ELEKTRONISK DOKUMENTHANTERING

EN RÄTTSLIG PROBLEMORIENTERING

RIKSARKIVET / LAGERLÖF & LEMAN

För många är elektronisk dokumenthantering en fråga om motsättningen mellan tekniska löften och rättsliga hinder. Syftet med denna skrift är att ge en översikt över det rättsliga läget och att visa på de möjligheter som redan idag finns att påbörja elektronisk dokumenthantering utan ingripande åtgärder i lag eller förordning. Skriften har utarbetats av rådmannen Per Furberg, numera vid Lagerlöf & Leman Advokatbyrå, på uppdrag av Toppledarforums projekt Elektronisk dokumenthantering. Den riktar sig till jurister och övriga inom förvaltningen som vill bilda sig en uppfattning om de rättsliga och tekniska sammanhangen.

RIKSARKIVET
Box 125 41, 102 29 Stockholm
Telefon 08 - 737 63 50

TOPPLEDAR FORUM
IT i offentlig samverkan

LAGERLÖF & LEMAN
Advokatbyrå

FRITZES

Postadress: 106 47 Stockholm
Fax: 08-690 91 91, Tel: 08-690 91 90

ISBN 91-38-31661-7
RAPPORT 2000:1

ELEKTRONISK
DOKUMENTHANTERING

EN RÄTTSLIG PROBLEMORIENTERING

RIKSARKIVET

LAGERLÖF & LEMAN

RAPPORT 2000:1

Riksarkivets rapportserie
riktar sig i första hand till statliga myndigheter men kan även användas av andra myndigheter och organ som har att tillämpa arkivlagen.

Rapporten "Elektronisk dokumenthantering – en rättslig problemorientering" har tagits fram inom Toppledarforums projekt för Elektronisk dokumenthantering (E-dok) som har finansierats av NUTEK inom ramen för FoU-programmet favorIT (Tjänsteproduktion och IT-användning). Den ges även ut av Statskontoret tillsammans med övrig avrapportering från E-dokprojektet.

Rapporten har utarbetats av rådmannen Per Furberg, numera vid Lagerlöf & Leman Advokatbyrå, på uppdrag av projektet. Torbjörn Hörnfeldt och Britt-Marie Östholm Riksarkivet har lämnat synpunkter på de delar som rör arkivfrågor.

Elektronisk dokumenthantering
– en rättslig problemorientering
Upplaga 1:1
ISBN 91-38-31661-7
ISSN 1402-9685

Publikationsansvarig: Per Jansson, arkivråd.
Grafisk form: Nils Möllerström AB, Stockholm.
Layout: Nora Liljeholm, Riksarkivet.
Tryck: Elanders Gotab AB, Solna 2000.

Skriften beställs från:
Fritzes kundtjänst, 106 47 Stockholm,
telefon: 08 - 690 91 90, orderfax: 08 - 690 91 91.

INNEHÅLL

FÖRORD

Publikationen Elektronisk dokumenthantering – en rättslig problemorientering behandlar ämnen som kommer att vara giltiga under lång tid. Hit hör bevarandet av viktig information, garanti av dokumentets äkthet och skydd av innehållets integritet.

Dokumentering av offentlig information har alltid varit en fråga om både teknik och rättsregler. Varje skede i utvecklingen har medfört förändring av regelverk. Namnteckningen, som vi i vår tid med självklarhet betraktat som den rättsligt bindande symbolen, har inte haft sin kraft under mer än några generationer. När vi under tidig medeltid med kyrkans hjälp fick ett nytt skriftspråk, övertog vi också bruket att visa dokumentets rättskraft genom att besegla det. Under lång tid var det sigillet, inte namnteckningen, som gav innehållet dess legitimitet. Trots bruket av kopieringsapparater, mikrofilm och datorer användes så sent som på 1980-talet lackstång och sigillstamp i den offentliga expeditionstjänsten för att bekräfta giltigheten.

Toppledarforums projekt Elektronisk dokumenthantering (E-dok) har haft som mål att undanröja hinder för hanteringen av information inom ramen för elektronisk dokumenthantering, ett skede i vilket vi inte längre så enkelt kan skilja mellan original och kopia, mellan tryckt och otryckt, mellan handling och information. För Riksarkivet har det varit naturligt att verka som värdmyndighet för detta projekt. Projektet har letts av avdelningsdirektör Torbjörn Hörnfeldt, Riksarkivet. Från Riksarkivets sida har han i första hand biträtts av förste arkivarie Britt-Marie Östholm.

För många är elektronisk dokumenthantering i första hand en fråga om motsättningen mellan tekniska löften och rättsliga hinder. E-dokprojektet vill nu i stället fästa uppmärksamheten på möjligheterna och stimulera till en övergång till elektronisk hantering. Förutsättningarna finns redan såväl tekniskt som rättsligt. De oklarheter som återstår är inte försumbara, men de kan belysas och förhoppningsvis hanteras inom en överskådlig framtid.

Denna skrift har på projektets uppdrag utarbetats av rådmannen Per Furberg, numera vid Lagerlöf & Leman Advokatbyrå. Per Furberg har IT-juridik som specialområde. Han har bl a varit sekreterare i Utredningen om lagstiftningsbehovet vid tulldatoriseringen, Datastraffrättsutredningen, IT-utredningen och Utredningen om elektroniska pengar samt expert i Redovisningskommittén och Datalagskommittén. Därtill kommer ett antal internationella uppdrag. Målgrupp för skriften är i första hand jurister, men projektet vill nå även andra som vill fördjupa sin syn på området.

Detta är den första delrapporten från E-dokprojektet. Innehållet har bedömts som så viktigt att den ges ut i en särskild utgåva av Riksarkivet. Den fullständiga avrapporteringen från projektet kommer att ges ut av Statskontoret.

Erik Norberg

1 UPPDRAGET

Projektet "Elektronisk dokumenthantering för ärenden som berör flera myndigheter i offentlig verksamhet" (E-dok), utgör en del av Toppledarforums initiativ för att uppnå en ökad användning av den befintliga elektroniska infrastrukturen. Projektets uppdrag, att skapa tekniska förutsättningar för elektronisk dokumenthantering och att eliminera hinder mot att utbyta elektroniska dokument, syftar till att ta ytterligare ett steg i riktning mot en elektronisk förvaltning.

Detta arbete, som utgör en del av E-dokprojektet, har sin bakgrund i en utbredd missuppfattning om att nuvarande rättsregler skulle utgöra ett absolut hinder mot en rationell användning av informationstekniken (IT). I själva verket är det emellertid redan idag möjligt att påbörja elektronisk hantering av ärenden, utan ingripande åtgärder i lag eller förordning. Denna skrift syftar i första hand till att sprida kunskap om dessa *möjligheter*.

En förutsättning för att en sådan genomgång skall föra arbetet framåt är emellertid *en riktig förståelse av IT*, från rättsliga utgångspunkter, och det är på denna punkt som det ofta visat sig brista. Det kan till och med vara så att en myndighet redan har grundläggande tekniska hjälpmedel och byggstenar för att införa elektronisk dokumenthantering – utan att dessa möjligheter har uppmärksammats. I bakgrunden kan man skymta en rädsla för IT och de komplexa frågor datoriseringen väcker, en hållning som tenderar att ge en bild av närmast oöverstigliga rättsliga hinder. I denna skrift läggs därför tyngdpunkten på att utifrån det utredningsarbete och de författningsändringar som genomförts beskriva elektroniska dokument och signaturer och den infrastruktur som kan behövas för sådana rutiner. Syftet är att lägga en grund för en riktig förståelse av sambanden mellan rättsreglerna och IT.

En fråga i detta sammanhang är vilken informationssäkerhet som bör krävas i det enskilda fallet. Det är t ex inte rimligt att säkerhetsrutiner som tillämpas för banktransaktioner alltid skall krävas för kommunikation inom och mellan myndigheter eller vid kommunikation med privatpersoner. Detta framgår redan av hur telefax och e-post idag används inom

offentlig förvaltning. Situationen kan något tillspetsat beskrivas så att det finns två trender – antingen att "köra helt utan skydd" eller att bygga modeller och inleda pilotprojekt som är så komplexa att de knappast kan hanteras utan synnerligen omfattande och kostnadskrävande åtgärder. I denna skrift antyds därför också behovet av balanserade avvägningar mellan effektivitet och säkerhet samt *fungerande* koncept vid valet mellan olika tekniska och administrativa lösningar.

Slutligen ges en sammanfattning av de rättsfrågor som vanligtvis kan antas bli aktuella på myndighetsområdet.

2 DE DIGITALA OBJEKTEN M M

Beskrivningen inleds här med en genomgång av de objekt i elektronisk form på vilka rättsreglerna skall tillämpas. Parallellt med detta arbete har Toppledarforum bedrivit teknikprojekt för att röja väg för rutiner för elektroniska signaturer och liknande säkerhetstjänster.

2.1 DATA OCH INFORMATION

Den fysiska manifestationen av data som representerar en viss uppgift utgörs av ett mönster av laddningar på en databärare. Ordens makt över tanken kan lätt locka till felaktiga slutsatser när traditionella termer används i denna nya miljö.

Traditionella beskrivningar av den pappersbaserade dokumenthanteringen brukar ta sin utgångspunkt i att en handling är en fysisk sak. Textens innehåll – föreställningsinnehållet – kommer ofta i andra hand. Distinktionen mellan vad som är ett konkret föremål, en sak, och vad som är ett abstrakt objekt är därvid ett generellt problem eftersom informationen vid den traditionella pappersbaserade hanteringen av uppgifter, bryts ned till digitala operationer (på förhand bestämda procedurer för databehandling). Härvid brukar data definieras som *representation* av uppgifter etc, medan uttrycket information ses som något abstrakt; *innebörden* i data.

Den fysiska manifestationen av just de data som representerar en viss uppgift utgörs av mönster av laddningar på en databärare. Det går inte att på traditionellt sätt skilja ett original*exemplar* från en kopia när data förs över från en databärare till en annan; informationen förekommer således endast som ett original*innehåll*, när erforderligt skydd har getts för dess äkthet.[1]

En rätt förståelse av hur databehandling av uppgifter fungerar är av avgörande betydelse för de rättsfrågor som elektronisk dokumenthantering aktualiserar. Lägg märke till hur ordens makt över tanken lätt kan locka läsaren till felaktiga slutsatser när termer som är vanliga i den traditionella miljön – t ex "skriftlig", "handling", "signerad" och "dokument" – används i IT-miljön. Ett exempel är att många tror att data lagras på samma sätt som man läser en vanlig handling – att den digitala representationen

[1] Dessa frågor har närmare behandlats av bl a Datastraffrättsutredningen som föreslagit beteckningen *kvasimateriell* för denna objektkategori (se betänkandet Information och den nya InformationsTeknologin – straff- och processrättsliga frågor m m, SOU 1992:110, bl a sid 96 ff.

av texten måste finnas i en fil som börjar där texten börjar och slutar där texten slutar. Sker bevaringen t ex i en relationsdatabas är data emellertid vanligtvis *lagrade* i en helt annan ordning.

2.2 HANDLINGAR OCH UPPTAGNINGAR

2.2.1 Traditionella egenskaper och nya förutsättningar i IT-miljön

De principer och skydd som gäller för traditionella urkunder är betydelsefulla för att förstå rättsfrågorna på IT-området. Motsvarande skydd behövs vid elektronisk dokumenthantering inom förvaltningen.

Vad som utgör en handling eller en urkund har i traditionell miljö uppfattats som självklart. Det kan noteras att den definition av urkund som ges i 14 kap 1 § brottsbalken endast utgörs av en exemplifierande uppräkning; såsom urkund anses protokoll, kontrakt, skuldebrev, intyg och annan handling, som upprättats till bevis eller eljest är av betydelse såsom bevis.[2] De principer som ligger bakom denna reglering har visat sig vara av intresse också för att förstå de rättsfrågor som aktualiseras vid elektronisk dokumenthantering. Vad är då en traditionell urkund och hur skiljer den sig från ett digitalt dokument?

Pappersurkunden kan sägas bestå av tre begrepp och tre däremot svarande fysiska enheter:

- bäraren (pappersarket)
- texten (eventuellt i förening med bilder etc), och
- utställarangivelsen (vanligtvis en underskrift).

Begreppet handling i brottsbalkens definition av urkund är härvid förknippat med en rad *underförstådda egenskaper* (dolda rekvisit), som allra tydligast framträder om man analyserar begreppet i samband med en jämförelse av en traditionell urkund och ett digitalt dokument. En handling måste ha en *utställare* för att straffskydd skall föreligga – en helt anonym skrift är inte en urkund. På samma sätt kan anonyma skrifter knappast användas vid handläggningen av ett ärende. Handlingen behöver också ge reella hållpunkter för en äkthetsprövning. Det enklaste exemplet på ett *äkthetstecken* är en underskrift. Den är avsedd att övertyga läsaren om att innehållet i en handling inte härrör från någon annan. Denna tillit till uppgifternas ursprung är av avgörande betydelse för att skriftlig kommunikation skall fungera i samhällslivet och för att elektronisk dokumenthantering skall fungera.

[2] Här bortses från bevismärken.

Kravet på att en handling skall innefatta ett visst mått av äkthetstecken för att kunna tillerkännas urkundskvalitet har efter hand kommit att försvagas[3] och olägenheter har framträtt till följd av att manipulationer har förenklats genom att pappershandlingens egenskaper delvis saknas i IT-miljön. En viktig skillnad mellan pappershandlingar och digitala representationer är härvid att pappersbaserade urkunder är unika originalexemplar medan samma innehåll i digital form inte kan få denna karaktär av original. Digitala dokument kan förändras och kopieras utan kvalitetsförluster och transporteras via nät. För att en handling skall anses som urkund enligt den straffrättsliga regleringen krävs att den har originalkaraktär. Därigenom kan den fylla en s k *symbolfunktion* – att i egenskap av fysiskt föremål vara bärare av en viss rättighet; jfr t ex innehavarskuldebrev och läkemedelsrecept.

Till detta kommer att traditionella handlingar är direkt läsbara redan i lagrad form medan ett elektroniskt dokument måste omvandlas från maskinläsbar till visuellt läsbar form när någon vill ta del av dokumentet. Vidare har bärare, text och utställarangivelse inte samma låsta och beständiga relationer som i ett pappersdokument och användaren vet nästan aldrig hur den fysiska lagringen går till eller vilka procedurer som genererar – återskapar – vad vi traditionellt kallar ett dokument. Tekniken bygger på att en dator på kommando utför automatiska procedurer enligt en bestämd plan i form av ett datorprogram. Lagrade data är normalt inte "låsta" av bäraren och en manipulation av data lämnar inga sådana spår efter sig som vid en manipulation av ett pappersdokument. Ett dokument i digital form kan således sägas vara en av en dator genererad funktion, dvs att det med lagrade data, databasprogram och andra datorprogram finns förutsättningar att återskapa – generera – samma dokument flera gånger, så länge dessa förutsättningar inte förändras. Det är bl a här de elektroniska signaturerna och liknande metoder för äkthetskontroll kommer in; se vidare Datastraffrättsutredningen beskrivning av de grundläggande drag som skiljer en elektronisk materialisering från en traditionell handling.[4]

2.2.2 Äkthetsprövningen – ett val av utgångspunkt

Genom att utgå från *texten* och skyddet av dess innehåll, istället för den *sak* som bär texten (pappersarket/hårddisken etc), kan moderna IT-rutiner i allt väsentligt förenas med gällande rätt. Det är ett sådant synsätt som har införts på bl a tull- och skatteområdet, där varje digitalt exemplar ("kopia") kan behandlas likvärdigt.

[3] Det har till och med hävdats att Datastraffrättsutredningen skulle ha tolkat regleringen felaktigt, och att det inte skulle finnas något sådant krav på originalkvalitet hos en urkund.

[4] SOU 1992:110 sid 261 ff och 279 ff.

Ett traditionellt, djupt rotat tänkande om vad som är ett original respektive en kopia i pappersmiljö för med sig rättsliga komplikationer, samtidigt som de associationer dessa termer ger kan föra tanken fel. Detta klargörs enklast med ett exempel utifrån valet av utgångspunkt för en äkthetsprövning, där frågan ställs på sin spets.

> Beda har framställt och vidimerat en fotokopia av en urkund som Ada ställt ut. I kopian har Beda emellertid manipulerat den av Ada utställda texten. Detta innebär att Beda dels har ändrat Adas text så att den inte längre helt härrör från henne, dels har lämnat en osann vidimationsförklaring. Det finns därmed två möjligheter att beivra detta förfarande – antingen som urkundsförfalskning (14 kap 1 § brottsbalken) eller som osant intygande (15 kap 11 § brottsbalken).

Ställningstagandet beror av *vem som är* att anse som *utställare av vad*. En konsekvens av att man i gällande svensk straffrätt utgår från vem som är garant för *saken* – pappersarket med text – är att en ovidimerad kopia inte är en urkund eftersom den som sak helt saknar utställarangivelse. Vidimeras en pappersbaserad kopia av urkunden blir den emellertid att anse som urkund eftersom den som vidimerar står som ett slags garant för det nya exemplarets bevisfunktion.[5] Den som sanningslöst intygar att kopian överensstämmer med originalet anses göra sig skyldig till osant intygande, medan den som tecknar annans namn anses begå urkundsförfalskning. Är kopian inte vidimerad kan missbruk av urkund föreligga, om någon sanningslöst utger den för att vara en riktig kopia av en viss urkund (15 kap 12 § brottsbalken).

Enligt ett annat synsätt, använt i t ex tysk straffrätt, utgår man i stället från den materialiserade *texten* och vem som står för den. Det är så IT fungerar, genom att bäraren delvis mister sin betydelse; jfr vid not 13. De regler om elektroniska dokument som har införts på t ex tull- och skatteområdet utgår därför från den materialiserade texten och vem som står för den, inte från bäraren. Regleringen behandlar därmed varje digitalt exemplar likvärdigt. Som exempel kan nämnas en deklaration som sänds via nät till skattemyndigheten. Därvid kopieras signalmönstret från avsändarens dator till mottagarens. En prövning av om ett sådant dokument är äkta som *sak* blir möjlig endast genom konstruerade resonemang som är svåra att förena med gällande rätt. Vilken av alla de "kopior" som genereras när ett elektroniskt dokument överförs via Internet skulle kunna ses som det

[5] Jfr Holmqvist m fl, Brottsbalken, sid 14:17.

unika skyddade exemplaret och vem bör ses som garant för det? Skulle bedömningen grundas på vem som står som garant för databäraren, leder detta till att avsändaren av ett e-postmeddelande är garant för exemplaret på den egna hårddisken och mottagaren för det exemplar som finns på dennes databärare. Detta synsätt är uppenbart oförenligt med det intresse av skydd för meddelandets autenticitet som ligger till grund för regleringen; jfr om avsändaren av ett telefaxmeddelande skulle ses som utställare av det avsända exemplaret och mottagaren som utställare av det mottagna exemplaret av samma telefaxmeddelande.[6]

IT kan alltså förenas med gällande rätt, om den justeringen görs – i tänkande, och författningsreglering när så krävs – att *texten* och skyddet av dess innehåll fungerar som utgångspunkt, inte den *sak* som bär texten. Därmed kan varje digitalt exemplar ("kopia") behandlas likvärdigt, och det är så IT-användningen inom förvaltningen fungerar.[7]

2.2.3 Nuvarande och föreslagna regler om signerade handlingar

En ny definition av dokument i IT-miljö har förts in i flera författningar och det finns olika förslag till sådana ändringar. Här ges en tämligen ingående beskrivning av dessa alternativa definitioner. Vid en ytlig granskning kan de olika varianterna framstå som förvirrande och ge intryck av att det skulle vara fråga om helt olika dokumentbegrepp. I själva verket baseras de emellertid på samma grundläggande synsätt – att bäraren delvis mister sin betydelse och att det *fysiska* skyddet, genom att låsa text på t ex ett pappersark, ersätts av ett *logiskt* skydd för det mönster av elektroniska laddningar som representerar text och utställarangivelse. Genom denna anpassning kan moderna IT-rutiner användas på ett fungerande och kostnadseffektivt sätt, även på myndighetsområdet.

Behovet av en reglering för IT-baserade ersättare för traditionella urkunder har tidigt uppmärksammats i Sverige. Arbetet inleddes av Utredning-

[6] Jfr de resonemang som förts i en promemoria upprättad inom justitiedepartementet av en utredare (Jörgen Almblad) där det som ett alternativ nämns att ett meddelande skulle anses utställt av avsändaren såvitt avser det exemplar av data som finns på avsändarens hårddisk, men av mottagaren när det gäller exemplaret på dennes hårddisk.

[7] I detta sammanhang har det brukat konstateras att de rättsliga funktioner som knyts till en originalurkund, att i egenskap av unikt exemplar *bära* en viss rättighet, inte kan återskapas i IT-miljön. Numera finns det emellertid också elektroniska pengar (e-pengar), som i praktiken fungerar som bärare av viss betalkraft. Det har alltså visat sig att även dessa funktioner kan återskapas, genom tekniska skydd mot dubbelspenderingar. På nuvarande stadium i utvecklingen av nya IT-rutiner inom förvaltningen blir sådana rutiner – där data på motsvarande sätt som ett fysiskt pappersbaserat exemplar bär en viss rättighet – dock knappast aktuella. Som exempel på ett område där de hade varit bra för att bibehålla den traditionella funktionaliteten kan emellertid nämnas läkemedelsrecept.

en om lagstiftningsbehovet vid tulldatoriseringen (TDL-utredningen), som föreslog att begreppet "elektroniskt dokument" skulle föras in i tullagen. En definition föreslogs dock endast i lagmotiven.[8] I det fortsatta lagstiftningsärendet förordade lagrådet att en definition skulle tas in i tullagen och att den av utredningen föreslagna definitionen skulle justeras så att den till omfång m m blev anpassad för att föras in i lag. Med upptagningsbegreppet som utgångspunkt (jfr 2 kap TF) samt tillkommande krav på informationssäkerhet i enlighet med utredningens förslag infördes följande definition.

> Ett elektroniskt dokument är en upptagning vars innehåll och utställare kan verifieras genom ett visst tekniskt förfarande.[9]

Samma definition har förts in i författningar på skatte-[10] och exekutionsområdet[11] samt i lagen (1994:448) om pantbrevsregister.[12] I samband med regleringen avseende skatte- och exekutionsväsendet har i motiven också introducerats termen elektronisk akt.

IT-utredningen har därefter i betänkandet Elektronisk dokumenthantering (SOU 1996:40) föreslagit generella regler om bl a dokument för hela förvaltningsområdet. Där föreslås bl a att följande definitioner skall tas in i förvaltningslagen.

I denna lag avses med

elektronisk handling: en bestämd mängd data som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel,

digitalt dokument: en elektronisk handling med digital signatur eller digital stämpel,

digital signatur: resultatet av en omvandling av en elektronisk handling som gör det möjligt att kontrollera om innehållet härrör från den fysiska person som framstår som utställare, och

digital stämpel: resultatet av en omvandling av en elektronisk handling som gör det möjligt att kontrollera om innehållet härrör från den juridiska person eller myndighet som framstår som utställare.

8 I utredningens delbetänkande Tullregisterlag m m (SOU 1989:20) definierades detta begrepp enligt följande. Ett elektroniskt dokument i tulldatasystemet är en språkhandling i förening med en uppgift om dess utställare som visserligen lagras genom ADB men där det väsentliga är att textenheten och utställarenheten entydigt kan bestämmas till sitt innehåll genom en ADB-teknisk kontrollprocedur knuten till databehandlingen.

9 Prop. 1989/90:40, bet. 1989/90:KU2 och bet. 1990/91:KU11.

10 Ds 1994:80, prop. 1994/95:93, bet. 1994/95:SkU15 och rskr. 1994/95:158.

11 Finansdepartementets promemoria den 22 december 1994, Nytt ADB-stöd för indrivningsverksamheten, Fi94/2903, prop. 1994/95:168, bet. 1994/95:LU27 och rskr. 1994/95:305.

12 Prop. 1993/94:197.

Datastraffrättsutredningen, som i betänkandet Information och den nya InformationsTeknologin – straff- och processrättsliga frågor (SOU 1992:110), föreslagit en IT-anpassning av bl a reglerna om urkunder i 14 och 15 kap brottsbalken, har utarbetat följande definition av dokument.[13]

> Med dokument avses i detta kapitel [en skriftlig originalhandling eller] en bestämd mängd data för automatisk informationsbehandling, om det är möjligt att fastställa att innehållet härrör från den som framstår som utställare. [Som dokument anses också legitimationskort, biljett och dylikt bevismärke.]

Utredningen om elektroniska pengar har konstaterat att motsvarande författningsändringar behövs för e-pengar, men utan att lägga fram några författningsförslag.[14] Här bör också nämnas att det finns lagregler som baseras på att elektroniska handlingar används, utan något krav på "underskrift", trots att fråga är om en tillämpning där kraven på rätts- och informationssäkerhet är högt ställda.

Vid en ytlig granskning av de återgivna definitionerna kan de olika varianterna framstå som förvirrande och ge intryck av att det skulle vara fråga om helt olika dokumentbegrepp. I själva verket baseras de emellertid på samma grundläggande synsätt – att bäraren delvis mister sin betydelse och att det *fysiska* skyddet, genom att låsa text på t ex ett pappersark, ersätts av ett *logiskt* skydd för det mönster av elektroniska laddningar som representerar text och utställarangivelse. Genom denna anpassning kan moderna IT-rutiner användas på ett fungerande och kostnadseffektivt sätt, även på myndighetsområdet.

IT-utredningens förslag har den fördelen att terminologin – från bl a pedagogiska utgångspunkter – ger "verktyg" för att inom förvaltning och näringsliv beskriva vissa företeelser. Begreppet digital signatur används som beteckning på en "underskrift" av en viss *fysisk* person, medan digital stämpel betecknar en myndighets eller en juridisk persons utställarangivelse, när det skall anges att en handling verkligen härrör från myndigheten, utan att någon fysisk person pekas ut som utställaren. Datastraffrättsutredningens förslag innebär att det straffrättsliga skyddet för traditionella urkunder och IT-materialiseringar skulle integreras[15], och

[13] Se vidare SOU 1992:110 sid 285 f angående vad som bör anses utgöra straffrättsligt godtagbar kontrollerbarhet beträffande dokumenten.

[14] Se vidare SOU 1998:122 sid 77 ff.

[15] Detta är betydelsefullt om ett dokument delvis utgörs av ett traditionellt fysiskt föremål (t ex det som trycks utanpå SEIS kort, identitetsuppgifter, foto, etc), delvis av digitala data (t ex identitetsuppgifter lagrade i SEIS kort).

den föreslagna dokumentdefinitionen har inte begränsats till utställarangivelser som avser viss (vissa) fysisk eller juridisk person eller myndighet. Som exempel kan nämnas en virtuell organisation som skapar "signaturer" knutna endast till organisationen. Dessa, marginella, skillnader mellan de aktuella definitionerna slår knappast igenom vid behandlingen av nu aktuella frågor inom förvaltningen.

De återgivna förslagen till författningsändringar är även förenliga med ett förslag till EG-direktiv om elektroniska signaturer och de förslag som regeringen nu har lagt fram för att införa direktivet; se avsnitt 2.5.

2.2.4 Upptagningar enligt olika författningar

Anpassningen av grundlagarna till nya medier har föranlett delvis svårtillgängliga resonemang, där begreppet upptagning använts i olika betydelser. Detsamma gäller vissa regler till skydd mot manipulationer av upptagningar. Eftersom dessa bestämmelser tillkommit under en tid när signerade elektroniska handlingar inte var aktuella eller med sikte på att lösa andra typer av frågor kan de knappast ge vägledning för myndigheternas användning av elektroniska signaturer och dokument.

Frågan om ett handlingsbegrepp för IT-miljö uppkom tidigt i anknytning till bestämmelserna i 2 kap tryckfrihetsförordningen (TF) om allmänna handlingars offentlighet. I TF har begreppet handling definierats som framställning i skrift eller bild samt *upptagning* som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel. Angående frågan om handlingen enligt gällande rätt skall ses som en sak, något immateriellt eller ett mellanting kan följande noteras. I det utredningsförslag som låg till grund för införandet av begreppet *upptagning* anfördes att de nya reglerna bör ta sikte på ett konkret föremål motsvarande en handling, inte på själva informationen.[16] Till följd av svårigheterna att i IT-miljön finna ett sådant konkret föremål fick begreppet upptagning emellertid, enligt departementschefen, avse själva informationsinnehållet, "dvs den uppgift som har fixerats på det tekniska mediet".[17]

När definitionen av upptagning i 2 kap TF några år senare ändrades framträdde en ytterligare förskjutning mot ett abstrakt synsätt. Enligt lagmotiven avgränsar den fysiska databäraren – pappersarket, boken – på ett för det mesta självfallet sätt vad som är en handling i förhållande till en

[16] SOU 1972:47 sid 72.

[17] Prop. 1973:33 sid 75.

annan. Motsvarande hållpunkter för en avgränsning saknas i betydande omfattning för ADB-upptagningar.[18] Möjligheterna att utifrån lagrade data sammanställa olika på förhand avsedda eller icke avsedda uppgiftskonstellationer ställdes alltså i förgrunden. I senare lagstiftningsärenden har frågor om nya uppgiftskonstellationer som genom databehandling kan produceras på grundval av lagrade data, s k *potentiella* handlingar, föranlett delvis svårtillgängliga resonemang för den som inte är tekniker.[19]

Begreppet (teknisk) upptagning, som nyligen förts in i yttrandefrihetsgrundlagen (YGL), för att anpassa reglerna till vissa nya medier, synes dock i det sammanhanget kommit att avse informations*bäraren*.[20]

Dessutom har begreppet upptagning sedan år 1973 använts i 21 § datalagen – numera överförd till 4 kap 9 c § brottsbalken – och i 2 § patientjournallagen (1985:562) med sikte på ett av en *utställare slutligt bestämt* innehåll. Dataintrång bestående i att olovligen ha ändrat en upptagning kan naturligtvis inte avse en potentiell handling och journalhandlingens innehåll måste naturligtvis ha bestämts slutligt av läkaren; jfr avsnitt 2.2.5.

Slutligen bär vad som kommit till uttryck under lagstiftningsarbete i andra sammanhang en tydlig prägel av ett synsätt begränsat till traditionella pappershandlingar. Som exempel kan nämnas reglerna i delgivningslagen. Enligt 6 § skall handlingen överbringas i original eller styrkt kopia, dock att en kopia som har framställts vid en myndighet inte behöver bestyrkas.[21] En bestämmelse i 22 § om delgivning av annat än handlingar avser inte nya medier utan "föremål" såsom varuprover och modeller.[22]

Anpassningen av grundlagar till nya medier och av vissa regler om skydd mot manipulationer av handlingar har alltså föranlett delvis svårtillgängliga resonemang, där begreppet upptagning används i tre olika betydelser. Denna reglering har dock tillkommit vid en tid när signerade elektroniska handlingar inte var aktuella eller med sikte på att lösa frågor som inte har samband med elektroniska signaturer och elektronisk dokumenthantering.

Därför kan dessa regler knappast ge någon vägledning för hur den elektroniska ärende- och dokumenthanteringen bör utformas. Risken är uppenbar att de leder tanken fel, och det är därför de har berörts här.

[18] Prop. 1975/76:160 sid 90; jfr Seipel, ADB-upptagningars offentlighet, IRI-rapport 1988:1 sid 66 m fl och SOU 1992:110 sid 107 f.

[19] Se bl a prop. 1981/82:37 och sid 9, 27 och 29 samt prop. 1990/91:60 sid 21 ff.

[20] Prop. 1997/98:43 sid 155.

[21] Prop 1990/91:11 sid 45, jfr SOU 1996:40 sid 79.

[22] NJA II 1971 sid 51. Jfr distinktionen i RB mellan skriftliga bevis och s k syneobjekt som är av intresse till följd av någon yttre egenskap, inte på grund av att de genom text eller på liknande sätt förmedlar ett visst föreställningsinnehåll.

2.2.5 Löpande text, register m m

För att undvika misstag – t ex till följd av de beskrivna terminologiska bristerna – bör tydliga gränser dras mellan löpande text, register och tekniska uppteckningar.

För den som behöver sätta sig in i de rättsfrågor som uppkommer när en myndighet går över till elektronisk dokumenthantering är det viktigt att skilja mellan olika typer av elektroniskt lagrade uppgiftssamlingar

- löpande text,
- (egentliga) register, och
- tekniska uppteckningar.

Kännetecknande för *löpande text* är att den har "ställts ut" (av människa eller maskin) med ett bestämt innehåll;[23] t ex en ansökan eller ett beslut. Den som tar del av texten är intresserad av vem som har ställt ut den – något som närmast underförstått och självklart brukar framgå av *handlingen*.

Kännetecknande för (IT-baserade egentliga) *register* är istället att vissa (typer av) uppgifter har samlats och strukturerats så att de kan sammanställas till den information som behövs i det enskilda fallet; t ex olika möjligheter till uttag ur ett register över patientbesök vid en vårdinrättning eller ur bilregistret, där uppgifts*mottagaren* delvis bestämmer innehållet genom sitt val av sökbegrepp; s k potentiella handlingar.[24] Den enskilde är alltså – beträffande register – vanligtvis inte intresserad av en på förhand utställd/bestämd uppgiftskonstellation, såsom t ex vissa signerade journalanteckningar, utan riktar sitt intresse direkt mot vissa uppgifter som selekterats med hjälp av det automatiska systemet och ordnats på lämpligt sätt. Den tilltro till uppgifterna som den som tar del av ett register har, knyts till att informationssystemet fungerat korrekt och att lagrade uppgifter är riktiga och aktuella, vilket i hög grad är beroende av huruvida den som ansvarar för registret (oftast en myndighet eller juridisk person), tekniskt och administrativt har skött detta korrekt. Man kan diskutera vilka krav som bör ställas på skyddet av ett register i IT-miljö, vilket handlar om s k datakvalitet och kan vara beroende dels av åtgärder från många olika personer, dels av kvaliteten hos de tekniska procedurer som utnyttjas.

[23] Med "innehåll" menas här inte den tolkning som görs vid t ex en tvist om innebörden i ett skriftligt avtal utan det "objektiva" innehåll vissa tecken såsom bokstäver sammanställda till ord och meningar har.

[24] Angående skillnaden mellan löpande text och register, se prop.1997/98:44 sid 132, SOU 1997:39 sid 391, SOU 1996:40 sid 165 f och Datainspektionens rapport till regeringen den 1 mars 1999, Personuppgifter på Internet.

Men man kan också behöva ställa krav på skyddet av den information som tas fram hos eller lämnar den ansvariga organisationen. Härvid kan vissa gränsdragningsfrågor uppkomma. En utskrift från ett register, som kanske till och med signeras av en handläggare innan den lämnas ut, bör ses som löpande text.[25] Den som tar del av en sådan handling knyter sin tillit till en utställare och att uppgifterna oförändrade härrör från denne och den organisation han arbetar för.

I detta sammanhang bör också nämnas *tekniska uppteckningar* av tillstånd och förlopp; t ex EKG, EEG, färdskrivardiagram och röntgenbilder. Avgörande är därvid inte vem som är utställare av en viss text eller bild utan att uppteckningsförloppet fungerat riktigt och att uppgifterna om t ex vem registreringarna avser eller när något ägt rum är riktiga.

En myndighet som avser att införa elektronisk dokumenthantering kan undvika misstag genom att, på ett tidigt stadium, göra klart för sig vilka typer av uppgiftssamlingar som datoriseringen avser. Om de tekniska och administrativa skydden, redan när kravspecifikationer och liknande material utarbetas, anpassas till respektive objektkategori, kan de nya rutinerna smidigare anpassas till olika regelverk. Frågan är då vilket skydd som behövs i IT-miljön.

2.2.6 Behovet av skydd från rättsliga utgångspunkter

Samma skyddsbehov som har identifierats för traditionell miljö föreligger vid en övergång till elektronisk dokumenthantering. Som en följd av att elektroniska signaturer införs ersätts den osäkerhet som IT fört med sig av möjligheter att lösa frågor vid elektronisk dokumenthantering inom ramen för gällande rätt.

En central fråga är härvid vilket behov av skydd myndigheter och enskilda har mot missbruk av signerade elektroniska handlingar. Följande något förenklade sammanställning, som har gjorts i doktrinen långt innan datorer fanns, överensstämmer väl med dagens behov av skydd mot manipulationer i IT-miljö;

- att framställa ett oäkta dokument (t ex att skriva någon annans namn),
- att använda oäkta dokument (jfr att använda ett manipulerat certifikat),
- att förstöra ett äkta dokument (undertryckande av urkund),
- att ge ett äkta dokument ett osant innehåll,

[25] Jfr Datalagskommittén som i sitt förslag till ändringar i 2 kap TF gick så långt att en databas som passerar en myndighetsgräns sägs bli ett dokument.

- att missbruka ett äkta och sant dokument för att verifiera något som dokumentet inte skall visa; t ex att använda någon annans ID-kort eller signaturcertifikat och ge sig ut för att vara denne, och
- att, utan något materiellt angrepp, hindra ett äkta och sant dokument från att fylla sin funktion (t ex förnekande av underskrift/signatur).

Denna sammanställning visar att de principer som gäller för traditionell dokumenthantering passar också för de elektroniska motsvarigheterna. Det är emellertid oklart om elektroniska handlingar – oberoende av om de har försetts med elektroniska signaturer – kan vara att bedöma som urkunder i brottsbalkens mening.[26] Datastraffrättsutredningen har, som framgått, föreslagit författningsändringar för att säkerställa ett sådant skydd men förslaget har ännu inte föranlett lagstiftning.

Detta har dock, såvitt bekant, inte i något fall ansetts hindra ett införande av elektronisk dokumenthantering på myndighetsområdet.[27] I stället har det visat sig att elektroniska signaturer ger möjligheter att skapa enhetliga regler och rutiner för traditionell miljö och IT-miljö, så att skyddet för såväl det allmännas som enskildas intressen – med undantag för straff skyddet – har kunnat bibehållas.

Flera utredningar har funnit att existerande rättsprinciper bör tas tillvara och när så erfordras anpassas till den nya miljön, i stället för att skapa ett helt nytt regelverk, med de risker detta innebär för att vissa frågor blir bortglömda eller felaktigt bedömda. Det är därmed möjligt att redan inom ramen för gällande rätt finna lösningar på rättsfrågor som uppkommer vid en datorisering på myndighetsområdet.

2.2.7 Vidimering i IT-miljö

Även scannade pappershandlingar och elektroniska handlingar utan signatur, som kommer in till en myndighet via nät, kan skyddas med elektroniska signaturer. Detta kan ske genom elektronisk vidimering, på motsvarande sätt som det genom en vanlig underskrift intygas att en fotokopia överensstämmer med originalet. Även automatiska rutiner med elektroniska s k stämplar kan användas för att skydda elektroniska handlingar.

[26] Att gränsdragningen mellan falska resp. endast osanna urkunder — grundad på en bedömning av ett visst fysiskt originalexemplar — knappast kan tillämpas på elektroniska handlingar, har närmare utvecklats av Datastraffrättsutredningen, se vidare SOU 1992:110 sid 229 f, jfr sid 315.

[27] En annan sak är att bestämmelserna i varusmugglingslagen och skattebrottslagen har ändrats för att säkerställa deras tillämpning även i IT-miljö.

När pappershandlingar scannas eller uppgifter annars överförs mellan medier kan det vara av intresse att kunna få besked om vem som har utfört arbetet, t ex om materialets äkthet ifrågasätts. Därför upprättas ofta protokoll över vidtagna åtgärder.[28] En naturlig utveckling är härvid att, i analogi med vidimering av avskrifter och fotokopior, använda elektroniska signaturer, eventuellt i förening med en förklaring av den som vidimerar att uppgifterna i enlighet med använda kontrollrutiner har överförts oförändrade till den nya bäraren. Sådana rutiner kan också användas när elektroniska handlingar utan signatur tas emot via nät. Om handlingarna signeras så snart de når mottagaren kan det kontrolleras om data därefter har förvanskats.

Det är också möjligt att automatisera sådana rutiner, t ex så att e-post som kommer in till en myndighet genast förses med myndighetens elektroniska stämpel. Därigenom kan det konstateras om meddelandet – avsiktligt eller oavsiktligt – har ändrats efter att det kom till myndigheten.

2.3 SIGNATUREN

Frågan om elektroniska dokument och andra ersättare för traditionella pappershandlingar har på senare tid fått stå tillbaka för det intensiva internationella arbetet rörande elektroniska signaturer. Frågan är då vad en elektronisk signatur är och vilka frågor sådana tillämpningar aktualiserar.

2.3.1 Den traditionella underskriftens funktioner

En underskrift med bläck ger skydd mot manipulationer. Underskriften låses vid pappersarket med dess text, eventuellt i förening med stämplar, vidimering etc. I vissa fall finns krav i författningsregleringen på att en handling skall vara undertecknad. I andra sammanhang kan det vara självklart att en rättshandling skrivs under.

Underskriften *identifierar* den som undertecknar och ger tillit till att viss text omanipulerat härrör från den som framstår som utställare (äkthetsfunktionen). Underskriften fyller också en *bevisfunktion* tillsammans med uppgifterna i den undertecknade handlingen. Den som undertecknat, knyts vanligtvis på ett säkert sätt till innehållet, och underskriften ger uttryck för en vilja att bekräfta och binda sig vid den undertecknade texten.

[28] Detta är också förenligt med Riksarkivets krav på överföring för långtidslagring av IT-material, där det sägs att en överföring till annan databärare skall dokumenteras. Det skall även dokumenteras vilken operatör som har gjort överföringen (RA-FS 1994:2, 5 kap 1 § och 3 kap 6 §).

Underskriften har vidare en *avslutsfunktion* och en *varningsfunktion*. Den som undertecknar ger uttryck för att den text som underskriften avser har fått sin slutliga utformning och den som skall skriva sitt namn blir medveten om att åtgärden kan medföra rättsliga förpliktelser. Underskrifter kan även fylla andra funktioner.

2.3.2 Elektroniska signaturer

Elektroniska signaturer kan vara av många olika slag; från att t ex skriva sitt namn på tangentbordet och därmed under texten i ett ordbehandlingsdokument, till avancerade kryptografiska metoder som skapar ett synnerligen säkert bevis för att utställarangivelsen är äkta. Sådana säkra kryptografiska bevis innefattar ett skydd för data som har signerats och som representerar texten. Ändras texten framgår detta när signaturen verifieras.

I praktiken litar vi emellertid ofta på t ex den signatur som återges i ett mottaget faxmeddelande, trots att det är enkelt att med stöd av IT foga en sådan "underskrift" till vilken text som helst efter att ha kopierat den elektroniska bilden av underskriften.[29] Vid sådan kommunikation behöver det alltså inte finnas något pappersbaserat original som avbildats. Faxmeddelandet kan ha skapats direkt i avsändarens dator och försetts med en scannad bild av avsändarens underskrift. På motsvarande sätt kan mottagaren läsa faxet direkt på sin skärm och bevara det endast elektroniskt.

För att ersätta dessa lättmanipulerade rutiner har säkra tekniska motsvarigheter till underskrifter tillskapats, baserade på kryptografi. Sådana, med en teknisk term kallade "digitala signaturer", skiljer sig i väsentliga avseenden från den traditionella namnteckningen. Enligt en standardiserad definition är digital signatur *"data* appended *to, or a cryptographic transformation of, a data unit that allows the recipient of that data to prove the source and integrity of the data unit. It protects against forgery, even by the recipient"* (ISO 7498-2); jfr följande definition i en skrift från Statskontoret *"omvandling av ett meddelande (eller ett kondensat av detta) på ett sätt som endast avsändaren kan utföra och som låter mottagaren kontrollera meddelandets äkthet, innehåll och avsändarens identitet"*.[30]

[29] Jfr hur domstolsutredningen föreslog att ett telefaxmeddelande skulle godtas som egenhändigt undertecknat enligt rättegångsbalken, om det "avsänts från en telefon med nummer som kan hänföras till någon som undertecknat meddelandet" (SOU 1991:106); ett förslag som inte föranlett lagstiftning sedan det klargjorts att avsändaren kan ställa in sin fax så att den anger vilket avsändarnummer som helst och enkelt kan manipulera med digitaliserade underskrifter.

[30] Statskontorets rapport 1997:18 "Svenska delen av Internet", Stockholm oktober 1997.

Den grundläggande principen för framställning av en digital signatur är att data, som representerar t ex en text databehandlas med en krypteringsalgoritm (en matematisk beräkningsregel) i förening med en personlig nyckel, unik för den individ som skall utföra signeringen. Resultatet av denna beräkning blir ett kontrolltal, som är unikt för denna händelse, och som vanligtvis kan kontrolleras av någon annan, utan att signatärens personliga nyckel behöver röjas eller annars göras tillgänglig så att den riskerar att komma till obehörigas kännedom.

Den digitala signaturen består alltså inte av undertecknarens namn utan av en serie "meningslösa" siffror som är en unik funktion av både datainnehåll och signatärens identitet. Knytningen av signaturen till individen sker genom en för varje person eller organisation unik kryptonyckel, som skall hemlighållas, till skillnad från traditionella underskrifter, som skyddas mot missbruk genom att de är fysiskt knutna till en enda individ genom dennes unika sätt att skriva sitt namn. I praktiken krävs datorkapacitet för att kunna verifiera den elektroniska signaturen, även om den i och för sig också kan skrivas ut på papper. En sådan signatur kan produceras på flera olika sätt. Metoderna bygger på en omvandling av den digitala representationen av texten efter en i förväg bestämd metod, en algoritm.

Man brukar skilja på symmetrisk och asymmetrisk kryptering. Den symmetriska tekniken baseras på att utställaren av text med signatur – dvs en signerad handling – och den som skall verifiera handlingen använder samma nyckel för kryptering och dekryptering. Nyckeln kan alltså inte hållas hemlig för den som skall verifiera och denne kan därmed missbruka nyckeln genom att signera. Kommunikation många till många med sådan teknik är därför knappast lämplig; nyckelhanteringen fungerar inte. I stället används s k asymmetrisk kryptering, vilket innebär att två skilda nycklar används – en privat och en publik. Nycklarna är matematiskt relaterade till varandra så att ett krypterat meddelande inte kan dekrypteras med samma nyckel i nyckelparet och så att den ena nyckeln inte med rimliga insatser kan beräknas utifrån den andra. Därmed förenklas administrationen av nycklarna avsevärt. Den publika nyckeln görs allmänt tillgänglig för dem som skall verifiera handlingar upprättade av den som tilldelats nyckelparet, medan den privata nyckeln skyddas.

Det är endast signaturer som är baserade på asymmetriska, även kallade publika, nyckelsystem som betecknas "digital" signatur, medan begreppet "elektronisk" signatur brukar anses inrymma alla tänkbara varianter, från de mest avancerade kryptografiska skydden till att på tangentbordet skriva sitt namn under en ordbehandlingstext.

De asymmetriska rutinerna – för "digital" signatur – kan något förenklat beskrivas enligt följande.

Som ett *första steg* skapar användaren den dataenhet som skall signeras, dvs ett exakt definierat informationsobjekt i digital form. Detta kan vara ett textdokument, en programvara eller vilken annan digitalt representerad information som helst. Ett *andra steg* innebär att användaren skapar ett s k hashvärde, ofta kallat ett "fingeravtryck" av meddelandet, vilket är resultatet av en matematisk process som baseras på dataenheten och en algoritm som skapar en komprimerad digital representation. Om dataenheten ändras kommer hashvärdet inte längre att motsvara dessa data. Denna teknik gör det möjligt att använda programvaran på små och förutsägbara datamängder. Som ett *tredje steg* krypterar avsändaren hashvärdet med sin privata nyckel. Kontrollsumman *(den digitala signaturen),* som är unik för både dataenheten och den privata nyckel som har använts för att skapa den, bifogas eller biläggas dataenheten. Som ett *sista steg* verifierar mottagaren den digitala signaturen genom att generera hashvärdet på basis av samma dataenhet och med samma algoritm. Detta hashvärde jämförs med det tal som blir resultatet när den digitala signatur som bifogats dataenheten "dekrypteras" med signatärens publika signaturnyckel. Är resultatet identiskt visar detta att det är den angivne användarens privata nyckel som har använts för att signera och att dataenheten inte har ändrats. En elektronisk signatur hindrar alltså inte att avsiktliga eller oavsiktliga ändringar görs i en signerad handling. Den gör det istället möjligt att upptäcka om något sådant har inträffat.

De skillnader som finns mellan traditionella underskrifter och digitala signaturer kan härvid förenklat sammanställas enligt följande.

Traditionella signaturer	Digitala signaturer
1. Skrivs på ett självklart sätt.	1. Bygger på kryptografi och innehavet av en hemlighet – en "nyckel".
2. Förmågan att underteckna är medfödd och dessa egenskaper – "skrivdonet" – kan inte komma på avvägar.	2. Användaren brukar en "nyckel". Var och en som har tillgång till den kan signera. Det finns därmed ett uppenbart behov av att skydda dessa nycklar.
3. En traditionell signatur undersöks vanligtvis inte närmare förrän någon bestrider att den är äkta. Materialet för att analysera signaturen samlas in i efterhand av experter.	3. Var och en som tar emot ett digitalt signerat dokument behöver kunna verifiera dess autenticitet. Materialet härför samlas in på förhand samt bevaras och hålls tillgängligt för läsarna. Därmed uppkommer ett behov av en ny infrastruktur.
4. Av erfarenhet vet vi att det är möjligt att lära sig att skriva en annan persons signatur så att andra än experter lätt vilseleds.	4. Det är i princip omöjligt att återskapa en annan persons digitala signatur utan att känna till den privata nyckeln. Denna nyckel måste skyddas mot obehörig åtkomst.
5. Procedurerna bygger på en allmän tillit till egenhändiga underskrifter. I vissa fall finns emellertid särskilda rutiner för att verifiera att en underskrift är äkta; t ex vidimering.	5. Det är avgörande, när en publik nyckel skall användas för verifiering av en digital signatur, att det går att lita på och att denna nyckel tillhör den person som framstår som utställare. Detta tillgodoses genom nyckel-certifikat. Särskilda subjekt – s k CSP, även benämnda CA – tillskapas för att uppnå tilltro till de procedurer där innehavaren av en nyckel identifieras.

Det är alltså helt avgörande att den som verifierar en signatur kan lita på att den publika nyckeln och den därtill relaterade privata nyckeln verkligen tillhör angiven person och att den privata nyckeln inte har kommit till obehörigas kännedom eller annars kunnat missbrukas. Från tekniska utgångspunkter kan dessa rutiner göras mycket säkra. Om de administrativa arrangemangen brister raseras emellertid hela informationssäkerheten eftersom det "elektroniska skrivdonet" kan komma på avvägar.

Den uppdelning som gjorts mellan dokument och signaturer, där det internationella arbetet begränsats till de elektroniska signaturerna, är delvis artificiell. En digital signatur måste skapas på grundval av något, data som representerar t ex en text eller en grafisk framställning. Den digitala signaturen kan alltså inte finnas "ensam"; jfr hur en underskrift på ett blankt papper knappast kan tjäna till annat än möjligen råmaterial för t ex en förfalskning.

2.4 PUBLIKA NYCKELSYSTEM

En användning av elektroniska signaturer "alla till alla" aktualiserar frågor om vilken infrastruktur som behövs för att säkerställa den grundläggande uppgiften om vem ett nyckelpar tillhör. Dessa frågor berörs i ett förslag till EG-direktiv om elektroniska signaturer och i en departementspromemoria om hur direktivet bör införas i svensk rätt.

2.4.1 Certifikat, CSP och PKI m m

För att säkerställa att den grundläggande uppgiften, om vem ett nyckelpar tillhör, är riktig behövs en helt ny infrastruktur för publika nyckelsystem – med en engelsk term, en Public Key Infrastructure (PKI), där s k certifikat utgör en viktig pusselbit. Certifikaten kan jämföras med traditionella ID-handlingar. Till följd av standardiserade och väl fungerande rutiner har en allmän tillit vuxit fram till att den person som överensstämmer med kännetecknen på en ID-handling har den identitet som framgår av handlingen. Att ID-handlingen har utfärdats i enlighet med de säkerhetsåtgärder som standarden kräver framgår av märkning (s k SIS-märke). ID-handlingar som försetts med SIS-märke har kommit att åtnjuta ett allmänt förtroende och har därigenom öppnat vägar för ett säkrare utbyte av varor och tjänster.

I IT-miljön motsvaras ID-handlingen av ett nyckelcertifikat, som är ett (signerat) elektroniskt dokument, som fyller motsvarande funktion som en fysisk ID-handling. En trovärdig part – en s k Certification Service Provider (CSP) även kallad Certification Authority (CA) – lämnar vissa uppgifter i elektronisk form om individen och signerar dessa; jfr hur informationen i en fysisk ID-handlingen säkras genom att den framställs på ett svårförfalskat sätt. Syftet är att aktörerna skall kunna lita på att en viss privat nyckel verkligen innehas av den som påstås vara innehavare.[31] Det är här som certifikat, kataloger för certifikat och anknytande rutiner för att generera certifikat kommer in.

En viktig fråga är härvid hur den privata nyckel som korresponderar med den publika skall kunna skyddas. Den privata nyckeln får, varken när den genereras eller senare när den förvaras av användaren, komma till någon obehörigs kännedom. Många förordar att den skall förvaras i ett chip på ett traditionellt ID-kort.[32]

[31] Traditionella identitetsattribut som t ex utseende, fingeravtryck och handstil ersätts alltså med innehav av de publika och privata nycklarna. Medan innehavaren föds med de traditionella attributen så att de inte kan "komma på avvägar", kan en privat nyckel dock användas (missbrukas) av var och en som får tillgång till den och i praktiken kan det ofta vara svårt att skilja en autentisk transaktion från en som har producerats av en obehörig.

[32] Se vidare http://www.seis.se.

Slutligen behövs funktioner för att verifiera att en viss privat nyckel var giltig vid den tidpunkt den användes. För detta ändamål används spärrlistor m m. Följande aktörer kan därmed identifieras.[33]

- **CSP/CA** – dvs utfärdare av certifikat.
- **Användare** – dvs innehavaren av den privata nyckel som korresponderar med den publika nyckeln i det utfärdade certifikatet.
- **Förlitande part** – dvs den som förlitar sig på certifikatet, exempelvis för att verifiera en digital signatur, eller för att säkerställa att bara rätt mottagare kan läsa ett meddelande.
- **"Registration authority"** (RA) som identifierar individer för CA:s räkning.

Det bör noteras att CSP och RA ofta kan vara samma subjekt, t ex en myndighet eller en bank. Systemen har hittills vidare vanligtvis varit slutna så att samma subjekt också varit "förlitande part", t ex tullen för elektroniska tulldeklarationer. I sådana fall föreligger inte något *publikt* nyckelsystem.

2.4.2 Certifikatpolicy och CPS

En förutsättning för att system för publika nycklar och elektroniska signaturer skall kunna fylla motsvarande funktioner som en egenhändig underskrift är att allmänhetens behov av att kunna lita på dem säkerställs. Det är detta skyddsintresse som ligger bakom kriminaliseringen av brotten mot urkunder. I traditionell miljö har detta skydd i förening med fungerande rutiner för kriminalteknisk analys av underskrifter m m vanligtvis erbjudit ett tillräckligt skydd för att urkunden skall kunna fylla sina funktioner. I vissa fall har rutinerna dock förenats med särskilda krav på bl a papperskvalitet, bläck, färgband etc eller på t ex vidimering av underskrifter, arkivering hos en myndighet eller kungörelse i någon form.

När kraven på juridisk, finansiell, administrativ och teknisk säkerhet ställs högt vidtas särskilda åtgärder för att säkerställa allmänhetens förtroende. Huvuddelen av den finansiella tjänsteproduktionen har ansetts kräva reglering och tillsyn av det allmänna. På motsvarande sätt kommer publika nyckelsystem att användas för betydelsefulla funktioner, bl a för att signera affärsdokument och inlagor till myndigheter, förfoga över

[33] Det finns även andra aktörer och en mängd olika termer för att beteckna dessa. De individer som CA tilldelar ett certifikat kallas för "subscriber". Som synonymer förekommer begreppen "subject end entity" eller bara "subject" eller "key holder". Den som får del av ett certifikat och fäster tilltro till uppgifterna i certifikatet kallas "relying party" eller "certificate user". Alla dessa aktörer brukar i den litteratur som förekommer på området kallas "entities". Om CA och RA undantas, brukar de övriga samlas under beteckningen "end entity", vilken i sin tur delas in i "subscriber", dvs den som har tilldelats ett certifikat, och "relying party", dvs den som litar på ett certifikat.

medel på konton och identifiera användare, system och resurser i öppna system. Publika nyckelsystem kommer alltså, om de får spridning, att innefatta betydande och legitima samhälleliga skyddsintressen.

Därför behövs det en *policy* (s k certifikatpolicy) och en *praxis* (s k Certification Practice Statement; CPS) för utfärdande av certifikat. Meningen är att det av policydokumentet i princip skall kunna utläsas hur hög trovärdighet certifikat utfärdade i enlighet med policyn bör anses ha och att det av praxisdokumement skall kunna utläsas vilka närmare rutiner som tillämpas inom ramen för den angivna policyn.[34]

Inget hindrar att samma person tilldelas flera certifikat, avsedda för olika ändamål och med olika skyddsnivåer. För betalningar till t ex kaffekassan kan ett certifikat förvarat på användarens hårddisk, som tilldelas med någon enkel rutin, kanske via nät, anses tillräckligt. För signering av t ex finansiella transaktioner eller betydelsefulla myndighetsbeslut kan däremot noggrann identifiering och användning av chipkort etc ofta ses som ett krav.

En anknytande fråga är om olika CSP skall godta varandra och om en myndighet som driver en sådan tjänst eller är ansluten till en viss tjänst skall godta certifikat som är utfärdade av en annan CSP. Det förekommer att två CSP genom att korscertifiera varandra anger att bådas certifikat bör kunna godtas.

2.5 EG-DIREKTIV OCH DEN SVENSKA ANPASSNINGEN

2.5.1 EG-direktivet om elektroniska signaturer

Europaparlamentets och rådets direktiv om ett gemenskapsramverk för elektroniska signaturer (signaturdirektivet) antogs den 30 november 1999. I direktivet ges bl a en reglering av organ som avser att erbjuda certifikattjänster.[35]

Syftet med direktivet är att underlätta användningen av elektroniska signaturer och att bidra till deras rättsliga erkännande genom att fastställa ett rättsligt ramverk för sådana signaturer och anknytande certifikattjänster. Från direktivets tillämpningsområde undantas emellertid frågor som avser ingående eller giltighet av avtal eller andra rättsliga förpliktelser, om den nationella lagstiftningen eller gemenskapslagstiftningen föreskriver vissa formkrav, och direktivet avses inte heller påverka bestämmelser och begränsningar i nationell lagstiftning eller gemenskapslagstiftning som

[34] Viktiga delar härav kan vara att bl a ange regler för utlämning och förvaring av den privata nyckeln samt, om chipkort används, krav på chip-kvalitet, utlämning, PIN-hantering, låsning, upplåsning och aktivering.

[35] Jfr http://europa.eu.int/eur-lex/sv/com/dat/1999/sv599PC195.html.

reglerar användningen av dokument. Direktivet kan därför – utöver frågor om terminologi, skadeståndsansvar för vissa CSP och tillsyn m m – antas få endast begränsad betydelse för de frågor om dokumenthantering som behandlas här.[36]

2.5.2 Genomförandet av signaturdirektivet

I departementspromemorian Elektroniska signaturer (Ds 1999:73) föreslås en lag om vissa sådana signaturer, i syfte att genomföra EG-direktivet. Förslaget innehåller, utöver bestämmelser om vissa elektroniska signaturer, föreskrifter om certifikat för elektroniska signaturer och säkra anordningar för signaturframställning samt om utfärdande av s k kvalificerade certifikat. Till detta kommer anknytande bestämmelser om skadeståndsskyldighet för certifikatutfärdare, behandling av personuppgifter, tillsyn och avgifter för tillsynen.

För de frågor om dokumenthantering som behandlas här kan förslaget främst antas få betydelse som en drivfjäder för den fortsatta utvecklingen. Förslaget innehåller emellertid också följande definitioner och en bestämmelse om "rättslig verkan" för elektroniska signaturer.

2 § I lagen avses med

elektronisk handling: en bestämd mängd data i digital form som kan läsas, avlyssnas eller på annat sätt uppfattas med tekniskt hjälpmedel,

elektronisk signatur: data i elektronisk form som är fogade till eller logiskt knutna till en elektronisk handling och som används för att kontrollera om innehållet härrör från den som framstår som undertecknare,

avancerad elektronisk signatur: en elektronisk signatur som
a) är knuten uteslutande till undertecknaren,
b) undertecknaren kan identifieras genom,
c) är skapad med medel som endast undertecknaren kontrollerar, och
d) är knuten till en elektronisk handling på ett sådant sätt att alla efterföljande ändringar av den elektroniska handlingen kan upptäckas,

kvalificerad elektronisk signatur: en avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat och som är skapad av en säker anordning för signaturframställning,

undertecknare: den som har kontroll över en anordning för signaturframställning,

[36] Jfr p 3 i rutan närmast efter rubriken till avsnitt 3.2.

signaturframställningsdata: unika data, såsom koder eller privata krypteringsnycklar, som undertecknaren använder för att skapa en elektronisk signatur,

anordning för signaturframställning: en konfigurerad maskin- eller programvara för att använda signaturframställningsdata,

signaturverifieringsdata: data, såsom koder eller öppna krypteringsnycklar, som används för att verifiera en elektronisk signatur,

certifikat: ett intyg i elektronisk form som kopplar ihop signaturverifieringsdata med en undertecknare och bekräftar dennes identitet,

certifikatutfärdare: den som utfärdar certifikat.

De föreslagna definitionerna kan, om de genomförs, antas få stor betydelse för den framtida terminologin på området. Som framgår av förslagets definitioner av bl a elektronisk handling och elektronisk signatur är den principiella utgångspunkten densamma som i redan genomförda och föreslagna svenska regler på området; se vidare avsnitt 2.2.3 ovan och Ds 1999:73 sid 58 ff och 106 ff Begreppet elektroniskt dokument, som beteckning på *signerade* data, torde dock få ersättas av uttrycket signerad elektronisk handling eller något liknande, som en anpassning till den nya terminologin, och den hittillsvarande användningen av begreppet digital (inte elektronisk) med sikte på säkra rutiner torde få utgå.

Bestämmelsen i 16 § förslaget är också av intresse i detta sammanhang. Där föreskrivs att "om det av lag eller annan författning följer vissa formkrav för att en rättshandling skall anses giltig eller en förpliktelse fullgjord och om dessa krav kan uppfyllas genom elektronisk kommunikation med användning av någon form av elektronisk signatur, skall en kvalificerad elektronisk signatur godtas." Läsaren bör dock iaktta viss försiktighet vid tolkningen eftersom det – trots bestämmelsens ordalydelse – uttalas i specialmotiveringen (s. 116) att bestämmelsen inte påverkar krav i lag eller annan författning som utesluter användning av elektroniska rutiner, oavsett hur detta har kommit till uttryck.

Eftersom departementspromemorian nu är föremål för remissbehandling kommenteras förslagen inte närmare här.

2.6 SKYDDET MOT OBEHÖRIG INSYN

Frågan om insynsskydd är intimt förknippad med digitala signaturer eftersom samma kryptografiska rutiner som används för att signera kan användas för att göra data oläsbara för den som inte har tillgång till nyckeln för att dekryptera. Detta aktualiserar motstående intressen av skydd mot insyn respektive åtkomst till information vid t ex brottsutredningar; se vidare Regeringens skrivelse 1998/99:116 om kryptografi.

2.7 ARKIVERING I IT-MILJÖ

2.7.1 Avgränsning och organisation

Allmänna bestämmelser om myndigheternas arkiv finns i arkivlagen (1990:782) och arkivförordningen (1991:446). För att tillgodose arkivlagens syften har Riksarkivet utfärdat verkställighetsföreskrifter.[37] De regler som rör IT-området återfinns främst i Riksarkivets allmänna regler om arkiv hos statliga myndigheter (RA-FS 1991:1, ändrad genom RA-FS 1997:4) och i reglerna om ADB-upptagningar (RA-FS 1994:2 och 1994:7, ändrad genom RA-FS 1997:7). Där framgår bl a att handlingar som tillhör en myndighets arkiv redan från början skall kunna skiljas från sådana handlingar som tillhör andra myndigheters och enskildas arkiv – något som får särskild aktualitet i dagens myndighetsöverskridande handläggningsprocesser. Vidare sägs att handlingar, som tillkommit under handläggningen av ett ärende eller under en annan avgränsad process, skall kunna presenteras samlat. I IT-miljön innebär detta bl a att varje handling i ett ärende måste ges en identitet som möjliggör att handlingarna i ärendet kan hållas samman och bilda någon form av "elektronisk akt". Arkivet skall ges en struktur som befrämjar tillgänglighet och återsökning av handlingar och som bidrar till att skydda handlingarna mot obehörig åtkomst. När det gäller IT kan det handla om att redan från början klassificera och vid behov "märka" handlingar som omfattas av sekretess eller som på annat sätt kräver särskilda åtgärder från säkerhetssynpunkt, t ex för att säkerställa handlingarnas äkthet.

Man kan tycka att frågor av detta slag, som egentligen rör "ordning och reda", inte skulle behöva författningsregleras. Erfarenheten har emellertid visat att rutiner och åtgärder som tidigare kunde förefalla självklara inte automatiskt får sin motsvarighet i dagens förvaltning som kännetecknas av upprepade omstruktureringar och en försvagad ämbetsmannatradition. Tendensen har förstärkts genom den kraftigt ökade IT-användningen. I pappersmiljön fanns det i allmänhet en möjlighet att i efterhand ordna upp handlingar som kommit i oordning – något som till och med har

[37] Riksarkivet föreskriver för statliga myndigheter. För kommunala och landstingskommunala myndigheter utfärdas endast allmänna råd.

kunnat ske efter det att myndigheten upphört och handlingarna levererats till arkivmyndigheten. I IT-miljön måste allt göras rätt från början, vilket förstärker behovet av klara riktlinjer. Om arkivfrågorna beaktas på ett tidigt stadium i hanteringen kan myndighetens arbete förenklas avsevärt. Exempelvis bör följande frågor besvaras redan i systemutvecklingsfasen:

- Hur skall inkommande och utgående elektroniska handlingar tas emot/expedieras och lagras?
- Hur bör ärenden och motsvarande processer avgränsas hos myndigheten?
- Hur skall handlingarna registreras och märkas på lämpligt sätt?
- Vilka krav skall ställas på struktur och sökbarhet när det gäller handlingar som hålls ordnade på annat sätt?
- Hur skall sambanden mellan elektroniska handlingar och sådana som upprättas i pappersform upprätthållas?
- Hur skall handlingar som tillhör ett ärende eller motsvarande kunna presenteras samlat även på längre sikt? Hur arkiveras tjänsteanteckningar och sammanställningar ur databaser? Är det möjligt att skapa elektroniska akter?
- Hur skall de elektroniska handlingarna skyddas mot förvanskning – i kommunikationsfasen och under långtidslagringen?

En akt kan beskrivas som ett eller flera dokument som tillhör en och samma ärendeprocess. I IT-miljön finns naturligtvis inte de pappersomslag och lådor som man använder för att hålla samman och förvara handlingar i den traditionella miljön. Det är inte heller av intresse var handlingarna förvaras fysiskt när de har elektronisk form (jfr outsourcing av databehandlingen). Avgörande är istället att de elektroniska handlingarna i oförvanskat skick vid behov kan verifieras och presenteras för handläggare och andra som skall ta del av dem och att de kan hänföras till rätt elektronisk akt så att kraven på struktur upprätthålls.

Även andra föreskrifter än de nämnda arkivreglerna kan sägas röra "ordning och reda". En sådan inriktning har bl a reglerna om "god offentlighetsstruktur" i 15 kap sekretesslagen. Dessa ordningsregler utgör inget hinder mot att införa elektronisk dokumenthantering m m. Regelverken kan emellertid behöva samordnas och vissa bestämmelser ersättas av regler som har anpassats till dagens IT-användning. Sådana frågor övervägs nu av kommittén (Ju 1999:06) om offentlighetsprincipen och IT samt översyn av sekretesslagen m m.

2.7.2 Bevarande och gallring

När elektroniska signaturer och anknytande tjänster för informationssäkerhet införs behöver det övervägas hur långtidslagringen av handlingar bör utformas för att äkthetsprövning av signerat material och omvandling till klartext av krypterat material skall kunna ske med bibehållen säkerhet under hela bevarandetiden.

Riksarkivets föreskrifter innehåller bl a en definition av begreppet gallring, enligt vilken all förstöring av allmänna handlingar och uppgifter i allmänna handlingar utgör gallring. Detta gäller även om data dessförinnan har överförts till en ny databärare, om överföringen medfört förlust av information, sökmöjligheter, sammanställningsmöjligheter eller av möjligheter att fastställa en handlings autenticitet. Sådana åtgärder får inte vidtas utan särskilt beslut som har stöd i lag förordning eller myndighetsföreskrifter.

Vid IT-baserad lagring ersätts den fysiska ordningen och den därtill knutna bevaringen delvis av logiska samband och – på sikt – överföringar till nya databärare, t ex från hårddisk till bandkassett, från papper till optisk skiva etc. Detta skapar nya möjligheter till effektiv lagring och åtkomst samtidigt som rutiner och kontroller i samband med överföringen blir avgörande för om läsbarhet och övriga kvaliteter hos handlingarna skall kunna bevaras. För att minimera förlusterna av läslighet vid överföringar mellan medier har särskilda krav införts på sådana rutiner. Arkivförfattningarna hindrar alltså inte elektroniska rutiner. Frågan blir istället hur vissa närmast självklara krav på bevaring, läsbarhet och autenticitet skall kunna uppfyllas på sikt inom ramen för en modern IT-användning, utan att utvecklingen av nya rutiner hindras.

En anknytande fråga har samband med att det blivit vanligt att disketter och andra databärare ges in till myndigheter. Frågan är då om själva bäraren med data bör bevaras eller om data skall läsas över till myndighetens databärare. En överföring mellan databärare innebär vanligtvis försumbara risker för fel och efter överföringen bör de ursprungliga handlingarna/databärarna kunna gallras i enlighet med Riksarkivets föreskrifter och allmänna råd om gallring av handlingar av tillfällig eller ringa betydelse.[38] Byte av medium kan dock leda till sådana informationsförlus-

[38] Ett sådant synsätt torde tillämpas också beträffande räkenskapsmaterial enligt 10 § första stycket 3 bokföringslagen (1976:125). Enligt 7 kap 1 och 6 §§ den nya bokföringslagen (1999:1078), som träder i kraft den 1 januari 2000, synes däremot en skyldighet föreskrivas att bevara vissa databärare – med de komplikationer detta uppenbarligen kan föra med sig inom ramen för sådana rutiner som numera är gängse inom företag och myndigheter.

ter att särskilda gallringsföreskrifter krävs. Medgivande till gallring av ursprungshandlingarna efter överföring knyts till krav på kompenserande åtgärder vid överföringen. Det kan t ex gälla krav på upprättande av sökingångar till de överförda handlingarna eller vidimering och stämpling av handlingarna efter kvalitetskontroll. Krav av detta slag ingår i Riksarkivets mediespecifika regler.

Från praktisk utgångspunkt är det svårt att motivera att alla de databärare som ges in med skilda format, teckenrepresentationer, etc skall bevaras. En myndighet kan knappast ha alla de hård- och mjukvaror tillgängliga som behövs för att kunna göra samtliga mottagna databärare läsbara och huvuddelen av de databärare som ges in är inte lämpliga för lagring av data under någon längre tid. Dessutom är det utrymmeskrävande att bevara alla databärare. Det traditionella synsättet, att det ingivna originalet bör bevaras, har som framgått inte sådan bärkraft i IT-miljön att säkerheten bör knytas till ett visst fysiskt föremål. Argumenten för att bevara ingivna databärare blir ännu svagare när det beaktas hur disketter och andra datamedier sänds med post och i övrigt förvaras under sådana former att man inte kan bortse från risken för manipulationer. På sikt torde det bli självklart att lagringen sker på myndighetens databärare genom att handlingarna sänds in via nät och förses med elektroniska signaturer. Den närmare utformningen av rutinerna får avgöras från fall till fall med utgångspunkt från att mottagna elektroniska handlingar skall bevaras säkert och med en sådan struktur att rättskipningens, förvaltningens och forskningens behov samt enskildas rätt att ta del av handlingar tillgodoses.

Samtidigt blir frågan om långtidslagring mer komplicerad när elektroniska signaturer införs. Signeringen baseras på mönster av laddningar, varför en konvertering av ett dokument – t ex för att göra det läsbart med en ny programvara (t ex WP 6 i stället för WP 5) – leder till att signaturen förstörs. Härvid kan olika tillvägagångssätt övervägas. En metod är att göra datalagringen så oberoende som möjligt av hård- och mjukvaror. Därmed inskränks emellertid möjligheterna att använda mer komplexa funktioner såsom digitala signaturer och kryptering. Vidare ökar behovet av systemdokumentation och annat material *utanför dokumentet,* där vissa förutsättningar anges för förståelsen av lagrade data. Motsatt metod, att bevara signaturer och (all) relevant information *inom dokumentet,* leder till komplicerade datastrukturer som knappast är kompatibla med nya versioner av datorprogram. En användning av sådana dokument förutsätter alltså noggranna överväganden rörande använda rutiner för att de skall kunna läsas på sikt. På senare år har visserligen många myndigheter och företag ifrågasatt de återkommande uppgraderingarna av pro-

grammen men hårdvarorna måste i vart fall bytas med vissa mellanrum och den tekniska utvecklingen bör inte hindras. Något tillspetsat kan alltså å ena sidan hävdas att säkra dokumentrutiner baserade på signering och andra tekniska skydd för signalmönstren blir sårbara på sikt, medan det å andra sidan kan hävdas att enkla rutiner, som är lämpliga för långtidslagring, knappast ger erforderligt tekniskt och rättsligt skydd för dokumenten under den tid dokumenten främst brukar användas. Myndigheterna behöver härvid närmare överväga hur de skall kunna hantera privata signaturnycklar och krypteringsnycklar och hur de bör möta matematiska framsteg eller andra förändringar som kan göra det möjligt att forcera de tekniska säkerhetsrutinerna. Det är knappast lämpligt eller ens möjligt att lagreglera sådana tekniska och snabbt föränderliga förutsättningar.

3 PRAKTISKA OCH RÄTTSLIGA GRÄNSDRAGNINGSFRÅGOR

3.1 ABSOLUT SÄKERHET ELLER INGET SKYDD ALLS?

Tekniska skydd baserade på kryptografi kan ge en hög säkerhet vid ärendehandläggning och kommunikation i IT-miljö. De tillämpningar som i praktiken har införts på myndighetsområdet – bl a för elektronisk post – är dock helt oskyddade. Myndigheternas överväganden för att skapa äkthets- och insynsskydd synes härvid ofta vara inriktade på att i ett sammanhang införa rutiner för en närmast hundraprocentig säkerhet. Resultatet blir komplext och tids- och kostnadskrävande. Alternativa lösningar bör tas tillvara redan nu, så att behoven av effektivitet och säkerhet kan balanseras. På sikt bör elektroniska signaturer och anknytande säkerhetstjänster emellertid införas på bred front. Därigenom underlättas tillämpning av gällande rätt vid elektronisk dokumenthantering.

När IT började användas inom den offentliga förvaltningen tillskapades särrutiner för att tillgodose behoven av stöd för bl a massärenden. Dessa rutiner präglades – i vart fall under den epok när den gängse beteckningen var ADB – av begränsade resurser för databehandling och bristande informationssäkerhet jämfört med ett traditionellt pappersbaserat förfarande. Dagens IT har dock en sådan kapacitet att eventuella hinder mot att rationalisera och effektivisera knappast kan ha sin grund i tekniska begränsningar. Det är istället myndigheterna och användarna som har haft svårt att följa med i de snabba förändringar som bl a Internet, grafiska gränssnitt, kryptografi och sekundsnabb kommunikation för med sig.

Rutiner baserade på signerade elektroniska handlingar, elektroniska akter och elektroniska arkiv – där de traditionella gränsdragningarna tas till vara – ger inte bara rättsliga förenklingar utan även pedagogiska fördelar eftersom användarna då kan bruka sina kunskaper och erfarenheter från traditionell miljö; de känner igen sig. Elektroniska signaturer och liknande kryptografiska skydd kan alltså, rätt använda, bli avgörande för en rationell och rättssäker IT-användning där sådana rutiner kan göras funktionellt likvärdiga med motsvarande pappersbaserade förfaranden.

Traditionella strukturer och skydd kan rent av överträffas genom att signaturer i elektronisk form och anknytande tjänster för informationssäkerhet gör det möjligt att återskapa motsvarande gränsdragningar som i traditionell miljö, men med högre säkerhet.

Utöver att säkerställa elektroniska handlingars äkthet kan elektroniska arkiv och andra förvar skyddas mot obehörig åtkomst och bevisning kan säkras, t ex om när en handling har kommit in eller avsänts.

I samband med införandet av signerade elektroniska handlingar inom bl a tull-, skatte- och exekutionsväsendet visade det sig också att *gällande rätt i allt väsentligt kan tillämpas*, i vart fall när elektroniska signaturer tas i bruk. Eftersträvade förenklingar och rationaliseringar kan därmed genomföras, utan att skyddet för den enskildes eller det allmännas intressen behöver sättas åt sidan.

Vad som i praktiken införts på myndighetsområdet under senare år är emellertid elektronisk post och liknande tillämpningar, utan några kryptografiska skydd mot manipulationer eller mot olovlig insyn. Sådan hantering har brukat jämföras med att sända vykort. Resonemangen om att skapa säkerhet har härvid ofta präglats av en vilja att nå en närmast *hundraprocentig* säkerhet genast. Behovet av skydd växlar emellertid från tillämpning till tillämpning. Det är knappast motiverat med samma säkerhet för att t ex avge en självdeklaration i elektronisk form och att sända en förfrågan om en myndighets öppettider.

I stället för att avvakta nationella lösningar för PKI-tjänster – och till dess utesluta modern teknik – eller att, utifrån den andra ytterligheten, helt underlåta att införa tekniska och administrativa skydd för elektroniska handlingar, bör alternativa lösningar tas tillvara. Behoven av effektivitet och säkerhet kan därmed balanseras. Det bör också noteras att en hundraprocentig säkerhet aldrig kan nås. Även om systemen tekniskt görs ytterst säkra kan den mänskliga faktorn, t ex genom en felaktig administration av kryptografiska nycklar, rasera det skydd som systemet avses ge.

3.2 ÖVERGRIPANDE REGLER RESPEKTIVE REGLER FÖR ENSKILDA ÄRENDEN

Elektronisk dokumenthantering och elektronisk ärendehandläggning kan studeras på olika nivåer.

1. Kan övergripande ställningstaganden – på nationell eller regional nivå om hur CSP-tjänster med ett brett användningsområde bör utformas och samverka – rymmas inom förvaltningsmyndigheternas sakliga och lokala kompetens?
2. Kan myndigheterna tillgodose behoven av säkra, sunda och stabila CSP-tjänster och kan frågor om tillsyn för sådana tjänster lösas utan författningsändringar?
3. Kan rättsfrågor som rör enskilda dokument och enskilda ärenden hos en viss myndighet lösas vid en övergång till elektronisk dokumenthantering? Det är i första hand denna typ av frågor som berörs i det följande.

En bred övergång till signerade elektroniska dokument på förvaltningsområdet, kan leda till skapandet av nationella CSP-tjänster eller en samordning mellan centrala, regionala och lokala myndigheter som ger motsvarande effekt; nämligen att "alla kan identifiera alla" elektroniskt. Därmed kan frågor uppkomma om förvaltningsorganisationernas *sakliga* kompetens – förvaltningsverksamheten innefattar arbetsuppgifter av skiftande slag som måste fördelas mellan organen – och *lokala* kompetens – det finns såväl centrala förvaltningsmyndigheter som myndigheter med särskilda delar av landet som sitt arbetsområde. Begränsningarna av myndigheternas kompetens, till vissa bestämda förvaltningsuppgifter och – för vissa – till ett geografiskt området, skulle kunna komma i konflikt med en strävan att införa omfattande CSP-tjänster. Någon författningsreglering, instruktion eller arbetsordning, som behandlar frågor om certifikat- eller dokumenthantering torde å ena sidan inte finnas. Å andra sidan finns det sannolikt inte heller några storskaliga planer för CSP-tjänster drivna av det allmänna, och anknytande frågor om s k korscertifiering skall inte behandlas här.

På samma sätt som en myndighet, när det behövs, kan "identifiera" t ex en sökande genom dennes namnteckning eller legitimation torde myndigheterna vara oförhindrade att använda moderna rutiner med samma syfte.

Utvecklingen på området påminner delvis om hur vanliga legitimationer används. Myndigheterna godtar ID-kort utfärdade av t ex banker och utvecklingen pekar mot att aktörer som Telia och Posten kommer att tillhandahålla motsvarande certifikat, bl a för myndigheter; jfr Statskontorets ramavtal rörande tjänster för elektronisk identifiering. I detta sammanhang bör dock noteras att det enligt 11 kap 6 § regeringsformen krävs stöd i lag om en CSP-tjänst som anlitas av en myndighet och drivs i privaträttslig regi till någon del skulle fylla en sådan funktion att en förvaltningsuppgift som innefattar *myndighetsutövning* överlämnas till det *privaträttsliga* subjekt som tillhandahåller tjänsten.

Ett annat område som rör övergripande frågor har samband med att CSP-tjänster, när de fått tillräcklig spridning, kräver motsvarande stabilitet och trovärdighet som t ex finansiella tjänster. System för elektroniska signaturer behöver vara säkra, sunda och stabila. Härvid aktualiseras sådana övergripande frågor om säkerhet, stabilitet och tillsyn för hela PKI-tjänster m m vilka berörs i EG-direktivet om elektroniska signaturer och det svenska förslag som nyligen presenterats för att införa direktivet; se vidare avsnitt 2.5.1. Dessa rättspolitiska frågor om utformningen av PKI-system och samhällsstrukturer behandlas inte vidare här.

Slutligen behöver de rättsfrågor övervägas som uppkommer när elektroniska handlingar används vid handläggningen av enskilda ärenden vid en myndighet. Det är sådana frågor som skall beröras i det följande.

4 RÄTTSFRÅGOR – EN ÖVERSIKT

Gällande rätt hindrar vanligtvis inte elektronisk dokumenthantering på myndighetsområdet. IT-baserade rutiner för ärendehandläggning kan rätt utformade tillgodose högt ställda krav på skydd för såväl enskilda som det allmänna. Därmed ersätts rättsliga hinder av *möjligheter* att skapa enhetliga rutiner för traditionell och elektronisk dokumenthantering, med bevarad rätts- och informationssäkerhet. I de fall där avancerade kryptografiska rutiner inte är nödvändiga bör enklare rutiner kunna godtas.

Frågan om gällande rätt hindrar en rationell hantering av elektroniska dokument och elektroniska akter har genomlysts av bl a Utredningen om lagstiftningsbehovet vid tulldatoriseringen, IT-utredningen och i en departementspromemoria om elektronisk dokumenthantering inom skatteförvaltningen. Utredningarna fann – med utgångspunkt från den syn på elektronisk dokumenthantering som beskrivits i avsnitt 2.2.3 – att rättsliga hinder kan ersättas av *möjligheter* att tillskapa enhetliga rutiner för traditionell och elektronisk dokumenthantering. De begränsade författningsändringar som genomförts har uppenbarligen utgått från detta synsätt. Det visade sig nämligen vara möjligt att med elektroniska signaturer och liknande tekniska och administrativa skydd

- skapa samma eller motsvarande skydd mot manipulationer och missbruk som i traditionell miljö, och
- lösa olika rättsfrågor inom ramen för gällande rätt; rätts- och informationssäkerheten kunde bevaras genom sådana *funktionellt likvärdiga* skydd, utan att effektiva och rationella IT-rutiner hindrades.

Vilka nivåer av säkerhet som skulle krävas sågs som tekniska och administrativa frågor vilka får lösas från fall till fall; jfr principen om fri bevisprövning som innebär att det inte genom lag läggs fast någon viss säkerhetsnivå för att en pappersurkund eller ett elektroniskt dokument skall anses vara äkta – domaren är fri att värdera den bevisning som läggs fram. Detta synsätt gäller för hela myndighetsområdet. De elektroniska signaturerna bör härvid inte ses som ett självändamål. Andra rutiner bör godtas när detta inte äventyrar skyddet för den enskildes eller det allmännas intressen. Enklare förfaranden bör ofta kunna användas för t ex sådan kommunikation där vanliga telefaxmeddelanden ger ett tillräckligt skydd.

I det följande skall dessa möjligheter att införa IT inom förvaltningen belysas genom att några rättsområden som ibland nämns som hinder mot en datorisering kortfattat berörs.

- *Förvaltningslagens författaranderegler:* De grundläggande reglerna i förvaltningslagen (1986:223; FL) för förvaltningsmyndigheternas formella behandling av ärenden gäller oberoende av om ärendehandläggningen sker manuellt eller med stöd av IT och bestämmelserna är allmänt hållna. Det har i samband med tull- och skattedatoriseringen visat sig att avvikelser från FL endast undantagsvis kommer i fråga vid en övergång till elektronisk dokumenthantering.[39]
- *Inkommande handlingar:* På en punkt kan de grundläggande reglerna i FL dock föra med sig svårigheter, nämligen vid tolkningen av reglerna om inkommande handlingar.[40] Sedan regeringen, i en proposition om bl a nya regler om deklarationer i elektronisk form, funnit att de nya rutinerna kunde genomföras utan ändringar av reglerna om inkommande handlingar är det svårt att finna att denna fråga skulle hindra myndigheter från att införa elektronisk dokumenthantering.
- *Vissa begrepp:* Ett vanligt påstående är att vissa begrepp – t ex "skriftlig" och "handling" – inte skulle kunna förenas med IT. Närmare studier har emellertid visat att begreppet "skriftlig" har tolkats så att även elektroniska rutiner innefattas; se vidare SOU 1996:40 sid 93 ff med hänvisningar. IT-utredningen har konstaterat att det inte krävs författningsändringar i denna del och att ordet skriftlig behövs också på IT-området för att skilja sådana rutiner från muntlig handläggning. Däremot kan begrepp som ställer krav på en traditionell underskrift, t ex att en handling skall vara "undertecknad", hindra elektroniska rutiner. Sådana krav förekommer emellertid endast undantagsvis.
- *Offentlighetsinsyn och sekretess:* Reglerna om offentlighetsinsyn och sekretess i IT-miljö är svårtillgängliga. Förslag till författningsändringar i 2 kap TF har lagts fram och ytterligare en utredning överväger nu såväl dessa frågor som reglerna om sekretess.[41] Eftersom de flesta myndigheterna redan har Internetuppkoppling och använder elektronisk post och liknande tillämpningar borde elektronisk dokumenthantering knappast föra med sig några rättsliga komplikationer som myndigheten inte redan är exponerad för. Dessutom bör de avgränsningar som krävs vid elektronisk dokumenthantering delvis kunna underlätta regeltillämpningen.

[39] En annan sak är att sekundsnabb elektronisk överföring av meddelanden och automatiserade rutiner kan inbjuda till rationaliseringar som vid en närmare genomgång visar sig stå i strid med de rättssäkerhetsgarantier som regleringen syftar till.

[40] Jfr 44 § förvaltningsprocesslagen och 33 kap 3 § rättegångsbalken.

[41] Datalagskommitténs betänkande (SOU 1997:39) Integritet Offentlighet Informationsteknik, sid 465 ff samt Kommittén (Ju 1999:06) om offentlighetsprincipen och IT samt en översyn av sekretesslagen m m.

- *Persondataskyddet:* Problem kan uppkomma för sådana tillämpningar för löpande text där det inte kan hindras att även s k känsliga uppgifter förekommer.[42] Inkomna handlingar som innehåller känsliga uppgifter som kanske *inte* behövs i ärendet får inte återsändas eller förstöras; jfr skyldigheten att bevara enligt arkivförfattningarna och offentlighetsprincipen. Av 13 § PUL framgår att det är förbjudet att behandla känsliga personuppgifter; t ex personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter eller religiös eller filosofisk övertygelse, eller personuppgifter som rör hälsa eller sexualliv. De undantag som anges – utöver den registrerades samtycke eller offentliggörande – förutsätter att behandlingen är *nödvändig* för vissa ändamål. Möjligen skulle undantaget med hänsyn till ett viktigt allmänt intresse kunna tillämpas (20 § PUL, jfr direktivet art. 8.4), även om det inte är uppgiften i sig som är nödvändig utan hanteringen av "omanipulerade" dokument i elektronisk form.
- *Arkiv, bevarande gallring:* Nuvarande arkivförfattningar hindrar inte en övergång till elektronisk dokumenthantering och elektronisk post. Rutinerna för arkivering behöver emellertid uppmärksammas redan på planeringsstadiet när traditionella rutiner skall ersättas av system för elektronisk dokumenthantering och myndigheten bör samråda med sin arkivmyndighet (6 § arkivförordningen) för att säkerställa att arkivförfattningarna följs. Detta gäller såväl avställning av egentliga register som bildande av elektroniska akter och gallring. Elektroniska signaturer förutsätter dock noggranna överväganden av vilka rutiner som används så att dokumenten kan läsas på sikt.
- *Bokföring – varannanlänksprincipen:* Kravet i bokföringslagen (1976:125) på att varannan länk i bokföringskedjan skall vara i vanlig läsbar form har upphävts genom bokföringslagen (1999:1078), som trädde i kraft den 1 januari 2000. Varje länk i bokföringen skall alltså kunna föreligga i elektronisk form. Komplikationer kan istället upp-

[42] Tanken är enkel; om handlingarna sänds in elektroniskt eller scannas av myndigheten måste alla uppgifter få tas med eftersom det är uteslutet att en handläggare först skulle läsa igenom handlingarna och "förfalska" genom att ta bort känsliga uppgifter. Som exempel kan nämnas skatteförvaltningens regionala register som enligt 11 § skatteregisterlag (1980:343) får innehålla bl a handling som kommit in eller upprättats i ett ärende som hänför sig till länet. En sådan handling får innehålla känsliga uppgifter om en enskild har lämnat uppgiften eller om den behövs för handläggningen av ärendet. För att hindra otillbörligt intrång i registrerades personliga integritet har emellertid i 13 § samma lag föreskrivits att som sökbegrepp i dessa handlingar får användas endast ärendebeteckning och beteckning på handling. Det innebär att känsliga uppgifter – på motsvarande sätt som i pappershandlingar – kan sökas fram endast genom att de läses manuellt. Till dessa handlingar är emellertid ett elektroniskt diarium/dagboksblad knutet beträffande vilket personnummer, organisationsnummer, namn, firma, ärendebeteckning, taxeringsår, beskattningsår, inkomstår, redovisningsperiod, handläggande enhet, datum och uppgift om var i handläggningsgången ärendet befinner sig får användas som sökbegrepp. – Motsvarande reglering finns i 6a § och 7b § utsökningsregisterlagen (1986:617) samt 11 och 18 §§ socialförsäkringsregisterlagen (1997:934) och samma principer synes ha tillämpats i DI:s tillståndsprövning.

komma i anknytning till den nya lagens krav på bevarande av vissa datamedier. Denna fråga torde emellertid normalt inte beröra myndigheternas ärendehandläggning.

- *Delgivning:* En fråga av intresse för myndigheterna är om handlingar kan delges elektroniskt, t ex med e-post. Utgångspunkten bör härvid, enligt IT-utredningen, vara att de krav som gäller i traditionell miljö från bl a rättssäkerhets- och integritetsskyddssynpunkt skall upprätthållas också i IT-miljön. Detta är tekniskt möjligt med digitala signaturer och anknytande säkerhetstjänster. Rätt utformade kan sådana rutiner ge ett effektivare skydd mot oavsiktliga och avsiktliga fel än traditionella pappersbaserade rutiner.
- *Elektroniska akter vid ett överklagande:* När ett beslut överklagas och den *beslutande* myndigheten har hanterat ärendet helt eller delvis elektroniskt uppkommer frågan hur "akten" skall överlämnas till domstolen. Rutinerna för att översända elektroniska akter kan utformas på olika sätt. Någon ny reglering torde dock inte krävas och det finns, som framgått, inte något hinder mot att åberopa IT-material som bevisning inför domstol. Det torde dessutom i praktiken vara en udda företeelse att en handlings äkthet ifrågasätts vid en domstol eller att originalet krävs in av andra skäl.
- *Straffrättsligt skydd för elektroniska dokument:* Straffrättsliga och straffprocessuella frågor har tagits upp av Datastraffrättsutredningen; jfr avsnitt 2.2.3. Att ett straffrättsligt skydd är av avgörande betydelse för allmänhetens tillit till IT-baserade rutiner framträder tydligt av den genomgång av skyddsvärda förfaranden som gjorts i avsnitt 2.2.6.

5 SLUTORD

En närmare genomlysning av de tekniska och juridiska förutsättningarna för elektronisk dokumenthantering visar att det vanligtvis inte finns hinder mot att införa sådana rutiner inom förvaltningen. Med elektroniska signaturer och anknytande säkerhetsrutiner ges ytterligare stöd för en tillämpning av vedertagna rättsprinciper på IT-området.

Myndigheterna bör därför kunna ta tillvara de investeringar som redan har gjorts i informationssystem och nät. Genom balanserade avvägningar mellan effektivitet och rättssäkerhet kan tillräckligt säkra rutiner skapas för enskilda tillämpningar. IT bör därvid kunna användas som stöd för förenklingar och förbättringar av hanteringen.

Detta betyder inte att det skulle saknas behov av att IT-anpassa författningsregleringen. Tvärtom kan den snabba utvecklingen – i vart fall på sikt – antas leda till en mängd anpassningar och förtydliganden av regelverket. Vad Riksarkivet velat lyfta fram i denna skrift är istället att behovet av anpassningar inte får missförstås så att myndigheterna utgår från att det skulle finnas en mängd rättsliga hinder mot att införa elektronisk hantering av ärenden, akter och dokument.

RAPPORTER