivestasjoner, roboter osv., måltall. Denne hardwaren er selvfølgelig del av et større system og må kunne fungere sammen med den. Den må kunne håndtere ulike typer lagringsmedier og lagringsformater,
- Energiforbruk,
- Fysisk medium,
- Klima og miljøbehov. Riktig klima kan være en kostnadsfaktor. De ideelle oppbevaringsbetingelsene for magnetbånd er 18 grader C $\pm$ 2 grader og 40% $\pm$ 5% relativ luftfuktighet. Nyere medier har større slingringsmonn,
- Lagringskapasitet. Kapasitet måles i MB, GB og TB. Den øker hvis dataene komprimeres. Det gjøres til en viss grad på magnetbånd, men ikke på optiske disker,

- Lagringstetthet. Lagringstettet måles i MB/liter,
- Lagringsteknikk,
- Levetid,
  - Fysisk levetid: den tid som et fysisk medium kan brukes for lagring av informasjon uten at ulike medbrytningsmekanismer forårsaket at noen del av informasjonen har blitt ødelagt,
  - Teknisk levetid: den tid som et datamedium eller programvare for et logisk format fins på markedet i en slik mengde at anvendelsen kan garanteres uten vesentlige merkostnader eller økt innsats fra brukernes side,
- Logisk format. Format for strukturering av data, så som format for dataorganisering og representasjon,
- Lokaler og innredningskostnader,
- Markedsandel. De forventede framtidige markedsandelene for ulike datamedier har betydning for den tekniske livslengden. Markedsandeler måles i antall solgte eksemplarer,
- Spredning blant offentlige etater. Hva slags medier riksarkiver skal velge, avhenger av hva slags utrustning offentlige etater har. Det viser seg å variere en hel del,
- Pris pr. MB,
- Miljøvernaspekter,
- Overføringskapasitet,
- Overføringshastighet. Overføringshastighet er den tiden det tar å overføre data mellom lagringsmedium og lese-/skrivestasjon. Ved generasjons-kopiering av store datamengder er overføringshastigheten avgjørende,
- Standarder. Når ny teknikk introduseres uten at det fins etablerte standarder, dukker det opp en mengde innbyrdes inkompatible produkter. Først når det fins eller utvikles offisielle og aksepterte standarder, øker den nye teknikken,

Viktige egenskaper ved langtidslagring er bla.:

- At mediene lever lenge, lang tid før feil oppstår,
- At man kan skrive én gang og lese mange ganger,
- At man ikke trenger spesialmekanismer for lesing,
- At lagringen skjer vanligvis off-line. Altså trenger man mekanismer til å finne riktig enhet og til å hente den effektivt.



Figur 46 Kostnadssammenhenger ved langtidslagring

Valget av lagringsmedier avhenger av mange faktorer [73] slik denne tegningen fra de nordiske statsarkivene illustrerer. Kvalitet holdes opp mot pris.

F Trusler og sårbarhet

F.1 Definisjoner

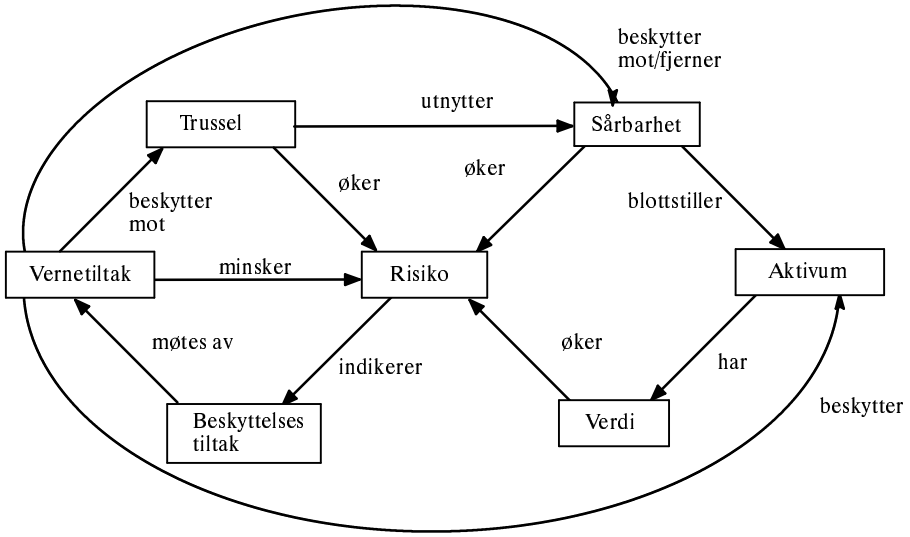
Innenfor datasikkerhetsfaget er følgende begreper mye brukt:

Aktiva assets, en organisasjons verdifulle ressurser som det vil være ubeleilig eller besværlig, hvis ble kompromittert, ødelagt eller tilgjengelig for ikke-autoriserte personer eller systemer.

Trusler en potensiell skade som vedrører aktivas konfidensialitet, integritet eller tilgjenglighet. Trusler kan eksistere pga. at uopplært personell gjør noe galt eller ved villet skade.

Sårbarhet en svakhet i sikkerhetsprosedyrer eller kontroller som åpner for at trusler kan skade en eller flere aktiva.

Risiko mulighet for tap. Defineres ofte som P(skade) * skadevirkning.



Figur 47 Trusler og sårbarhet

F.2 Egenskaper ved sikrede data

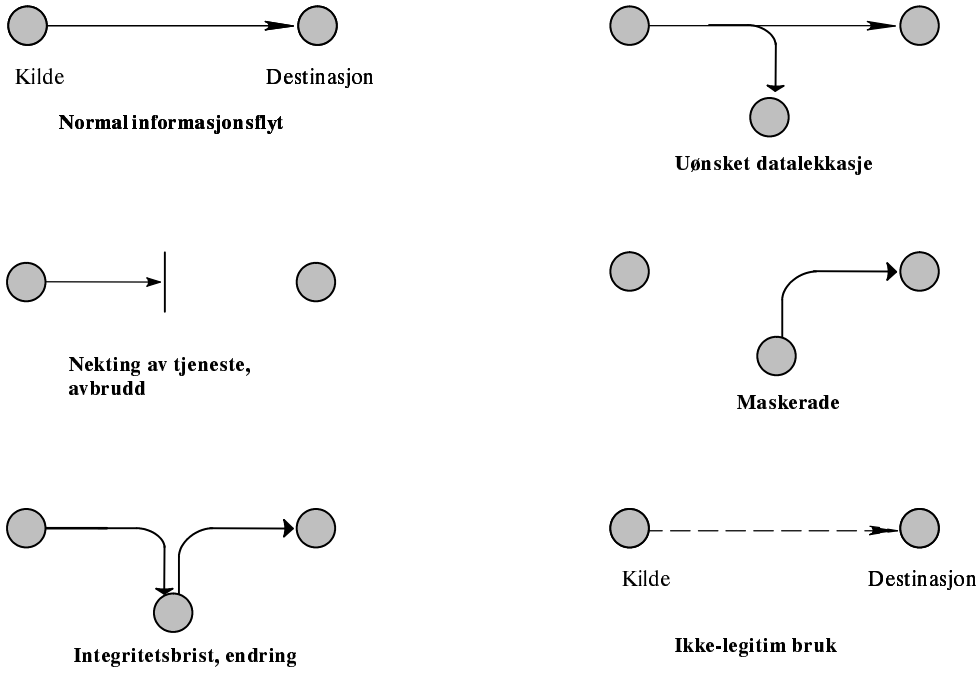
Tønnes Brekne [14] regner data som sikrede hvis og bare hvis:

1 De er tilgjengelige,
2 Deres tilgjengelighet er begrenset til de som har tillatelse fra eier (konfidensialitet),
3 Det er bare opprettet, endret, eller slettet av autoriserte subjekter (integritet),
4 Deres autentisitet (korrekt opphav) er bevart,
5 De bare kan brukes under vilkårene bestemt av eier (legitim bruk) eller den lovmyndighet eier er underlagt,
6 De er ajour/tidsmessige, og
7 De er korrekte (har mer med kvaliteten på innmatede data å gjøre).

F.3 Grunnleggende trusseltyper

En trusseltype beskriver essensen i det som skjer når en trussel realiseres i form av et uhell eller et angrep. De grunnleggende trusseltypene er

1 Uønsket datalekkasje i strid med sikkerhetspolicien eller rettmessig eiers vilje. F.eks. usikre elektroniske postsystemer som gir inntrengere privilegerte lese-rettigheter.
2 Nekting av tjeneste. En hendelse eller tilstand der bruker ikke har adgang til de ressurser brukeren er autorisert til å bruke, f.eks. bortfall av en kommunikasjonsforbindelse.
3 Maskerade. En vellykket identitetsforfalskning.
4 Ikke-legitim bruk.
5 Integritetsbrist. En hendelse der data slettes, endres, eller opprettes uten autorisasjon.



Figur 48 Sikkerhetstrusler

I Norge er det aldersgruppen fra 30 år og oppover som forøver de fleste forholdene [77]. Hele 61 % av organisasjoner tilknyttet finansbransjen som deltok i undersøkelsen, var utsatt for datakriminalitet. I 1989 hadde man statistisk grunnlag for å hevde at dersom det blir begått datakriminalitet, var sannsynligheten mer enn 50 % for at det var interne angripere. I 1997-undersøkelsen tilhørte 49 % av forøverne gruppen "utenfra virksomheten", 33 % tilhørte gruppen ansatte og 18 % var ukjent. Undersøkelsen har ikke noe om samarbeid mellom ansatte og folk utenfor virksomheten.

Mørketallsundersøkelsen [77] referer til en ikke offentliggjort rapport fra Ernst & Young 1997 der hendelser som rapporteres, er forårsaket av følgende:

Tabell 5 Rapporterte hendelser

Prosent	**Hendelse**
45 %	Utilgjengelig telekommunikasjon
43 %	Uaktsomme feil
42 %	Virus (ikke makro)
34 %	Makro virus
25 %	Planlagte ødeleggende handlinger av ansatte
23 %	Planlagte ødeleggende handlinger av utenforstående
22 %	Naturkatastrofer
19 %	Industrispionasje

F.4 Innenfor gjerdet

Dorothy Denning [21] har definert fire risikogrupper som det kan være verd å angripe: spionasje mot stat og militære, økonomisk spionasje, spionasje mot bedrifter og kompromittering av personinformasjon.

For å oppnå tilgang til en organisasjon, kan personer med teknisk bakgrunn tilby sine tjenester til forskningsområder, universiteter eller til leverandører av forsvarsprodukter.

Ansatte kan noen ganger lokkes til å gi bort stats- eller forretningshemmeligheter for kjærlighet eller samvær. Det fins tilfeller av ansatte som tar med seg forretningshemmeligheter, når de begynner å arbeide for konkurrenten. Noen ganger tar ansatte med seg informasjon for å finne en som er villig til å betale for den. F.eks. kan et firma være interessert i å vite hvordan lederne i en etat vurderer en sak før de sender inn en søknad. Ansatte kan kompromittere personalinformasjon.

I forbindelse med joint ventures må firmaer ofte avgi bedriftshemmeligheter til samarbeidspartneren. Det kan de seinere angre på hvis samarbeidspartneren bruker informasjonen til eget beste.

'Social engineering' er kjente angrep overfor ansatte. Det kan være vanskelig å forstå hensikten med en del spørsmål i en vennlig atmosfære. Det kan være lett å avdekke intern informasjon uten å ville det.

Det fins mange eksempler på utro tjenere som forfalsker betalingstransaksjoner. I den største skattesvindelsaken i New York mottok ansatte bestikkelser for å fjerne krav om $ 13 millioner skatt fra skattesystemet. Byen tapte $ 7 millioner i renteinntekter.

Ansatte har sabotert fysisk utstyr og endret programvare for å hindre tilgang til informasjon og tjenester.

Sikkerhetshindre

I hht. Dorothy Denning [21] kan man finne informasjonens verdi ved å se på tre kostnadsområder:

- Kostnader ved å måtte erstatte tapt informasjon.
- Kostnader ved at informasjon ikke er tilgjengelig.
- Kostnader ved at informasjon offentliggjøres ved konfidensialitetsbrudd, dvs. at ansatte går ut over sine fullmakter eller handler uomtenksomt.

Denning refererer en undersøkelse fra 1997 om de viktigste hindringene for å holde på et adekvat sikkerhetsnivå. Svarene hadde følgende fordeling:

Tabell 6 Hva hindrer riktig sikkerhetsnivå?

Prosent	Type hindring
62 %	Budsjettbegrensninger
56 %	Opplæring av ansatte

Prosent	Type hindring
55 %	Manglende forståelse hos sluttbrukerne
40 %	Teknisk kompleksitet
39 %	Uklar ansvarsfordeling
39 %	Manglende forståelse hos ledelsen
37 %	Manglende støtte fra ledelsen
35 %	Mangel på gode sikkerhetsverktøy
31 %	Sikkerhetssvakheter ved produktene som er i bruk
30 %	Manglende intern sikkerhetspolicy og standarder
26 %	Manglende sentral autoritet
24 %	Mangel på kompetent sikkerhetspersonell
19 %	Manglende industristandarder
15 %	Personvern og etiske problemstillinger
12 %	Juridiske, lovmessige eller reguleringsproblemer
5 %	Annet

F.5 Trusler ved lagring av data

Brekne [14] tar opp spesielle trusler ved langtidslagring.

Manglende eller utilstrekkelige reservekopier

Hvis deler av eller hele systemets lagringsmedia svikter, og det ikke finnes tilstrekkelig med reservekopier, vil det oppstå nekting av tjeneste. Det kan også oppstå integritetsbrist, dersom systemets egne sikkerhetsdata ikke kan fullt rekonstrueres fra reservekopier slik at inkonsistenser og sikkerhetshull kan dukke opp.

Utilstrekkelig tilgangskontroll for lagrede objekter

Tilgangskontroll kan dreie seg om både den fysisk tilgangskontrollen til stedet der lagringsmediene geografisk befinner seg, og om den logiske tilgangskontrollen som bestemmer hvilke brukere som får manipulere hvilke objekter. Eksempel på utilstrekkelig fysisk tilgangskontroll er uautoriserte personer som blir med autoriserte personer gjennom en sluse.

Upålitelig lagringsmedium

Dette kan føre til nekting av tjeneste fordi upåliteligheten fører til at noen lagrings-/leseoperasjoner ikke kan gjennomføres. Det kan gi opphav til integritetsbrist fordi lagrede data ofte korrumperes, eller ikke lar seg avlese riktig.

Miljøfaktorer

I tillegg til spenningsvariasjoner og elektromagnetiske feltpåvirkninger, er det en del trusler som skyldes miljøfaktorer eller ekstremer av miljøfaktorer. Brann,

vannskader, naturkatastrofer, temperatur, luftfuktighet, partikkelinnhold i luften, gasser i luften og liknende kan utgjøre trusler mot lagringsmediet. Én risiko er nekting av tjeneste fordi mediet skades eller ødelegges fullstendig. En annen er integritetsbrist fordi miljøfaktoren korrumperer dataene lagret på eller i lagringsmediet.

Manglende bevis for lagringsmediets plassering

Hvis det ikke er mulig å bevise eller i akseptabel grad sannsynliggjøre plasseringen logisk eller geografisk til et lagringsmedium, blir det ikke mulig å avgjøre hvorvidt mediet faktisk befinner seg i lagringsområdet. Det blir ikke mulig for systemet å håndheve tilgangspolitikken korrekt uten at det på én eller annen måte vet hvor mediet befinner seg.

Manglende bevis for lagringmediets integritet

Det er ikke mulig å vite hvorvidt integriteten til data lagret på et lagringmedium er ivaretatt eller ikke uten en form for kontrollmekanisme. Dette er det svært få operativsystemer som har. Det må ikke være mulig for en angriper å endre, slette eller opprette data uten at det innfører en inkonsistens som kan oppdages ved rutinekontroll.

Manglende bevis for lagringsmediets identitet

Hvis det ikke er mulig å bevise eller i akseptabel grad sannsynliggjøre lagrings-mediet identitet, blir maskerade og integritetsbrist mulig. Maskerade skjer ved at to lagringsmedier med samme logiske (eventuelt fysiske) navn, men med forskjellig innhold byttes. Uten bevis eller sannsynliggjøring klarer ikke systemet å se forskjell på de to. Samtidig har det skjedd en integritetsbrist fordi objekter er endret, slettet eller opprettet uten autorisasjon. F.eks. kan en harddisk byttes med en annen.

Mangel på bevis for tidsangivelse

Gyldigheten av en melding signert ved hjelp av data fra et sertifikat, avhenger av gyldigheten av dataene i sertifikatet på signeringstidspunktet.

F.6 Aktuelle straffebestemmelser

Datakriminalitet

"..kriminalitet der utnyttelsen av datateknologi har vært vesentlig for overtredelsen." (Straffelovrådet NOU 1985:31)

Datarelatert kriminalitet

Alle former for kriminalitet der bevis kan være lagret elektronisk. Alt fra narko-tikaomsetning til distribusjon av barnepornografi....

Inntrenging/avlytting

Straffelovens § 145, 2. ledd:

- Avlytting av dataanlegg/-system

- Inntrenging i dataanlegg/-system
  - Typisk hacking eller datasnoking
  - Der noen har brutt en beskyttelse for å skaffe seg adgang til data
  - Det skal være krav til beskyttelse

Databedrageri

Straffelovens § 270 nr. 2: når noen "Rettsstridig påvirker resultatet av en automatisk databehandling". Handlingen må volde tap eller fare for tap.
§ 174: Pengefalsk

Forretningshemmelighet

Straffelovens § 294: (indistrispionasje)	Misbruk av datalagret forretningshemmelighet
Straffelovens § 405 a:	Innsyn i datalagret forretningshemmelighet.

Heleri

Straffelovens § 317:	Heleri av datainformasjon

Skadeverk

Straffelovens § 151 b	har reaksjon mot å ødelegge samfunnsviktig informasjons-samling.
§ 291	Skadeverk på datalagringsmedier (ødeleggelse av data)
§ 292	Grovt skadeverk på datalagringsmedier
§ 391, 3. ledd	Uaktsomt grovt skadeverk på datalagringsmedier

Misbruk av andres datamaskiner

§§ 261 og 393 har om ulovlig bruk av løsøregjenstand, rettsstridig forføyning av datasystem mv.

Piratkopiering

Åndsverkloven § 2 ev. § 12 eller §19 har om ulovlig kopiering og ulovlig spredning av programvare.

Personlig krenkelse

Straffelovens § 135 a	Diskriminiering via datasystemer
§§ 246, 247	Ærekrenkelse via datasystemer.

G Institusjoner og personer jeg har kontaktet for informasjon

Tusen takk for tid, tanker og engasjement!

American Bar Association

Avdeling for forvaltningsinformatikk (AFIN), UiO: Dag Wiese Schartum

British Telecom: Mike Kenning

Brønnøysundregistrene: Kari Bjørkhaug

Bundesamt für Sicherheit ind der Informationstechnik: Klaus Keus

Cambridge University, UK: Ross Anderson

Department of Computer Science and Engineering, Helsinki University of Technology: Kiril Kesarev

Det juridiske fakultet, København: Mads Bryde Andersen

Det norske Veritas: Bo Johanson, Mikkel Skou

EU

Finansdepartementet: Johanne Slinning

Forsvarets overkommando/ Sikkerhetsstaben: Kjell Bergan

Government of Canada Public Key Infrastructure

iD2 Tehcnologies: Hans Nilsson

Institutt for informatikk, UiO: Tone Brattetidg, Ragnar Norman

Institutt for nordistikk og lingvistikk, UiO: Tor Guttu

Institutt for rettsinformatikk, UiO: Rolf Riisnæs, Jon Bing

Interdisciplinary Centre for Law and Information Technology, ICRI, Det juridiske fakultet, Leuven, Belgia: Gavan Gravensen, Patrik Van Eecke

ISTEV, Istituto per lo Studio della Vulnerabilità delle Società Tecnologicamente Evolute, Italia.

IT-sikkerhetsrådet, Danmark

Justervesenet: Leif Halbo

Justisdepartementet: Karin Fløistad, Tove M. Voldbæk

KITH: Torbjørn Nystadnes

Kommunal- og regionaldepartementet: Arne Økstad, Odd Grønvold

Kreditkassen: Audun Ekeberg

Logica: Deborah Moir

Løsøreregisteret: Kari Bjørkhaug

National Information Systems Security Conference, 1998 og 1999: Charles Pfleeger, ARCA, Mark Pollit, FBI

Nordisk Ministerråd

Norges Bank: Svein Solheim, Turid Wammer

Norges forskningsråd: Torstein Pedersen

Norsk Regnesentral: Guri Verne, Jon Ølnes, Anund Lie

Norsk Teknologistandardisering: Knut Lindelien, Ulf Leirstein

NTNU: Svein Knapskog, Kjell Bratbergsengen

Næringslivets sikkerhetsorganisasjon: Petter Christensen

Nærings- og handelsdepartementet: Amund Eriksen, Jens Nørve

OECD

PenOp: Ben Wright, Christopher Smithies

Posten SDS: Sven Christiansen, Terje Kolnes, Egil Årrestad

Riksarkivaren: Trond Sirevåg, Ivar Fonnes

Rikstrygdeverket: Svein Burkeland

Royal Holloway, University of London: Chris Mitchell

Secured Electronic Information in Society, SEIS, Sverige

SINTEF Tele & Data: Jan-Erik Kosberg

Skattedirektoratet: Randi Eng, Jostein Vindspoll, Kristin Vestmo

Statens arkiver, Danmark

Statistisk Sentralbyrå: Hanne Modahl

Statoil: Arve Tjåland

Statskonsult: Maria Strøm

Thomson-CSF: Leif Nilsen

USIT: Tone Sandahl

Verdipapirsentralen: Tom Kolberg

Verisign: Warwick Ford

Referanseliste

[1] Almnes, Thomas et al.: *Innføring av elektronisk pasientjournal på Lungeavdelingen, Rikshospitalet, våren 1998*. Studentrapport In364, 11. mai 1998, Institutt for informatikk, Universitetet i Oslo

[2] American Bar Association: *Digital Signature Guidelines*. Legal Infrastructure for Certification Authorities and Secure Electronic Commerce. August 1, 1996. ISBN 1-57073-250-7

[3] Anderson, Ross J.: *Why Cryptosystems fail*. Computer Laboratory, Proceedings of 1993 ACM Conference on Cryptology and Computer Security pp 215--227.

[4] Anderson, Ross, and Kuhn, Markus: *Tamper Resistance - a Cautionary Note*. The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, November 18-21, 1996, pp 1-11, ISBN 1-880446-83-99. http://www.cl.cam.ac.uk/users/rja14/#Reliability [sett 12.4.99]

[5] Arkivforskriften: *Forskrift om offentlege arkiv.* 1998-12-11 nr. 1193

[6] Arkivloven: *Lov av 4. desember 1992 nr 126 om arkiv,* http://www.lovdata.no/all/tl-19921204-126-004.html [sett 30.11.98]

[7] Arkivloven, høringsutkast: *Utkast til forskrift om offentlege arkiv, med heimel i lov av 4. desember 1992 nr 126 om arkiv - høyring*, http://www.dep.no/kd/hoering/arkiv [sett 30.11.98]

[8] Baum-Waidner, Birgit: *SEIS-SAT-project, Qualified Certificates and their Relation to Certificates in Standards and Profiles*. Entrust Technologies Europe, August 30, 1999. SEIS Interfaces.

[9] Berg, Marc: *Medical work and the Computer-Based Patient Record: A sociological Perspective,* i Blandingskompendium Artikkelsamling del 2, In364 systemutvikling teori og modeller, våren 1998.

[10] Bjerke, Lucie og Søraas, Haakon: *Engelsk-norsk ordbok*, Aschehoug 1963

[11] Boehm, Barry W.: *Verifying and Validating Software Requirements and Design Specifications*. IEEE Software, January 1984, pp 75-88

[12] *Bokmålsordboka*. Universitetsforlaget 1990, ISBN 82-00-07667-9

[13] Bratbergsengen, Kjell: *Filsystemer. Lagring og behandling av store datamengder*, Foreløpig utgave høsten 1996, Institutt for datateknikk, NTNU.

[14] Brekne, Tønnes: *Sikkerhet i distribuerte systemer*. Unik 27. januar 1999.

[15] British Standards Institute: *BS Draft 7799. Information Security management - Part 1: Code of Practice for Information Security Management.* 1998-09-07.

[16] Brown, John Seely og Duguid, Paul: *Borderline Issues: Social and Material Aspects of Design*. I Human-Computer Interaction, Volume 9, 1994, pp. 3-36

[17] Bråten, Stein: *Asymmetrisk samtale og selvstendig syn: Opphevelse av modellmonopol* i "Dialogens vilkår i datasamfunnet", Universitetsforlaget 1983 ss. 165 - 183.

[18] Bundesministerium für Wirtschaft und Technologie: *Article 3 Digital Signature Act - (Signaturgesetz - SigG).* http://www.iid.de/iukdg/

[19] *Computing and communications in the Extreme. Research for Crisis management and Other Applications*. National Academy Press 1996. ISBN 0-309-05540-7.

[20] *Dansk Fremmedordbok*, Munksgaard 1998

[21] Denning, Dorothy E.: *Information Warfare and Security*. Addison Wesley 1999. ISBN 0-201-43303-6

[22] Denning, Dorothy E. and Denning, Peter J.: *Internet Besieged*. Addison Wesley 1998. ISBN 0-201-30820-7

[23] Department of Defense Standard: *Department of Defense Trusted Computer System Evaluation Criteria (The Orange Book)*. DoD 5200.28-STD. Dec. 1985.

[24] DLM-Forum: *Guidelines on best practices for using electronic information*. Office for official Publications of the European communities, 1997. ISBN 92-828-2285-0. http://europa.eu.int

[25] Dumortier, Jos and Van Eecke, Patrik: *The Legal Aspects of Digital Signatures. Part III: The digital signature as alternative for the hand-written signature.* ICRI, Interdisciplinary Centre for Law and Information Technology, 1999 Faculty of Law, University of Leuven

[26] EU: *Proposal for a European parliament and Council Directive on a common framework for electronic signature*s. COM(1998)297final, 13.05.98. http://www.law.kuleuven.ac.be/icri/ [sett 27.10.98]

[27] EU: *Rammenotat. Forslag fra Kommisjonen, COM(1998) 297 Final, til Europaparlamentets og Rådets direktiv om et felle rammeverk for elektroniske signaturer*. Utkast 4.08.99 tam/jno

[28] Fillingham, David: *A Comparison of Digital and Handwritten Signatures*. Paper for MIT 6.805/STS085: Ethics and Law on the Electronic Frontier, Fall 1997, http://www.dnd.no/ostlandet/eldoc/index.htm [sett 12.4.99]

[29] Ford,Warwick & Baum, Michael S. : *Secure Electronic Commerce*, Prentice Hall 1997, ISBN 0-13-476342-4.

[30] *FSP-1, Forvaltningens Sertifikatpolicy - 1*. High assurance X.509 certificate for the Norwegian public sector. The Royal Norwegian Ministry of labour and Government Administration (AAD). Ver. 1.0. august 1999.

[31] Galtung, Andreas og Riisnæs, Rolf: *Rettslige aspekter ved digitale signaturer*, Universitetet i Oslo, Mars 1994

[32] Gasser, Les: *The Integration of Computing and Routine Work* i ACM Transactions on Office Information, nr. 4 (3) 1986 ss. 205-225. ISBN: ISSN 0734-2047.

[33] Gilb, Tom: *Principles of Software Engingeering Management*. Addison-Wesley 1988. ISBN 0-201-19576-2.

[34] Gollmann, Dieter: *Computer Security*. Wiley 1999. ISBN 0-471-97844-2

[35] *Gyldendals fremmedordbok*. 1969

[36] Henriksen, Roger: *Signature and Evidence in the International Trade and Transport Society without Documents.* Januar 1980. UN ECE dok. TRADE/WP.4/R.98. CompLex no. 10/83

[37] Holst, Per A.: *Datasikring - Metoder og Prinsipper*. Per A. Holst Forlag 1995. ISBN 82-996820-9-0.

[38] ISO/IEC 9594-8: Information technology - Open Systems Interconnections - *The Directory: Authentication Framework*. 1993.

[39] ISO/IEC SC27.2 CD 9796-2 Information technology - Security Techniques - *Digital signature scheme giving message recovery - Part 2: Mechanisms using a hash-function* 1997-09-01

[40] ISO/IEC SC27.2 CD 9796-4 Information technology - Security Techniques - *Digital signature scheme giving message recovery - Part 4: Discrete logarithm based mechanisms* 1997-02-07

[41] ISO/IEC FDIS 9797-1: Information technology - Security techniques - *Message authentication codes (MACs) - Part 1: Mechanisms using a block cipher.* (Revision of IS 9797: 1994). 1998-11-13

[42] ISO/IEC CD 9797-2: Information technology - Security techniques - *Message authentication codes (MACs) - : Part 1: Mechanisms using a hash-function*. (Revision of IS 9797: 1994). 1999-2-26

[43] ISO/IEC DIS 9798-1: Information technology - Security techniques - *Entity authentcation: Part 1: General*. 1996

[44] ISO/IEC SC27 IS 10118-3 Information technology - Security Techniques - Hash-functions - *Part 3: Dedicated Hash-functions using an n-bit block cipher algorithm*. 1997-12-22

[45] ISO/IEC SC27.2 IS 10118-4 Information technology - Security Techniques - *Hash-functions - Part 4: Hash-functions using modular arithmetic*. 1998-07-01

[46] ISO/IEC DIS 10181-4.2: Information technology - Open Systems Interconnections - *Security frameworks in Open Systems - Part 4: Non-repudiation*. 1995-04-20

[47] ISO/IEC DIS 11770-1.2: Information technology - Security techniques - *Key management - Part 1: Framework*. 1996-11-11

[48] ISO/IEC FDIS 13888-3: Information technology - Security techniques - *Non-repudiation - Part 3: Using asymmetric techniques*. 1997-07-29.

[49] ISO/IEC PDTR 14516: Information technology - Security techniques - *Guidelines on the use and management of TTP services*. February 26, 1999.

[50] ISO/IEC FDIS 15408: *Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model*. May 1998, Versjon 2.0. CCIB-98-026.

[51] ISO/IEC SC27 WD 15443 Information technology - Security Techniques - *A framework for IT security assurance*. Draft 5.0 N2334, 1999-09-15.

[52] ISTEV: *Legal Issues of Evidence and Liability in the Provision of Trusted Services (CA and TTP services)* Final Report, October 1998, Istituto per lo Studio della Vulnerabilità delle Società Tecnologicamente Evolute. ftp://ftp.cordis.lu/pub/infosec/docs/legal-final-report.doc [sett 2.11.99]

[53] IT-Sikkerhetsrådet: *Digitale dokumenters bevisværdi - Introduksjon og vejledning med bilag.* Købehavn, Desember 1998. http://www.fsk.dk/fsk/div/itsikraad/ ISBN (Internet): 87-90777-69-0.

[54] Jervell, Herman Ruge og Olsen, Kai A.: *Hva datamaskiner ikke kan*. Universitetsforlaget 1984. ISBN 82-00-07140-5

[55] Jueneman, Robert R., & Robertson Jr., R.J.: *Biometrics and Digital Signatures in Electronic Commerce*. http://www.siu.edu/~lawsch/faculty/robertso/biblio.htm

[56] Justis- og politidepartementet: *Adgangen til å treffe avtaler elektronisk og beviskraften av elektroniske dokumenter.* Brev til NHD 5.5.1999, ref. 99/00663 E KHR/Kf/bj.

[57] Justis- og politidepartementet: *Kartlegging av bestemmelser i lover, forskrifter og instrukser som ikke legger til rette for elektronisk kommunikasjon*. 15.3.1999. http://www.dep.no/je/publ/1999/kartl.html [sett 8.9.99]

[58] Jøsang, Audun og Knapskog, Svein J.: *A Metric for Trusted Systems*. 21st National Information Systems Security Conference, October 5-8, 1998.

[59] Karstoft, Susanne: *Elektronisk dokumentudveksling - retlige aspekter.* Jurist- og Økonomforbundets Forlag 1994. ISBN 87-574-7220-3.

[60] Kent, Peter: *PGP Companion for Windows*. Ventana Press 1995. ISBN 1-56604-304-2.

[61] Kesarev, Kiril: *Digital Signatures And Encryption in The European Union*. Tik-109.300 Telekommunications Architechtures, 22 November 1998, Department of Computer Science and Engineering, Helsinki University of Technology. http://www.tcm.hut.fi/Stidoes/Tik-110.300/1998/Essays/crypto_eu.html

[62] KITH: *Elektronisk pasientjournal (EPJ) standardisering. Trinn 1: En fullgod erstatning for papirbaserte journaler. Prosjektplan.* 11.3.99. http://www.kith.no/epj [sett 12.10.99].

[63] KITH: *Elektronisk pasientjournal (EPJ) standardisering. Del 1: Enkel arkivstandard. Versjon 0.3. Høringsutkast*. 1999. http://www.kith.no/epj [sett 12.10.99].

[64] Latour, Bruno: *Technology is Society Made Durable.* I (Red.) Law, John: "A Sociology of Monsters", Routledge 1991 ss. 103-131, ISBN: 0-415-07139-9.

[65] Latour, Bruno: *Visualization and cognition: Thinking with eyes and hands.* Knowledge & Society, 6, 1-40, 1986.

[66] Lundberg, Nina og Sandahl, Tone Irene: *What do artifacts mean to us in work?* http://internet.informatik.gu.se [sett 12.8.99]

[67] Masse, David G.: *The ABC's of authentication*, Summit 97, http://www.callacbd.ca/summit/auth−masse.html

[68] McBride Baker & Coles: *Table 2 Definitions of the Term "Electronic Signature" in Enacted Legislation*, September 29, 1998

[69] McBride Baker & Coles: *Table 3 Definitions of the Term "Digital Signature" in Enacted Legislation*. September 29, 1998

[70] Menezes, Alfred J., van Oorschot, Paul C. & Vanstone Scott A.: Handbook of Applied Cryptography. CRC Press 1996. ISBN 0-8493-8523-7

[71] Maartmann-Moe, Erling: *Multimedia*, 2. utgave, Universitetsforlaget 1992, ISDN 82-00-21165-7.

[72] Nilsson, Hans & Pinkas, Denis: *Validation of Electronic Signatures*. White Paper. January 27, 1999. Sett 11.2.99 http://www.id2tech.com/news/pdf/ES_validation.pdf

[73] Nordisk Ministerråd: *To Preserve and Provide Access to Electronic Records*. TemaNord 1996:549, , ISBN 92-9120-872-8.

[74] Norsk EDIPRO: *Digitale signaturer og tiltrodde tredjeparter Versjon 1.0*, 07.11.96. ISBN 82-7813-004-3

[75] Norsk EDIPRO: *Meldingssikkerhet: Tiltrodde tredjeparter og digitale signaturer*. Norsk EDIPRO, Norges forskningsråd. Sluttrapport, versjon 1.0, Norsk EDIPRO 1994. ISBN 82-7813-000-0

[76] NOU 1999:26: *Konvergens. Sammensmelting av tele-, data- og mediesektorene*. ISBN 82-586-0497-6.

[77] Næringslivets Sikkerhetsråd (NSR): *Datakriminalitet og mørketall*. mai 1998.

[78] Nærings- og handelsdepartementet: *Næringsrettet IT−plan for perioden 1998−2001*. http://odin.dep.no/nhd/it−plan/plan/

[79] OECD: *Certification in the Electronic Environment*. DSTU/ICCP/REG(97)5, 25-aug-1997. Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy.

[80] Ot.prp. 41 1998-99: *Om lov om finansavtaler og finansoppdrag (finansavtaleloven)*

[81] Ot.prp. 92 1998-99: *Forslag til lov om behandling av personopplysninger (personopplysningsloven)*. http://odin.dep.no/repub/98−99/otprp/92/

[82] Parnas, David L. and Clements, Paul C.: *A Rational Design Process: How and Why to Fake It*. IEEE Transactions on Software Engineering, Vol. SE-12, No.2 (February 1986) pp. 251-57.

[83] Personlig kommunikasjon: E-post fra Kari Bjørkhaug, Brønnøysundregistrene, 28.10.98.

[84] Personlig kommunikasjon: Samtale med Svein Burkeland, RTV, 7.10.99.

[85] Personlig kommunikasjon: Samtale med Petter Christensen, Næringslivets Sikkerhetsråd, 21.10.99.

[86] Personlig kommunikasjon: Samtale med Audun Ekeberg, Kbank, 22.9.99.

[87] Personlig kommunikasjon: E-post fra Randi Eng, SKD, 20.4.99.

[88] Personlig kommunikasjon: Samtale med Amund Eriksen, NHD, År 2000-prosjektet, 18.10.99.

[89] Personlig kommunikasjon: Samtale med Jens Nørve, NHD, 19.10.99.

[90] Personlig kommunikasjon: Samtale med Ivar Fonnes, Riksarkivaren, 20.9.99.

[91] Personlig kommunikasjon: E-postdiskusjon med Tor Guttu, Institutt for nordistikk og lingvistikk, Universitetet i Oslo, 16.6.99.

[92] Personlig kommunikasjon: Samtale med Bo Johanson, DnV, 7.10.99.

[93] Personlig kommunikasjon: Samtaler med Torbjørn Nystadnes, KITH, 1.12.98 og 12.10.99.

[94] Personlig kommunikasjon: Konferanseinnlegg fra Charles Pfleeger, Arca, på 22nd National Information Systemes Security Conference, Washington 18.10.99.

[95] Personlig kommunikasjon: Konferanseinnlegg fra Mark Pollitt, FBI, på 22nd National Information Systemes Security Conference, Washington 18.10.99.

[96] Personlig kommunikasjon: Møte med Terje Kolnes m.fl., Posten SDS 4.10.99.

[97] Personlig kommunikasjon: Samtale med Rolf Riisnæs, IRI, 1.9.99.

[98] Personlig kommunikasjon med Rolf Riisnæs: Informasjonsmøte 17.6.99 om Forvaltningsnettsamarbeidet i regi av AAD.

[99] Personlig kommunikasjon: Samtale med Tone Sandahl, USIT, 23.9.99.

[100] Personlig kommunikasjon: Samtale med Trond Sirevåg, Riksarkivaren, 8.9.99.

[101] Personlig kommunikasjon: Samtale med Dag Wiese Schartum, AFIN, 3.11.99.

[102] Personlig kommunikasjon: Samtale med Mikkel Skou, DnV, 18.8.99.

[103] Personlig kommunikasjon: Samtale med Maria Strøm, Statskonsult, 7.12.98.

[104] Personlig kommunikasjon: Samtale med Guri Verne, NR, 7.10.99.

[105] Personlig kommunikasjon: Samtale med Tove M. Voldbæk, JD, september 98 og 4.11.99.

[106] Personlig kommunikasjon: E-postdiskusjon med Ben Wright 11. 5.99.

[107] Personlig kommunikasjon: Møter med Arne Økstad og Odd Grønvold, KRD, 14.8.98 og 6.10.99.

[108] Personlig kommunikasjon: Samtale med Jon Ølnes, NR, 28.9.99.

[109] Personlig kommunikasjon: E-post fra Egil Årrestad, SDS, 15.4.99.

[110] Planleggings- og samordingsdepartementet og Kommunienes Sentralforbund: *Forvaltningsnettprosjektet. Overordnet prosjektbeskrivelse.* 7.7.97/12.3.98

[111] Reid, Jim: *Plugging the Holes in Host-based Authentication*. Computers & Security, 15 (1996) 661-671.

[112] RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile: http://www.ietf.org/rfcf/rfc2459.txt

[113] Riksarkivaren: *Arkivering av elektroniske saksdokumenter*. Brev til Kulturdepartementet 11.02.97, ref. 95/245 A.336 TS/AR.

[114] Riksarkivaren: *NOARK-4, Norsk arkivsystem versjon 4. Del 1: Funksjonsrettet beskrivelse og kravspesifikasjon.* 1999 Kommuneforlaget AS. ISBN 82-446-0628-2.

[115] Roe, Michael: *Cryptography and Evidence*. A dissertation submitted for the degree of Doctor of Philosophy in the University of Cambridge. sett 6.4.99. http://godzilla.ccsr.cam.ac.uk/techreports/tr1/index.html

[116] Rådet for IT-sikkerhet: *Digitale signaturer gir tillit til elektronisk kommunikasjon: Forslag til tiltak for aksept og utbredelse.* Rapport med forberedende utredning fra arbeidsgruppe oppnevnt av Nærings- og handelsdepartementet, avgitt til Rådet for IT-sikkerhet 30.11.98.

[117] Sandahl, Tone Irene: *From Paper to Digital Documents* University of Oslo, Department of Informatics, January 1999. ISBN 82-7368-208-0.

[118] Schartum, Dag Wiese: *Rettssikkerhet og systemutvikling i offentlig forvaltning*. Universitetsforlaget 1993. ISBN 82-0021867-8.

[119] Schneier, Bruce: *Why Cryptography is harder that it looks*. counterpane Systems 1997.

[120] Seberry, Jennifer and Peprzyk, Josef: *Cryptography: An Introduction to Computer Security*. Prentice Hall1989. ISBN0-13-194986-1.

[121] Seip, Anne Karen: *Oversikt over teknologien som anvendes i betalingssystemer i Norge,* Norges Bank 1995.

[122] Seipel, Peter: *Documents Related to the Swedish EDI-system for Custom Authorities*. s 141 i Kilian, Wolfgang & Wiebe, Adreas (red.): *Data Security in Computer Networks and Legal Problems* Proceedings of a Working Conference in Hannover/Bermany on September 23, 24, 1991, Beiträge zur juristischen Informatic, Band 17, 1992, S. Toeche-Mittler Verlang, Darmstadt, ISBN 3-87820-087-0.

[123] Skattedirektoratet: *System for ligning av næringsdrivende. Brukerkravspesifikasjon*. Versjon 2.0. 28. mai 1997.

[124] Skattedirektoratet, Brønnøysundregistrene, Statistisk sentralbyrå: *Rapport fra Samarbeidsgruppen. Samordnet løsning for elektronisk overlevering av opplysninger fra næringsdrivende til Skattedirektoratet, Brønnøysundregistrene og Statistisk sentralbyrå.* Versjon 2.0 28.05.97.

[125] Sommerville, Ian: *Software Engineering*. Fifth edition. Addison-Wesley, 1996. ISBN 0-201-42765-6.

[126] Sosial- og helsedepartementet: *Høringsnotatet - Lov om helseregistre og elektronisk behandling av helseopplysninger*. 1998. http://www.odin.dep.no/shd/publ/1998/helseregistre [sett 12.10.99].

[127] Staksto n, Silje Grid: *Elektronisk eiendomshandel*. Rapport nr. 940, Norsk Regnesentral 1999. ISBN 82-539-0423-1.

[128] Stallings, William: *Cryptography and Network Security: Principle and Practice*. Second Edition, Prentice Hall 1998. ISBN 0-13-869017-0.

[129] Statens Arkiver: *Elektronisk arkivering: Statens Arkivers krav til systemene*. Januar 1998, versjon 1.04. Danmark. http://www.sa.dk/sa/public.htm

[130] Statskonsult: *Elektronisk saksbehandling*. Statens generelle kravspesifikasjon, november 1997, http://www.statskonsult.no/public/publiste/inform.htm#sksbeh [lest 23.11.98]

[131] Statskonsult: *Elektronisk samhandling med og i offentlig sektor. Forslag til strategi for elektronisk datautveksling for offentlig sektor 1997 - 2001*. Notat 1997:5.

[132] Statskonsult: *Juridiske problemstillinger ved elektronisk saksbehandling og dokumenthåndering*, Rapport 1998:13, september 1998.

[133] Statskonsult: *Konvertering mellom tekstbehandlere*. Mai 1995.

[134] Statssekretærutvalget for IT: *Den norske IT-veien. Bit for bit*. Samferdselsdepartementet 1996. ISBN 82-7452-016-5.

[135] Steiner, Jennifer G. et. al.: *Kerberos: An Authentication Service for Open Network Systems*. USENIX Winter Conference, February 9-12, 1988, Dallas, Texas.

[136] Stinson, Douglas R.: *Cryptography. Theory and Practice*. CRC Press LLC 1995. ISBN 0-8495-8521-0.

[137] St meld nr 41 (1998-99) *Om elektronisk handel og forretningsdrift*. Det kongelige nærings- og handelsdepartement

[138] *Aschehoug og Gyldendals Store norske leksikon*. Kunnskapsforlaget 1980

[139] Aschehoug og Gyldendals *Store norske ordbok*. Kunnskapsforlaget 1992. ISBN 82-573-0312-7

[140] Thoresen, Kari: *Computer Use*. Dr. Philos thesis, March 1999, University of Oslo, Department of Informatics, ISBN 82-7368-210-2.

[141] *UNCITRAL Model Law on electronic Commerce with Guide to Enact*. United Nations 1996. http://www.un.or.at/unicitral/english/texts/electcom/ml-ex.htm, [sett 9.22.98]

[142] UN/EDIFACT: http://www.c-lab.de/~aisch/edifact/edi/ www.premenos.com/unedifact/untdid/d300_s.html [sett 29.10.99]

[143] Valmot, Odd Richard: *Data forsvinner*. Teknisk Ukeblad 146. årgang, nr. 32, 2. september 1999.

[144] Voges, Mickie A.: *Authenticating Legal Documents*, Summit 97, Chicago-Kent College of Law, Illinois Institute of Technology. http://www.callacbd.ca/summit [sett 21.8.98]

[145] *Webster's New World Computer Ordbok*. Schibsted 1984. ISBN 87-88165-13-2.

[146] Wright, Benjamin: *Alternatives for Signing Electronic Documents* http://www.penop.com, [sett 4.5.99]

[147] Økstad, Arne og Grønvold, Odd: *Elektronisk dokumentuteksling i norsk administrasjon, EDNA*. Kommunal- og regionaldepartementet, 1999.

[148] Ølnes, Jon: *Infrastruktur for sikker kommunikasjon - TTP-tjenester og offentlig engasjement*. Norsk Regnesentral, NR Notat: OMNI/01/97, april 1997.

Ordbok

ABA
American Bar Association

Akkreditere
Gi en person fullmakt (til et eller annet) [12]

Akkreditiv
Data som overføres for å hevde en entitets identitet [41].

Aktant
An actant is a list of answers to trials - a list which, once stabilized, is hooked to a name of a thing and to a substance. [64]. Jo lengre listen er, jo mer aktiv er aktøren/aktanten. Jo kortere listen er, jo mindre er viktig er aktøren. En aktant kan være både mennesker, maskiner, programvare og lovverk i oppgavens sammeneheng.

ANSI
American National Standards Institute.

Artefakt
kunstverk, kunstprodukt (biler, dataprogrammer) i motsetning til naturlige ting som steiner og trær. Ordet brukes i systemerermiljø, men jeg har ikke klart å finne en definisjon.

ASCII
American Standard Code for Information Interchange. En standard syv-bit kode [145].

Assurance
forsikring, sikkerhet, selvtillit [10]. Se Tiltro

Autentisk
fullt ut ekte og pålitelig [12].

Autentisering
prosessen med å bekrefte en oppgitt identitet. (fra datasikkerhetsdirektivet) [116].

Autentisering av kilde
Data origin authentication. Bekreftelsen at data kommer fra den kilden som det påstås/hevdes de kommer fra [41].

Autorisering
Tilordning av rettigheter til aktører en person har i tilknytning til et IT-system [116]. ?

Benekting
Benekting fra en av partene involvert i kommunikasjon/forsendelse over å ha deltatt i alt eller deler av kommunikasjonen [41].

Bursdagsangrep
Sannsynligheten for at minst 2 personer i et rom med 23 mennesker har fødselsdag på samme dag er beregnet til $\approx 0{,}507$ hvilket er et forbausende høyt tall [70]. Begrepet brukes i forbindelse med hash-algoritmer som helst ikke skal beregne den samme hash-koden for to ulike tekster.

Chiffer
Hemmelig skrifttegn, siffer [35].

Confidence
tillit, selvtillit [10]. Se tillit.

Data
er en grunnleggende enhet av informasjon. Data kan samles til å danne dokumenter eller lister [24]. Data regnes også som enhetene som lagres på et elektronisk medium og som først blir informasjon når et menneske leser det.

Databærer
data carrier, et datamedium som er laget for lagring og/eller transport av data [122].

Dataintegritet
Egenskapen at data ikke har blitt endret eller slettet på en uautorisert måte [41].

Data origin authentication
se Autentisering av kilde.

Denial of service
hindring av autorisert tilgang til ressurser eller utsettelse/forsinkelse av tidskritiske operasjoner [41].

DES
Data Encryption Standard

Digital signatur
Data tilføyd til, eller en kryptografisk transformasjon av, en dataenhet som tillater mottaker av dataene å bevise dataenes kilden og dataenes integritet og som beskytter mot forfalskning dataene f.eks. av mottakeren [41].

Dokument
(fra lat.) (belærende) eksempel, bevis av skriftstykke, aktstykke, skriftlige utgreiing i en rettssak, kildeskrift; vitnesbyrd [12] . En avgrenset og sammenhengende informasjonsmengde, framstilt for et bestemt formål. Informasjonen kan bestå av av en kombinasjon av tekst, data, grafikk, bilder og multimedia. Et dokument kan også bestå av flere dokumenter (sammensatte dokumenter) [130]. "..a data carrier and the data recorded on it, that is generally permanent and that can be read by man or machine" [142].

DSA
Digital Signature Algoritm, amerikansk algoritme, basert på [40].

EBCDIC
Extended Binary Coded Decimal Interchange Code. En standard åttebit kode anvendt til representasjon av karatkerer [145].

Egenskap
1) grunndrag; 2) (karakter)trekk, side, natur [12]

Elektronisk saksbehandling
innebærer at saksbehandlingen kan utføres med støtte av informasjons-teknologi.

Elektronisk signatur
Et unikt bitmønsteret koplet til et elektronisk dokument som erstatter en håndskreven underskrift der lover og regler krever det.

Entitet
enhet [12]. En entitet kan referere til et menneske, en organisasjon, en hardwarekomponent eller et stykke programvare [49]

Entitetsautentisering
en bekreftelse på at entiteten er den den påstår å være, [43].

FNS
Forvaltningsnettsamarbeidet.

Formkrav
oppsett av dokumenter med felter som skal fylles ut, brevhoder, underskrift nederst på arket osv.

Funksjon
1) virksomhet, gjøremål, tjeneste, oppgave; 2) språkv.: bruksmåte; 3) mat.: det at en variabel størrelses verdi er avhengig av en annen størrelses verdi [12]

Genre
sjanger. 1) avgrenset område av en kunstart; 2) stil, maner, klasse; 3) slags, sort. [12]

Giverkapasitet
hvor fort kan du ta i mot og gi data

HTML
Hyper Text Markup Language [114]

Identifisere
1) kjenne igjen, fastslå identiteten av;
2) regne seg som ett (med), ha samfølelse (med);
3) påvise identitet mellom (to eller flere ting) bringe under samme begrep [12].

Identisk
fullstendig lik, en og den samme, ensbetydende. Identitiet 1) det å være identisk; 2) navn, stilling o l til en person [12].

Ikke-benekting
Uavviselighet. En mekanisme slik at en av partene i en kommunikasjon/forsendelse av data kan ikke benekte at parten har deltatt. Målet for en ikke-benektingstjeneste er: *To collect, maintain, make available and validate irrifutable evidence conserning a claimed event or action in order to resolve disputes about the occurrence or non occurrence of the event or action.* [46]. *Non-repudiation involves the generation of evidence that can be used to prove that some kind of event or action has taken place, so that this event or action cannot be repudiated lager.*

Informasjon
“an indication or an event brought to the knowledge of a person” [24].

Integritet
se Dataintegritet

ISO
International Standards Organization

Kassasjon
arkivmateriale som har vært gjenstand for saksbehandling eller har hatt verdi som dokumentasjon, blir tatt ut av arkivet og slettet eller destruert, [5].

Kjennetegn
kjennemerke, karakteristikk [12]

Kryptering
Prosessen å omgjøre klartekst til chiffertekst [37].

Kryptografi
Hemmelig, skjult skrift [35]. Læren om chiffer og koder og deres anvendelse [138]. Disiplinen som samler prinsippene, midlene og metodene for transformasjon av data for å gjemme informasjonsinnholdet, hindre uoppdagete endringer og/eller hindre uautorisert bruk [41].

Kryssertifisering
To eller flere sertifiseringsautoriteter tilhørende forskjellige PKI'er gir hverandre sertifikater for å stadfeste et tillitsforhold [116].

Langtidslagring
Offentlige etater er pålagt å arkivere en del dokumenter for ettertiden. Enten dokumentene er fysiske eller elektroniske, skal de kunne lagres i mange hundre år. De skal kunne gjenfinnes og leses. De skal være autentiske og ikke være endret.

Lukket system
Et sett av datamaskiner som har en underliggende avtale som gir tillit til hva slags informasjon som skal sendes dem i mellom. Minibanksystemet i Norge er et lukket system. Det er noen som har kontroll med helheten.

MAC
Message Authentication Code

Noark-standarden
Norsk arkivsystem. Bestemmes av Riksarkivet etter høringsuttalelser. Noark-4 er en kravspesifikasjon for elektroniske arkivsystemer i offentlig forvaltning [114].

Non-repudiation
se ikke-benekting.

Norsk EDIPRO
er en brukerstyrt, privat samfunnsgagnlig stiftelse med formål å ivareta brukernes interesser i forbindelse med innføring av EDI (elektronisk datautveksling). http://www.edipro.no.

Norsk TEDIS
se Norsk EDIPRO

Notarius publicus
(lat. en som opptegner en talendes ord, hurtigskriver), i norsk rett embetsmann som utfører notarforetninger, dvs. som ved sin underskrift sikrer beviset for visse rettslige handlinger, f.eks. borgerlig vigsel, vekselprotest og attestasjoner. (byfogd eller sorenskriver), [138].

NSA
National Security Agency.

Nøkkel
En sekvens av symboler som kontrollerer operasjonene for kryptering og dekryptering [41].

Nøkkeladministrasjon
Generering, lagring, distribusjon, arkivering og anvendelse/bruk av nøkler i samsvar med et regelverk (policy) [41].

ODIN
Offentlige dokumenter og informasjon i Norge

Original
noe opprinnelig el. ekte, førstehåndsarbeid [12].

OSI
Open Systems Interconnection

PDF
Portable Document Format [114]

Privacy
Privat karakter, ensomhet, enerom, tilbaketrukkenhet, hemmelighet, fortrolig [10]. Individers rett til å kontrollere eller påvirke hvilken informasjon relatert til dem som kan samles og lagres av hvem og til hvem informasjonen kan avdekkes [41].

Rolle
1) de replikker en skuespiller skal si; 2) den person en skuespiller skal framstille; 3) i forbindelsen ha noen betydning; 4) uskrevne regler og mønstre for oppførsel og handlemåte som knytter seg til en bestemt sosial posisjon eller status.[12]

RSA
Rivest-Shamir-Adleman cryptosystem

SEIS
Secure Electronic Information in Society, Sverige

Sertifisering
Prosessen å knytte sammen en nøkkel og unik identitet på en for alle praktiske formål uadskillelig måte [14].

Sertifikat
Den eksplisitte og tolkbare representasjonen av koplingen mellom en nøkkel og unik identitet [14].

SGK
Statens generelle kravspesifikasjon

SGML
Standard Generealized Markup Language, ISO 8879:1986 [114]

Signatar
den som underskriver [12].

Signatur
1) merke, tegn; 2) navnetrekk, underskrift [12] I oppgavens sammenheng er det naturlig å legge vekt på at signaturen eies av et bestemt menneske.

SSL
Secure Sockets Layer [29].

Standard
normal, vanlig. Å standardisere er å fastsette, gjøre ensartet [12].

Sterk autentisering
2048 bit RSA [116]

TIFF
Tagged Image File Format [114]

Tillit
en egenskap ved de tekniske og/eller organisatoriske systemene som samlet utgjør en TTP-tjeneste. Denne egenskapen sier noe om i hvor stor grad sikkerhet, funksjonalitet og andre tekniske og organisatoriske aspekter er hensiktsmessige og tilstrekkelige i forhold til TTP-ens tjenester og formålene for disse. Engelsk: "confidence" eller "trust". [74]

Tillitskjede
Hvis A stoler på B som stoler på C som stoler på D, så er det ikke sikkert at A bør stole på D eller at D bør stole på B. For mange ledd gir ofte svakere tillit.

Tiltro
summen av de forventninger og antakelser myndigheter, brukere o.a. har til at TTP-tjenester iverksettes, drives og ytes på en måte som er i samsvar med lover, regler, generelle retningslinjer, tilbyders påståtte sikkerhetsmessige egenskaper o.l. Allmenn tiltro. Engelsk: "assurance" [74]

Tiltrodd tredjepart, TTP
er en organisasjon som yter en eller flere sikkerhetstjenester, og som to, for hverandre ukjente, kommuniserende parter, har tiltro til. TTPens rolle er å øke tiltroen til at meldinger og transaksjoner overføres til den tilsiktede mottaker til rett sted og på en korrekt måte. I tilfelle tvister skal det finnes metoder for å generere bevis for hendelsesforløpet [49]. TTP-tjenester kan f.eks. være sertifikatutsteding eller tidsstempling.

Trojansk hest
I dag brukes begrepet om en programbit som er lagt inn i andres programmer på en slik måte at det skjuler sine ødeleggende egenskaper [21]. Eksempler er å hente informasjon om passord eller signere en ekstra betalingstransaksjon.

Trust
Tillit, tro, tillitsfullt, stole på [10]. Se tillit.

Uavviselighet
se ikke-benekting.

UNCITRAL
United Nations Commission on International Trade Law

Underskrift
navnetrekk under dokument (som tegn på godkjenning eller samtykke), [12].

Unik
(gj. fra. fra lat. 'eneste', av unus 'en') som det fins bare ett eksemplar av, enestående, sjelden. [12]

Validere
gjøre/være gyldig [12]. Validering innebærer å sjekke at programmet som implementeres møter forventningene som brukere eller kunder har. "Lager vi det riktige produktet?" s. 446 i [125].

Verifisere
1) attestere riktigheten av, bekrefte; 2) undersøke og fastslå riktigheten av[5].

Verifikasjon innebærer å sjekke at programmet er i overensstemmelse med spesifikasjoenen. “Lager vi produktet riktig?“[125].

WORM
Write Once Read Many. CD-ROM-plater som bare kan skrive stil én gang, men som kan leses mange ganger.

XML
Extensible Markup Language [114]

Åpne systemer
Selvstendige, heterogene, datasystemer som kommuniserer vha. aksepterte standarder med andre systemer uten å kjenne dem eller vite hva slags informasjon som kommer fra dem. I lukkete systemer har systemene underliggende avtaler som gir tillit til hva som skal overføres. Den tilliten har man ikke i åpne systemer. Hvem som helst kan sende hva som helst, f.eks. på Internett.

Stikkord

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Ø

Å