

# FÖRORD

Jag vet inte om det är så vanligt förekommande att man skriver ett förord till en tillämparuppsats, men jag känner att det är så många personer som jag vill uppmärksamma och tacka så därför gör jag det ändå. Jag har haft den stora turen att ha valt ett ämne som det visade sig finnas ett otroligt stort intresse för. Det har känts givande och stimulerande att så många har visat så stort intresse för min uppsats. Först och främst vill jag passa på att tacka Parallel Systems AB i Stockholm, för att de gav mig uppslaget till att skriva om detta ämne. Framför allt vill jag tacka Anna Bostam och Anders Lindberg på Parallel Systems. Speciellt stort tack till Anna, för att hon så förtjänstfullt agerat som min mentor under uppsatsskrivandet.

Vidare vill jag tacka Rickard Wallentin vid Kommunikationsdepartementet, för att han var så vänlig och lät mig delta vid de möten som hölls med den externa referensgrupp som bildats för att utarbeta Sveriges ståndpunkter till det direktivförslag avseende digitala signaturer som lagts fram inom EU under våren 1998. Detta har varit mycket givande för mig, genom att det gett mig värdefulla insikter inte bara i vilka reaktionerna varit mot detta direktivförslag, utan även i hur de rättsliga frågeställningarna och diskussionerna kring elektroniska signaturer ser ut samt hur de utvecklar sig.

Slutligen vill jag naturligtvis även rikta ett stort tack till min handledare vid Juridiska institutionen vid Handelshögskolan vid Göteborgs universitet, professor Christina Hultmark. Den seminarieform som hon använder sig av vid sin handledning av de studenter som skriver uppsats för henne har fungerat mycket bra. Diskussionerna inom denna seminariegrupp har varit givande och till stor hjälp vid uppsatsskrivandet.

Stockholm i december 1998

*Katja Keränen*

E-post: [katja.keranen@swipnet.se](mailto:katja.keranen@swipnet.se)

## SAMMANFATTNING

Elektroniska signaturer är olika tekniska metoder som kan användas för att underteckna, signera, elektroniska dokument. En elektronisk signatur kan alltså sägas vara en i IT-miljön existerande motsvarighet till den traditionella namnteckningen i ”pappersvärlden”. Rent tekniskt kan elektroniska signaturer idag fylla samma funktioner som namnteckningen, dvs *identifiera* utställaren av ett dokument, garantera dokumentets *äkthet*, ha *bevisverkan*, fylla en *viljefunktion*, samt (i vissa fall) tjäna en *varningsfunktion*. Dock råder fortfarande osäkerhet kring frågan om den elektroniska signaturen även juridiskt kan anses likvärdig med den handskrivna namnteckningen, dvs om den kan ha samma rättsverkan. Syftet med föreliggande uppsats är att undersöka denna fråga. Frågan har betydelse i två fall; dels då det i lag eller avtal, dels då det i övrigt, ställs krav på underskrift för att genomföra en transaktion. När det gäller legala eller avtalade krav på underskrift, s k formkrav, är frågan om dessa krav kan uppfyllas även av elektroniska signaturer. I övriga fall, då underskrift krävs främst i bevissyfte, gäller frågan om elektroniska signaturer kan fylla samma bevisverkan som egenhändiga namnteckningar.

När det gäller frågan om elektronisk signatur kan användas istället för traditionell namnteckning i de fall då det finns formkrav, har i svensk rätt lagstiftning redan genomförts inom vissa områden av den offentliga förvaltningen, på så sätt att elektroniska dokument godtas istället för egenhändigt undertecknade handlingar i vissa fall. I övriga fall råder dock fortfarande osäkerhet. Undersöker man motiven till de lagstiftningsåtgärder som har genomförts verkar dock lagstiftarens åsikt vara att elektroniska signaturer inte, enligt gällande rätt, kan godtas istället för handskrivna underskrifter i de fall då det i lagar eller föreskrifter finns formkrav, utan att det krävs lagstiftningsåtgärder för att jämställa dessa två. Denna åsikt tycks motiverad på den grunden att den språkliga lydelsen av dessa bestämmelser skulle förhindra användande av elektronisk signatur. Om man istället anlägger ett funktionellt perspektiv på rätten (dvs går efter principen att elektroniska motsvarigheter till traditionella pappersbaserade rutiner, som lika väl kan fylla samma funktioner som sistnämnda, bör tillerkännas samma rättsverknings) skulle man dock, redan enligt gällande rätt, kunna godta elektroniska signaturer istället för traditionella namnteckningar. Man skulle då nämligen kunna tillämpa de regler som idag ställer krav på ”underskrift” etc även på elektroniska signaturer. Frågan om rättsverkan av elektronisk signatur har dock hittills ej prövats i svensk rätt. Tills dess den har gjort det – eller klagoranden från lagstiftaren skett – råder därför osäkerhet i denna fråga. I uppsatsen framförs den åsikten att det funktionella perspektivet bör vara det avgörande, inte den språkliga lydelsen av ifrågakvarande rättsregler.

Vad gäller frågan om bevisverkan av elektronisk signatur, är det dock klart att det i svensk rätt ej föreligger några rättsliga hinder att åberopa elektroniska signaturer som bevisning, detta beroende på att vi i svensk rätt tillämpar principerna om fri bevisprövning och fri bevisvärdering. I detta avseende kan dock bevisvärderingen ge anledning till viss tveksamhet. Inte heller i detta avseende föreligger nämligen något avgörande i svensk rätt, och därför är det svårt att idag veta vilket bevisvärde en domstol skulle åsätta en elektronisk signatur. Detta är dock ingen fråga som måste lösas på rättslig väg, utan denna fråga löses lämpligast tekniskt. Om de tekniska procedurerna och rutinerna kring elektroniska signaturer utformas på ett sådant sätt att bevisföringen säkras och tillit skapas till elektroniska signaturer, skulle dessa nämligen kunna tillerkännas samma bevisverkan som traditionella namnteckningar (kanske t o m högre).

Den slutsats som dras i denna uppsats är, att när det gäller de fall där det ej finns formkrav, så bör det inte innebära några större problem att använda sig av elektroniska signaturer istället för traditionella namnteckningar. Detta gäller dock under förutsättning att man säkerställer att det system för elektronisk signering som man valt tillgodoser alla de funktioner som den traditionella namnteckningen fyller. När det gäller de fall där det finns formkrav, gör man nog dock klokast i att vara lite försiktigare. Detta innebär främst vissa hinder att använda sig av elektronisk signering inom förvaltningsrättsområdet, dvs vid kommunikation med myndigheter, men inom detta område har lagstiftningsåtgärder redan skett och utreds kontinuerligt. I övrigt utgör det dock inte något större hinder för den elektroniska handeln, då de situationer där det finns formkrav i lag trots allt är ganska få och ofta rör sådana slags transaktioner som ändå inte är särskilt vanligen förekommande för avtalsslutande via Internet.

## FÖRKORTNINGAR

BrB	Brottsbalken
CA	Certification Authority
Ds	Departementsskrivelse
EDI	Electronic Data Interchange
EU	Europeiska Unionen
HD	Högsta domstolen
IT	Informationsteknologi
NJA	Nytt Juridiskt Arkiv (avdelning I)
Prop.	Proposition
RB	Rättegångsbalken
RSV	Riksskatteverket
SEIS	Säkrad Elektronisk Information i Samhället
SOU	Statens offentliga utredningar
TDS	Tulldatasystemet
TDU	Tulldatautredningen
UNCITRAL	United Nations Commission on International Trade Law

# INNEHÅLL

<b>FÖRORD</b>	<b>I</b>
<b>SAMMANFATTNING</b>	<b>II</b>
<b>FÖRKORTNINGAR</b>	<b>III</b>
<b>1 INLEDNING</b>	<b>3</b>
1.1 Syfte	3
1.2 Metod	4
1.3 Avgränsningar	5
1.4 Disposition	6
<b>2 ELEKTRONISKA SIGNATURER</b>	<b>7</b>
2.1 Vad är en elektronisk signatur?	7
2.2 Hur fungerar en elektronisk signatur?	7
2.3 Digital signatur	8
2.3.1 Kryptering	8
2.3.2 Asymmetrisk kryptering	9
2.3.3 Hashfunktionsteknik	9
2.3.4 Skapande och verifiering av digital signatur illustrerat	10
<b>3 JÄMFÖRELSE MED EGENHÄNDIG NAMNTECKNING</b>	<b>11</b>
3.1 Syftet med namnteckning	11
3.1.1 Identifikation	11
3.1.2 Äkthet	12
3.1.3 Bevisverkan	12
3.1.4 Viljefunktion	13
3.1.5 Varningsfunktion	13
3.2 Hur den elektroniska signaturen kan fylla namnteckningens funktioner	13
3.2.1 Identifikation	13
3.2.2 Äkthet	15
3.2.3 Bevisverkan	16
3.2.4 Viljefunktion	16
3.2.5 Varningsfunktion	17
3.3 Sammanfattning	17
<b>4 ELEKTRONISKA SIGNATURER I SVENSK RÄTT</b>	<b>18</b>
4.1 Elektroniskt uppgiftslämnande inom tullverket	19
4.1.1 Tulldatautredningen	19
4.1.2 Införande av begreppet elektroniskt dokument	19
4.1.3 Tulldatasystemet – TDS	19
4.1.4 Elektronisk signering i TDS	20

4.2	Elektroniska deklamationer	20
4.3	Straffrättens bestämmelser om brott mot urkund	21
4.4	Utredningen om elektronisk dokumenthantering	22
4.5	Föreningar som verkar inom området elektroniska signaturer	23
4.5.1	Toppleddarforum	23
4.5.2	SEIS	24
4.6	Sammanfattning	24
<b>5</b>	<b>INTERNATIONELLA HARMONISERINGSARBETEN AVSEENDE ELEKTRONISKA SIGNATURER</b>	<b>25</b>
5.1	EU:s direktivförslag om en gemensam ram för elektroniska signaturer	25
5.1.1	Direktivets tillämpningsområde	26
5.1.2	Rättsverkan av elektroniska signaturer	26
5.1.3	Hur kommer detta direktiv att påverka svensk rätt?	27
5.2	UNCITRAL:s modellregler för elektroniska signaturer	28
5.2.1	Modellagen för elektronisk handel	28
5.2.2	Modellreglerna för elektroniska signaturer	29
5.2.3	Två olika typer av elektroniska signaturer	29
5.2.4	Skillnaderna mellan de två typerna av elektroniska signaturer	30
5.3	Sammanfattning	31
<b>6</b>	<b>SLUTSATSER</b>	<b>32</b>
6.1	Elektronisk signatur i de fall då det uppställs formkrav	32
6.1.1	Lagstiftarens syn	32
6.1.2	På vilken grund baseras lagstiftarens åsikt?	33
6.1.3	Andra synpunkter på denna fråga – det funktionella perspektivet	34
6.1.4	Exempel från praxis där man tillämpat det funktionella perspektivet	35
6.1.5	Andra invändningar mot strikt bokstavstolkning	36
6.1.6	Egna slutsatser	37
6.2	Elektronisk signatur i övriga fall då namnteckning brukas	37
6.3	Behövs det ytterligare lagstiftningsåtgärder?	38
6.4	Sammanfattning	40
	<b>KÄLLFÖRTECKNING</b>	<b>41</b>

# 1 INLEDNING

Elektronisk kommunikation och elektronisk handel är högaktuella diskussionstemata idag och ett av de ämnen inom detta område som för närvarande diskuteras mest är elektroniska signaturer. Med hjälp av dessa är det tänkt att den elektroniska kommunikationen och handeln skall kunna utvecklas och därmed också öka ytterligare. Detta möjliggörs genom att man med användande av elektroniska signaturer skall kunna börja kommunicera och handla säkert även över öppna, oskyddade nät såsom exempelvis Internet, och inte såsom tidigare enbart i slutna nät, där alla användare är kända sedan tidigare. Detta skulle innebära att elektronisk kommunikation skulle kunna bli enklare och mer lättillgängligt för flertalet användare, vilket i sin tur skulle medföra en ökning av elektronisk kommunikation och handel. Ökad elektronisk kommunikation och handel bedöms som önskvärt då detta kan medföra positiva samhällsekonomiska effekter i form av möjligheter till stora förenklings- och rationaliseringsvinster. Det som hittills uppmärksammats mest kring de elektroniska signaturerna är de tekniska aspekterna, nämligen hur dessa skall göras så tekniskt säkra som möjligt. Nu har tekniken dock nått därhän att man hittat godtagbara lösningar på dessa problem, och då har istället ett ytterligare problem uppmärksammats – de rättsliga aspekterna. För att den elektroniska kommunikationen och handeln skall kunna fungera fullt ut måste säkerhet även uppnås beträffande de många rättsliga frågor som aktualiseras i samband med dessa, inklusive de rättsfrågor som uppkommer i anknytning till elektroniska signaturer. En av dessa rättsfrågor är frågan om vilken rättsverkan en elektronisk signatur har, eller närmare bestämt om den kan ha samma rättsverkan som en traditionell, handskriven namnteckning.

## 1.1 Syfte

Denna uppsats har skrivits på uppdrag av Parallel Systems AB i Stockholm. Detta företag, som är verksam inom IT-branschen, önskade få utrett frågan ”vad en elektronisk signatur är värd”. Översatt till juristens språkbruk blir frågan ”vilken rättsverkan en elektronisk signatur har”. Närmare bestämt ville de veta om en elektronisk signatur kan ha samma rättsverkan som en traditionell, handskriven namnteckning. Syftet med denna uppsats är alltså att undersöka om en elektronisk signatur kan ha samma rättsverkan som en ”vanlig”, handskriven namnteckning. Denna frågeställning kan uppdelas i två delfrågor:

1. Kan man använda sig av elektronisk signatur istället för egenhändig namnteckning i de fall då det i lag eller avtal ställs krav på undertecknande (så kallade formkrav<sup>1</sup>), dvs kan formkrav uppfyllas även med elektronisk signatur?
2. I majoriteten av fall då underskrift krävs finns det dock inget legalt eller avtalat krav på detta, utan det främsta syftet är att säkra bevisning om att ett dokument härrör från, eller har bekräftats av, en viss person. I dessa fall är alltså frågan om elektroniska signaturer kan fylla samma bevisverkan som egenhändiga namnteckningar.

---

<sup>1</sup> Formkrav innebär att det ställs krav i lag eller avtal på viss form, t ex skriftlighet och/eller underskrift, för att genomföra en transaktion, exempelvis för att ett giltigt avtal skall föreligga. Som exempel på formkrav i lag kan nämnas 4 kap 1 § jordabalken, där det stadgas att ”köp av fast egendom slutes genom upprättande av en köpehandling som underskrives av säljaren och köparen”, och 2 kap 2 § 3 st årsredovisningslagen (1980:1103), varav framgår att en årsredovisning skall skrivas under av den redovisningsskyldige.

I denna uppsats skall ovanstående två frågor undersökas mot bakgrund av gällande rätt för att se om elektroniska signaturer redan enligt gällande regler kan ha samma rätts- och bevisverkan som namnteckningen, eller om lagändringar krävs i något av dessa fall.

## 1.2 Metod

Frågan om vilken rättsverkan en elektronisk signatur har kan också beskrivas som en fråga om hur befintliga rättsregler kan/skall tillämpas på en ny företeelse. I detta fall är alltså frågan om, och i så fall på vilket sätt, de rättsregler som är tillämpbara på egenhändiga namnteckningar kan tillämpas också på elektroniska signaturer. Det bör dock påpekas att det inom rättsvetenskapen finns de som anser att man inte bör resonera så här, dvs att man inte alltid bör ta sin utgångspunkt i existerande regler och – som de skulle uttrycka det – försöka ”pressa in” nya företeelser i dessa. De anser att vissa nya företeelser ibland istället behöver egna, nya regler. Enligt min mening faller det sig dock naturligt att utgå ifrån traditionella pappersdokument och reglerna kring dessa; dels av den anledningen att pappersmediet har en lång tradition bakom sig, dels på grund av att så gott som alla existerande regler är utformade med avseende på brukandet av pappersdokument.<sup>2</sup> En ytterligare fördel med att i möjligaste mån anpassa tillämpningen av ny teknik till rättssystemets gällande ordning är att detta gynnar rättssäkerheten, genom att man på detta sätt kan fortsätta att tillämpa redan existerande och kända regler, för vilka det dessutom oftast redan föreligger en viss praxis.<sup>3</sup>

När man undersöker befintliga rättsregler för att se hur, och i så fall på vilket sätt, dessa kan tillämpas även på elektroniska signaturer bör man lämpligen anlägga ett funktionellt perspektiv, som bygger på principen om funktionell likvärdighet (*functional equivalency*)<sup>4</sup>, på rätten. Denna princip innebär att elektroniska motsvarigheter till traditionella pappersbaserade rutiner, som lika väl kan fylla ”pappersmediets” funktioner, bör anses likvärdiga med – och därmed även tillerkännas samma rättsverknningar som – dessa. I linje med denna princip måste man alltså börja med att undersöka det bakomliggande syftet med ifrågavarande bestämmelser. Varför har vi dessa regler? Varför finns det legala eller konventionella krav på namnteckning i vissa fall? Vilket syfte anses en namnteckning fylla i dessa fall? När man vet svaret på dessa frågor kan man sedan gå vidare och undersöka om dessa bakomliggande syften kan uppfyllas även av elektroniska signaturer. Kan de det så bör de alltså, i enlighet med principen om funktionell likvärdighet, kunna tillerkännas samma rättsverkan som namnteckningar, dvs man bör kunna tillämpa de befintliga rättsregler som rör traditionella namnteckningar även på elektroniska signaturer.

Vid min undersökning av frågan om rättsverkan av elektroniska signaturer har jag främst använt mig av det material som publicerats i samband med de offentliga utredningar som har gjorts de senaste åren med anledning av övergången till elektronisk dokumenthantering inom vissa områden inom den offentliga förvaltningen.<sup>5</sup> Dessa utredningar, liksom de lagändringar som de givit upphov till, utgör en viktig informationskälla i det avseendet att man av dessa kan utläsa hur lagstiftaren anser att de rättsfrågor som elektroniska signaturer aktualiserar kan/bör lösas. Man kan alltså med andra ord i dessa utredningar och lagförslag spåra de ten-

---

<sup>2</sup> Jfr Karstofts åsikter i Elektronisk dokumentutveksling – retlige aspekter, s 178.

<sup>3</sup> Se SOU 1989:20, s 87 f samt Ds 1994:80, s 102.

<sup>4</sup> På denna princip bygger t ex den modelllag för elektronisk handel (Model Law on Electronic Commerce) som FN-organet UNCITRAL utarbetat.

<sup>5</sup> T ex SOU 1987:40, SOU 1989:20, SOU 1989:40 och SOU 1996:40. Detta år (1998) har dessutom publicerats en departementspromemoria, Ds 1998:14, som enbart behandlar ämnet digitala signaturer.

denser som idag finns i svensk lagstiftning avseende elektroniska signaturer. Vad gäller rättsfrågorna kring elektroniska signaturer finns det även viss litteratur inom detta område.<sup>6</sup> När det sedan gäller faktainformation om elektroniska signaturer har denna inhämtats främst från den litteratur som finns inom detta område, samt från diverse artiklar i dagspress och facktidningar, liksom naturligtvis även från Internet. Till stor nytta i detta avseende har även de många utredningar, inom området elektronisk handel, som de senaste åren gjorts på privata initiativ av organisationer och föreningar som exempelvis Toppledarforum och SEIS (Säkrad Elektronisk Information i Samhället), varit. Ytterligare information och inspiration har jag vidare kunnat inhämta tack vare att man på Kommunikationsdepartementet låtit mig få delta i den externa referensgrupp som departementet upprättat för att utforma Sveriges inställning till det direktivförslag angående elektroniska signaturer som lagts fram inom EU i maj i år. Detta har gett mig värdefulla insikter inte bara i vilka reaktionerna varit mot detta direktivförslag, utan även i hur de rättsliga frågeställningarna och diskussionerna kring elektroniska signaturer ser ut samt hur de utvecklar sig. Vidare har jag införskaffat information genom att intervjua diverse personer som är insatta i dessa frågor. Bl a har jag talat med rådmann Per Furberg, som medverkat i ett flertal av de offentliga utredningar som jag undersökt. Jag har även talat med personer som arbetar på de myndigheter där man infört elektroniskt uppgiftslämnande.

Avslutningsvis vill jag göra några anmärkningar angående innehållet i denna uppsats. För det första skulle jag vilja förklara anledningen till varför jag även behandlar elektroniska dokument i så stor utsträckning i uppsatsen. Detta beror dels på att då det i lag ställs krav på underskrift, detta krav alltid är förenat med ett krav på skriftlighet (dvs krav på en skriftlig handling), dels på att även elektroniska dokument och elektroniska signaturer, genom den definition det elektroniska dokumentet givits i svensk lagstiftning, kommit att bli intimt sammanbundna med varandra. Det elektroniska dokumentet förutsätter nämligen enligt sin definition i svensk rätt att det har blivit försett med en elektronisk signatur.<sup>7</sup> För det andra kommer att märkas att jag ofta tar digitala signaturer som exempel när elektroniska signaturer diskuteras i uppsatsen. Detta beror på att den digitala signaturen är den i skrivande stund vanligast förekommande typen av elektronisk signatur. Faktum är, och detta förtjänar också att påpekas redan här inledningsvis, att elektroniska signaturer och digitala signaturer ofta används synonymt när man idag talar om elektroniska signaturer. ”Elektronisk signatur” är dock det vidare begreppet av de två; det innefattar samtliga tekniska metoder som finns för att signera elektroniska dokument. ”Digital signatur” är, som ovan nämndes, endast en typ av elektronisk signatur. Slutligen vill jag göra den anmärkningen att då denna uppsats är skriven inte bara för jurister utan även för tekniker så har jag försökt att anpassa mitt språk därefter. Detta innebär att jag, när det gäller de juridiska avsnitten, har förenklat mitt juridiska språk så att även tekniker skall förstå vad jag menar. Likaså är det tekniska avsnittet om elektroniska signaturer skrivet på ett lättfattligt språk, så att även icke-tekniker skall kunna förstå hur de fungerar.

### 1.3 Avgränsningar

Elektroniska signaturer och elektronisk handel ger upphov till en mängd olika juridiska frågor, men att utreda dem alla inom ramen för en tillämparuppsats på 20 poäng vore näst intill omöjligt. Som har framgått av det ovanstående har jag därför valt att göra den begränsningen

---

<sup>6</sup> T ex Hultmark, Elektronisk handel och avtalsrätt, och Lindberg, Elektroniska originaldokument och elektronisk signatur.

<sup>7</sup> Se t ex 12 § tullagen (1994:1550).



att jag i denna uppsats endast behandlar frågan om rättsverkan av elektronisk signatur. Övriga frågor som rör elektroniska signaturer, som t ex ansvarsregleringen mellan berörda parter i elektroniska transaktioner liksom regleringen av CA-verksamhet etc, lämnas därhän.<sup>8</sup> Vidare har jag när det gäller frågan om rättsverkan av elektronisk signatur gjort den avgränsningen att jag inte behandlar sådana problem som uppstår i samband med att en handling av något slag skall presenteras i original. Denna fråga skiljer sig nämligen avsevärt från övriga frågor kring den elektroniska signaturs rättsverkningar, och bör därför enligt min mening behandlas för sig.

Ytterligare en avgränsning består däri att uppsatsen behandlar den elektroniska signaturs eventuella rättsverkningar främst utifrån svensk rätt, trots att de internationella aspekterna gör sig starkt gällande inom detta område. Även detta är beroende av tids- och utrymmes-skäl, och inte alls av att det skulle vara ointressant att se till vad som sker internationellt. Tvärtom är det viktigt att studera dessa ansträngningar och hela tiden ha dem i åtanke när man försöker utreda/utveckla de svenska reglerna avseende elektroniska signaturer. Inte minst kan sådana arbeten som UNCITRAL:s modellag för elektronisk handel samt modellregler för elektroniska signaturer tjäna som inspiration under denna process. Likaså är det naturligtvis viktigt att följa utvecklingen inom EU, eftersom detta påverkar vår lagstiftning i allra högsta grad. Därför behandlas även dessa två lagstiftningsarbeten kort i uppsatsen.

## 1.4 Disposition

I kapitel två förklaras först vad en elektronisk signatur är och hur den fungerar. Den digitala signaturen, som idag är den vanligast förekommande typen av elektronisk signatur, tas som exempel i detta kapitel. Därefter diskuteras i det tredje kapitlet syftet med ett undertecknande och de funktioner som en namnteckning anses fylla. I samband med detta undersöks också om detta syfte och dessa funktioner kan tillgodoses även av en elektronisk signatur. I kapitel fyra redogörs för de lagstiftningsåtgärder som hittills vidtagits i svensk rätt för att införa elektroniska dokument och elektroniska signaturer inom vissa områden av den offentliga förvaltningen. I kapitel fem presenteras de lagstiftningsarbeten som pågår inom EU och UNCITRAL (FN:s handelsrättskommission). Slutligen diskuteras i kapitel sex vilka slutsatser som kan dras, av undersökningen av det bakomliggande syftet bakom krav på namnteckning samt av de lagstiftningsåtgärder som hittills vidtagits i svensk rätt, angående frågan om rättsverkan av elektronisk signatur. Frågan om ytterligare lagstiftningsåtgärder är nödvändiga för att elektroniska signaturer skall kunna tillerkännas samma rätts- och bevisverkan som traditionella namnteckningar diskuteras också kort i det avslutande kapitlet.

---

<sup>8</sup> Intresserade hänvisas istället till andra framställningar inom dessa områden. För en diskussion om ansvarsregleringen se t ex Averstén, Digitala signaturer och ansvarsproblem framförallt nyckelinnehavarens och Certification Authority's ansvar mot förlitande part.

## 2 ELEKTRONISKA SIGNATURER

### 2.1 Vad är en elektronisk signatur?

En elektronisk signatur kan sägas vara en i IT-miljön existerande motsvarighet till den traditionella namnteckningen i ”pappersvärlden”. Den elektroniska signaturen är alltså ett sätt att underteckna, signera, ett elektroniskt dokument. Tekniskt kan detta utföras på flera olika sätt. Man kan använda sig av alltifrån enkla metoder, som att t ex scanna in en handskriven namnteckning i ett ordbehandlingsdokument, till mer avancerade metoder som exempelvis digitala signaturer, som använder sig av krypterings- och hashfunktionsteknik (se mer om detta nedan). Gemensamt för alla typer av elektroniska signaturer är dock att de kan användas för att identifiera avsändaren av ett elektroniskt dokument. Vissa typer av elektroniska signaturer, exempelvis digitala signaturer, kan även säkerställa att innehållet i ett elektroniskt dokument ej har blivit förvanskat sedan avsändandet. Dessa två egenskaper hos den elektroniska signaturen identifieras också i den definition som i svensk lagstiftning givits åt det elektroniska dokumentet, exempelvis i tullagen (1994:1550) där det i 12 § stadgas:

*Med ett elektroniskt dokument avses en upptagning vars innehåll och utställare kan verifieras genom ett visst tekniskt förfarande* (egen fetstil).

I den senaste versionen av EU:s direktivförslag om elektroniska signaturer ställer man upp följande definition av en elektronisk signatur:

*”[E]lectronic signature” means data in electronic form attached to, or logically associated with, other electronic data and which serves as a method of authentication.*<sup>9</sup>

”Authentication” kan närmast översättas till svenska som äkthetsbevisning, verifiering. I nästföljande kapitel, kapitel tre, diskuteras den rättsliga betydelsen av sådan här ”äkthetsbevisning” närmare, men först skall i detta kapitel förklaras hur denna verifiering sker tekniskt.

### 2.2 Hur fungerar en elektronisk signatur?

Denna uppsats avser ej att behandla de många tekniska aspekterna av elektroniska signaturer, men för att underlätta förståelsen i följande kapitel – då namnteckningens funktioner, och frågan om även den elektroniska signaturen kan fylla dessa funktioner, skall behandlas – är det dock nödvändigt att först ge en kort beskrivning av hur en elektronisk signatur kan fungera i praktiken. Den idag mest förekommande typen av elektronisk signatur är den så kallade digitala signaturen. Denna skall därför tas som exempel i det följande när frågan om hur en elektronisk signatur fungerar skall besvaras.

---

<sup>9</sup> Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om en gemensam ram för elektroniska signaturer, KOM(1998) 297 slutlig, 13.05.98, omarbetad version från 18.11.98, art 2.

## 2.3 Digital signatur

Digital signatur definieras på följande sätt i ISO 7498-2 standarden<sup>10</sup>:

*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.*

Statskontoret har i skriften Svenska delen av Internet uppställt följande förklaring över en digital signatur:

*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.<sup>11</sup>*

En digital signatur skapas genom en kombination av asymmetrisk kryptering och hashfunktionsteknik. Dessa tekniker förklaras kortfattat i det följande.

### 2.3.1 Kryptering<sup>12</sup>

Genom kryptering kodas innehållet i ett meddelande så att det blir oläsligt. Detta sker genom utnyttjande av en så kallad nyckel (en algoritm) som anger hur informationen i dokumentet skall ändras. Mottagaren avkodar, dekrypterar, sedan meddelandet med antingen samma eller en annan nyckel (beroende på vilket system som används, se mer om detta nedan), och det ursprungliga innehållet kommer då fram. Kryptering användes ursprungligen för att skydda information mot insyn, dvs för konfidentialitet, men på senare tid har nya krypteringsmetoder utvecklats som gör det möjligt att även skapa ett upphovs- och manipuleringskydd. Det är dessa senare metoder som öppnat vägen för digitala signaturer.

Det finns idag två sorters krypteringsalgoritmer, symmetriska och asymmetriska. Den symmetriska är den äldsta och mest beprövade tekniken. Den går ut på att sändare och mottagare använder samma (gemensamma) nyckel för både kryptering och dekryptering. Eftersom samma nyckel används måste denna hållas hemlig. Därför kallas denna teknik ibland även för en-nyckelsystem, eller hemlig-nyckelsystem. Att nyckeln måste hållas hemlig är en stor nackdel med detta system. Detta medför nämligen en hel del problem vid hanteringen av dessa nycklar, särskilt i öppna nätverk såsom Internet. Framför allt är det distributionen av nycklar som blir komplicerad i detta system, då det krävs att man tillhandahåller sin hemliga nyckel till samtliga motparter som skall kunna dekryptera ens meddelanden. Förutom att detta är besvärligt så innebär det givetvis även betydande säkerhetsrisker. Symmetrisk kryptering används därför idag endast för skydd av konfidentialitet, inte för signering. För detta ändamål används istället asymmetrisk kryptering.

---

<sup>10</sup> ISO = International Standards Organisation. Fastställdes som Svensk Standard år 1989.

<sup>11</sup> Statskontorets rapport 1997:18.

<sup>12</sup> Informationen avseende kryptering liksom hashfunktionstekniken har inhämtats från Ds 1998:14, s 18 ff; Wild-Nordlund, Digital Signatures, s 8 ff; Lloyd, Information Technology Law, s 481 f.

### 2.3.2 Asymmetrisk kryptering

Asymmetrisk kryptering är en förhållandevis ny teknik som istället för en enda nyckel utnyttjar två skilda nycklar vid kryptering respektive dekryptering. Den ena nyckeln i nyckelparet är en hemlig, privat nyckel och den andra en öppen, publik nyckel. Asymmetrisk kryptering kallas därför även för publik-nyckelsystem. Denna teknik präglas av två viktiga faktorer:

- 1) trots kunskap om den ena nyckeln i nyckelparet är det omöjligt att beräkna den andra nyckeln, och
- 2) ett krypterat meddelande kan inte dekrypteras med samma nyckel i nyckelparet.

De två nycklarna är därmed beroende av varandra och bildar ett unikt par. För att skapa signaturen krävs tillgång till den privata nyckeln, men för att läsa signaturen och verifiera denna räcker det med att ha tillgång till den publika nyckeln. Detta är också den stora fördelen med tekniken, då den förenklar och säkrar nyckelhanteringen avsevärt. Den privata nyckeln bevaras hemlig hos ägaren, medan den publika kan göras tillgänglig för omvärlden. Därigenom kan säkerheten bevaras, samtidigt som man får en snabb och enkel distribution av nycklarna.

Asymmetrisk kryptering är således en förutsättning för digitala signaturer, där sändaren skapar signaturen med sin privata nyckel och mottagaren verifierar med den korresponderande publika nyckeln. Denna teknik, kombinerad med hashfunktionsteknik (som förklaras nedan), möjliggör att man kan skicka meddelanden säkert även över öppna nät, och är därmed viktig för att den elektroniska kommunikationen och handeln över sådana nät skall kunna utnyttjas och utvecklas.

### 2.3.3 Hashfunktionsteknik<sup>13</sup>

För att skapa en digital signatur kombineras asymmetrisk kryptering med en kontrollsumma, ett så kallat hashvärde, som är ett matematiskt framtaget sammandrag (kondensat) av innehållet i meddelandet. Sannolikheten att två olika meddelanden skulle ge upphov till identiska kontrollsummor är praktiskt taget obefintlig. Det är alltså denna hashfunktion som säkerställer att innehållet i meddelandet ej har förändrats sedan avsändandet. När kontrollsumman sedan krypterats med avsändarens hemliga nyckel har en digital signatur skapats. Den asymmetriska krypteringen används alltså för att binda upphovsmannen till den komprimerade datamängden, hashvärdet.

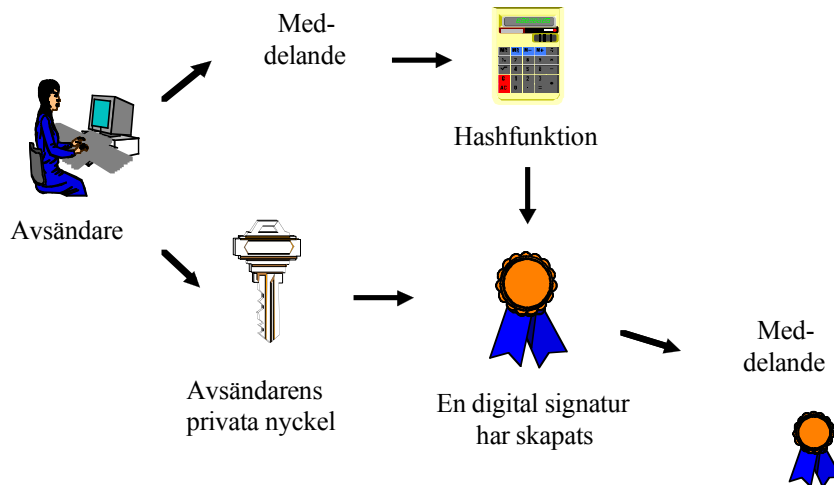
Genom att sedan dekryptera kontrollsumman och jämföra denna med en kontrollsumma skapad av det mottagna meddelandet kan mottagaren sedan försäkra sig inte enbart om att meddelandet härrör från avsändaren, utan också att informationen i meddelandet inte har ändrats sedan avsändandet.

---

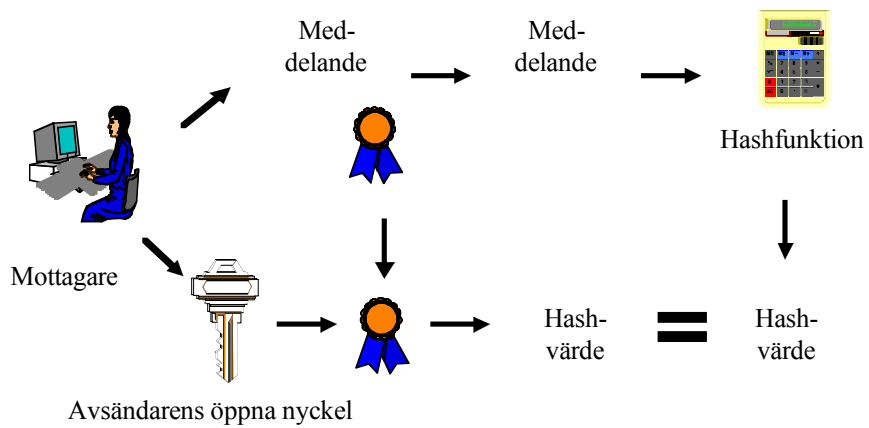
<sup>13</sup> Se föregående not.

### 2.3.4 Skapande och verifiering av digital signatur illustrerat

Skapandet av en digital signatur kan illustreras på följande sätt:



Verifieringen av den digitala signaturen går sedan till så här:



## 3 JÄMFÖRELSE MED NAMNTECKNING

Syftet med detta kapitel är att undersöka varför det i vissa fall ställs krav, antingen i lag/avtal eller av tradition, på egenhändig namnteckning för att genomföra vissa transaktioner. Det syfte som en namnteckning anses fylla i dessa fall skall utredas. När detta syfte utretts, och de funktioner som en namnteckning anses fylla förklarats, skall den elektroniska signaturen undersökas mot bakgrund av dessa funktioner. Avsikten med detta är att utreda om även den elektroniska signaturen kan fylla de funktioner som en namnteckning fyller minst lika bra (funktionell likvärdighet<sup>14</sup>), om inte kanske till och med bättre i vissa fall.

### 3.1 Syftet med namnteckning

Om man undersöker syftet bakom de bestämmelser som ställer krav på egenhändig namnteckning, samt även undersöker syftet med namnteckning i de övriga situationer där de används, finner man att en namnteckning av tradition anses fylla fem olika funktioner.<sup>15</sup>

Namnteckningen:

1. *identifierar* den som har undertecknat,
2. säkerställer det undertecknades *äkthet*,
3. har *bevisverkan*,
4. kan också sägas fylla en slags *viljefunktion*, samt
5. anses i vissa fall ha en *varningsfunktion*.

I det följande skall innebörden av ovanstående fem funktioner förklaras lite närmare. Det kommer då att framgå att dessa funktioner inte alltid är så lätta att hålla isär, utan ofta flyter ihop och går in i varandra. Jag har dock funnit att denna funktionsuppdelning ändå är det – i detta sammanhang – mest pedagogiska sättet att förklara syftet med namnteckning, och därför bygger diskussionen i det följande på ovanstående uppdelning.

#### 3.1.1 Identifikation

Namnteckningen identifierar den som har undertecknat ett dokument. Man kan också uttrycka det så att namnteckningen visar vem som är utställare av ett visst dokument. Genom att kontrollera en namnteckning kan man också verifiera att det är rätt person man har att göra med. Denna funktion kan en namnteckning fylla beroende på att den är personlig. I princip har varje människa en unik namnteckning. Därför kan denna användas för att identifiera en person. Detta förutsätter dock att man sedan tidigare vet hur en viss persons namn-

---

<sup>14</sup> Se ovan, kap 1.2, angående detta begrepp.

<sup>15</sup> Se bl a SOU 1987:40, s 107; Lindberg, Elektroniska originaldokument och elektronisk signatur, s 30 f; SOU 1996:40, s 232; Ds 1998:14, s 134 ff; Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om en gemensam ram för elektroniska signaturer, KOM(1998) 297 slutlig, 13.05.98, art 2; Hultmark, Elektronisk handel och avtalsrätt, s 29.

teckning ser ut, eller att man är närvarande när personen ifråga skriver sin namnteckning och i detta sammanhang kontrollerar dennes identitet.

### 3.1.2 Äkthet

Äkthetsfunktionen anses ofta, jämte identifieringsfunktionen, som en av de viktigaste funktionerna hos en namnteckning. Att en handling är äkta är ofta av den allra största vikt för dess betydelse och nytta för mottagaren. Att en handling är äkta innebär först och främst att dess innehåll härrör från den som framstår som utställare, dvs från den som undertecknat. En namnteckning på ett dokument anses garantera att uppgifterna i detta härrör från undertecknaren. Man kan också säga att innehållet i dokumentet genom namnteckningen på visst sätt knyts till den som undertecknat. I ett betänkande från Tulldatautredningen (TDU; se mer om denna nedan, kap 4.1) uttrycker man det så här:

*Det som skapar en signatur är dess unika form, som legalt binder ihop en person och en text.<sup>16</sup>*

Äkthetsfunktionen är möjlig på grund av att namnteckningen är personlig och därmed kan användas för att identifiera en person. För att kunna fastställa en viss namntecknings anknytning till en viss person krävs dock normalt, som också sades ovan, att man har en annan namnteckning, som man med säkerhet vet härrör från personen ifråga, som man kan jämföra med. Möjligheten att på detta sätt avslöja t ex förfalskningar varierar dock. Det är ju absolut inte omöjligt att förfalska en namnteckning. Vidare så kontrolleras oftast inte namnteckningar så särskilt noga i de flesta vardagliga transaktioner. Det är oftast först när det händer något som en namnteckning undersöks noggrannare.

En ytterligare aspekt på en handlingens äkthet är att en namnteckning ofta anses som ett slags garanti för att en handling i oförändrat skick härrör från den som undertecknat den, dvs att handlingen ej har förvanskats eller på något sätt har manipulerats sedan undertecknandet. Tanken är att då texten och underskriften fästs på papper skall man kunna se förändringar gjorda i efterhand. Denna funktion hos en namnteckning kan dock starkt ifrågasättas idag. De flesta handlingar skrivs nämligen idag ut med moderna metoder, inte för hand, och i dessa ”maskinskrivna” handlingar är det med dagens teknik relativt enkelt att göra förändringar i efterhand utan att detta framgår.

### 3.1.3 Bevisverkan

En namnteckning, liksom det dokument som är undertecknat med denna, fyller en viktig bevisfunktion. Förklaringen till detta är att ett pappersdokument anses relativt beständigt till sin natur och av tradition kan åberopas som skriftlig bevisning i domstol. Också denna funktion hos namnteckningen kan dock starkt ifrågasättas. Papper är ett ganska ömtåligt material, som både kan förfalskas och förstöras mycket enklare än många av de andra medel som idag kan användas för att lagra information (jämför ovan).

Namnteckningens bevisverkan följer av att man genom ett undertecknande förutsätts acceptera att ta på sig ett ansvar för ett dokumentets äkthet, korrekthet och fullständighet. Man förutsätts alltså genom undertecknandet erkänna sig bunden till dokumentets innehåll. Denna

---

<sup>16</sup> Se SOU 1987:40, s 107.

funktion beror på att en namnteckning anses ge uttryck för en vilja hos den som undertecknar, se mer om detta nedan.

### 3.1.4 Viljefunktion

En namnteckning kan sägas ha en viljefunktion på så sätt att den anses ge uttryck för undertecknarens vilja att bekräfta och/eller binda sig till innehållet i det undertecknade. Man brukar också uttrycka det så att den ger uttryck för och bekräftar en avsiktsförklaring hos undertecknaren.

### 3.1.5 Varningsfunktion

Namnteckningen anses i vissa fall även fylla en slags varningsfunktion. Tanken är att man genom att man måste underteckna en handling skall bli medveten om att man genom denna åtgärd kan bli rättsligt förpliktigad på ett eller annat sätt. Denna funktion ligger ganska nära viljefunktionen på så sätt att också denna funktion bygger på att man aktivt skall göra något, i detta fall underteckna en handling med sin namnteckning. Det är dock tveksamt om namnteckningen fyller en varningsfunktion i särskilt många situationer i dagens samhälle. Det har blivit så vanligt förekommande att man måste skriva under med sin namnteckning i nästan alla typer av transaktioner idag, så att i de allra flesta fall sker det nästan med mer eller mindre automatik, utan någon närmare eftertanke. Tanken bakom vissa av de krav på egenhändig namnteckning som finns i lag är dock, bl a, att det skall tjäna som en slags varnings-signal. Som exempel på en lagbestämmelse som bl a har detta som syfte kan nämnas 4 kap 1 § jordabalken (JB), som föreskriver att ett avtal om fastighetsköp, som ju oftast rör betydande värden, skall undertecknas av både säljare och köpare (annars är avtalet ogiltigt).

## 3.2 Hur den elektroniska signaturen kan fylla den traditionella namnteckningens funktioner

Det finns i svensk rätt inga krav på hur en namnteckning skall se ut eller hur den skall utföras. Därför finns det alltså inga hinder i detta avseende för att istället för namnteckning använda sig av elektronisk signatur. Däremot måste den elektroniska signaturen för att kunna accepteras, och därmed kunna användas i samma utsträckning som den traditionella namnteckningen, kunna fylla samma funktioner som denna. I det följande skall därför den elektroniska signaturen undersökas med avsikt att se om, och i så fall på vilket sätt, också denna skulle kunna fylla de funktioner som namnteckningen anses fylla.

### 3.2.1 Identifikation

Även den elektroniska signaturen kan användas för att identifiera en person. Detta är möjligt om den elektroniska signaturen kan verifieras på något sätt, t ex genom något tekniskt förfarande. Exempelvis kan en digital signatur verifieras med hjälp av den öppna nyckeln. Att man kan verifiera en elektronisk signatur innebär att man kan kontrollera vem den härrör ifrån. Det faktum att den elektroniska signaturen kan verifieras är dock inte tillräckligt för att identifieringsfunktionen skall kunna uppfyllas. Detta beror på att den elektroniska signaturen



inte är personlig på samma sätt som en namnteckning. Det finns inget naturligt eller nödvändigt samband mellan en person och dennes elektroniska signatur, så som fallet är med en namnteckning. Det enda som binder användaren till exempelvis en digital signatur är tillgången till en privat nyckel, och därför kan en sådan signatur i sig endast sägas bekräfta att det är innehavaren av den privata nyckeln som har signerat ett meddelande. För att dessutom kunna verifiera vem denna person är, dvs identifiera avsändaren, förutsätter systemet med elektroniska signaturer att kopplingen mellan en elektronisk signatur och en bestämd person fastställs. Detta kan ju givetvis skötas av parterna själva, genom att avsändaren – på något för mottagaren tillfredsställande sätt – bevisar sin identitet. Detta kan dock inte alltid ske, på grund av praktiska eller andra skäl. Ett annat alternativ är att uppdraga åt någon utomstående, en så kallad betrodd tredje part (TTP – Trusted Third Party), att fastställa och intyga sambandet mellan en signatur och en person. Denna uppgift är det tänkt att så kallade certifieringsorgan (Certification Authority, CA, eller Certification Service Provider, CSP, som de betecknas i EU:s direktivförslag) skall inneha. Dessa organ skall ge ut så kallade certifikat. Ett certifikat beskriver vem som är innehavare av en viss elektronisk signatur, dvs det binder samman en person med dennes elektroniska signatur. Vid användande av en digital signatur binder certifikatet alltså samman en person med ett visst nyckelpår.<sup>17</sup> Certifikatet kan vidare garantera identiteten hos innehavaren av en elektronisk signatur på så sätt att dennes identitet kan kontrolleras då denne registreras som innehavare av den elektroniska signaturen.

Frågorna kring hur de så kallade certifieringsorganens verksamhet bör regleras skall inte behandlas närmare i denna uppsats, men det är ändå viktigt att i detta sammanhang notera, att om denna verksamhet regleras på ett sådant sätt att tillit och förtroende skapas till dessa organ, så skapas även tillit till de certifikat som ges ut av dem – och därmed också till de elektroniska signaturer som utförs med stöd av certifikaten. Hur denna verksamhet skall regleras är alltså av stor betydelse för utvecklingen av elektroniska signaturer och deras rättsverkan. Regleras denna verksamhet på ett sådant sätt att den nödvändiga tilliten till elektroniska signaturer skapas, torde dessa signaturer – till och med bättre än den traditionella namnteckningen – kunna fylla identifieringsfunktionen hos en signatur. Som nämndes i avsnittet ovan om namnteckningens identifieringsfunktion, så behöver man känna till en viss persons namnteckning sedan tidigare eller kunna kontrollera denna mot en identitetshandling av något slag, men detta problem kommer man ifrån med systemet med elektroniska signaturer där en tredje part skall verifiera motpartens identitet.

Att sambandet mellan en elektronisk signatur och en bestämd person kan fastställas är dock inte i sig tillräckligt för att uppfylla identifieringsfunktionen. På detta sätt garanteras ju ej att det verkligen är rätt person som skapat den elektroniska signaturen. Exempelvis kan vem som helst, som har tillgång till den privata nyckeln till en digital signatur, och som vet hur denna nyckel fungerar, egentligen skapa en identisk digital signatur. Tanken är dock att även den elektroniska signaturen skall göras personlig på så sätt att endast en person skall kunna skapa den. Detta kan man åstadkomma på flera olika sätt. När det t ex gäller den digitala signaturen är det idag vanligast att den skapas med hjälp av ett så kallat smart kort (smart card; i Sverige används även benämningen aktivt kort) som man endast skall kunna använda sig av om man kan PIN-koden<sup>18</sup> till kortet. Det fungerar alltså ungefär på samma sätt som ett bankomatkort. En PIN-kod anses dock inte garantera ett fullständigt skydd mot obehörigt nyttjande. Det är omöjligt att helt förhindra att personer avslöjar sina PIN-koder till utomstående. Man håller dock på att utveckla säkrare alternativ till PIN-koden. Bl a undersöks olika

---

<sup>17</sup> Se Hultmark, Elektronisk handel och avtalsrätt, s 31.

<sup>18</sup> PIN står för Personal Identification Number.

så kallade biometriska metoder, dvs avläsning av fingeravtryck, iris eller liknande.<sup>19</sup> Med dessa metoder kan den elektroniska signaturen göras ännu säkrare än den är idag, och framför allt så skulle den bli personlig på så sätt att endast en person skulle kunna skapa en viss elektronisk signatur (jag bortser då från tvångs- och hotsituationer, men dessa situationer gäller ju på samma sätt vid användande av traditionella namnteckningar).

Av intresse i detta sammanhang, när identifieringsfunktionen diskuteras, är dessutom ett antal rättsfall inom processrättens område (bl a NJA 1981 sid 853, se mer om detta nedan, kap 6.1.2), som gäller det krav som tidigare fanns i rättegångsbalken (RB) att ett överklagande skulle vara egenhändigt undertecknat av klaganden eller dennes ombud. I dessa rättsfall har under vissa omständigheter nämligen godtagits även icke egenhändigt undertecknade överklaganden. Detta har motiverats mot bakgrund av en diskussion om syftet med föreskriften att ett överklagande skall vara egenhändigt undertecknat. Syftet med denna bestämmelse var enligt HD att göra det möjligt för rätten att konstatera att överklagandet härrörde från rätt person. Om överklagandet ej är egenhändigt undertecknat, men det av andra omständigheter kan bekräftas vem det härrör från, så fick enligt HD i dessa fall kravet på ett egenhändigt undertecknande anses uppfyllt ändå. I dessa rättsfall skulle man kunna säga att HD har tillämpat det funktionella perspektivet på den aktuella lagbestämmelsen, dvs man har utrett syftet med regeln och sedan accepterat att detta syfte har kunnat tillgodoses på annat sätt. Dessa rättsfall visar alltså att man med avseende på identifieringsfunktionen, i enlighet med det funktionella perspektivet, skulle kunna godkänna även en elektronisk signatur som uppfyllande kravet på egenhändigt undertecknande.

### 3.2.2 Äkthet

Denna funktion är, liksom nämndes ovan under 3.1.2, den jämte identifieringsfunktionen viktigaste funktionen hos en namnteckning. I ett betänkande från TDU diskuteras äkthetsfunktionens betydelse, samt den väsentliga frågan hur denna skall kunna uppfyllas av elektroniska dokument, på följande sätt:

*Det är viktigt att de dokument som skall överföras elektroniskt...skyddas. Det måste gå att med rimlig säkerhet bevisa att ett dokument är äkta, det vill säga att förklaringsinnehållet inte är manipulerat och att det verkligen härrör från den angivna utställaren.  
— — — Låset/staketet utgör enligt vår mening själva kärnan i ett fungerande system för elektronisk kommunikation med rättsverkningar.<sup>20</sup>*

Såsom framgår av detta citat samt av diskussionen om äkthetsfunktionen ovan under kap 3.1.2 består denna av två delar. En aspekt av äkthetsfunktionen är att det skall framgå att ett dokument verkligen härrör från den som framstår som utställare; den andra att man skall kunna säkerställa att dokumentet ej har förvanskats sedan avsändandet. Förstnämnda del av äkthetsfunktionen har ett nära samband med identifieringsfunktionen och därför hänvisas beträffande denna del till vad som anförts strax ovan, under kap 3.2.1, angående möjligheterna att säkerställa identifiering även med elektronisk signatur. Av framställningen i 3.2.1 följer att även den elektroniska signaturen skulle kunna fylla namnteckningens äkthetsfunktion vad gäller dess första del, dvs att kunna säkerställa att ett dokument verkligen härrör från den som framstår som utställare av dokumentet.

---

<sup>19</sup> Se Ds 1998:14, s 34 ff.

<sup>20</sup> Se SOU 1989:20, s 69 och 99.

Med hjälp av exempelvis kryptering och hashfunktionsteknik kan man garantera även den andra aspekten av äkthetsfunktionen vid elektronisk signering, dvs man kan säkerställa att dokumentet ej har förändrats – vare sig beroende på tekniska komplikationer eller obehöriga manipulationer – sedan avsändandet. Detta möjliggörs genom att det vid dekryptering av ett krypterat meddelande direkt framgår om meddelandet har förvanskats på vägen (se ovan, kap 2.2.3, angående denna teknik). I avsnittet om namnteckningens äkthetsfunktion ovan ifrågasattes denna funktion med den traditionella namnteckningen. Med elektronisk signering torde man dock kunna uppnå denna funktion bättre.

### 3.2.3 Bevisverkan

Frågan om bevisverkan kan uppdelas i två huvudfrågor. Den första gäller de formella kraven på bevisning, den andra de materiella. De formella rekvisiten regleras i ett lands processrättsliga regler och avser frågan vilka bevismedel som tillåts/accepteras enligt lag. De materiella rekvisiten rör trovärdigheten, dvs det så kallade bevisvärdet, av viss bevisning.<sup>21</sup>

När det gäller den första frågan, om formella krav på bevisning, så har vi i svensk rätt något som kallas fri bevisprövning. Detta innebär att vi inte har några regler om vad som utgör bra eller ”rätt” bevisning, utan i princip kan vad som helst accepteras som bevisning i en rättegång. Det finns alltså i svensk rätt inga formella processrättsliga hinder att åberopa en elektronisk signatur som bevisning om att t ex ett avtal ingåtts.

När det gäller den andra frågan så har vi även fri bevisvärdering i Sverige. Principen om fri bevisvärdering innebär att domstolarna fritt kan pröva den förebringade bevisningens styrka, dvs det finns inga legala bevisvärderingsregler i svensk rätt som domstolarna måste följa. Det kan emellertid vara tveksamt vilket bevisvärde en domstol skulle åsätta en elektronisk signatur. Det finns, vad jag vet, inga rättsfall hittills i Sverige där en domstol bedömt det juridiska bevisvärdet av ett elektroniskt dokument eller en elektronisk signatur. Om man vill åberopa en elektronisk signatur som bevisning beträffande något faktum, hur skall man då visa att den elektroniska signatur som användes i det aktuella fallet var säker nog för att kunna tjäna som fullgod bevisning? Denna fråga behöver dock inte nödvändigtvis lösas på rättslig väg, utan är snarare en teknisk fråga. Med teknikens hjälp kan man göra den elektroniska signaturen så säker att den får ett lika högt bevisvärde som en namnteckning har. Troligtvis kommer den, någon gång i framtiden, till och med att kunna ges ett högre bevisvärde än namnteckningen. (Vidare är det viktigt att de anknytande rutinerna utformas så att bevisföringen förenklas. Detta innebär att de ofta mycket tekniskt komplicerade rutinerna måste gå att förklara för rätten vid en eventuell process, utan alltför kostsamma och tidskrävande åtgärder.<sup>22</sup>)

### 3.2.4 Viljefunktion

När det gäller den digitala signaturen så utformas t ex kortrutinerna ofta så att användaren måste ange en särskild PIN-kod för att utföra själva signeringen. På detta sätt förutsätter signeringen ett visst mått av aktivt och medvetet handlande från den signerandes sida. Därmed kan även den digitala signaturen anses vara ett uttryck för användarens vilja att bekräfta och bli bunden av det meddelande denne signerar med sin privata nyckel, och därmed kan vilje-

<sup>21</sup> Mitrakas, *Open EDI and Law in Europe*, s 56.

<sup>22</sup> Furberg, *Rättsliga frågor rörande elektroniska ID-kort*, s 3.

funktionen uppfyllas också med den digitala signaturen. Samma sak gäller även för övriga former av elektroniska signaturer.

### 3.2.5 Varningsfunktion

Också varningsfunktionen skulle kunna tillgodoses vid användande av elektronisk signatur. För att återigen ta den digitala signaturen som exempel, så utformas nämligen oftast själva proceduren vid skapandet av en digital signatur så att användaren klart och tydligt blir varse när han verkligen signerar något och inte bara t ex loggar in på någon tjänst (se ovan). På detta sätt uppmärksammas han/hon på det faktum att en signatur håller på att skapas. Håller man bara den elektroniska signaturens olika funktioner klart åtskilda på detta sätt, och kanske även låter användaren bekräfta ytterligare en gång innan denne signerar något, så uppfylls varningsfunktionen med ett undertecknande även med en elektronisk signatur.

## 3.3 Sammanfattning

Av ovanstående jämförelse framgår att den elektroniska signaturen lika väl, i vissa fall till och med bättre, kan fylla de funktioner som en egenhändig namnteckning normalt fyller. Den kan, med hjälp av ett system med så kallade betrodda tredje parter, användas för att identifiera avsändaren av ett elektroniskt meddelande. Med nyttjande av krypterings- och hashfunktionsteknik kan den garantera äktheten av ett elektroniskt dokument, dvs säkerställa att dokumentet inte har förvanskats sedan avsändandet. Det finns inga processrättsliga hinder i svensk rätt att åberopa elektronisk signering som bevisning i en rättegång. Det kan dock i ett inledningsskede innebära vissa problem att utvärdera denna typ av bevisning, och de tekniska rutinerna bör därför lämpligen utformas så att denna bevisvärdering underlättas. Vidare kan de tekniska rutinerna utformas så att också vilje- och varningsfunktionerna uppfylls på ett tillfredsställande sätt även vid elektronisk signering. Sammanfattningsvis kan alltså även den elektroniska signaturen fylla de funktioner som namnteckningen fyller idag.

## 4 ELEKTRONISKA SIGNATURER I SVENSK RÄTT

När det gäller rättsverkan av elektroniska signaturer har i svensk rätt lagstiftning redan genomförts inom vissa områden av den offentliga förvaltningen, på så sätt att elektroniska dokument godtas istället för egenhändigt undertecknade handlingar i vissa fall. Tullverket var först i Sverige med att övergå från enbart pappersbaserade rutiner till att tillåta även elektroniskt uppgiftslämnande. Detta gjorde man år 1991. Då började tullverket ge företag möjligheten att digitalt signera handlingar för export- och importklarering. Därefter har man övergått till elektronisk dokumenthantering inom flera förvaltningsområden, men endast inom tre av dessa har man dessutom infört elektroniskt uppgiftslämnande som alternativ till det traditionella, skriftliga förfarandet. Detta har man gjort inom exekutionsväsendet (möjlighet att ge in ansökningar om verkställighet på medium för automatisk databehandling), skatteförvaltningen (möjlighet att inlämna elektroniska deklARATIONER) samt ifråga om pantbrevsregistret (möjlighet att ge in elektroniska ansökningar om registrering av datapantbrev). För närvarande undersöks även möjligheterna att införa ett elektroniskt ansökningsförfarande i inskrivningsärenden.<sup>23</sup>

I det följande skall några av ovannämnda lagstiftningsåtgärder undersökas. Därigenom får man insikt i de rättsfrågor som aktualiseras vid en övergång från pappersbaserade rutiner till elektroniska rutiner. Vidare får man förslag på hur frågorna kan lösas. Då tullverket var den första myndigheten i Sverige med att införa elektronisk dokumenthantering samt elektroniskt uppgiftslämnande, och därmed också har den längsta erfarenheten av elektronisk signering, har jag valt att undersöka tullverkets system mest ingående. Det har dessutom i stor utsträckning tagits efter inom de flesta andra myndighetsområden där möjligheter till elektroniskt uppgiftslämnande införts. Jag har dock även valt att ta upp de lagändringar som nyligen genomförts inom skatteförvaltningen i detta avsnitt. Detta på grund av att dessa lagändringar är det senaste som skett inom detta område samt för att dessa åtgärder troligtvis kommer att få störst genomslagskraft i det svenska samhället, eftersom de kommer att beröra så många människor.

Vidare skall i detta kapitel de straffrättsliga frågorna kring urkundsbroten kort beröras, liksom resultaten av en utredning som nyligen genomförts om elektronisk dokumenthantering inom hela förvaltningen och näringslivet. Avslutningsvis presenteras några av de föreningar som inom Sverige arbetar med att främja utveckling och användning av elektroniska signaturer samt med att utarbeta standarder för elektroniska signaturer. Dessa föreningar tas upp i detta kapitel då deras arbete kan komma att påverka svensk rätt genom att de standarder och riktlinjer som de utarbeta kan komma att utvecklas till handelsbruk.

---

<sup>23</sup> Se Ds 1997:84 Elektroniskt ansökningsförfarande i inskrivningsärenden m.m.

## 4.1 Elektroniskt uppgiftslämnande inom tullverket<sup>24</sup>

### 4.1.1 Tulldatautredningen

Möjligheterna till införande av elektroniskt uppgiftslämnande inom tullens verksamhetsområde började utredas redan år 1986. Då tillsattes en särskild tulldatautredning att utreda och lämna förslag till genomförande samt lagändringar. Resultaten av denna utredning, som blev mycket omfattande, finns att läsa i betänkandena Datorisering av tullens export- och importrutiner – Förstudie<sup>25</sup>, Tullregisterlag m.m. (delbetänkande)<sup>26</sup> samt Datorisering av tullrutinerna – Slutrapport<sup>27</sup>. Alla de utredningar som därefter gjorts hänvisar ofta till denna utredning. I utredningen redogörs t ex ingående för skillnaderna mellan det traditionella pappersdokumentet och dess elektroniska motsvarigheter. Även namnteckningens funktioner undersöks i ett av betänkandena (se om detta nedan, under 4.1.4).

### 4.1.2 Införande av begreppet elektroniskt dokument

Ett resultat av tulldatautredningen var införandet av ett nytt begrepp i svensk lagstiftning, nämligen begreppet ”elektroniskt dokument”. Syftet var att elektroniska dokument i tullagstiftningen skulle kunna jämföras med undertecknade urkunder på papper. Ett elektroniskt dokument definieras i tullagen som ”en upptagning vars innehåll och utställare kan verifieras genom ett visst tekniskt förfarande”.<sup>28</sup> I tullagen definieras dock inte vilket tekniskt förfarande som skall användas för denna verifiering, utan det har överlämnats till generaltullstyrelsen att reglera detta i författningar av lägre valör (se mer om detta nedan, kap 4.1.3). På detta sätt har man velat säkerställa att nya tekniska lösningar skall kunna tas i bruk när den tekniska utvecklingen går framåt. Begreppet ”elektroniskt dokument”, samt den definition det givits i tullagstiftningen, har man sedan tagit efter och använt sig av i nästan samtliga (alla utom de inom exekutionsväsendet) efterföljande lagändringar som genomförts i svensk rätt med anledning av införandet av elektronisk dokumenthantering inom vissa offentliga myndighetsområden.

### 4.1.3 Tulldatasystemet – TDS

Som ett resultat av tulldatautredningen upprättades även ett nytt datasystem för elektronisk ärendehantering inom tullen, kallat TDS (TullDataSystemet). I samband med införandet av TDS gavs också företag möjlighet att lämna in uppgifter till tullen på elektronisk väg. För detta krävs dock särskilt tillstånd. I 12 § tullagen föreskrivs att sådant tillstånd skall lämnas av generaltullstyrelsen. Där stadgas även att generaltullstyrelsen får förena ett sådant tillstånd med villkor om det tekniska förfarandet för uppgiftslämnandet samt om förfarandet i övrigt. Detta innebär alltså att generaltullstyrelsen har getts rättsliga befogenheter att utfärda närmare föreskrifter om det elektroniska förfarandet vid elektroniskt uppgiftslämnande. I det

---

<sup>24</sup> Informationen i detta avsnitt avseende Tulldatasystemet (TDS) har inhämtats från informationsbroschyerna ”Elektronisk uppgiftslämnande till tullverket” och ”TDS – Enkelt, Snabbt, Säkert”, samt ur Användarhandbok för TDS-anslutning; samtliga utgivna av generaltullstyrelsen.

<sup>25</sup> SOU 1987:40.

<sup>26</sup> SOU 1989:20.

<sup>27</sup> SOU 1989:40.

<sup>28</sup> För närvarande 12 § i denna lag.

följande skall dessa föreskrifter, samt hur själva systemet har byggts upp avseende signeringen, studeras närmare.

#### 4.1.4 Elektronisk signering i TDS

Den personliga namnteckningen har i TDS ersatts av ett system med elektroniska signaturer i form av elektroniska sigill. För att detta skulle kunna vara möjligt, dvs för att det elektroniska sigillet skulle erhålla samma status som en vanlig underskrift på papper, skall enligt generaltullstyrelsens föreskrifter följande grundregler gälla:

- 1) *Dokumentets innehåll måste låsas genom en teknisk metod.*
- 2) *Dokumentets utställare (personanknutet) måste kunna identifieras med en teknisk metod.*
- 3) *Enbart lösenord ger inte ett tillräckligt äkthetsskydd för dokument i TDS, vilket ställer krav på ett kortbaserat behörighetskontrollsystem (BKS) hos företagen.*
- 4) *Utställaren måste ha möjlighet att kontrollera innehållet i dokumentet innan han åsätter det elektroniska sigillet samt vidtaga någon medveten fysisk åtgärd när han godkänner detsamma (t ex knapptryckning).<sup>29</sup>*

I dessa grundregler kan man klart spåra tankarna bakom samtliga de funktioner som namnteckningen anses fylla, som diskuterades i föregående kapitel.

Företagen kommunicerar med tullverket via en mottagningsfunktion (MF). På uppdrag av tullverket svarar Telia AB för denna funktion. Den är dock fortfarande juridiskt en del av tullverket. I MF sker säkerhetskopiering av all överförd data. Direkt efter det att en datafil mottagits av MF, sker en säkerhetsarkivering. Detta arkiv tjänar som en referenspunkt över vad som skickats till eller från tullverket. Denna arkivering samt åsättandet av sigill (elektronisk signatur) anses uppfylla de krav på bevisning som kan komma att ställas vid en eventuell tvist.

Det elektroniska sigillet skall enligt generaltullstyrelsens föreskrifter produceras genom en av dem godkänd metod. För närvarande använder man ett system där det elektroniska sigillet (utställarsigillet) består av en kontrollsumma som erhålls genom kryptering, med hjälp av en hemlig nyckel, av en meddelandekontrollsumma (dokumentsigill). Dokumentsigillet beräknas automatiskt med ledning av innehållet i meddelandet och en öppen sigillnyckel. Nycklarna distribueras i de behörighetskort (smarta kort) som tullverket utfärdar själv. Tullverket har alltså valt att arbeta utan en extern CA. Idag finns ca 7 000 kort i daglig användning i 500 företag, och tre fjärdedelar av det totala antalet klareringshandlingar hanteras idag helt elektroniskt.<sup>30</sup>

## 4.2 Elektroniska deklARATIONER

Redan år 1994 föreslogs, i samband med en offentlig utredning om vilka lagändringar som var nödvändiga för en övergång till elektronisk dokumenthantering inom skatteförvaltningen,<sup>31</sup> införandet av möjligheten att inlämna självdeklARATIONER på elektronisk väg. Denna

<sup>29</sup> Se Elektronisk uppgiftslämning till tullverket, s 12.

<sup>30</sup> Dessa sifferuppgifter tagna ur Ds 1998:14, s 68.

<sup>31</sup> Ds 1994:80.

möjlighet infördes dock inte vid detta tillfälle, beroende på att det var tveksamt om skattebrottslagen (1971:69) omfattade även elektroniska handlingar. Regeringen valde därför att avvakta översynen av skattebrottslagen.<sup>32</sup> I samband med de lagändringar som genomfördes vid denna översyn utmönstrades begreppet ”handling” ur skattebrottslagen och ersattes av uttrycket ”på annat sätt än muntligen”. Denna förändring syftade till att undanröja det tvivel som kunde uppkomma beträffande frågan om en oriktig uppgift som lämnas på ADB-medium eller liknande sätt omfattas av skattebrottslagen.<sup>33</sup> Därmed kvarstod inte längre detta som hinder för tillåtande av elektroniskt uppgiftslämnande inom skatteförvaltningen, och då upprättades ett nytt lagförslag<sup>34</sup> där denna möjlighet slutligen infördes. Detta förslag antogs år 1997 och de nya bestämmelserna om elektroniska deklARATIONER trädde i kraft den 1 november samma år.<sup>35</sup>

Numera stadgas i 2 kap 1 § 2 st lagen (1990:325) om självdeklaration och kontrolluppgifter att självdeklaration, efter särskilt medgivande av Riksskatteverket eller skattemyndighet som Riksskatteverket bestämmer, får avges i form av ett elektroniskt dokument. Elektroniskt dokument definieras på liknande sätt som i tullagen, nämligen som ”en upptagning som gjorts med hjälp av automatisk databehandling och vars innehåll och utställare kan verifieras genom ett visst tekniskt förfarande”. Liksom i tullagstiftningen har det överlämnats till Riksskatteverket (RSV) att tillse att den tekniska lösning som väljs för signering garanterar att tillräcklig säkerhet uppnås. Som följer av lagtexten skall det också, på samma sätt som i tullagstiftningen, krävas tillstånd för att få inlämna uppgifter i elektroniska dokument. I dessa tillstånd kommer parternas åtaganden och ansvar för informationen och förmedlingen att regleras närmare. RSV skall också ha möjlighet att i verkställighetsföreskrifter bestämma vilka tekniska och administrativa förfaranden som skall krävas för att en deklARATION skall få avges i ett elektroniskt dokument.<sup>36</sup> Dessa föreskrifter, liksom det system som skall användas inom skatteförvaltningen, har dock inte färdigställts ännu. Visserligen trädde bestämmelserna om att deklARATIONER skall få lämnas i form av elektroniska dokument i kraft den 1 november 1997 och skall egentligen kunna tillämpas fr o m taxeringsåret 1998, men enligt uppgift från RSV kommer systemet med elektroniska deklARATIONER troligtvis inte att kunna börja tillämpas förrän tidigast någon gång efter sekelskiftet. Detta är den tid som det beräknas ta att komma fram till den tekniska lösning som skall väljas för det elektroniska uppgiftslämnandet samt för utarbetande av de tillstånd som kommer att krävas.<sup>37</sup>

### 4.3 Straffrättens bestämmelser om brott mot urkund

Att brotten mot urkund innefattar även elektroniska dokument och elektroniska signaturer är av största vikt för att skapa allmänt förtroende till dessa dokument och signaturer. Om inte exempelvis förfalskning eller förnekande av en elektronisk signatur är straffbart, såsom fallet är med traditionell namnteckning, kan det nämligen vara svårt att uppnå den för denna nya teknik nödvändiga tilliten bland dess användare. År 1989 tillsattes en särskild utredare att undersöka om förändringar av de straff- och processrättsliga reglerna var nödvändiga med hänsyn till utvecklingen inom data- och teletekniken. Denna utredning (benämnd datastraff-

---

<sup>32</sup> Ds 1994:80, s 21 f.

<sup>33</sup> Se prop. 1995/ 96:170, s 161.

<sup>34</sup> Prop. 1996/97:100.

<sup>35</sup> Infördes genom SFS 1997:495.

<sup>36</sup> Se 8 § förordningen (1990:1237) om självdeklaration och kontrolluppgifter.

<sup>37</sup> Källa: Gunilla Berg, ADB-jurist vid RSV.



rättsutredningen) överlämnade sitt betänkande<sup>38</sup> år 1992. Av utredningen framgår att det krävs lagändringar för att ge elektroniska dokument och elektroniska signaturer ett likvärdigt straffrättsligt skydd som deras traditionella, pappersbaserade motsvarigheter. Detta bedömdes som nödvändigt på grund av att brottsbalkens bestämmelser om urkundsbroten– och då framför allt brottsbeskrivningarna – ansågs vara präglade i alltför hög grad av den skriftliga handlingens, som oftast är angreppsobjektet för dessa brott, utpräglat materiella och specifika natur.<sup>39</sup>

Vidare anförde datastraffrättsutredningen att elektroniska dokument visserligen åtnjuter visst skydd inom redan gällande strafflagstiftning (bl a genom straffbestämmelserna om dataintrång, skadegörelse, olovlig avlyssning och bedrägeri), men detta skydd ansågs som klart otillräckligt.<sup>40</sup> Utredningen påpekade också att man visserligen i rättspraxis, under trycket av den tekniska utvecklingen, godtagit vissa elektroniska dokument som urkunder. Detta ”trots att den ofrånkomliga prövningen av det berörda objektets äkthet endast varit möjlig genom resonemang som inte är förenliga med BrB:s synsätt och systematik”.<sup>41</sup> Man påpekade i detta sammanhang att man i praxis därmed ibland tangerat gränsen för vad som kan anses vara straffrättsligt godtagbar analogibildning. Därför krävdes enligt utredningens mening lagstiftningsåtgärder för att även elektroniska dokument och signaturer skulle innefattas av urkundsbroten.

Ännu har dock inga lagstiftningsåtgärder vidtagits med anledning av datastraffrättsutredningen. Ärendet är fortfarande under behandling inom Regeringskansliet. När det gäller urkundsbroten utarbetades i början av året (1998) en promemoria inom straffrättsenheten på Justitiedepartementet.<sup>42</sup> I denna promemoria dras slutsatsen att inga lagstiftningsåtgärder är nödvändiga beträffande urkundsbroten. Detta på grund av att man anser att urkundsbegreppet även kan innefatta handlingar som framställts med tekniska hjälpmedel. Möjligen anses en lagändring dock kunna behövas i ett avseende, nämligen vad gäller förnekande av digital signatur. För närvarande är det belagt med straff att förneka en urkunds uppgift om utställare, men endast om uppgiften utgörs av en underskrift. Man anser därmed i promemorian att förnekande av digital signatur inte innefattas av denna straffbestämmelse. Även ett sådant förnekande skulle dock, menar man, ”kunna beivras om bestämmelsen om förnekande av underskrift gavs en mer generell utformning”.<sup>43</sup> Inom Justitiedepartementet är man dock tveksam till slutsatsen att inga andra lagändringar behövs och därför skall i slutet av november en hearing hållas med representanter från offentlig förvaltning för att utröna om lagstiftningsåtgärder är nödvändiga eller ej. Det får därför anses i vart fall oklart om och i vilken utsträckning elektroniska dokument och elektroniska signaturer idag åtnjuter ett straffrättsligt skydd.

#### 4.4 Utredningen om elektronisk dokumenthantering<sup>44</sup>

År 1994 tillsattes en särskild utredare med uppdrag att utarbeta förslag till rättslig reglering som kan behövas när elektroniska dokument och tjänster för förmedling av elektroniska

<sup>38</sup> SOU 1992:110 Information och den nya Informationsteknologin – straff- och processrättsliga frågor m.m.

<sup>39</sup> A bet, s 230 och 268.

<sup>40</sup> A bet, s 267.

<sup>41</sup> A bet, s 249 f.

<sup>42</sup> Straffrätt och informationsteknik – en grundläggande inventering av lagstiftningsbehovet, daterad 1998-03-17.

<sup>43</sup> Straffrätt och informationsteknik, s 59.

<sup>44</sup> SOU 1996:40.

meddelanden skall ersätta traditionella rutiner inom hela förvaltningen. Denna utredning, som antog namnet IT-utredningen, slutfördes år 1996. Utredningen föreslog att definitioner av begreppen elektronisk handling, digitalt dokument, digital signatur och digital stämpel förs in i förvaltningslagen. På detta sätt ansågs nämligen rättsregler skrivna för traditionell pappersbaserad uppgiftshandling – med endast smärre justeringar – kunna tillämpas också i IT-miljö, utan att de allmänna principerna för en rättssäker ärendehandläggning behöver rubbas. Vidare föreslogs, för de fall där en förfaranderegulering i lag, om handläggning av förvaltningsärenden, föreskriver något som medför att elektronisk dokumenthantering inte kan användas – t ex att handlingar skall vara egenhändigt undertecknade – en bestämmelse om att regeringen får föreskriva att digitala dokument eller, när det kan anses tillräckligt, elektroniska handlingar utan digital signatur får användas. Utredningens förslag behandlas för närvarande inom Justitiedepartementet. För närvarande avvaktar man dock det direktiv om elektroniska signaturer som skall antas inom EU innan man vidtar några åtgärder inom detta område.<sup>45</sup>

## **4.5 Föreningar som verkar inom området elektroniska signaturer**

Det finns flera föreningar i Sverige som verkar inom området elektronisk handel och kommunikation, och som därmed också på ett eller annat sätt arbetar även med elektroniska signaturer. Här kan inte alla dessa presenteras, utan jag har valt att ta upp de två föreningar vars arbete jag bedömer har varit/är av störst betydelse för utvecklingen av elektroniska signaturers rätts- och bevisverkan. Dessa föreningar är Toppledarforum och SEIS.

### **4.5.1 Toppledarforum<sup>46</sup>**

Toppledarforum är ett samarbete mellan Svenska Kommunförbundet, Landstingsförbundet och staten i syfte att skapa förutsättningar för förnyelse inom den offentliga förvaltningen med hjälp av IT-användning. Inom Toppledarforum startades hösten 1994 projektet ”Elektronisk handel”. Avsikten med detta projekt var att utreda och lämna förslag till hur ett införande av elektronisk handel för kommuner, landsting och stat skulle kunna genomföras. I juni 1997 antog Toppledarforum ett förslag om en gemensam IT-säkerhetslösning inom den offentliga sektorn. Lösningen baseras på användning i tjänsten av smarta kort med de tre grundläggande säkerhetsfunktionerna enligt SEIS specifikationer (se nedan). Som ett resultat av detta projekt har 70 procent av landets kommuner, 91 procent av landstingen och 69 procent av de statliga myndigheter som har minst hundra anställda påbörjat förberedelserna till övergången till elektronisk handel.<sup>47</sup> Att stat, kommuner och landsting börjar utnyttja den nya tekniken med elektronisk kommunikation är viktigt, inte bara för de samhällsekonomiska vinster som kan uppnås, utan även för att deras användande av denna nya teknik bidrar till att skapa förtroende för den hos allmänheten.

---

<sup>45</sup> Källa: Roger Pettersson vid Justitiedepartementet.

<sup>46</sup> Informationen inhämtad från skriften Elektronisk handel för kommuner, landsting och stat.

<sup>47</sup> Dessa siffror är från 1 januari 1998, källa: Staffan Sundström, projektledare för projektet ”Elektronisk handel”; från artikeln ”Offentlig sektor tar nästa steg med elektronisk handel”.

#### 4.5.2 SEIS<sup>48</sup>

SEIS, som står för Säkrad Elektronisk Information i Samhället, är en ideell förening vars medlemmar är privata och statliga företag i Sverige. SEIS, som bildades våren 1995, har till syfte att arbeta för en säker elektronisk kommunikation i öppna nät. För att kunna möjliggöra detta har arbetet inom SEIS inriktats på att utveckla tekniska specifikationer samt standarder för tekniska metoder som skall möjliggöra att elektronisk information skall kunna skyddas mot förfalskning, förvanskning, manipulation samt okontrollerad åtkomst. Det skall även vara möjligt att kunna fastställa informationens ursprung och innehåll. Som ett resultat av detta arbete har man inom ramen för SEIS tagit fram en standard för ett elektroniskt ID-kort, EID. Detta är ett smart kort som skall möjliggöra säker identifiering och signering över öppna nät. Kortet innehåller för detta ändamål tre funktioner: elektronisk identifiering, digital signatur samt stöd för kryptering.

Arbetet inom SEIS, i synnerhet arbetet med att ta fram standarder inom detta område, kan bli betydelsefullt för rättsverkan av elektroniska signaturer. Utvecklingen av standarder är betydelsefull på så sätt att de kan förenkla förfarandet i rättsliga tvister genom att bevisföringen underlättas.

## 4.6 Sammanfattning

Sammanfattningsvis kan konstateras att lagstiftning redan genomförts på en rad områden där elektroniska dokument godtas istället för egenhändigt underskrivna handlingar. Dessa lagar inom förvaltningsrätten har alla det gemensamt att den myndighet som skall tillämpa lagen också har ett inflytande över tillämpningen av reglerna om elektronisk dokumenthantering och myndigheten har getts befogenhet att utfärda närmare anvisningar om hur denna hantering skall gå till. Dock bör påpekas att, även om regleringarna är snarlika till sin utformning, så förekommer en hel del avvikelser – främst som ett resultat av de föreskrifter som respektive myndighet gett ut – och dessa avvikelser medför att vad som gäller för en myndighet inte automatiskt kan appliceras på en annan myndighet för vilken annan lagstiftning är tillämplig, dvs det saknas enhetliga regler vad gäller rättsverkan av digital signatur. Detta kan skapa rättsosäkerhet (se mer om detta nedan, kap 6.1.6).

---

<sup>48</sup> Informationen om SEIS inhämtad från föreningens hemsida [www.seis.se](http://www.seis.se); informationen om EID inhämtad från pressinformation från ITS (Informationstekniska standardiseringen) 1998-09-29.

## **5 INTERNATIONELLA HARMONISERINGSARBETEN AVSEENDE ELEKTRONISKA SIGNATURER**

I denna uppsats skall, som nämndes inledningsvis, den lagstiftning som i många andra länder införts kring elektroniska signaturer inte behandlas. Den som är intresserad av detta hänvisas till andra framställningar inom detta område. Exempelvis innehåller departementspromemorian om digitala signaturer (Ds 1998:14) en internationell utblick. Emellertid skall i detta kapitel två viktiga internationella rättsliga harmoniseringsarbeten avseende elektroniska signaturer uppmärksammas. Dessa är för det första det direktivförslag om elektroniska signaturer som lagts fram inom EU, för det andra de modellregler för elektroniska signaturer som för närvarande håller på att utarbetas inom UNCITRAL. Direktivförslaget är av intresse för denna uppsats då detta framtida direktiv så småningom måste implementeras i, och därmed kommer att ha direkt påverkan på, svensk rätt. UNCITRAL:s modellregler har jag valt att presentera i denna uppsats då dessa, med sina förslag till lösningar på rättsfrågorna kring elektroniska signaturer, kan tjäna som inspiration och mall för eventuella framtida svenska bestämmelser – oavsett om i form av lag eller avtal – angående rättsverkan av elektroniska signaturer. Vidare skulle de även kunna komma att få direkt påverkan på svensk rätt, genom att de skulle kunna utvecklas till handelsbruk.

### **5.1 EU:s direktivförslag om en gemensam ram för elektroniska signaturer**

I maj i år (1998) lade Kommissionen fram ett första direktivförslag om en gemensam ram för elektroniska signaturer.<sup>49</sup> Man har inom EU bedömt det som nödvändigt att införa en gemensam rättslig ram för elektroniska signaturer inom unionen för att de möjligheter som elektronisk kommunikation och handel kan erbjuda skall kunna utnyttjas på bästa sätt. Lagstiftning inom detta område har redan påbörjats i flera medlemsstater, vilket kan leda till olika bestämmelser för bl a rättsligt erkännande av elektroniska signaturer i medlemsstaterna. Detta i sin tur kan skapa hinder för elektronisk kommunikation och elektronisk handel och därigenom hindra utvecklingen av den inre marknaden. Därför anser man inom EU att det behövs en harmoniserad rättslig ram avseende elektroniska signaturer på europeisk nivå. Det främsta syftet med direktivet skall vara att garantera rättsligt erkännande, i synnerhet över gränserna, av elektroniska signaturer och av certifieringstjänster. Tyngdpunkten i direktivet ligger dock på det sistnämnda, dvs frågan vilka krav som skall ställas på tillhandahållare av certifieringstjänster inom unionen.

Direktivförslaget har under sommaren och hösten bearbetats inom EU (i ministerrådets telearbetsgrupp) på så sätt att alla medlemsstater har fått framföra synpunkter. En hel del förändringar har skett. Framställningen i det följande baseras på det omarbetade direktivförslag som idag<sup>50</sup> föreligger. Det skall dock påpekas att det fortfarande kan komma att ske en hel del förändringar i detta innan direktivet slutligt antas. Enligt tidtabellen skall detta ske nästa vår, och medlemsstaterna skall ha infört erforderlig lagstiftning senast 1 januari 2001.

---

<sup>49</sup> Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om en gemensam ram för elektroniska signaturer, KOM(1998) 297 slutlig, 13.05.98. Finns att läsa på Internet, på adressen [europa.eu.int/comm/dg15/en/media/infso/com297sv.pdf](http://europa.eu.int/comm/dg15/en/media/infso/com297sv.pdf) (svensk version).

<sup>50</sup> November 1998.

De för denna uppsats intressanta artiklarna i direktivförslaget är artiklarna 1 och 5. I artikel 1 fastslås direktivets tillämpningsområde, i artikel 5 regleras rättsverkan av elektronisk signatur.

### 5.1.1 Direktivets tillämpningsområde

Enligt artikel 1 syftar direktivet till att underlätta användning av elektroniska signaturer samt till att bidra till deras rättsliga erkännande. Från början var det tänkt att direktivet skulle tillerkänna elektroniska signaturer rättsligt godkännande, men den artikel som gäller rättsverkningarna av elektroniska signaturer (artikel 5; se mer om denna nedan) är en av de bestämmelser som stött på hårdast motstånd från medlemsstaterna. Denna bestämmelse har därför ständigt förändrats under arbetets gång, och idag återstår inte mycket av det från början tilltänkta rättsliga erkännandet av elektroniska signaturer. Vidare sägs i artikel 1 att direktivet inte skall gälla frågor med avseende på ingående av och giltighet av avtal eller andra rättsliga förpliktelser för vilka formkrav uppställs i nationell rätt eller gemenskapsrätt, och att det inte heller skall påverka regler och begränsningar som finns i nationell rätt eller gemenskapsrätt avseende brukandet av handlingar. Detta innebär att bestämmelsen om elektroniska signaturers rättsverkningar inte skall vara tillämplig på sådana fall där det i lag uppställs formkrav. Detta gäller formkrav inom förvaltningsrätten såväl som inom avtalsrätten. Detta motiveras i direktivet med att direktivet inte skall syfta till att harmonisera nationell avtalsrätt eller andra utomobligatoriska formaliteter som kräver signatur. Denna begränsning av direktivets tillämpningsområde är ytterligare en bidragande orsak till att direktivet inte tillerkänner elektroniska signaturer någon större grad av rättsligt godkännande (se mer om detta nedan).

### 5.1.2 Rättsverkan av elektroniska signaturer

Artikel 5 reglerar frågan om rättsverkan av elektroniska signaturer. Den har följande lydelse i den senaste versionen av direktivförslaget (den engelska versionen återges här, då det i skrivande stund ännu ej finns någon svensk översättning):

#### *Article 5*

#### *Legal effects*

1. *Member States shall ensure that advanced electronic signatures which are based on a qualified certificate [and which are created by devices meeting the requirements laid down in Annex III]*
  - a) *satisfy the legal requirement of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies that requirement in relation to paper-based data, and*
  - b) *are admissible as evidence in legal proceedings.*
2. *Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that the signature is in electronic form, or is not based upon a qualified certificate, or is not based upon a qualified certificate issued by an accredited certification service provider [or is not created by a signature device meeting the requirements laid down in Annex III].*

En ”advanced electronic signature” definieras i artikel 2 (1) (bis) som en elektronisk signatur som uppfyller följande krav:

- a) *it is uniquely linked to the signatory;*
- b) *it is capable of identifying the signatory;*
- c) *it is created using means that the signatory can maintain under his sole control; and*
- d) *it is linked to the data to which it relates in such a manner that any subsequent alteration of the data is detectable.*

I artikel 5 fastställs alltså vad gäller rättsverkan av elektronisk signatur att en så kallad ”avancerad elektronisk signatur” skall tillerkännas samma rättsliga status i förhållande till elektroniska dokument som en handskriven namnteckning har i förhållande till pappersdokument. Vad innebär då detta? Enligt uppgifter om vad som har framkommit vid de förhandlingar som pågått inom EU med anledning av direktivet (och som har vidarebefordrats till den externa referensgrupp som bildats inom Kommunikationsdepartementet) innebär detta att direktivet – när det gäller frågan om rättsverkan av elektronisk signatur – inte syftar till att jämställa elektroniska signaturer med namnteckningar över lag, utan endast syftar till att säkerställa att elektroniska signaturer skall tillerkännas samma rättsverkningar som traditionella namnteckningar *i de fall där elektroniska dokument godtas i nationell rätt*. Detta är dock inte särskilt enkelt att sluta sig till efter att ha läst artikeltexten. Skall direktivet – och då särskilt artikel 1 och 5 – tolkas på detta sätt, så vore det önskvärt att detta framgick med större tydlighet.

Vidare stadgas i artikel 5 att ”avancerade elektroniska signaturer” även skall kunna användas som bevis vid rättsliga förfaranden. I andra punkten fastslås att övriga typer av elektroniska signaturer inte skall få diskrimineras ur rättslig synvinkel enbart därför att de är i elektronisk form, eller för att de inte baseras på så kallade kvalificerade certifikat (certifikat som uppfyller vissa krav som specificeras i en bilaga till direktivförslaget).

### 5.1.3 Hur kommer detta direktiv att påverka svensk rätt?

I motiveringen till direktivet sägs att en mycket viktig del av harmoniseringen är harmoniserade regler beträffande elektroniska signaturers rättsverkan. Det sägs att de rättsverkningar som elektroniska signaturer medför är ett nyckelelement i ett öppet men samtidigt trovärdigt system för elektroniska signaturer. Dock kommer direktivet inte att ha någon större påverkan på frågan om rättsverkan av elektroniska signaturer då alla de fall då det uppställs formkrav i nationell rätt undantas från direktivets tillämpningsområde. Detta innebär att direktivet, inklusive dess bestämmelse om rättsverkan av elektronisk signatur (artikel 5), endast kommer att ha betydelse för sådana fall där elektroniska dokument godtas enligt nationell rätt. Detta torde inte ha någon inverkan på svensk rätt, då den lagstiftning som idag i svensk rätt godtar elektroniska dokument just syftar till att tillerkänna dessa samma rättsliga status som undertecknade urkunder på papper (jfr ovan, kap 4.1.2). Det enda som egentligen fastslås angående rättsverkan av elektronisk signatur i direktivet är i stort sett att det måste säkerställas att de skall kunna användas som bevis vid rättsliga förfaranden i alla medlemsstater. Detta innebär inte heller någon påverkan på svensk rätt. Som nämndes ovan under avsnittet om bevisverkan så har vi redan fri bevisprövning i svensk rätt, vilket innebär att elektroniska signaturer redan kan godtas som bevis vid rättsliga förfaranden i Sverige.

Direktivet kommer alltså inte att få någon större inverkan på svensk rätt. Dock bör i detta sammanhang även nämnas att man nyligen<sup>51</sup> lagt fram ett nytt direktivförslag inom EU, som

---

<sup>51</sup> Den 18 november 1998.

syftar till att etablera en enhetlig rättslig ram för utvecklingen av elektronisk handel inom den inre marknaden. Detta direktiv planeras gå längre i harmoniseringsarbetet. I detta direktivförslag föreslås nämligen att medlemsstaterna skall bli skyldiga att ändra sina lagar så att alla regler som förhindrar eller begränsar elektroniskt avtalsslutande tas bort. Med andra ord föreslås att medlemsstaterna skall ändra alla de formkrav där enbart traditionella handskrivna namnteckningar godkänns. Detta direktiv är avsett att komplettera direktivet om elektroniska signaturer. Om detta direktiv skulle gå igenom och medlemsstaterna skulle bli skyldiga att avskaffa alla formkrav i sina nationella lagar skulle elektroniska signaturer kunna bli helt jämställda med handskrivna namnteckningar. Frågan är dock om medlemsstaterna kommer att gå med på detta ganska stora ingrepp i deras nationella rättssystem. Som utretts i kapitel 3 ovan, föreligger det, enligt min mening, inga principiella hinder mot att jämställa elektroniska signaturer med traditionella namnteckningar, men det finns troligtvis psykologiska ”spärrar” mot detta. Förslaget att ändra på formkraven i de olika nationella rättsordningarna kommer därför sannolikt att stöta på motstånd.

## 5.2 UNCITRAL:s modellregler för elektroniska signaturer<sup>52</sup>

UNCITRAL, FN:s handelsrättskommission, har till syfte att främja harmonisering av internationell handelsrätt, i syfte att underlätta internationell handel. UNCITRAL utarbetar internationella konventioner, modellagar och modellregler inom handelsrättsområdet. Syftet med modellagar och -regler är, att medlemsstater, om de så önskar, skall kunna antaga dessa som nationell rätt, alternativt utforma egen nationell lagstiftning med dem som förebild. De kan även tjäna som riktlinjer vid tolkningen av redan befintliga allmänna regler. År 1996 antogs inom UNCITRAL en modellag för elektronisk handel.<sup>53</sup> För närvarande pågår även arbete med att utforma modellregler för elektroniska signaturer. Dessa modellregler är avsedda att komplettera modellagen för elektronisk handel. Därför skall denna först kort presenteras, innan modellreglerna för elektroniska signaturer behandlas.

### 5.2.1 Modellagen för elektronisk handel

Syftet med modellagen för elektronisk handel är att förenkla och främja elektronisk kommunikation i internationell handel. Modellagen för elektronisk handel bygger på principen om funktionell likvärdighet (*functional equivalency*), dvs att elektroniska motsvarigheter till traditionella pappersbaserade rutiner, som lika väl kan fylla ”pappersmediets” funktioner, bör anses likvärdiga med – och därmed även tillerkännas samma rättsverkningar som – dessa. Denna princip fastslås i modellagens artikel 5, som stadgar att information inte skall förnekas rättsverkningar, giltighet eller verkställighet enbart på grund av att den är i elektronisk form. I nästföljande artiklar fastslås sedan i vilka fall elektroniska motsvarigheter till pappersbaserade koncept skall anses funktionellt likvärdiga med de sistnämnda. I artikel 7 stadgas i vilka fall funktionell likvärdighet skall anses föreligga när lagen ställer krav på underskrift. Denna artikel reglerar alltså med andra ord i vilka fall ett lagstadgat krav på underskrift skall anses vara uppfyllt när det gäller elektroniska meddelanden. Artikel 7 (1) har följande lydelse:

*Article 7. Signature*

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

<sup>52</sup> Informationen i detta avsnitt har inhämtats från UNCITRAL:s hemsida [www.un.or.at/uncitral](http://www.un.or.at/uncitral).

<sup>53</sup> UNCITRAL Model Law on Electronic Commerce.

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

*(b) That method is as reliable as was appropriate for the purpose for which the data was generated or communicated, in the light of all the circumstances, including any relevant agreement.*

I denna bestämmelse synes man ha tagit fasta på identifierings- och viljefunktionerna som de viktigaste funktionerna hos en namnteckning. Möjligen skulle även äkthetsfunktionen kunna inrymmas i denna bestämmelse. I förslaget till modellregler för elektroniska signaturer finns mer detaljerade bestämmelser om de tekniska metoder som kan användas för att uppfylla kravet under punkten a) ovan. Där regleras också frågan om bevisverkan av de olika metoder för elektronisk signering som kan användas.

## 5.2.2 Modellreglerna för elektroniska signaturer<sup>54</sup>

Syftet med modellreglerna är dels att etablera en säkerhetsram för elektroniska signaturer, dels att tillerkänna skriftliga och elektroniska meddelanden likvärdig status när det gäller rättsverknningar – allt detta för att främja brukandet av elektronisk kommunikation. I det följande skall de för denna uppsats mest intressanta modellreglerna presenteras. Det är dock viktigt att notera att, då reglerna ännu ej är färdigställda, denna framställning baseras på det underlag som hittills har utarbetats (inför de senaste förhandlingarna inom UNCITRAL, som hölls i månadsskiftet juni/juli 1998), men att dessa regler alltså kan komma att ändras flera gånger innan de slutligen antas.

## 5.2.3 Två olika typer av elektroniska signaturer

Modellreglerna utgår – liksom EU-direktivet – från två olika typer av elektroniska signaturer. Förutom ”vanliga” elektroniska signaturer skall det även finnas en kvalificerad form av elektroniska signaturer, så kallade ”säkra” elektroniska signaturer.<sup>55</sup> I modellreglerna finns därför två olika definitioner av elektronisk signatur; en definition för en ”elektronisk signatur”, en definition för en ”säker elektronisk signatur”. En elektronisk signatur definieras i artikel 1(a) som:

*[D]ata in electronic form in, affixed to, or logically associated with, a data message, and [that may be] used to [identify the signer of the data message and indicate the signer's approval of the information contained in the data message][satisfy the conditions set forth in article 7(1)(a) of the UNCITRAL Model Law on Electronic Commerce];<sup>56</sup>*

En ”säker elektronisk signatur” definieras i sin tur i artikel 1(b) i förslaget till modellregler för elektroniska signaturer som:

*[A]n electronic signature which [is created and][as of the time it was made] can be*

<sup>54</sup> UNCITRAL Draft Uniform Rules on Electronic Signatures.

<sup>55</sup> Det bör dock påpekas att denna term inte är slutligen bestämd ännu. Ett annat begrepp som föreslås i modellreglerna är ”enhanced electronic signature”, som på svenska närmast kan översättas till förhöjd eller förstärkt elektronisk signatur.

<sup>56</sup> Text inom hakparenteser indikerar text som kanske inte skall ingå i den slutliga utformningen av en artikel.



*verified through the application of a security procedure or combination of security procedures that ensures that such electronic signature:*

*(i) is unique to the signer [for the purpose for][within the context in] which it is used;*

*(ii) can be used to identify objectively the signer of the data message;*

*(iii) was created and affixed to the data message by the signer or using a means under the sole control of the signer; [and]*

*[(iv) was created and is linked to the data message to which it relates in a manner such that any change in the data message would be revealed].*

#### 5.2.4 Skillnaderna mellan de två typerna av elektroniska signaturer

Distinktionen mellan en ”vanlig” elektronisk signatur och en ”säker” sådan har gjorts av den anledningen att man har velat behålla modellreglerna teknikneutrala (dvs att de skall tillåta brukande av alla möjliga typer av elektroniska signaturer) samtidigt som man ändå har velat reglera rättsverkan av elektroniska signaturer under vissa givna förutsättningar. Därför finns dessa två typer av elektroniska signaturer, för vilka åsyftas finnas skillnader i rättslig status i modellreglerna. De så kallade säkra elektroniska signaturerna kommer att ha den fördelen att de skall åtnjuta på förhand bestämt erkännande som funktionellt likvärdiga med handskrivna signaturer. Men även övriga typer av elektroniska signaturer, än de som på förhand klassificerats som ”säkra”, skall kunna uppnå rättsligt erkännande som elektroniska signaturer med rättsverkan, under förutsättning dock att de uppfyller det tillförlitlighetsprov som fastställs i artikel 7(1)(b) i modellagen (se ovan, kap 5.2.1). Skillnaden är dock att i dessa fall måste denna rättsverkan fastställas i efterhand, efter det att den elektroniska signaturen brukats, vid någon form av rättslig prövning. En ytterligare fördel med de säkra elektroniska signaturerna är att med brukandet av dessa kommer att följa vissa presumtioner. Exempelvis presumeras enligt artikel 3 ett meddelande ha blivit signerat om (alternativt från och med den tidpunkt då) en säker elektronisk signatur tillfogats ett meddelande. I artikel 4 finns en presumptionsregel för frågan om från vem en elektronisk signatur skall anses härröra (så kallad *presumption of attribution*). För närvarande föreligger två varianter till denna artikel. Variant A placerar bevisbördan på den som av omständigheterna ser ut att ha undertecknat. Variant B placerar bevisbördan på den förlitande parten istället. Vidare finns i artikel 5 en presumptionsregel om ett elektroniskt meddelandes äkthet (i detta avseende avser jag med äkthet att ett meddelande inte har förvanskats sedan avsändandet; på engelska *integrity*). Enligt denna bestämmelse skall ett elektroniskt meddelande eller en elektronisk signatur (eventuellt i brist på bevis på motsatsen) presumeras att inte ha förvanskats, om den som signerat använt sig av en säkerhetsprocedur som kan producera (eventuellt krav på tillförlitliga) bevis på att ett meddelande eller någon säker elektronisk signatur därpå inte har förändrats sedan den tidpunkt då säkerhetsproceduren applicerades på meddelandet eller signaturen. Nämda presumptionsregler skall dock eventuellt, om arbetsgruppen för elektronisk handel inom UNCITRAL skulle finna det mer lämpligt, omformuleras så att de uppställer rättsverkningar istället för presumtioner.

I artikel 6 i modellreglerna anges hur man skall bestämma vilka elektroniska signaturer som skall utgöra så kallade säkra elektroniska signaturer (*Pre-determination of [enhanced] [secure] electronic signature*). Enligt denna artikel skall en säkerhetsprocedur, eller en kombination av säkerhetsprocedurer, klassificeras som en säker elektronisk signatur, antingen genom att det organ eller den myndighet som utses av staten att besluta i dessa frågor beslutar om detta, eller – vad gäller förhållandet mellan den person som signerar ett meddelande och

någon som förlitar sig på det signerade meddelandet – om parterna uttryckligen kommer överens om detta.

### 5.3 Sammanfattning

EU:s direktivförslag om en gemensam ram för elektroniska signaturer kommer, som ovan nämndes, troligtvis inte (som direktivförslaget ser ut idag) att påverka svensk rätt i någon nämnvärd utsträckning. Det enda som direktivet egentligen stadgar angående rättsverkan av elektronisk signatur är att elektroniska signaturer skall kunna användas som bevisning i rättsliga förfaranden. Detta påverkar ej svensk rätt då vi tillämpar principen om fri bevisprövning. I övrigt innebär direktivet att elektroniska signaturer, i de fall där elektroniska dokument godtas i nationell rätt, skall tillerkännas samma rättsverkningar som traditionella namnteckningar har i förhållande till pappersdokument. Detta torde inte heller ha någon inverkan på svensk rätt, då den lagstiftning som idag i svensk rätt godtar elektroniska dokument just syftar till att tillerkänna dessa samma rättsliga status som undertecknade urkunder på papper (jfr ovan, kap 4.1.2).

UNCITRAL:s förslag till modellregler innehåller som ovan nämnts två olika typer av elektroniska signaturer. En av dessa, de så kallade ”säkra” elektroniska signaturerna, erbjuder den fördelen att den dels skall åtnjuta på förhand bestämt erkännande som funktionellt likvärdig med handskrivna signaturer, och dels skall kunna ge upphov till vissa presumtioner. Detta system utgör en lämplig avvägning mellan alternativen att helt reglera elektroniska signaturer, och tillåta självreglering med därmed bibehållen teknikneutralitet. Observera dock att de bestämmelser som här behandlats ännu så länge bara föreligger som förslag, och att det alltså inte alls är säkert att de kommer att se ut så här i den slutgiltiga versionen av modellreglerna.

## 6 SLUTSATSER

Vilka slutsatser kan man då dra av de föregående kapitlen angående frågan vilken rättsverkan en elektronisk signatur har?

Denna diskussion bör lämpligen indelas i två delfrågor.

1. Vad gäller i de fall då det i lag eller avtal ställs krav på undertecknande (så kallade formkrav)?
2. Vad gäller i de fall då det i övrigt krävs, alternativt förväntas, att man skall underteckna något?<sup>57</sup> Det kan t ex ofta följa av sedvänja eller handelsbruk att man skall underteckna något. Vad gäller i dessa fall?

### 6.1 Elektronisk signatur i de fall då det uppställs formkrav

Kan en elektronisk signatur användas istället för en egenhändig namnteckning när det i lag(eller avtal) ställs krav på ”underskrift”, ”undertecknande”, ”egenhändigt undertecknande” etc?

#### 6.1.1 Lagstiftarens syn

I flera av de lagstiftningsärenden samt offentliga utredningar som nämndes i fjärde kapitlet har man ansett att då det i lag ställs krav på ”underskrift” etc, torde detta krav inte kunna uppfyllas med elektroniska rutiner. Exempelvis skriver man både i SOU 1996:40 (s 95) och i Ds 1998:14 (s 77 f och 131) att det torde krävas lagändringar för att elektroniska signaturer skall tillerkännas samma rättsverkan som den traditionella namnteckningen, på så sätt att de regler som innehåller formkrav ändras så att elektroniska signaturer – som tillkommit med erforderlig grad av säkerhet – tillskrivs samma verkan som egenhändiga namnteckningar.

Vad gäller begreppet underskrift kan även nämnas de uttalanden som gjordes i den departementspromemoria angående straffrättsliga frågor med anknytning till utvecklingen av informationstekniken, som nämndes ovan under kap 4.3. I denna ansågs en lagändring kunna behövas i ett avseende, nämligen vad gäller förnekande av elektronisk/digital signatur. Man ansåg nämligen straffbestämmelsen om förnekande av underskrift inte kunna innefatta även elektronisk signatur.<sup>58</sup>

Som ytterligare exempel på lagstiftarens syn på frågan hur den nya företeelsen med elektroniska dokument och elektroniska signaturer passar in i det befintliga regelverket kan nämnas de lagändringar som nyligen genomförts inom skatteområdet, då bl a bestämmelserna om skattetillägg i 5 kap 1, 2 och 4 §§ taxeringslagen (1990:324), liksom bestämmelsen om förseningsavgift i 5 kap 5 § samma lag, samt 7 kap 1 och 4 §§ lagen om punktskatter och pris-

---

<sup>57</sup> Adlercreutz använder termen ”konventionella formkrav” för vissa av dessa fall, se Adlercreutz, Allmän avtalsrätt, s 123.

<sup>58</sup> Straffrätt och informationsteknik, s 59.

regleringsavgifter ändrades så att dessa skulle omfatta även uppgifter som getts in elektroniskt. Exempelvis har bestämmelsen om förseningsavgift i 5 kap 5 § taxeringslagen ändrats på så sätt att den inte längre endast talar om att förseningsavgift tas ut om en deklarationshandling inte är behörigen undertecknad, utan även om den *inte är i form av ett elektroniskt dokument*.<sup>59</sup> Dessa lagändringar tyder även de i hög grad på att lagstiftaren anser att elektroniska signaturer inte kan intolkas under begreppen, och därmed uppfylla kraven på, ”underskrift”, ”undertecknande”, ”skriva under” etc.

Sammanfattningsvis så verkar alltså lagstiftarens åsikt vara den att det krävs lagstiftningsåtgärder för att jämställa elektroniska signaturer med traditionella namnunderskrifter. Detta innebär med andra ord, att enligt lagstiftarens åsikt kan inte elektronisk signering, enligt gällande rätt, godtas istället för en traditionell namnteckning, i de fall då det i lagar eller föreskrifter ställs krav på underskrift.

### 6.1.2 På vilken grund baseras lagstiftarens åsikt?

Man kan då ställa sig frågan på vilken grund man från lagstiftarens sida baserar denna sin åsikt att elektroniska signaturer ej kan innefattas i begreppen ”underskrift”, ”undertecknande” etc. Det yttrande som riksåklagaren (RÅ) gjorde i sitt remissyttrande över förslagen i Ds 1994:80 till ändringar i skattelagstiftningen, liksom de yttranden som skattebrottsutredningen gjorde till följd av RÅ:s yttrande, illustrerar detta ganska väl. Dessa yttranden rör visserligen i detta fall handlingsbegreppet, men kan även appliceras på ovanstående begrepp. RÅ yttrade att det, med hänsyn till den innebörd ordet handling har i det allmänna språkbruket, var nödvändigt att i skattebrottslagen införa en definition av vad som i lagen förstås med begreppet handling. Skattebrottsutredningen anförde vidare följande angående denna fråga:

*Begreppet handling, eller dess ibland använda synonym skriftlig handling, har haft en tämligen självklar och entydig betydelse både i det allmänna språkbruket och inom rättstillämpningen. Till följd av den lagstiftning som varit påkallad med anledning av utvecklingen på dataområdet har termen emellertid mist sin tidigare givna betydelse. I vissa sammanhang, men inte andra, har lagstiftaren givit ordet handling en ny innebörd, där de s k upptagningarna för ADB innefattas. — — — Mot bakgrund av vad Datastraffrättsutredningen påpekat beträffande ”upptagning” i tryckfrihetsförordningen – att begreppet inte syftar på information som läses på samma sätt som innehållet i en urkund... – synes emellertid under alla förhållanden gälla att tryckfrihetsförordningens definition av ”handling” inte är helt adekvat för den betydelse som bör tilläggas begreppet i skattebrottslagen. Om ”handling” bibehålls som ett rekvisit i skattebrottslagen fordras således en närmare precisering av begreppet för att även elektroniska deklARATIONER skall omfattas av lagens straffbestämmelser.*<sup>60</sup>

Om man ifrån detta uttalande drar paralleller till elektroniska signaturer så skulle man kunna dra den slutsatsen att ett hinder mot att innefatta även elektronisk signering i de lagbestämmelser som ställer krav på ”underskrift”, ”undertecknande” etc är den betydelse som dessa uttryck har i det allmänna språkbruket. De som ansluter sig till detta synsätt gör det på den grunden att de anser att då dessa uttryck ej särskilt definieras i svensk rätt så måste de därmed förstås och definieras på samma sätt som i det allmänna språkbruket. Det bör i detta sammanhang tilläggas att myndigheterna, som är de som i första hand tillämpar lagar och föreskrifter, i varje fall inte tar det steget; att tolka dessa regler som innefattande även elektro-

<sup>59</sup> För definitionen av ett elektroniskt dokument, se ovan, kap 4.1.2.

<sup>60</sup> SOU 1995:10, s 214 ff.

niska signaturer. Det skulle därför troligtvis krävas att någon först drev ett fall till högsta instans för ett klargörande. De som anser att den språkliga lydelsen av ifrågasvarande regler förhindrar brukandet av elektroniska signaturer är därför av den uppfattningen att de lagregler och myndighetsföreskrifter som stadgar krav på underskrift etc troligtvis måste ändras så småningom.<sup>61</sup>

Vidare kan även noteras att även det resonemang som i ovannämnda citat förs om att lagstiftaren i vissa fall, men inte i andra, har givit ordet handling en ny innebörd, har relevans även för elektroniska signaturer. Genom de lagändringar som diskuterades i fjärde kapitlet har elektroniskt signerade dokument nämligen accepterats som jämställda med undertecknade pappershandlingar inom vissa områden, medan det råder oklarhet vad som gäller inom de områden där så ej skett. Detta bidrar ytterligare till rättsosäkerheten (jfr ovan, kap 4.6).

Avslutningsvis kan även nämnas att man i SOU 1996:40 anger det faktum att telefaxmeddelanden tidigare i praxis inte ansetts uppfylla rättegångsbalkens krav på att text ett överklagande skall vara egenhändigt undertecknat som ett exempel på att elektroniska rutiner inte torde godtas när det krävs egenhändigt undertecknande i lag.<sup>62</sup>

### 6.1.3 Andra synpunkter på denna fråga – det funktionella perspektivet

Om man anlägger ett funktionellt perspektiv på rätten (dvs går efter principen att elektroniska motsvarigheter till traditionella pappersbaserade rutiner, som lika väl kan fylla "pappersmediets" funktioner, bör anses likvärdiga med dessa och därmed även tillerkännas samma rättsverkningskraft) skulle man dock kunna godta elektroniska signaturer istället för traditionella namnteckningar redan enligt gällande rätt. Man skulle då kunna tillämpa de regler som idag ställer krav på "underskrift" etc även på elektroniska signaturer. Tolkar man lagen på detta sätt brukar man även tala om att man tillämpar en teleologisk (ändamålsinriktad) lagtolkningsmetod. Detta innebär att man ser till ändamålet, syftet, med en lagregel och låter detta vara avgörande i det enskilda fallet, dvs om detta syfte kan uppfyllas lika väl på något annat sätt än det i lagregeln angivna sättet så kan detta godtas.<sup>63</sup>

Tillämpar man det funktionella perspektivet fullt ut, så skulle man kunna tillämpa de regler som uppställer formkrav direkt även på elektroniska signaturer. Denna slutsats bygger på den grunden att en språklig analys av orden "underskrift", "undertecknande" etc inte leder någon vart, för vad är en underskrift? Det finns inga lagstadgade krav på en underskrift, utan den kan i princip se ut hur som helst. Det viktigaste är, i grund och botten, att det av denna "underskrift" – i vilken form den än må vara – ger uttryck för något slags godkännande av, eller ansvar för, innehållet i ett dokument. Detta syfte kan även den elektroniska signaturen fylla.

---

<sup>61</sup> Rådman Per Furberg, som medverkat i ett flertal av de utredningar som nämnts i denna uppsats, är exempelvis av denna åsikt. Han anser det mycket tveksamt att en domstol skulle intolka elektroniska signaturer som uppfyllande lagstadgade formkrav. Källa: Per Furberg.

<sup>62</sup> SOU 1996:40 s 95.

<sup>63</sup> Christina Hultmark, professor i handelsrätt vid Göteborgs Universitet, anser att samtliga de problem som elektroniska signaturer ger upphov till kan lösas med hjälp av redan befintliga allmänna regler. Som Sveriges representant i UNCITRAL, anser hon att elektroniska signaturer kan jämföras med handskrivna underskrifter i sådana fall där syftet bakom kravet på underskrift också kan tillgodoses med elektronisk signering, dvs enligt modellagens princip om funktionell likvärdighet. Se bl a Elektronisk handel och avtalsrätt, s 43 f samt Digital signatur – internationella utvecklingstendenser, Anförande vid XIV Nordiske konferens om retsinformatik 9-11 september 1998.

Det bör dock i detta sammanhang även påpekas att det funktionella perspektivet kan tillämpas även i det fall att man skulle anse att begreppet ”underskrift” skall tolkas enligt dess betydelse i allmänt språkbruk. Man skulle då nämligen enligt det funktionella perspektivet kunna tillämpa de regler som talar om underskrifter analogt på elektroniska signaturer.<sup>64</sup>

Tolkar man lagen i enlighet med det funktionella perspektivet, och alltså undersöker syftet bakom de regler som innehåller krav på underskrift etc, så kommer man att märka att alla dessa regler inte nödvändigtvis har samma syfte, trots att ofta samma begrepp används i dessa lagrum. Detta innebär att trots förekomsten av samma begrepp i två olika lagrum så kan de inte automatiskt tolkas på samma sätt. Som exempel kan nämnas att begreppet ”handling” inte nödvändigtvis behöver innebära ett krav på att något finns nedtecknat på papper. Som exempel på att så inte behöver vara fallet kan nämnas det syfte som begreppet ”handling” ansågs ha i den gamla skattebrottslagen. Vid översynen av denna lag togs detta begrepp bort ur skattebrottslagen år 1996 (se ovan under 4.2), och ersattes av uttrycket ”på annat sätt än muntligen”. Detta var nämligen enligt skattebrottsutredningens mening det bakomliggande syftet med begreppet ”handling” i skattebrottslagen, att skilja mellan muntliga uppgifter (som inte kan leda till straffansvar) och uppgifter i handlingar.<sup>65</sup> På samma sätt har inte heller kravet på egenhändigt undertecknande samma syfte i alla de regler där det förekommer. Som exempel på detta kan nämnas att det krav som förut fanns i RB att vissa handlingar, exempelvis överklaganden, skulle vara egenhändigt undertecknade hade som syfte att möjliggöra för rätten att konstatera att handlingen härrörde från rätt person (se mer om detta nedan), dvs syftet var att möjliggöra identifiering. Detta är dock inte det enda syftet med alla de lagregler som ställer krav på undertecknande. Många andra sådana regler har exempelvis som främsta syfte att säkra bevisning. Ett exempel på en sådan bestämmelse är formkravet för fastighetsköp i 4 kap 1 § JB.<sup>66</sup>

#### 6.1.4 Exempel från praxis där man tillämpat det funktionella perspektivet

Det finns exempel i praxis där man använt sig av metoden att undersöka syftet bakom en rättsregel. Bland dessa kan nämnas NJA 1968 s 81, NJA 1981 s 853, NJA 1991 s 407 och NJA 1991 sid 595. Alla dessa fall rör det krav, som nämndes ovan, som förr fanns i RB på att ett överklagande skulle vara egenhändigt undertecknat. Av dessa fall har jag här valt att ta upp NJA 1981 s 853, som jag bedömer som det för denna uppsats mest intressanta av dessa rättsfall. I detta rättsfall hade en besvärslinaga (dvs ett överklagande) undertecknats med ”Prisoner 1006”, istället för med den dömdes rätta namn. Enligt 52 kap 3 § 3 st RB i dess då gällande lydelse skulle en besvärslinaga vara egenhändigt undertecknad av den klagande eller dennes ombud (detta krav avskaffades år 1994). HD godtog dock ”undertecknandet” i detta fall. Detta beslut motiverades mot bakgrund av en diskussion om syftet med föreskriften att en besvärslinaga skulle vara egenhändigt undertecknad. Syftet med denna bestämmelse var enligt HD att göra det möjligt för rätten att konstatera att inlagan härrörde från rätt person. Om inte namnet används försvaras visserligen denna identifiering, men HD uttalade att ”om det av andra omständigheter framgår vem som undertecknat inlagan, får kravet på egenhändigt undertecknande anses uppfyllt”.

---

<sup>64</sup> Analogisk rättstillämpning innebär att man tillämpar en lagregel utanför dess språkliga betydelseområde när det i övrigt föreligger likheter mellan det aktuella fallet och det fall som omfattas av lagtexten. Se angående rättstillämpning och lagtolkning t ex Lehrberg, Praktisk Juridisk metod.

<sup>65</sup> Se prop. 1995/96:170, s 104.

<sup>66</sup> Se motiven till detta lagrum, bl a prop. 1970:20 Del B, s 125.

Detta rättsfall visar att ett krav på undertecknande inte nödvändigtvis behöver innebära ett ovillkorligt krav på att man måste underteckna med sitt rätta namn. Kanske skulle det även kunna tolkas så att det inte heller nödvändigtvis måste röra sig om ett undertecknande med ett namn över huvud taget, utan att det viktigaste är att det framgår från vem en handling härrör och att det alltså är oväsentligt *hur* detta framgår. I så fall så skulle man även kunna godkänna en elektronisk signatur som uppfyllande kravet på egenhändigt undertecknande, åtminstone i identifieringshänseende. I detta sammanhang bör dock kanske nämnas att det finns de som anser att dessa rättsfall inte kan tolkas på detta sätt, utan som anser att det enda som dessa rättsfall utsäger är att kravet på underskrift i dessa fall inte var absolut. Med andra ord skall de enligt denna åsikt tolkas så att det i vissa fall gick bra *utan* namnteckning, men inte så att elektronisk signatur skulle kunna användas istället för traditionell namnteckning.<sup>67</sup> Enligt min åsikt skulle de dock *även* kunna tolkas på det sätt som jag ovan tolkat dem. Det ena utesluter nämligen inte det andra. Kommer man fram till att ett krav på undertecknande inte är absolut i ett enskilt fall så innebär ju detta att inget hinder föreligger för att använda en elektronisk signatur i dess ställe. Det enda som kvarstår är ju syftet med regeln, nämligen att man skall kunna utröna att en handling härrör från rätt person, och om kravet på egenhändigt undertecknande inte är absolut kan man fastställa detta på vilket sätt som helst bara det fyller sitt ändamål – att identifiera avsändaren. Detta kan en elektronisk signatur, som vi har sett ovan, göra.

#### 6.1.5 Andra invändningar mot strikt bokstavstolkning

Det i avsnittet ovan nämnda resonemanget om ordens språkliga betydelse som hinder för att tillämpa befintliga regler på elektroniska signaturer skall kommenteras i det följande. Detta resonemang aktualiserar en intressant fråga, nämligen frågan i vilken utsträckning den språkliga tolkningen av rättsreglerna skall vara styrande för hur de tillämpas. I detta sammanhang kan den s k begreppsjurisprudensen<sup>68</sup> nämnas. Detta var en rättsvetenskaplig skola som uppstod i mitten på 1800-talet i Tyskland. Den gick ut på att man inom juridiken ville uppnå en likadan exakthet som man hade inom naturvetenskaperna. Detta gjorde man genom att systematisera juridikens begrepp och ge dem ett slags objektiv och tidlös giltighet av samma slag som naturvetenskapens begrepp. Varje juridiskt begrepp skulle alltså ha sitt en gång för alla bestämda innehåll. Rättsreglerna skulle sedan med hjälp av detta system kunna tillämpas genom enkel, logisk subsumtion under de etablerade juridiska begreppen. Denna skola fick mycket kritik, och kritiken består än idag. De kritiska åsikter som har framförts mot begreppsjurisprudensen skulle även kunna riktas mot det ovan nämnda resonemanget om språkets betydelse som hinder för att acceptera elektroniska signaturer som substitut för namnteckningar. Bl a kan den invändningen resas mot detta resonemang, att språket faktiskt inte alltid kan vara styrande för rättstillämpningen. Exempelvis är lagtext inte så sällan vag och/eller tvetydig, så att den inte kan ge bestämt besked i ett enskilt fall. Faktum är att det är omöjligt att utforma lagtext så att den är helt otvetydig vid alla tänkbara fall. Ibland kan visserligen ledning om vad ett ord eller uttryck i en lagregel skall anses betyda inhämtas t ex i motiven, men inte heller de begreppsdefinitioner som kan finnas i dessa kan alltid ge fullständiga svar på alla frågor. Det skall dock påpekas att det faktum att lagtext ofta är tvetydig inte alltid nödvändigtvis behöver vara något ont. Tvärtom kan det i vissa fall vara bra. Detta kan nämligen ge domstolarna ett visst svängrum i vissa fall, när det gäller att komma fram

<sup>67</sup> Per Furberg är av denna åsikt. Källa: Per Furberg.

<sup>68</sup> Se om begreppsjurisprudensen Strömholm, Rätt, rättskällor och rättstillämpning – En lärobok i allmän rättslära, s 87 samt Lehrberg, Praktisk juridisk metod, s 128 f.

till en lämplig och rimlig lösning i det enskilda fallet. På detta sätt kan man alltså säkerställa att det finns ett visst mått av flexibilitet i rättssystemet.

### 6.1.6 Egna slutsatser

Som framgått föreligger i svensk rätt två olika åsikter angående frågan om lagstiftningsåtgärder krävs eller ej för att elektroniska signaturer skall vara jämställda med traditionella namnteckningar. Båda åsikterna har fog för sig. Personligen är jag dock mer benägen att ansluta mig till dem som anser att det funktionella perspektivet bör vara avgörande. Faktum är att detta också är det inom svensk avtalsrätt vanligaste sättet att tolka lagen. Vi har inom detta område ingen strikt bokstavstrogen tolkningslära, utan ändamålsöverväganden får oftast vara avgörande. Jag måste dock erkänna att det faktum att det idag redan genomförts lagändringar inom vissa rättsområden – men inte i andra – för att jämställa elektroniska dokument med pappersdokument, har givit upphov till viss tveksamhet från min sida. Enligt min mening skulle nämligen dessa lagändringar kunna ge upphov till en viss risk för att domstolarna, istället för att göra analogislut med anledning av dessa (dvs dra paralleller till dessa), gör e contrario-slut<sup>69</sup> (dvs motsatsslut) i vissa fall. Beroende på det sätt som en domstol väljer att tillämpa rätten<sup>70</sup>, kan resultatet alltså bli väldigt olika, och vilket sätt en domstol kommer att använda sig av är svårt att förutse. Det är detta som man kan få kunskap om genom att studera praxis, men inom detta område finns, mig veterligen, ännu inga rättsfall och därför kan man inte undersöka denna fråga i detta fall.

Enligt min åsikt så bör dock en ändamålsenlig lagtolkning ske, så att de regler och föreskrifter som stadgar om ”underskrift”, ”undertecknande” etc kan tillämpas analogt även på elektroniska signaturer. Detta är inget främmande för svensk rättstradition, att låta ändamålet med en lagregel vara avgörande, särskilt i sådana här fall där särskild reglering saknas. Att låta ändamålet med rättsreglerna vara avgörande leder också oftast till det mest välharmoniserade resultatet i slutändan. Det gagnar även rättssäkerheten att tillämpa samma regler på de olika företeelser som kan användas för att fylla samma syfte samt för att nå samma resultat.

## 6.2 Elektronisk signatur i övriga fall då namnteckning brukas

Ovan har diskuterats vad som gäller om en elektronisk signatur används istället för en traditionell namnteckning när det uppställs krav på undertecknande i svensk rätt. Svensk rätt kräver dock sällan underskrifter för att uppnå rättsverkan och rättsföljder. Ofta krävs alternativt förväntas det att man godkänner eller bekräftar diverse handlingar med en namnteckning ändå. I dessa fall är det oftast i bevissyfte som man ställer krav på namnteckning, dvs i dessa fall är det närmast en fråga om bevisverkan. I kapitlet där namnteckningens funktioner diskuterades konstaterades redan att det i denna avsikt ej fordras några lagändringar då vi i svensk rätt tillämpar principerna om fri bevisprövning och fri bevisvärdering. I detta avseende kan dock bevisvärderingen ge anledning till viss tveksamhet när det gäller elektroniska

---

<sup>69</sup> Att en domstol gör ett e contrario-slut innebär att domstolen resonerar ungefär så här: Om nu lagstiftaren har ansett det nödvändigt att lagstifta inom vissa områden för att jämställa dessa två dokumenttyper så måste lagstiftaren anse att de inte redan är att jämställa. Och detta måste i sin tur innebära att, inom de områden där lagstiftaren ej har genomfört några förändringar, måste denne vara av den åsikten att dessa inte bör jämställas i dessa fall.

<sup>70</sup> Se mer om rättstillämpning samt de olika lagtolkningsmetoder som finns exempelvis i Lehrberg, Praktisk juridisk metod.



signaturer. Som nämndes i avsnittet om bevisverkan av elektroniska signaturer (3.2.3), är det svårt att idag förutspå hur en domstol skulle värdera en elektronisk signatur som åberopades som bevisning i en rättslig tvist. Frågan är alltså vilket bevisvärde en domstol skulle åsätta en elektronisk signatur. Detta är naturligtvis beroende av hur säkert man kan bedöma att den aktuella signaturen verkligen härrör från den som påstås, alternativt utger sig för att, vara avsändare. Och detta är i sin tur beroende av hur säker den elektroniska signatur som brukats i det aktuella fallet är. Även i detta avseende kan tveksamhet uppstå. Fråga kan nämligen uppstå hur domstolen skall kunna utvärdera en elektronisk signatur. Hur skall domstolen kunna uttröna att den elektroniska signaturen i det aktuella fallet var säker, åtminstone lika säker som en traditionell namnteckning? Såsom också påpekades i avsnittet ovan om bevisverkan av elektroniska signaturer är detta dock inga sådana frågor som behöver lösas på rättslig väg, utan dessa frågor löses lämpligast av de som utformar de tekniska systemen för elektronisk signering. Dessa måste utforma de tekniska procedurerna och rutinerna kring elektroniska signaturer – i vilken form de än må vara – på ett sådant sätt att bevisföringen säkras och förenklas i görligaste mån för användarna. Viktigt att tänka på i detta hänseende är bl a att de tekniska procedurerna och rutinerna dels bör kunna kontrolleras i efterhand (jfr tullens system med säkerhetsarkivering, se ovan 4.1.4), dels bör relativt enkelt kunna förklaras för en domstol. Säkras bevisföringen på detta sätt kan tillit skapas till de elektroniska signaturerna, och då skulle de även kunna tillerkännas samma bevisvärde (och därmed samma bevisverkan) som traditionella namnteckningar.

Vad gäller rättstillämpningen är det dock viktigt att notera, och i synnerhet viktigt för domstolarna att tänka på, att man inte bör ställa för höga krav på elektroniska signaturer. Man bör inte ställa högre krav på dessa än på traditionella namnteckningar. Som en amerikansk rättsvetenskapsman mycket riktigt påpekat, så är en namnteckning endast en symbol – vilken som helst – som man brukar för att visa sitt godkännande av, eller ansvar för, ett dokument. Denna symbol måste inte i sig själv nödvändigtvis vara säker, pålitlig eller omöjlig att förfälska.<sup>71</sup> Så varför ställa alla dessa krav på elektroniska signaturer?

Vidare bör i detta sammanhang nämnas att det finns de som anser att man kanske borde införa vissa presumtionsregler för elektroniska signaturer, men detta skall inte utvecklas närmare inom ramen för denna uppsats då avsikten med denna inte är att djupare behandla processrättsliga frågor.

### **6.3 Behövs det ytterligare lagstiftningsåtgärder?**

Som ovan nämndes föreligger tveksamhet kring frågan om namnteckningen vid lagstadgade krav på underskrift kan ersättas av en elektronisk signatur. Viss tveksamhet föreligger också kring frågan om vilken exakt bevisverkan en elektronisk signatur har. Frågan kan då ställas om man bör lagstifta för att skapa klarhet i dessa fall, eller om man bör överlämna utvecklingen till marknaden, dvs låta dessa frågor bli föremål för självreglering.

Som argument för lagstiftning brukar nämnas att man på detta sätt snabbare uppnår tydliga spelregler. En nackdel med att lagstifta är dock att detta skulle kunna innebära hinder för teknisk utveckling.

---

<sup>71</sup> Se Wright, *The Law of Electronic Commerce*, s 16:2.

För alternativet att överlämna utvecklingen åt marknaden talar främst att detta skulle kunna innebära en mer flexibel lösning på problemen. Som argument emot brukar anföras att med denna lösning viktiga tolkningsfrågor överlämnas till praxis, och därmed troligtvis kommer att vara olösta under en längre tid. Detta alternativ skulle alltså kunna leda till en längre tid av rättsosäkerhet än det förra.

Såsom framförs i Ds 1998:14 så vore kanske en lämplig blandning av dessa båda metoder att föredra. På detta sätt skulle man kunna åstadkomma erforderlig stadga inom detta rättsområde, utan att för den skull nödvändigtvis hämma utvecklingen. Till de som motsätter sig detta alternativ, och som absolut inte vill lagstifta över huvud taget, skulle jag vilja göra det påpekandet att man inte bör glömma att syftet med lagar är just att underlätta samhällslivet. Nu har det utvecklats en ny teknik i samhället, som kan ge stora samhällsekonomiska vinster som resultat. För att kunna utnyttja denna teknik på ett effektivt sätt så skulle ny lagstiftning kunna underlätta. Så varför inte använda lagstiftningsinstrumentet på det sätt som det är tänkt? Vidare kan den anmärkningen göras att visserligen så kan det begränsade antal användare som finns idag, dvs mestadels företag, klara sig en tid framöver genom självreglering (dvs genom avtal), men på längre sikt kommer troligtvis att krävas lagstiftningsåtgärder för att kunna införa elektronisk signering generellt, till alla användare. På samma sätt som vi kan använda namnteckningen för olika ändamål behöver vi nämligen generella lösningar för identifiering och bekräftelse vid elektronisk kommunikation som inte kräver speciell teknik och separata juridiska överenskommelser med varje part som vi skall göra affärer eller ha annat utbyte med. För att kunna införa detta kommer troligtvis lagstiftningsåtgärder att vara nödvändiga. Dessutom bör påpekas att även alternativet att inte lagstifta kan verka hämmande för utvecklingen av ny teknik inom detta område. Innan visshet uppnås beträffande frågan om rättsverkan av elektronisk signatur kommer nämligen troligtvis alla viktiga dokument att upprättas i skriftlig form på papper och signeras för hand. Likaså kommer majoriteten av de aktörer som finns på marknaden (med undantag möjligen för de allra största som har de största resurserna) inte våga ta risken att investera tid och pengar på att utveckla system för elektronisk signering som kanske senare – på grund av ny lagstiftning – inte accepteras juridiskt. Avsaknaden av lagstiftning kan alltså verka avskräckande och på detta sätt hämma användandet samt därmed också utvecklingen av system för elektronisk signering. En lämplig avvägning mellan lagstiftnings- och självregleringsalternativet kan alltså kanske vara det bästa alternativet. Man skulle också kunna säga att detta är den väg som Sverige redan slagit sig in på, genom att man redan infört lagstiftning om elektroniskt uppgiftslämnande inom vissa rättsområden.

Skulle man välja att lagstifta ytterligare i Sverige så är det enligt min mening värt att titta på tulldatalagstiftningen och ta efter denna. Denna lagstiftning är enligt min åsikt mycket fördömlig. Den har karaktären av en ramlagstiftning, på så sätt att den inte låser tillämpningen till en viss teknik. På detta sätt tar den hänsyn till utvecklingen av ny teknik, samtidigt som den dock anger spelreglerna för användningen av denna. Den är därmed teknikoberoende. Det är viktigt att all eventuell framtida lagstiftning inom detta område görs teknikoberoende. Av denna anledning utgör tulldatalagstiftningen ett så gott föredöme.

Slutligen skulle jag bara vilja göra den korta kommentaren att, skulle man komma fram till att de lagregler som stadgar om ”undertecknande”, ”underskrift”, ”skriva under” etc måste ändras för att också inbegripa elektroniska signaturer (exempelvis kan ju detta bli ett resultat av EU-direktivet), så varför inte ändra dessa uttryck till ”signatur”, ”signera” etc? I dessa begrepp kan ju både förfarandet med det traditionella undertecknandet med en egenhändig namnteckning liksom elektronisk signering inbegripas.

## 6.4 Sammanfattning

Sammanfattningsvis kan man alltså dra den slutsatsen angående rättsverkan av elektroniska signaturer att, när det gäller de fall där det ej uppställs formkrav, så bör det inte innebära några större problem att använda sig av elektroniska signaturer istället för traditionella, handskrivna namnteckningar. Detta gäller under förutsättning att man säkerställer att det system för elektronisk signering som man valt tillgodoser alla de funktioner som den traditionella namnteckningen fyller. Viktigt är också att säkerställa att bevisföringen säkras samt förenklas i görligaste mån, för det fall att en rättslig tvist skulle uppstå. Det är med andra ord viktigt att komma ihåg att den tillämpade tekniken med anknytande rutiner blir avgörande för bedömningen av den elektroniska signaturens bevisvärde.

När det gäller de fall där det finns formkrav, gör man nog dock klokast i att vara lite försiktigare. Som framgått ovan är det tveksamt ifall elektroniska signaturer kan ersätta namnteckningar i dessa fall. Tills denna fråga klarlagts, antingen genom lagstiftning eller genom avgörande i praxis, så bör man nog avvakta med att använda sig av elektroniska signaturer när det ställs krav exempelvis i lag på underskrift. Detta innebär främst vissa hinder att använda sig av elektronisk signering inom förvaltningsrättsområdet, dvs vid kommunikation med myndigheter, men det är också just inom detta område i svensk rätt som lagstiftningsåtgärder redan har skett och utreds kontinuerligt. I övrigt utgör det dock inte något större hinder för den elektroniska handeln, då de situationer där det finns formkrav i lag trots allt är ganska få och ofta rör sådana slags transaktioner som ändå inte är särskilt vanligen förekommande för avtalsslutande via Internet.

# KÄLLFÖRTECKNING

## Offentligt tryck

### Offentliga utredningar

Ds 1994:80 Elektronisk dokumenthantering inom skatteförvaltningen

Ds 1997:84 Elektroniskt ansökningsförfarande i inskrivningsärenden m.m.

Ds 1998:14 Digitala signaturer – en teknisk och juridisk översikt

SOU 1987:40 Datorisering av tullens export- och importrutiner – Förstudie

SOU 1989:20 Tullregisterlag m.m.

SOU 1989:40 Datorisering av tullrutinerna – Slutrapport

SOU 1992:110 Information och den nya InformationsTeknologin – straff- och processrättsliga frågor m.m.

SOU 1995:10 Översyn av skattebrottslagen

SOU 1996:40 Elektronisk dokumenthantering

### Propositioner

Prop. 1970:20 Förslag till jordabalk

Prop. 1994/95:93 Elektronisk dokumenthantering inom skatteförvaltningen , m.m.

Prop. 1995/96:170 Översyn av skattebrottslagen

Prop. 1996/97:100 Ett nytt system för skattebetalningar, m.m.

## Övrigt tryck

*Användarhandbok för TDS-anslutning*, utgiven av generaltullstyrelsen.

*Aversten*, Digitala signaturer och ansvarsproblem framförallt nyckelinnehavarens och Certification Authority's ansvar mot förlitande part, IRI-rapport 1998:2.

*Elektronisk handel för kommuner, landsting och stat*, skrift utgiven av Toppledarforum och Svenska kommunförbundet.

*Elektronisk uppgiftslämning till tullverket – Om papperslös informationsöverföring mellan näringslivet och tullverket*, informationsbroschyr utgiven av generaltullstyrelsen, TV 101.17.

*Furberg*, Rättsliga frågor rörande elektroniska ID-kort, dokument SEIS G06, 1996-06-25.

*Hultmark*, Elektronisk handel och avtalsrätt, uppl 1:1, 1998.

*Karstoft*, Elektronisk dokumentudveksling – retlige aspekter, Danmark 1994.

*Lehrberg*, Praktisk juridisk metod, 2 uppl, 1993.

*Lindberg*, Elektroniska originaldokument och elektronisk signatur, IRI-rapport 1987:7.

*Lloyd*, Information Technology Law, Second edition, Butterworths, London 1997.

*Mitrakas*, Open EDI and Law in Europe, Kluwer Law International, The Netherlands 1997.

*Nu kommer det elektroniska ID-kortet*, pressinformation från ITS – Informationstekniska standardiseringen, 1998-09-29.

*Offentlig sektor tar nästa steg med elektronisk handel*, artikel i annonsbilagan ”elektroniska affärer”, utgiven av EDIS – EDI-föreningen i Sverige, Dagens Industri 1998-09-29.

*Strömholm*, Rätt, rättskällor och rättstillämpning – En lärobok i allmän rättslära, 5 uppl, 1996.

*TDS – Enkelt, Snabbt, Säkert*, informationsbroschyr utgiven av generaltullstyrelsen, TV 101.20 utgåva 1.

*Wild-Nordlund*, Digital Signatures – Determination of Origin and Protection of Electronic Documents within the Construction Industry, M.Sc. Thesis, Department of Real Estate and Construction, Royal Institute of Technology, Stockholm, 1997.

*Wright*, The Law of Electronic Commerce – EDI, E-mail and Internet; Proof and Liability, 2nd edition, New York 1996.

## **Övriga källor**

Telefonintervju med Gunilla Berg, ADB-jurist på RSV, 1998-09-17

Telefonintervju med Per Furberg, rådman, 1998-10-15