JURIDISKA FAKULTETEN
vid Lunds universitet

Fredrik Malm

Avtalsrättsliga aspekter på elektroniska signaturer

– En fallstudie på Anotopennan –

Examensarbete
20 poäng

Handledare: Ulf Maunsbach

Ämnesområde: Kommersiell IT-rätt

Termin VT-2001

Innehåll

Förord

Mitt val av ämnesområde kommer sig av att jag tog kontakt med Anoto AB och presenterade min idé. Anoto visade direkt ett stort intresse och utifrån en ömsesidig dialog skapades arbetets huvudsakliga form. Arbetet har tidvis varit krävande, då ämnet som behandlas är relativt nytt och delvis outforskat. Ett stort stöd har under arbetets gång varit min kontinuerliga kontakt med Kristofer Skantze på Anoto. Jag vill därför framföra ett stort tack till Kristofer för hans stora engagemang och intresse för mitt arbete. Resultatet hade inte blivit vad det blev utan din medverkan. Tack! Jag vill också rikta ett tack till min handledare, doktorand Ulf Maunsbach för all hjälp.

Jag tar gärna emot kommentarer eller frågor beträffande arbetet på följande e-postadress: fkmalm@hotmail.com

Lund i juni 2001

Fredrik Malm

Förkortningar

AvtL	Lag om avtal och andra rättshandlingar på förmögenhetsrättens område (Avtalslagen)
BrB	Brottsbalken
CA	Certification Authority
CEN	Comité Européen de Normalisation/The European Committee for Standardization
CPS	Certification Practice Statement
CSP	Certification Service Provider
Ds	Departementsskrivelse
EES	Europeiska ekonomiska samarbetsområdet
ETSI	European Telecommunications Standards Institute
EU	Europeiska Unionen
HD	Högsta domstolen
IT	Informationsteknologi
JB	Jordabalken
SkL	Skadeståndslagen
KkredL	Konsumentkreditlagen
KöpL	Köplagen
LKS	Lagen om kvalificerade elektroniska signaturer, m.m.
NJA	Nytt Juridiskt Arkiv (avdelning I)
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PKI	Public key infrastructure
Prop.	Proposition
PTS	Post och telestyrelsen
RB	Rättegångsbalken
SFS	Svensk Författnings Samling
SOU	Statens offentliga utredningar
SWEDAC	Swedish Board for Accreditation and Conformity Assessment /Styrelsen för ackreditering och teknisk kontroll
TTP	Trusted Third Party
UETA	Uniform Electronic Transaction Act
UNCITRAL	United Nations Commission on International Trade Law

Del ?

1 Inledning

1.1 Bakgrund

Under de senaste åren har användandet av Internet ökat explosionsartat. Internet har skapat en helt ny grund för nationella affärstransaktioner i allmänhet och internationella affärstransaktioner i synnerhet. Handeln över Internet har trots detta inte fått de genomslag som marknaden räknat med. Den senaste tiden har en rad konkurser och dåliga resultat skakat E-handelsföretagen runt om i världen. Framförallt har Internetföretag med inriktning mot handel med konsumentvaror drabbats. En orsak kan vara bristande säkerhet. Säkerhet och Internet har länge varit en omdiskuterad fråga. Svårigheter som kan uppstå vid avtalsslut i en digital miljö är bl.a. att säkra bevis, motpartens identitet eller att innehållet inte blivit förändrat. Vid avtalsslut som inte sker i digital miljö brukar namnunderskriften fylla flera av dessa funktioner. I en digital miljö går det självklart inte att fysiskt signera dokument. Men med modern teknik, såsom kryptoteknik går det att framställa elektroniska signaturer. De elektroniska signaturerna kan både garantera identiteten hos avsändaren och säkerställa att informationen som skickats är oförändrad.[1] Det finns således en teknisk lösning som möjliggör att elektroniska dokument kan signeras digitalt. Med hjälp av elektroniska signaturer ökar säkerheten över Internet, och därmed förutsättningarna för att fler ska använda Internet vid ingående av rättsliga transaktioner. De elektroniska signaturerna ingår i en infrastruktur där certifikatutfärdare fungerar som garanter för strukturens tillförlitlighet. Tillit och säkerhet är således en förutsättning för att elektronisk kommunikation (som inte sker i slutna nätverk, där alla användare är kända sedan tidigare), ska ersätta traditionell ”penna papper” kommunikation.

De senaste åren har det både nationellt och internationellt dykt upp flera nya lagar. Dessa har bidragit till en mer ingående rättslig diskussion avseende användandet av elektronisk kommunikation. Idag har tekniken för att åstadkomma säker elektronisk kommunikation nått mycket långt. I informationsteknikens lavinartade utveckling, dyker det ständigt upp nya företag och produkter med syfte att underlätta och effektivisera elektronisk handel och kommunikation. I arbetets del ?? kommer ett av dessa företag och dess produkt rättsligt analyseras. Företaget är som framgår av arbetets titel, Anoto AB. Anoto är ett intressant företag med en unik och ur rättslig synpunkt mycket intressant produkt.

[1] Ds 1998:14, Digitala signaturer en teknisk och juridisk översikt, s 11-18.

1.2 Frågeställningar och syfte

Arbetet är uppdelat i två delar och syftet skiljer sig mellan de båda delarna.

I arbetets första del görs ett försök att skapa klarhet i den rättsliga infrastruktur som omgärdar de kvalificerade elektroniska signaturerna. Tanken är att undersöka vilken rättsverkan som de elektroniska signaturerna har, och besvara frågan om en elektronisk signatur kan motsvara en traditionell handskriven signatur när det i lag eller avtal ställs krav på underskrift? Eftersom signaturens huvudsakliga syfte är att binda undertecknaren vid ett bestämt innehåll, har jag funnit det relevant att också undersöka de elektroniska dokumentens rättsverkan. En signatur förekommer ju alltid tillsammans med någon sorts informationsbärare. Det är därför viktigt att även undersöka om ett elektroniskt dokument rättsligt kan motsvara ett traditionellt pappersdokument? Framställningens första del inriktar sig huvudsakligen på de elektroniska signaturerna, men diskussionen omfattar även rättsliga aspekter på elektronisk kommunikation i allmänhet. Arbetets första del fungera som en ”uppbyggnad” inför arbetets andra del.

Det primära syftet med arbetets första del är att undersöka vilken rättsverkan som elektroniska signaturer och dokument har vid användande av modern kommunikationsteknik.

Den andra delen av arbetet utgår ifrån två fiktiva fall. Min avsikt är att med utgångspunkt i varje fall, analysera ett antal avtalsrättliga problem som kan uppstå när Anotos digitala penna och papper används vid elektronisk kommunikation. Frågeställningar och diskussionsunderlag har huvudsakligen uppstått ur en regelbunden dialog mellan mig och Kristofer Skantze på Anoto. Min förhoppning är därför att resultatet från analysen ska komma Anoto till nytta. Med utgångspunkt i de resultat som framkommer av analyserna, föreslås tekniska samt rättliga lösningar som jag anser ändamålsenliga.

Syftet med arbetets andra del är att, utifrån ett antal fiktiva avtalssituationer, redovisa sannolika lösningar samt ge förslag på hur tekniken praktiskt kan anpassas till gällande rätt.

1.3 Metod material

Arbetet består som bekant av två delar. Del ? bygger både på en deskriptiv- och en analytisk metod, medan del ?? huvudsakligen bygger på en analytisk metod.

För att besvara de frågeställningar och fall som uppställts i arbetet har jag främst sökt svaren i befintliga rättsregler och principer. En fördel med en sådan metod är att befintliga regler och principer ofta har en lång tradition bakom sig, som t.ex. den traditionella signaturens bakomliggande syfte. En viss försiktighet bör dock iakttas, så att inte alltför långtgående analogier används. Metoden är även bra, då den möjliggör en rättslig kontinuitet, som är positivt ur rättssäkerhetssynpunkt. Metoden ökar nämligen möjligheten för avtalskontrahenterna att förutse de rättsliga effekter som kan uppstå vid elektronisk kommunikation.

Det material som använts för framställningen har främst utgjorts av lagtext, lagförslag, förarbeten, offentliga utredningar, doktrin, artiklar och telefonintervjuer. En viktig källa för arbetets andra del har dessutom varit kontakten med Anoto. Med förarbeten och lagförslag inberäknas även EG-rättsligt material, såsom direktiv, direktivförslag och förarbeten till dessa. Även material som framtagits av olika EU-organ har använts. Framförallt har de olika utredningar och förarbeten som finns på området varit vägledande. Utifrån dessa har lagstiftaren syn på flera av de situationer som behandlats kunnat utläsas. Det finns endast ett fåtal böcker som direkt berör de frågeställningar som behandlas i arbetet. Detta kan bero på att området fortfarande är relativt nytt och därför i mindre omfattning än de mer traditionella områdena behandlats i doktrinen. För övrigt har en stor mängd material som inte direkt kommit till uttryck i arbetet lästs, för att på bästa sätt förstå det material som arbetet baserats på.

1.4 Avgränsningar

Framställningen utgår i första hand ifrån svensk rätt. Den svenska lagen avseende elektroniska signaturerna är implementerad efter ett EG direktiv, därför motsvarar redogörelsen om elektroniska signaturer i stort rådande rättsläge inom EU. Vägledning har även hämtats från internationella källor, t.ex. UNCITRAL:s modellag för elektronisk handel. I arbetets första del har jag av utrymmesskäl valt att endast beröra certifikatutfärdarnas verksamhet. De avtalsrättsliga aspekter som kan uppstå mellan en utfärdare och dess medkontrahenter, lämnas därför därhän. Arbetets andra del utgår primärt från svensk avtalsrätt, med viss vägledning från internationell reglering. Sammanfattningsvis kan arbetets kapitel 2-4 definieras som generella i sin framställning, medan arbetets kapitel 5-6 är mer djuplodande.

1.5 Disposition

Arbetet är disponerat på följande sätt: Det inledande kapitel 2 börjar med en beskrivning av tekniken bakom skapandet av elektroniska signaturer. Avsikten är att ge läsaren en grundläggande teknisk inblick, för att underlätta förståelsen av framställningen i övrigt. I kapitel 3 kommenteras lagen om kvalificerade elektroniska signaturer, som trädde i kraft den 1 januari i år. Kapitel 3 är allmänt utformat, med undantag för en djupare diskussion avseende de ”säkra anordningarna”. Avsikten med kapitel 3 är främst att ge läsaren allmänna kommentarer till lagtexten. Den fördjupade behandlingen av de ”säkra anordningarna”, avser att förtydliga innebörden av direktivets[2] bilaga ???. Min förhoppning har varit att bringa klarhet i de frågetecken som tillverkare av sådana anordningar står inför (t.ex. Anoto). I kapitel 4 diskuteras namnunderskriftens primära funktioner. Även pappersdokumentet och dess funktioner genomgår motsvarande behandling. I samband med respektive behandling undersöks också om funktionerna likväl kan uppfyllas på elektronisk väg. I kapitel 5 behandlas alternativa regleringar och synsätt. I kapitlet försöker jag utreda vilka alternativa regleringar och principer som en domstol kan använda sig av när inte nationella lagregler eller principer är direkt tillämpbara. I Kapitel 6, arbetets del ??, görs en fallstudie på Anoto AB:s elektroniska penna. Kapitlet är baserat på två fiktiva fall, där ett antal avtalsrättsliga situationer analyseras. Arbetet avslutas med en sammanfattning i kapitel 7.

[2] Europaparlamentets och rådets direktiv om ett gemenskapsramverk för elektroniska signaturer 1999/93/EG.

2 Elektroniska signaturer

2.1 Inledning

En i mitt tycke bra definition av elektronisk signatur har stadskontoret givit i rapporten ”Svenska delen av Internet”.

”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.”[3]

2.2 Teknisk beskrivning

Den tekniska och praktiska biten vid avsändande, mottagande och skapande av elektroniska signaturer är mycket komplicerad. För att läsaren på bästa sätt ska kunna ta till sig och förstå detta arbete, krävs en grundläggande förståelse och inblick i tekniken bakom de elektroniska signaturerna. Följande kapitel innehåller därför en grundläggande teknisk beskrivning av elektroniska signaturer och dess tillkomst. Framställningen bygger på den infrastruktur som omgärdar skapandet av elektroniska signaturer, den s k. Public key infrastructure (PKI) eller det öppna nyckelsystemet som den även kallas.

2.2.1 Kryptering

Den kryptografiska tekniken har främst använts för att göra meddelanden oläsliga och har tidigare mest använts i militära sammanhang. På senare tid har krypteringsteknik utnyttjats i affärslivet för att skydda datamängder över Internet. Vid kryptering förändras en ursprunglig datamängd av en s.k. hemlig nyckel (parameter), så att den ursprungliga datamängden inte kan läsas. Kryptering används för identifiering, autenticering och för att säkerställa innehållet i ursprungstexten. Tekniken används för framställande av elektroniska signaturer, som i sin tur har till uppgift att säkerställa dessa delar.[4] Grundläggande säkerhetskrav som kan uppfyllas med hjälp av kryptering är:

att säkra identiteten hos avsändare och mottagare av dokument eller meddelande,
att säkerställa att dokument eller meddelande inte förvanskas,
att göra dokument eller meddelandet oläsligt för obehöriga,
att en avsändare inte kan förneka sina dokument eller meddelanden[5]

[3] Statskontoret 1997:18, Svenska delen av Internet, Struktur, säkerhet och regler, s 14.
[4] Ds 1998:14 s 18f, SOU 1996:40, Elektronisk dokumenthantering, s 237f. Aversten David, Digitala signaturer och ansvarsproblem, 1998, s 15f.
[5] Regeringens skrivelse 1998/99:116 om kryptografi, s 1-3.

2.2.2 Symmetrisk kryptering

Vid symmetrisk kryptering används samma nyckel för både kryptering och dekryptering.[6] Detta innebär att avsändaren och mottagaren använder samma gemensamma nyckel för kryptering respektive dekryptering av meddelandet. Symmetrisk kryptering är dessvärre inte helt säker. Framförallt är det problemet med nyckelhanteringen som orsakar osäkerhet i systemet. Företag som vill utbyta krypterade meddelanden måste lita på att mottagaren håller nyckeln hemlig. För företag med ett stort antal affärsrelationer och som använder sig av symmetrisk kryptering uppstår betydande problem. Företaget bör för att hålla en hjälplig säkerhetsnivå förfoga över en unik nyckel för varje kund.[7] Här är nyckeldistributionen viktig eftersom säkerheten beror på om nyckeln är hemlig för utomstående. Symmetrisk kryptering anses sakna förutsättningar för att skapa en säker elektronisk signatur, eftersom både den signerande och den mottagande parten kan skapa en signatur. Kännetecknet för en elektronisk signatur är ju bl.a. att signaturen endast kan härröra från en bestämd person.[8]

2.2.3 Asymmetrisk kryptering

Till skillnad från symmetrisk kryptering, används vid asymmetrisk kryptering två nycklar, en privat och en publik nyckel. Den privata nyckeln för kryptering och den publika för dekryptering. Nycklarna bildar tillsammans ett unikt par, då samma nyckel inte både kan kryptera och dekryptera ett dokument. Det är i princip omöjligt (beroende på nyckelns ”längd”) att med vetskap om den ena nyckeln beräkna den andra nyckeln i paret.[9] Asymmetrisk kryptering anses vara en förutsättning för skapande av säkra elektroniska signaturer. PKI bygger på asymmetrisk kryptering. Till skillnad från symmetrisk kryptering underlättas nyckeladministrationen avsevärt. Avsändaren håller den privata nyckeln hemlig medan den publika nyckeln görs tillgänglig för allmänheten.

2.2.4 Hashfunktionen

Hashfunktionen har en viktig roll vid skapande av elektroniska signaturer. Funktionen möjliggör att stora meddelanden kan signeras elektroniskt. Den reducerar nämligen den datamängd som ska krypteras respektive dekrypteras. Genom en kombination av asymmetrisk krypteringsteknik och hashfunktionsteknik skapas den elektroniska signaturen. Hashfunktionen skapar en komprimerad mängd data (kondensat) av ursprungsmeddelandet. Kondensatet eller hashvärdet kan liknas vid ett fingeravtryck från ursprungsmeddelandet, och likt ett fingeravtryck skapas ett unikt värde. De

[6] Ds 1998:14 s 18.
[7] Lehrberg Bert, Moderna Betalningsformer, 1999, s 47-49.
[8] Aversten s 16-17.
[9] En säker ”längd” på den privata nyckeln anses vara 1024 bitar.

hasfunktionstekniker som används vid skapande av elektroniska signaturer måste vara s.k. *envägs-hashfunktioner* som skapar ett unikt värde som inte är vändbart.[10] Det ska därför vara omöjligt att med utgångspunkt i ursprungsmeddelandet räkna fram ett identiskt hashvärde. Det omvända, att beräkna meddelandet utifrån hashvärdet ska likaså vara omöjligt. Praktiskt medför detta att minsta lilla ändring av dokumentets innehåll kommer att förändra hashvärdet. Tekniken säkerställer därmed dokumentets ”originalitet”. De vanligaste hashfunktioner som infriar de ovan uppställda kraven är MD2, MD5 och SHA-1.[11]

2.2.5 Skapande och mottagande av elektronisk signatur[12]

Signering av ett dokument med en elektronisk signatur, går till på följande vis (se fig.1 nedan)[13]. Dokumentet (1) som ska signeras bearbetas med en envägs-hashfunktionsteknik (2) som skapar ett unikt hashvärde (3). Hashvärdet krypteras sedan med avsändarens privata nyckel (4) som skapar den elektroniska signaturen. Därmed tillförs den elektroniska signaturen dokumentet (5). Det signerade dokumentet skickas nu till mottagaren (6). Mottagaren separerar sedan signaturen från dokumentet för att möjliggöra verifieringen av meddelandet (7,9). Samma hashfunktionsteknik (ex MD2) som avsändaren använde, använder nu mottagaren för att bearbeta det mottagna dokumentet (8). Mottagaren får därmed ett hashvärde som grundas på avsändarens dokument (12). Mottagaren dekrypterar även det krypterade hashvärdet (signaturen), med avsändarens publika nyckel (10) och ett okrypterat hashvärde skapas (11). Om de två hashvärdena vid en jämförelse är identiska, kan mottagaren vara säker på dokumentets originalitet och att det verkligen härrör från innehavaren av den privata nyckeln (garanteras av en CA se kap 3.4) (11,12). Mottagaren kan vara säker på detta eftersom det endast är avsändarens privata nyckel som kan ha krypterat hashvärdet, och att denna endast går att dekryptera med den publika nyckeln. Samt att det bara är ett identiskt meddelande som kan skapa ett identiskt hashvärde. Om hashvärdena inte är identiska kan endera någon felaktigt ha utgett sig för att vara avsändare eller så kan dokumentet ha förändrats efter det att avsändaren signerat dokumentet. Det ska avslutningsvis påpekas att ovanstående moment i praktiken sker i en automatiserad process.

[10] Ds 1998:14 s 21-22.
[11] Se föregående not.
[12] Prop. 1999/2000:117, Lag om elektroniska signaturer, m m., s 20-21, Ds 1998:14 s 22-23, Aversten s 20-22.
[13] Lehrberg, s 49.

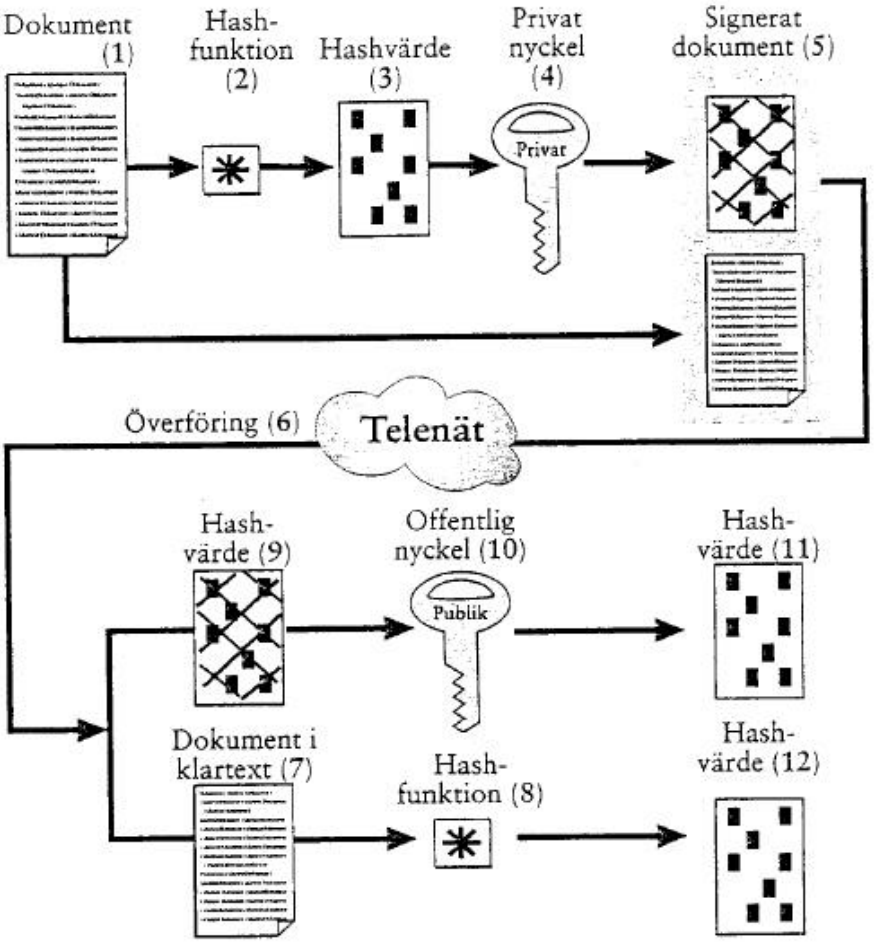


Fig.1

2.3 PKI det öppna nyckelsystemet

PKI är ett vitt begrep som innefattar alla de parametrar som är nödvändiga i en infrastruktur för användande och skapande av elektroniska signaturer. PKI innebär alltså själva ramverket för ett system med elektroniska signaturer. Infrastrukturen behövs för att få ett fungerande system med elektroniska signaturer, där bl.a. autenticering och kryptering av meddelanden ingår. Genom autenticering garanteras parternas ”identitet” i relationen. Basen är den privata och den publika nyckeln. Grunden för PKI strukturen består något förenklat av en treparts konstellation med en avsändare, en mottagare och en Certification Authority (CA/utfärdare). Förutom dessa finns en mängd viktiga aktörer. Bland dessa har bland annat Post och telestyrelsen (PTS) och Styrelsen för ackreditering och teknisk kontroll (SWEDAC) viktiga funktioner.[14]

[14] Aversten, s 15ff. Affärsvärlden 2000-09-27.

3 Den svenska lagen

3.1 Bakgrund

Lagen om kvalificerade elektroniska signaturer, m.m. (LKS) är ett resultat av Europaparlamentets och rådets direktiv om ett gemenskapsramverk för elektroniska signaturer 1999/93/EG (direktivet). Enligt art 13 p1 ska medlemsstaterna senast den 19 juli 2001 implementera direktivet. Den svenska lagen trädde i kraft den 1 januari 2001.

I takt med att användningen av Internet ökar har det ställts krav på gemenskapen att agera för att underlätta denna utveckling. En global kommunikation ansågs viktig för att främja nya affärsmöjligheter. En förbättrad kommunikation är förenligt med de grundläggande målen för EU:s gemensamma handelspolitik. Av den orsaken intresserade sig kommissionen tidigt för elektronisk handel. Den 16 april 1997 lade kommissionen fram en utredning ("Ett europeiskt initiativ inom elektronisk handel") där elektroniska signaturer ansågs vara en av de viktigaste grunderna för utvecklingen av elektronisk handel.[15] Som ett resultat av utredningen följde en ny utredning (”säkerhet och tillförlitlighet vid elektronisk kommunikation – Mot en europeisk ram för digitala signaturer och kryptering”) från kommissionen den 8 oktober 1997. Den senare följdes av en uppmaning från rådet att kommissionen snarast skulle lägga fram ett förslag till Europaparlamentet och rådet angående direktiv om digitala signaturer.

Kommissionen upptäckte att flera medlemsstater redan lagstiftat på området. Medlemsstaternas regleringar visade sig ha stora skillnader, vilket sågs som ett hot mot den inre marknaden. Kommissionen lade i maj 1998 fram ett förslag till Europaparlamentet och rådet, direktiv ”om en gemensam ram om elektroniska signaturer”.[16] Målet med direktivförslaget var att undanröja hinder mot den elektroniska handeln och skillnader mellan medlemsstaternas regleringar. Främst var det skillnaderna rörande elektroniska signaturer och certifikattjänster som ansågs hämma den fria marknaden.[17] Som ett resultat av förslaget lade Europaparlamentet och rådet i december 1999 fram direktiv om ett gemenskapsramverk för elektroniska signaturer. Direktivet trädde i kraft den 19 januari 2000.

Det svenska arbetet med lagstiftning beträffande elektroniska signaturer började på allvar 1998 då en departementspromemoria framställdes på initiativ av regeringskansliets beredningsgrupp för digitala signaturer. Promemorian var avsedd att ligga till grund för Sveriges fortsatta arbete och

[15] KOM (1997) 157, slutlig, Ett europeiskt initiativ inom elektronisk handel.
[16] KOM(1998) 297 slutlig, säkerhet och tillförlitlighet vid elektronisk kommunikation – Mot en europeisk ram för digitala signaturer och kryptering.
[17] KOM(1998) 297 slutlig, s 15. Prop. 1999/2000:117, s 26ff.

inställning till elektroniska signaturer.[18] Europaparlamentets direktivförslag låg även till grund för en diskussion bland berörda organ i norden, beträffande tolkning och genomförande av direktivet. Det nordiska samrådet bidrog till att Näringsdepartementet i samarbetet med Justitiedepartementet under hösten 1999 utarbetade departementspromemorian ”Elektroniska signaturer”.[19] I maj 2000 lade regeringen fram ett förslag avseende en lag om kvalificerade elektroniska signaturer.[20] Förslaget accepterades och en ny lag om kvalificerade elektroniska signaturer, m.m. trädde därmed i kraft den första januari 2001.[21]

3.2 Allmänt om lagens syfte och tillämpningsområde

Lagen omfattar de CA som är etablerade i Sverige och som utfärdar kvalificerade certifikat för elektroniska signaturer till allmänheten, 1 §. Syftet med lagen är att främja användandet av elektroniska signaturer med en hög säkerhetsnivå. Målet är att dessa signaturer ska få ett allmänt erkännande, så att parter som inte tidigare haft fasta avtalsrelationer med varandra ska använda elektroniska signaturer som säker affärskommunikation. Till skillnad från direktivet där stor vikt läggs vid diskussionen om de elektroniska signaturernas rättsliga verkan, inriktar sig den svenska lagen mer på reglerna för dem som utfärdar certifikat. Signaturernas rättsliga verkan utgör inte en central fråga i Sverige, eftersom principerna om den fri bevisföringen och den fri bevisvärderingen sedan länge är etablerade här.[22] Principen om fri bevisföring innebär att allt som parterna kan föra fram inför rätten i princip är tillåtet. Den fria bevisvärderingen medför att domstolarna fritt kan pröva den framförda bevisningen utan hinder från eventuella bevisvärderingsregler.[23]

Lagen är inte tillämplig på system som endast omfattas av ett bestämt antal personer, s.k. slutna system.[24] Ett exempel på ett slutet system är bankernas Internettjänster eller när ett certifikat endast utfärdats för att användas internt inom ett företag. I bankfallet föreligger ett på förhand ingånget avtal mellan utfärdaren (banken) och kunden och därför är det bara banken själv som behöver förlita sig på certifikatet. Enligt direktivet ska lagen endast omfatta certifikat som är utfärdade till allmänheten, s.k. öppna system. Huvudregeln för att certifikatet ska anses var ”utfärdat till allmänheten”, är att en tredje part utan att ett kontraktsförhållande existerar kan verka som mottagare. De öppna systemen består av avsändare, mottagare och en CA. Ett öppet system föreligger således när en CA utfärdar certifikat, utan att begränsa kretsen av möjliga mottagare på ett mer precist sätt. Lagen

[18] Ds 1998:14.
[19] Ds 1999:73, Elektroniska signaturer.
[20] Prop. 1999/2000:117.
[21] SFS 2000:832. lag om kvalificerade elektroniska signaturer, m.m.
[22] Prop. 1999/2000:117, s 35.
[23] Lindberg Agne, Westman Daniel, Praktisk IT-rätt, 1999, s 63.
[24] Ingressen till direktivet 1999/93/EG, p 16.

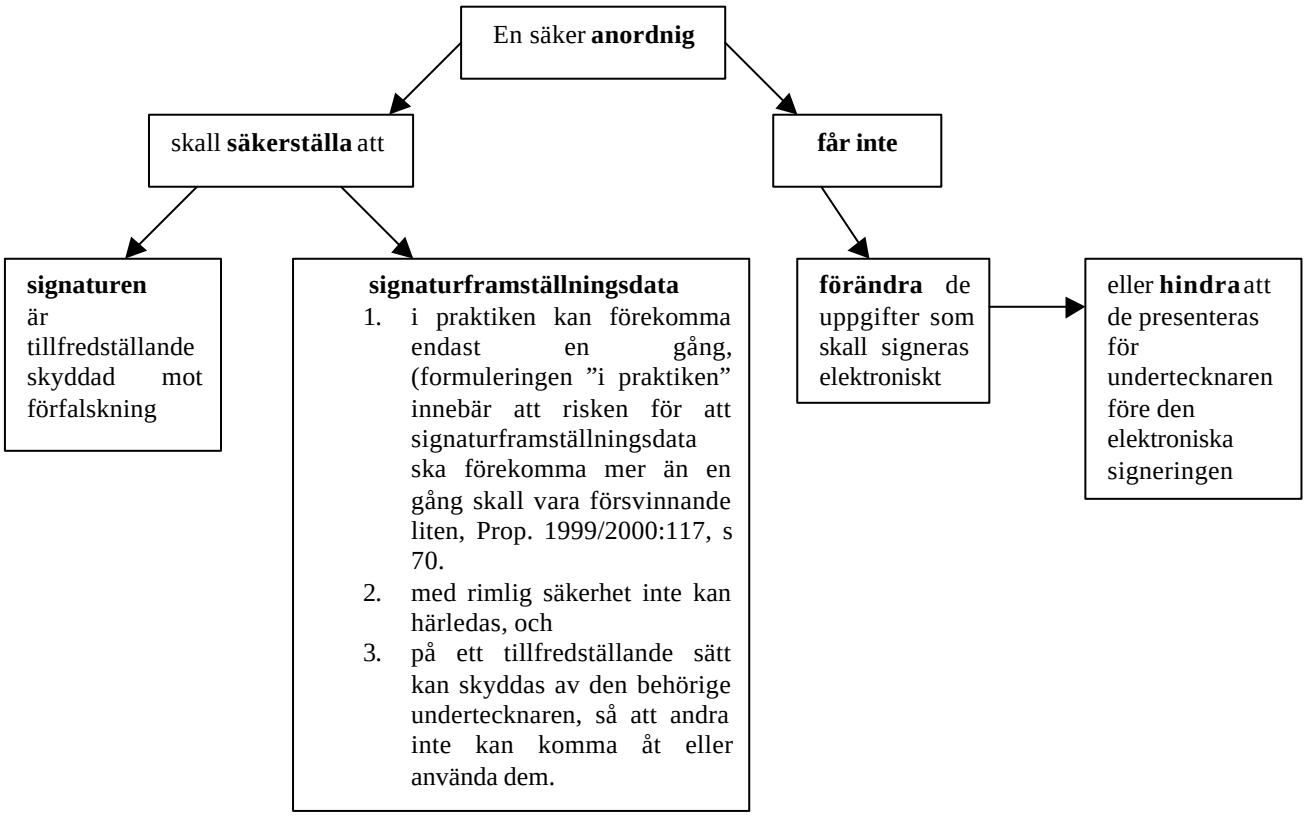
omfattar inte utfärdande av ”enkla” certifikat (som utfärdaren inte betecknat som ”kvalificerade”). Det finns emellertid inget som hindrar en utfärdare från att utfärda enkla certifikat. Sådana certifikat underkastas inte lagens tillsyn och behöver inte uppfylla de övriga i lagen uppställda kraven för utfärdande av kvalificerade certifikat. Certifikat som utfärdats till juridiska personer eller andra sammanslutningar regleras inte heller av lagen.[25] Detta framgår redan av lagens 1 § ”till allmänheten”, men tål att förtydligas.

Vid arbetet med lagen uppstod oenighet angående rubriken på lagen. Lagrådet framförde i sitt förslag, att då lagen huvudsakligen reglerar utfärdande av certifikat, så vore en mer adekvat benämning ”lag om kvalificerade certifikat för elektroniska signaturer”.[26] Förslaget avslogs med motiveringen att lagens bestämmelser om certifikat, certfikatutfärdare och anordningar för signaturframställning tillsammans syftar till att skapa ett regelverk för att öka tillförlitligheten för de kvalificerade elektroniska signaturerna. Den nuvarande rubricering ansågs därför väl motiverad och saklig.[27]

[25] Prop. 1999/2000:117, s 34-36.
[26] Ibid. Bilaga 6, s 105.
[27] Ibid. s 33-34.

3.3 Säkra anordningar

I följande avsnitt ska säkra anordningarna för signaturframställning behandlas. En anordning för signaturframställning (anordning) kan generellt utgöras av maskin eller programvara för användning av signaturframställningsdata. Signaturframställningsdata är de unika data (koder och krypteringsnycklar) som används för att skapa elektroniska signaturer.[28] För att en anordning ska få användas för skapande av elektroniska signaturer måste den vara ”säker”. En anordning anses vara säker och får släppas ut på marknaden om den uppfyller kraven i lagens 3-5 §§. Nedan presenteras kraven på en säker anordning enligt lagens 3 § med hjälp av ett schema.[29]



Paragrafen motsvarar de krav på säkra anordningar för skapande av elektroniska signaturer som uppställs i direktivets bilaga ???. De krav som uppställs i lagens 3 § och direktivets bilaga ??? är emellertid inte tillräckligt detaljerade för att skapa en klar bild av vad som krävs av en säker anordnig. Arbetet med att ta fram en standard för säkra anordningar pågår. Kommissionen har gett i uppdrag till flera europeiska standardiseringsorgan att analysera framtida behov av standardisering enligt direktivet och avge en

[28] LKS, 2 §.
[29] Anoto dokument, Per Furberg. Dokumentet är utarbetat av Per Furberg på uppdrag av Anoto AB. Dokumentet innehåller sekretessbelagt information, som författaren tagit del av i förtroende. Den information som använts har godkänts av Anoto.

plan för att utveckla dessa. Härigenom skapades European Electronic Signature Standardization Initiative (EESSI), som resulterade i att en expertgrupp på uppdrag av EESSI tog fram en rapport.[30] Rapporten ger en viss vägledning avseende vad en kommande standard kan komma att ställa för krav på de säkra anordningarna.

Den ”officiella” standarden för de säkra anordningarna har det europeiska standardiseringsorganet, Comité Européen de Normalisation (CEN) i uppdrag att slutföra. Med andra ord har CEN fått i uppdrag att slutföra den rapport som EESSI:s expertgrupp tagit fram. Målsättningen med CEN:s arbete är att förse marknaden med en standard som stöder genomförandet av direktivet. Resultatet ska slutligen klargöra kraven i direktivets bilaga ???. CEN:s arbete beräknas vara klar någon gång under tredje kvartalet 2001. Standarderna ska sedan presenteras i den europeiska standardserien EN 45 000. Syftet med standardserien är att skapa ett förtroende för certifiering, enhetlig kontroll och beviskrav, oberoende var de aktuella organen verkar.[31]

Utifrån EESSI:s rapport kan vissa antaganden avseende innebörden av lagens 3 § dras. Det bör observeras att paragrafens 1st alltid läses tillsammans med punkterna 1-3 i paragrafen. Enligt 3 § 1p ska en signatur ”i praktiken endast förekomma en gång”.

Följande förtydligande kan ges för paragrafens 1p;

- En anordning som skapar nycklar inuti en säker anordning eller hos en CA ska vara konstruerad så att risken är ”försvinnande liten” för att två likadana nyckelpar skapas. Anordningen bör därför vara baserad på en s.k. *”random or pseudo-random generator”* av hög kvalitet för att undvika att två användare får samma par nycklar.
- Lagringen av den privata nyckeln ska vara skyddad mot yttre angrepp inuti en anordning med ett ”starkt” skydd (skal). Det får inte vara möjligt att reproducera eller kopiera den privata nyckeln. Detta innebär att den dolda nyckeln endast får förekomma en gång och att det ska vara omöjligt att skapa en kopia av nyckeln, inkluderat ”back-up kopior”. Nyckeln måste vara lagrad i en s.k. *”tamper-proof device”*, vilken medför att den privata nyckeln aldrig kan lämna anordningen. Den elektroniska signaturen måste därför skapas inuti anordningen och ingen annanstans.

För paragrafens 2p ”med rimlig säkerhet inte kan härledas” kan nedanstående förtydligande ges;

- Den kryptografiska algoritmen och nyckelns längd (antal bitar) måste var tillräckligt stor för att motstå en beräkningsmetod som medför att den privata nyckelns värde beräknas utifrån den publika

[30] Final Report of the EESSI Exepert Team, 990720.
[31] Telefonintervju med Kenneth Olofsson på PTS, 03/12-01. Prop. 1999/2000:117, s 44-47.

nyckeln eller ur själva signaturen. En sådan beräkning måste åtminstone vara omöjlig under certifikatets giltighetstid.

- Det hashvärde som skapas vid en elektroniska signatur ska vara så avancerat att ett meddelande inte ska kunna prepareras med ett givet hashvärde eller att två meddelanden med samma hashvärde förekommer.

För paragrafens 3p ”på ett tillfredställande sätt kan skyddas av den behörige undertecknaren, så att andra inte kan komma åt eller använda dem” kan slutligen följande förtydligande ges;

- Den privata nyckeln ska vara skyddat mot obehörigt nyttjande med hjälp av lösenord, PIN-kod, fingeravtryck (biometrisk lösning) eller motsvarande. De olika metoderna ska vara tillräckliga för att motstå de vanligaste forceringsmetoderna. Anordningen ska även ha en programvara som motverkar *”exhaustive search”* efter rätt lösenord.

Enligt 3 § 2st får anordningen inte förändra de uppgifter som ska signeras eller hindra att dessa visas för undertecknaren före signeringen. Här uppkommer frågan, hur och på vilket sätt uppgifterna ska ”presenteras för undertecknaren”? Måste uppgifterna som ska signeras presenteras av den säkra anordningen eller kan dessa uppgifter presenteras avskilt från anordningen? Frågan lämnas obesvarad och innebörden av ”presenteras för undertecknaren” i 2st är därför oklart.[32]

Det råder skilda uppfattningar om de anordningar som finns för skapande av kvalificerade elektroniska signaturer. Oenigheten avser frågan, om vilka anordningar som ska anses uppfyller minimikraven i direktivets bilaga ???. Den nu vanligaste och mest accepterade lösningen för uppfyllande av de ovan givna kriterierna är ett smart-kort i kombination med en kortläsare. Även andra anordningar såsom PCMCIA-kort, mobiltelefon med SIM-kort, handdatorer (palmpilots) eller andra liknade anordningar, kan också bli betecknade som säkra anordningar.[33]

3.3.1”Hårda” respektive ”mjuka” lösningar

För att skapa en elektronisk signatur kan olika sorters anordningar användas. Lagen ställer som ovan visats höga krav på den utrustning som används. En avgörande egenskap är hur väl dessa anordningar kan skydda den privata nyckeln. De lösningar som används för att skapa elektroniska signaturer kan generellt delas upp i ”hårda” respektive mjuka ”lösningar”.[34] För

[32] Final Report of the EESSI Exepert Team. s 46-47.
[33] Ibid. s 48.
[34] Prop. 1999/2000:117, s 23.

elektroniska signaturer kan tre säkerhetsnivåer urskiljas, hög, medel och låg säkerhetsnivå. En hög säkerhetsnivå är överensstämmande med LKS.[35]

Med hårda lösningar menas en speciell utrustning som används vid skapande av elektroniska signaturer. Denna utrusning har i regel tillverkats efter strikta metoder och innehar ett skyddande fysiskt skal mot yttre angrepp. Aktiva s.k. ”smart-cards” är ett typexempel på en ”hård lösning”. Chipet i ett smart-card kan beskrivas som en liten dator med en mikroprocessor och minne integrerat. En fördel med dessa kort är att de kan lagra den dolda nyckeln och skydda den mot exponering. Nyckeln lagras i kortets minne. Minnet kan endast nås genom kortets mikroprocessor, vilket skapar en hög säkerhet. I jämförelse med vanliga magnetkort som är lätta att förfalska, är de smarta-korten i det närmsta omöjliga att förfalska. Lösningen möjliggör nämligen att signeringsprocessen kan ske i en skyddad rutin. Den ”förpackning” som kan tänkas inrymma chipet kan vara liten och behändig. Storleken innebär också en viktig säkerhetsaspekt. En behändig storlek möjliggör nämligen att innehavaren fysiskt kan ansvara för sin ”elektroniska identitet”.[36]

Allmänt ställs följande krav på de smarta-kort som används;

- de ska ha en beräkningskapacitet som är tillräcklig för att göra en krypteringsberäkning på kortet samt
- en minneskapacitet som är tillräcklig för att lagra nödvändig information,
- ett format och innehåll som är standardiserat och
- kunna lagra information på kortet på ett säkert sätt.[37]

Av central betydelse för en säker anordning är att den dolda nyckeln endast ska kunna aktiveras av den rättmätige innehavaren. För att säkerställa detta ”blockeras” kortet tills innehavaren har låst upp det. Den vanligaste metoden för aktivering är med en PIN-kod. Metoden är sedan länge använd på bankomatkort, mobiltelefoner osv. Autenticering kan även ske genom olika biometriska lösningar såsom fingeravtryck. Trots de smarta-kortens mycket höga säkerhet kan de utsättas för angrepp. Angreppen kan vara rent fysiska såsom onormala spänningsnivåer, onormala temperaturer eller kraftig bestrålning av kortet osv. Mjukvaran inuti kortet kan också utsättas för angrepp, såsom försök att uttömma interna data och därigenom förorsaka ”feltillstånd”. För att kunna motstå angrepp bör mjukvaran vara av hög kvalitet. Vidare anses en inkapsling av den dolda nyckeln vara bristfällig om den kan dyrkas upp och den dolda nyckeln kopieras utan att innehavaren märker något. Ett smart-card måste motstå ett angrepp under så lång tid att innehavaren har en chans att upptäcka manipulationsförsöket.[38]

---

[35] Statskontoret rapport 2000:40, Elektroniska signaturer och elektronisk identifiering för myndigheters e-tjänster, s 20.
[36] Aversten, s 18. Prop.1999/2000:117, s 23.
[37] Ds 1998:14, s 32-33.
[38] Ibid. s 57-58.

”Mjuka lösningar” där istället en PC:s programvara används för att skapa ett nyckelpar, anses inte lika säkra och tillförliga som de hårda lösningarna. I de ”mjuka lösningarna” skyddas den dolda nyckeln efter framställningen med hjälp av vanlig kryptering. Då mjukvaran inte anses vara en säker plattform som skydd mot ”yttre angrepp”, är inte heller aktivering med PIN-kod säker genom en PC. En angripare kan använda sig av en mängd metoder för att komma åt information i en dators mjukvara. Med hjälp av Internet och via e-post kan en angripare t.ex. inplantera en s.k. ”trojansk häst” i datorns mjukvara och därigenom komma åt den dolda nyckeln. En ”trojansk häst” kan ha formen av en skärmsläckare. Under tiden som skärmsläckaren skapar ett mönster eller ett motiv, skannas datorns minne efter ”strängar” som är karakteristiska för lösenord, kreditkortsnummer osv.[39] För biometriska lösningarna gäller samma försiktighet, eftersom en ”trojansk häst” även kan kopiera och komma åt biodata.[40] De krav som lagen uppställer för de säkra anordningarna kommer inte i samma utsträckning som de ”hårda lösningarna”, kunna uppfyllas med ”mjuka lösningarna”.[41]

3.3.2 Prövning och standardisering

Enligt lagens 4 § presumeras en säker anordning uppfylla lagens krav när den överensstämmer med EU-kommissionens fastställda standarder för produkter för elektroniska signaturer samt referensnummer till EU:s officiella tidning offentliggjorts. Detta framgår även av direktivets art 3.5:

”…Member States shall presume compliance with the requirements laid down in point (f) of Annex ?? and Annex ??? when an electronic signature product meets those standards.”

Standarder för de säkra anordningarna är som tidigare nämnts, under framtagande.

Det har vidare framförts krav i direktivet på att kommissionen och medlemsstaterna ska agerar snabbt för att systemet med elektroniska signaturer ska fungera väl på den inre markanden. Varje medlemsstat ska utse ett nationellt organ som ska ansvara för bedömning av de säkra anordningarnas överensstämmelse med bilaga ??? i direktivet.[42] I Sverige ska enligt 5 § en prövning om kraven är uppfyllda göras av ett organ som anmälts (anmälda organ) för detta ändamål enligt lagen (1992:1119) om teknisk kontroll. De anmälda organen eller s.k. ”notified bodies” som får utföra en sådan bedömning ska anmälas till EU-kommissionen. SWEDAC kommer att fungera som ackrediteringsmyndighet och avgör vilka organ

[39] Baum Michael, Ford Warwick, Secure Electronic Commerce. Building the Infrastructure for Digital Signatures and Encryption, 2000, s 96.
[40] Ds 1998:14, s 59, 61.
[41] Prop. 1999/2000:117, s 23. Ds 1998:14, s 32. Statskontorets rapport 2000:40, s 18.
[42] Direktiv 1999/93/EG, ingressen p 15.

som anses kompetenta för uppgiften. Ackrediteringen är tvingande.[43] De anmälda organen ska avgöra vilka säkra anordningar som överensstämmer med bilaga ??? i direktivet. Endast de anordningar som ett sådant organ anser uppfylla kraven får framställas eller saluförs på den gemensamma marknaden under beteckningen ”säker anordning”. Bedömningen sker inte bara av den produkt som organet vill certifiera. De anmälda organen avgör även om verksamhet i sin helhet uppfyller vissa krav, t.ex. granskas personal, ledningssystem och kvalitetssystem.[44] Att en anordning överensstämmer med en standard som fastställts av kommissionen (se 4 §) räcker dock inte, utan ska endast ses som en riktlinje för de anmälda organen. Regeln innebär en obligatorisk kontroll av de säkra anordningar som har för avsikt att släppas ut på marknaden, dock med en presumtion för de anordningar som uppfyller de standarder som 4 § hänvisar till.[45]

En ackreditering som utförts i en medlemsstat av ett anmält organ får verkan i samtliga EES stater. Detta innebär att ett beslut som fattats av ett organ i en medlemsstat ska erkännas av samtliga medlemsstater. Tillverkare och övriga intressenter är alltså inte hänvisade till de olika nationella organen, utan det räcker med att anordningen godkänns i ett land inom EES för att få marknadsföras och saluföras inom samtliga medlemsländers territorier.[46]

3.4 Kvalificerade certifikat

Det krävs i lagen att ett certifikat ska uppnå en hög säkerhetsnivå för att få betecknas kvalificerat. Med certifikat menas här ett intyg i elektronisk form som kopplar ihop den dolda och den publika nyckeln med undertecknaren och bekräftar dennes identitet.

De krav på vad ett sådant certifikat måste innehålla framgår av lagens 6 § och bilaga ? i direktivet. Ett kvalificerat certifikatet får endast vara utfärdat för vis tid. De höga krav som uppställs avseende innehållet för de kvalificerade certifikaten är nödvändigt för att en mottagare ska kunna förlita sig på certifikatet. Mottagaren av ett signerat meddelande måste ges möjlighet att tillgodogöra sig certifikatets information. Detta kan ske genom att den aktuella informationen presenteras tillsammans med certifikatet eller

[43] SWEDAC kommer även att erbjuda frivillig ackreditering för certifieringsorgan som utfärdar certifikat för utfärdare av kvalificerade certifikat. Syftet med ackreditering är att öka tilliten för systemet. Enligt direktivet bidrar ett frivilligt ackrediteringssystem till att höja nivån på utfärdarnas tjänster. Antagligen kommer marknadskrafterna driva certifieringsorganen till att ackreditera sin verksamhet. Tanken är att de organ som ackrediterats ska få ett stärkt förtroende i förhållande till allmänheten. Av stor betydelse för utvecklingen med frivillig ackreditering blir således resultatet av hur ackrediteringen sköts och hur den utnyttjas av aktörerna i deras konkurrens om kunderna. Med andra ord höjs marknadens krav för ackreditering utifrån antalet ackrediterade organ. Se Prop. 1999/2000:117 s 23-26 och Ingressen till Direktivet 1999/93 EG, Europaparlamentets och rådets direktiv om ett gemenskapsramverk för elektroniska signaturer, p11.

[44] Prop. 1999/2000:117 s 23-26 och s 44-47. http://www.swedac.org

[45] Prop. 1999/2000:117, s 23-26, 44-47. Final Report of the EESSI Exepert Team, 990720, s 49. LKS. SFS (1992:1119), Direktiv 1999/93/EG.

[46] LKS, 5 § 2st. Prop. 1999/2000:117, s 47.

att informationen presenteras på något annat sätt i samband med mottagandet av den elektroniska handlingen.[47]

Ett kvalificerat certifikat måste innehålla följande uppgifter:[48]

1. Att det utfärdats som ett kvalificerat certifikat. *Det räcker t.ex. inte att utfärdaren endast nämnt detta i sin marknadsföring, utan informationen måste framgå på något mer bestående sätt.*
2. Utfärdarens namn, adress och uppgift om etableringsland. *Detta är synnerligen viktigt eftersom det kan vara avgörande för om lagen är tillämplig eller ej*.
3. Undertecknarens namn och om en pseudonym används uppgift som klargör att det rör sig om en pseudonym. *Emellertid kan värdet av en signatur med pseudonym vara begränsat, inte minst med tanke på eventuella formkrav. Krav på underskrift brukar generellt innefatta undertecknarens verkliga namn och inte dennes pseudonym.*
4. Särskilda uppgifter om undertecknaren som är relevanta för ändamålet med certifikatet, *kundnummer osv*.
5. Signaturverifieringsdata, *den öppna nyckeln i PKI-systemet måste finnas i certifikatet. Det är därför inte acceptabelt att mottagaren tvingas vända sig till utfärdaren eller någon annan för att få tillgång till den öppna nyckeln.*
6. Certifikatet måste alltid utfärdas på viss tid, *certifikatets giltighetstid måste därför anges*.
7. Certifikatets identifieringskod
8. Utfärdare ska signera certifikatet med sin elektroniska signatur, så att den som förlitar sig på certifikatet kan identifiera utfärdaren och eventuellt avslöja om det skett några förändringar i certifikatet sedan utfärdaren signerat dokumentet.
9. Uppgifter om certifikatets användningsområde och om det finns några begränsningar. *Exempelvis ska minimibelopp och maximibelopp anges för certifikatet användning*.[49]

Utöver dessa punkter kan regeringen eller PTS ytterligare precisera kraven och ange hur de ska infrias.

De certifikat som uppfyller de ovan och de i bilaga ? till direktivet uppställda kraven är alltid att anse som kvalificerade inom EES området.

Under särskilda förutsättningar anses dock ett certifikat som utfärdats av en certifikatutfärdar i tredje land (utanför EES) under beteckningen kvalificerat som likvärdigt med de kvalificerade certifikat som utfärdats inom EES. De särskilda förutsättningar som krävs, är att utfärdaren får utfärda dessa certifikat i tredje land och uppfyller de i direktivet uppställda villkoren eller har ackrediterats i en medlemsstat. Dessutom kan ett tredje lands certifikat erkännas som likvärdigt gemenskapens certifikat om en CA som är

[47] LKS, 6 §. Prop. 1999/2000:117, s 41.
[48] LKS 6 §.
[49] Prop. 1999/2000:117, s 55f, 70f.

etablerad inom EES området garanterar certifikatet eller om utfärdaren eller certifikatet har erkänts genom ett internationellt avtal.[50]

3.4.1 Utfärdande

I Sverige använder vi ofta det engelska uttrycket CA som benämning på en betrodd tredje part, men även Trusted Third Party (TTP) och Certification Service Provider (CSP) används.[51]

Som tidigare berörts ska ett certifikat som betecknas kvalificerat vara utfärdat av en CA.[52] Lagen uppställer stränga krav på utfärdarens organisation för att utfärdaren ska få kalla sina certifikat kvalificerade. En CA bör därför ha en utarbetad policy en s k. Certifikation Practice Statment (CPS) där verksamhetens rutiner, säkerhetskrav, ansvarskrav osv. framgår och regleras.[53] De krav som en CA måste uppfylla enligt LSK överensstämmer med direktivets bilaga ??.

Enligt bilaga ?? till direktivet och lagens 9 § ska en CA som utfärdar kvalificerade certifikat till allmänheten bedriva verksamheten tillförlitligt och se till att personalen har en tillräcklig kompetens och erfarenhet för den speciella verksamheten. Utfärdarens rutiner för ledning och administration ska uppfylla erkända standarder. European Telecommunications Standards Institute (ETSI) är ett standardiserings institut som bl.a. tar fram standarder för certifieringsorgan. Flertalet av marknadens framtida certifieringsorgan kommer troligtvis att utforma sin CSP efter ETSI:s modell. ETSI standarden är den mest vedertagna standarden och anses därför som den ”officiella”. [54] De system och produkter som en CA använder sig av måste vara skyddade mot ändringar och garantera en hög säkerhet. Dessa anses uppfylla lagens krav på säkerhet om de överensstämmer med den standard som är under utveckling för de säkra anordningarna (se kap 3.3 ovan). Utfärdaren ska även ha säkra rutiner för identitetskontroll av de personer som certifikaten utfärdas för. Om utfärdare brister i sin identitetskontroll kan problem med försök att förvärva falska identiteter uppstå.

En CA måste även förfoga över ett snabbt och säkert system för återkallande av registrerade certifikat.[55] En CA ska omedelbart återkalla certifikatet om undertecknaren begär det eller när det finns någon annan anledning. En ”annan anledning” kan vara att det står klart att den privata nyckeln röjts för någon obehörig eller använts av någon annan än den rättmätige innehavaren. En exakt tidpunkt för när certifikatet utfärdats eller återkallats ska en CA

[50] LKS, 7 §. Prop. 1999/2000:117, s 31, 41-42.
[51] Telefonintervju med Gunnar Lindström på SWEDAC, 2001-03-16.
[52] LKS, 6 §.
[53] Aversten, s 29.
[54] Prop. 1999/2000:117 s 41-43. Electronic signature formats (Standard); ETSI TS 101 733 v.1.2.2. http://www.etsi.org
[55] LKS, 9 §. Prop. 1999/2000:117, s 42-43, 72-73. ETSI-standard, TS 101 456 V1.1.1, 2000-12.

alltid kunna säkerställa. Med hjälp av s.k. tidsstämpling kan en precis tids och datum angivelse säkras av utfärdaren. Visserligen antecknas oftast en datum angivelse i dokumentet, men det är inte alltid som parterna anger ”rätt” tidsangivelse i dokumentet. Parterna kan exempelvis ha fördaterat dokumentet. En tidsstämpling går till så att avsändaren hos en CA registrera sin elektroniska signatur (dvs. det från dokumentet uträknade hashvärdet som krypterats med avsändarens privata nyckel). Härmed har ett bevis skapats för att dokumentet existerade vid tidpunkten för registreringen. Vid en eventuell tvist kan en tidsstämpling ge ett högre bevisvärde, än en ”vanlig” tidsangivelse i dokumentet.[56]

En utfärdare är även skyldig att lagra all relevant information om certifikatet under så lång tid som är motiverad med hänsyn till typen av certifikat och övriga omständigheter som anses relevanta. Det är dock strängt förbjudet för utfärdaren att lagra eller kopiera den dolda nyckeln. Den ska bara vara tillgänglig för undertecknaren och ingen annan.[57]

Lagen uppställer vissa formkrav för utfärdande av kvalificerade certifikat. Utfärdaren ska på ett lättförståeligt språk skriftligen informera motparten, så att tjänsten med enkelhet kan värderas. Med ”skriftligt” menas ”inte muntligt”, och därför omfattas även information som skickas elektroniskt. Att lämna informationen på en webbsida där utfärdaren när som helst kan ändra informationen, uppfyller emellertid inte lagens krav.[58]

3.4.2 Skadestånd

En CA kan i vissa situationer bli skadeståndsskyldig för den skada som drabbat den som förlitat sig på certifikatet, t.ex. om certifikatet innehållit felaktiga uppgifter. Det är inte bara mottagaren som kan erhålla skadestånd, även undertecknaren kan kräva ersättning. Den senare kan också efter ingånget avtal med en CA, lida skada vid brister i certifikatet. Utfärdaren är däremot inte skyldiga att ersätta skada, om den kan visa att skadan inte orsakats p.g.a. vårdslöshet hos utfärdaren själv eller om certifikatet använts i strid med begränsningar som gällde för det aktuella certifikatet. En CA har således ett presumtionsansvar med möjlighet att exculpera sig.[59] Enligt allmänna skadeståndsrättsaliga principer är det som huvudregel den skadelidande som har bevisbördan för att oaktsamhet har förekommit. Den skadelidande ska även bevisa att kausalitet förelegat mellan skadan och de fel som en CA begått.[60] Bestämmelsen är enligt 15 § LKS tvingande till förmån för den som förlitar sig på certifikatet. I den mån det finns ett avtal mellan utfärdaren och den som ska förlita sig på certifikatet, kan därför inte utfärdaren avtala bort någon del av sitt skadeståndsansvar.[61] Det går dock bra att utöka utfärdaren ansvar till förmån för den förlitande parten.

---

[56] Aversten, s 24.
[57] LKS, 10-11 §§. Prop. 1999/2000:117, s 73-74.
[58] LKS, 12 §, Prop. 1999/2000:117, s 74.
[59] LKS, 14 §, Prop. 1999/200:117, s 75ff.
[60] Hellner Jan, Johansson Svante, Skadeståndsrätt, 2000, s 145.
[61] Prop. 1999/2000:117, s 76.

3.4.3 Tillsyn

Post och telestyrelsen kommer att fungera som tillsynsmyndighet för de CA som väljer att agera på den svenska marknaden. För att utge kvalificerade certifikat uppställer lagen en anmälningsskyldighet. Anmälan ska ske till PTS innan verksamheten startar.[62]

Enligt EG direktivet får det inte förekomma krav på förhandstillstånd för att få utfärda kvalificerade certifikat till allmänheten. Anmälningsplikten kan därför vid en första anblick, anses strida mot direktivets art 3.1 om förbud mot regler om förhandstillstånd för certifikatutfärdare. Men PTS fungerar endast som tillsynsmyndighet med syfte att kartlägga marknaden, för att reda ut vilka utfärdare som tillsynen ska omfatta. Det är inte fråga om att PTS ska godkänna eller avslå någon CA verksamhet.[63] Utgångspunkten för PTS är att låta marknaden agera så självständigt som möjligt.[64] Tillsynen ska utformas så att den inte lägger för stora administrativa bördor på utfärdarna. En närmare kontroll av en CA:s verksamhet kan t.ex. förekomma efter framförda klagomål. Flertalet av utfärdarna kommer välja att certifiera sin verksamhet mot vedertagna standarder. Vid en eventuell kontroll av en CA som blivit certifierad mot en viss standard kan PTS nöja sig med en kontroll av själva certifieringen.[65]

Med tanke på den framtida omfattningen av certifikatutfärdande finns det inte någon pratisk möjlighet för PTS att i detalj granska varje enskild utfärdare. Myndigheten kommer därför mer få en funktion som garant för att missförhållanden följs upp och åtgärdas.[66]

Vid konstaterad överträdelse av lagen kan PTS förelägga rättelse eller att verksamheten helt eller delvis ska upphöra. Föreläggande om att verksamheten ska upphöra får endast meddelas om mindre ingripande åtgärder visat sig vara verkningslösa. Förelägganden och förbud kan även förenas med vite.[67] Lagens utformning skapar emellertid incitament för att undgå tillsyn. Till exempel kan en utfärdare försöka undgå lagen genom att inte kalla sina certifikat för kvalificerade. Utfärdare kan kanske istället kalla sina certifikat för ”starka” certifikat. En sådan utveckling kan undergräva hela strukturen för det öppna nyckelsystemet. En hög kostnad för utfärdande av kvalificerade certifikat kan även leda till att utfärdarna väljer mindre säkra lösningar.

[62] Prop. 1999/2000:117 s 60-63.
[63] LKS, 8 §. Prop. 1999/2000:117, s 71-72.
[64] Telefonintervju med Bo Bergner på PTS, 18/10-00.
[65] Prop. 1999/2000:117, s 60ff.
[66] Ibid. s 78.
[67] LKS, 20, 21 §§.

3.5 Kvalificerade elektroniska signaturer

Enligt direktivet ska medlemsstaterna säkerställa att kvalificerade elektroniska signaturer får en viss särställning. Det innebär att signaturerna ska ha en särskilt hög säkerhetsnivå. Den eftersträvade säkerhetsnivån uppfylls när signaturerna baseras på ett kvalificerat certifikat, och signaturen skapats med en säker anordning. ”Säkerställa” innebär att varje medlemsland ska se till att de kvalificerade elektroniska signaturerna ska:

”*satisfy the legal requirements in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data”*.[68]

Vid arbetet med LKS ansåg några remissinstanser att innebörden av artikel 5 var att de kvalificerade signaturerna måste jämställas med den egenhändiga namnteckningen. Detta avfärdades av övriga instanser som ansåg att artikeln inte kunde läsas isolerat från övriga artiklar i direktivet. Av särskild betydelse var enligt lagstiftaren syftet med direktivet, som enligt art 1 är att underlätta användningen av elektroniska signaturer och bidra till signaturernas rättsliga erkännande. Direktivet omfattar inte nationell lagstiftning, gällande ingående av avtal, andra rättsliga förpliktelser eller föreskrifter om formkrav. Direktivet inverkar inte heller på nationella bestämmelser om användning av dokument. Lagstiftarens ansåg därför att direktivet inte inom något rättsområde föreskriver medlemsstaterna ett krav på att generellt acceptera de elektroniska signaturerna. Den svenska lagstiftaren tolkade därför det berörda som att direktivet inte förbjuder den enskilda staten från att ha vissa nationella formkrav som utesluter användandet av elektroniska signaturer.[69]

Enligt LKS ska om det i svensk lag eller annan författning ställs krav på egenhändig underskrift eller motsvarande och om det är tillåtet att uppfylla kraven med elektroniska medel, en kvalificerade elektronisk signatur anses uppfylla kraven.[70]

Trots de kvalificerade signaturernas särställning, får det inte ställas högre krav på icke kvalificerade signaturer (inte baserade på ett kvalificerat certifikat) än de kvalificerade. Många gånger kan en icke kvalificerad signatur vara tillräcklig för att uppfylla de krav som ställs på underskrift eller liknade. Resultatet blir att när det är tillåtet att uppfylla ett rättsligt förfarande på elektronisk väg, ska de kvalificerade signaturerna automatiskt anses uppfylla kraven. Medan ett accepterande av de icke kvalificerade signaturerna först kan ske, efter avgörande från fall till fall. Vid konstaterande om de icke kvalificerade signaturers kan användas, måste det avgöras om signaturen uppfyller de bakomliggande krav som situationen

[68] Direktiv. 1999/93/EG, Art 5.1.a.
[69] Hultmark Christina, European and U.S. perspective on electronic documents and electronic signatures, 1999, s 143-144. Prop. 1999/2000:117, s 55ff.
[70] LKS, 17 §.

eller bestämmelsen kräver.[71] Praxis kan även i vissa fall skapas som gör att också signaturer med lägre säkerhetsnivå erkänns. I dessa fall kan också icke kvalificerade signaturer ”automatiskt” accepteras.

Direktivet föreskriver att alla elektroniska signaturer ska erkännas rättslig verkan och giltighet som bevis vid rättsliga förfaranden. Som tidigare nämnts utgör detta inget problem för Sverige, då principen om den fria bevisprövningen tillämpas här. Lagstiftaren har därför inte ansett sig behöva införa någon reglering om detta i den svenska lagen.[72]

[71] Ds 2001:13, E-handelsdirektivet – Genomförande av direktivet 2000/31/EG om vissa rättsliga aspekter på informationssamhällets tjänster s 110. Lindberg Agne, Elektroniska originaldokument och elektroniska signatur, rättsliga konsekvenser av papperslös dokumenthantering, 1987, s 33.
[72] Direktiv 99/93/EG, Art 5.

4 Signatur och dokument i traditionell resp. elektronisk miljö

4.1 Inledning

Som konstaterats ovan måste en kvalificerad elektronisk signatur enligt LKS erkännas rättslig verkan i de fall krav på underskrift, egenhändigt undertecknande eller motsvarande får uppfyllas med elektroniska medel. Lagen ger emellertid ingen vägledning för när en underskrift får uppfyllas med elektroniska medel. En intressant fråga är därför om en elektronisk signatur rättsligt kan motsvara en traditionell signatur? I de flesta fall när en underskrift används är den förbunden med ett dokument. Varken direktivet eller lagen reglerar användandet av elektroniska dokument. När det uppställs krav på att dokumentet ska förses med en underskrift, kan då även ett elektroniskt dokument användas?[73] Rättsverkan och bevisverkan är av central betydelse vid en diskussion angående ovan ställda frågor. Dessa är några av de problem och frågeställningar som ska beröras nedan.

4.2 Traditionell namnteckning – elektronisk signatur

Att jämföra eller att likställa en elektronisk signatur med en traditionell namnteckning är komplicerat. Särskilt eftersom de båda skiljer sig markant från varandra på flera punkter. Den elektroniska signaturen bygger på ett avancerat och komplicerat krypteringsförfarande där flera parametrar spelar in. En elektronisk signatur är dessutom direkt kopplad till den information som signerats och inte fristående på samma sätt som den traditionella namnteckningen.

Rättssystem reglerar sällan hur en signering skall utföras. I svensk rätt finns det inte någon bestämmelse som reglerar detta. Här följer några frågeställningar som inte direkt kommer att behandlas i arbetet, men som belyser ämnets komplexitet: Vad är en signatur? Är en signatur uteslutande de fall då ett namn skrivs på ett papper, och kan det då räcka med ett ”x” på ett papper? Är det en signatur om ett namn ristats in i ett träd, skrivits i blöt sand, skapats med hjälp av en skrivmaskin, eller är det en signatur om jag skriver en annan persons namn? osv. Kan en signatur också inbegripa ett digitaliserat fingeravtryck, ett e-mail med avsändarens namn längst ner på dokumentet eller ett namn på ett faxat dokument? Enligt Hultmark är det

[73] Behandlas under kap 4.3.

inte hur symbolen för signaturen ser ut som är avgörande, utan det bakomliggande syftet med användandet.[74]

En signatur har olika syfte beroende på vilken bestämmelse som i det aktuella fallet krävt en signatur, underskrift eller motsvarande. Vid en studie av dessa bestämmelser eller andra situationer där signaturer används, kan ett antal grundläggande funktioner hos signaturen konstateras. Den traditionella signaturen (penna och papper) kan sägas fylla fem grundläggande funktioner. Funktionerna är av central betydelse vid en diskussion angående de elektroniska signaturernas rättsverkan.[75]

En signatur anses ha en:[76]

1. Identifieringsfunktion – identifierar undertecknaren
2. Äkthetsfunktion – säkerställa att innehållet är äkta
3. Bevisfunktion – signaturen är varaktig och kan på ett säkert sätt binda undertecknaren till innehållet
4. Avslutsfunktion – genom signeringen får dokumentet sitt slutgiltiga utförande
5. Varningsfunktion – signeringen uppmärksammar undertecknaren på att vissa rättsliga konsekvenser kommer att uppstå

Med hjälp av ovanstående funktioner ska den inledande frågan om en elektronisk signatur kan motsvara en traditionell signatur försöka besvaras. Nedan ska varje funktion analyseras för sig, för att se om funktionen kan uppfyllas på elektronisk väg. Avslutningsvis kommer resultatet från analysen att utmynna i en sammanfattande slutsats.

4.2.1 Identifieringsfunktionen

Signaturen har bl.a. till syfte att identifiera dokumentets undertecknare. Den som får det signerade dokumentet kan utifrån undertecknarens signatur bekräfta att dokumentet signerats av rätt person. Men ger en traditionell signatur verkligen möjlighet till en säker identifiering? Varje människa har visserligen en unik signatur, men då undertecknarens signatur inte är känd för motparten eller den inte kan jämföras med en ”gammal” signatur är identifieringen inte vidare säker. För en vanlig lekman utan erfarenhet från tydning av signaturer (grafologi) framstår en mer omfattande kontroll av namnet föga realistisk.

När det gäller elektroniska signaturer och framförallt kvalificerade sådana kan en betydligt säkrare identifiering åstadkommas. De kvalificerade signaturerna bygger som ovan beskrivits på ett PKI system där ett nyckelpar har en central roll. En säker identifiering kan utföras eftersom en CA vid utfärdandet av certifikatet (reg. av nyckelpar osv.) kontrollerat

[74] Hultmark Christina, Elektronisk handel och avtalsrätt, 1998, s 30.
[75] Lindberg, Westman, s 30f.
[76] SOU 1996:40, s 232. Lindberg, s 30ff. Hultmark, 1998, s 29f.

nyckelinnehavarens identitet. Undertecknaren som signerar sitt dokument med den dolda nyckeln, kan sedan identifieras genom utfärdaren. Certifikatutfärdaren kan intyga att undertecknaren är innehavare av den publika nyckeln. Som bekant är det endast avsändarens publika nyckel som kan öppna ett dokument som signerats med den privata nyckeln i nyckelparet. En förutsättning för säker identifiering är att utfärdaren har en acceptabel kontroll vid registrering av nya nycklar. Eftersom utfärdaren kan bli ersättningsansvarig för skada som förorsakats den som förlitat sig på ett felaktigt certifikat, kommer sannolikt kontrollen att vara sträng.[77] Att sambandet mellan signaturen och en viss person konstaterats är bra men inte tillräckligt för att uppfylla identifikationsfunktionen. Vem som helst som har tillgång till den dolda nyckeln kan skapa dess signatur, därför behövs ytterligare funktioner. Den dolda nyckeln måste ”personaliseras”, så att den endast kan användas av den registrerade innehavaren. Detta kan ske med hjälp av olika metoder för autenticering, t.ex. PIN-kod.[78] Med en PIN-kod aktiveras således den säkra anordningen som är en förutsättning för att innehavaren ska kunna signera ett dokument. Följaktligen uppfylls identifieringsfunktionen elektroniskt genom certifikatet och aktiveringen av den säkra anordningen.[79] En signatur som utförts enligt ovan uppställda premisser uppnår därför med lätthet identifieringseffekten.

4.2.2 Äkthetsfunktionen

Äkthetsfunktionen påminner till viss del om identifieringsfunktionen. För att fastställa att dokumentet är äkta måste detta härröra från upphovsmannen. Signaturen kan fylla denna funktion eftersom en signatur i regel har skrivits så många gånger att underskriften liknar en reflexrörelse med små variationer gång från annan. Signaturen blir därför utmärkande för undertecknaren och ett förfalskningsförsök kan bli en besvärlig procedur. Signaturer fungera som en presumtion för att innehållet inte förändrats eftersom undertecknaren förutsätts ha skrivit under just den text som sedan presenterats för motparten. Dock kan med dagens teknik, förfalskningar som tidigare var tidskrävande och besvärligt enkelt skapas av traditionella signaturer. De traditionella signaturerna anses därför ha förlorat i styrka och förmåga, att garantera ett innehåll sin äkthet.[80]

För att äkthetsfunktionen ska uppnås med en (kvalificerad) elektronisk signatur, måste det först säkerställas att dokumentet härrör från den som signerat dokumentet. För det andra att innehållet inte förändrats sedan signaturen påförts. Säkerställande av dokumentets upphovsman motsvarar resonemanget under kap 4.2.1 ovan. När ett elektroniskt dokument signerats med en elektronisk signatur säkerställs innehållet huvudsakligen genom den elektroniska signaturens tekniska förfarande. Till skillnad från

[77] Aversten, s 26ff. Lindberg, Westman, s 31. Hultmark, 1998, s 31 och 35.
[78] Final Report of the EESSI Exepert Team, 990720, s 47.
[79] Winberg Gustav, Elektroniska betalningssystem på Internet, Om teknisk säkerhet och juridisk osäkerhet, 1997, s 58.
[80] Hiselius Patrik, Elektroniska avtalsslut med signatur (EDI och smartkort), 1989, s 65.

identifieringen som huvudsakligen sker utifrån certifikatet.[81] Innehållet i en elektronisk signatur kan inte ändras eller förvanskas utan att mottagaren (som ”öppnar” dokumentet med den publika nyckeln) direkt upptäcker detta. Innehållsförvanskning omöjliggörs av den krypterings och hashfunktionsteknik som används vid skapande av en elektronisk signatur.[82] Med ovanstående i beaktande torde därför den kvalificerade elektroniska signaturen bättre uppnå äkthetsfunktionen än den traditionella signaturen.

4.2.3 Bevisfunktionen

Signaturen ska enligt bevisfunktionen fungera som bevis för att det undertecknade är ett ”original” som speglar undertecknarens slutgiltiga vilja.[83] Signaturen och dokumentet fyller tillsammans en bevisfunktion. Dokument som fysiskt är bärare av signaturen utgör därför ett bevismedel. En av de viktigaste egenskaperna med den traditionella signaturen är att den är bestående. Signaturens varaktighet är viktig framförallt om det uppstår en tvist angående dokumentet. Signaturens existens är således avgörande för dokumentets bevisvärde. Traditionella signaturer är av varaktig natur och kan åberopas som skriftligt bevis inför rätten. Osignerade dokument har följaktligen ett lågt bevisvärde. Men är signaturen verkligen så varaktig? Med utgångspunkt i att signaturen skrivits på ett pappersdokument finns en risk för att dokumentet förstörs, förfalskas osv. Pappret i sig är ju inte något speciellt motståndskraftigt material.

Därför är det intressant att jämföra den traditionella signaturens ”bärare” med den elektroniska signaturens bärare. Pappersdokumentet fungerar som den traditionella signaturens bärare och den ”säkra anordningen” (se 5 § LKS och kap 3.3 ovan) som den kvalificerade elektroniska signaturens bärare. En förutsättning för signaturens bevisvärde är ju att avgöra dess varaktighet. För att avgöra detta måste respektive bärares varaktighet prövas. Begreppet ”varaktig” torde även innefatta resistens mot manipulationsförsök, t.ex. förfalskningar osv. Signaturen lagras inte för obestämd tid i den säkra anordningen. Anordningen behöver endast ha en minneskapacitet som är tillräcklig för att lagra nödvändig information. Lagring av signatur och information sker sedan på ett säkert sätt genom exempelvis en CA:s försorg. Med elektroniska signaturen kan även en mängd funktioner införas för att höja bevisvärdet, t.ex. ”tidsstämpling”. Pappersdokumentet har också en ”tidsstämpling”. Papprets ålder går ju att fastslå om ett datum är skrivet på dokumentet eller om dokumentet börjat gulna etc. Det är således flera parametrar som påverkar signaturens bevisfunktion. Jämförelsen kan verka något drastisk, då ett pappersdokument skiljer sig markant från den ”säkra anordningen”. Men

[81] Winberg, s 58.
[82] Se kapitel 2.2.3 - 2.2.4.
[83] Lilian Edwards, Charlotte Waelde, Law & the Internet regulating cyberspace, Lloyd Ian, Legal Barriers to Electronic Contracts: Formal Requirements and Digital Signatures, 1997, s 140.

jämförelsen kräver ett visst ”tålamod”, då den endast vill belysa de praktiska likheter i effekt som en traditionell respektive elektronisk signatur medför.

4.2.4 Avslutsfunktionen

En signatur har en funktion där undertecknaren avslutningsvis ger uttryck för sin vilja att binda sig vid det aktuella innehållet. Det kan även uttryckas som undertecknarens avsiktsförklaring. Avslutsfunktionen påminner i stort om varningsfunktionen som nedan ska behandlas.

Den elektroniska signaturen har motsvarande funktion, eftersom den även avser att slutligen binda undertecknaren vid signerat innehåll.[84]

4.2.5 Varningsfunktionen

Signaturen har också en funktion att varna undertecknaren. Tanken med denna funktion är att undertecknaren vid signeringen av dokumentet, ska bli medveten om att handlingen är rättsligt förpliktigande. Funktionen motverkar att ogenomtänkta eller omedvetna handlingar inträffar. Den traditionella signaturen uppfyller varningsfunktionen, framförallt då den bygger på en aktiv handling, skriva sitt namn. Det traditionella tillvägagångssättet med att skriva sitt namn längst ner på dokumentet är därtill allmänt känt. Det får även anses känt bland gemene man att en underskrift medför rättsliga konsekvenser.

Den elektroniska signaturen uppfyller inte i sig varningsfunktionen, då denna mycket enkelt eller omedvetet kan skapas. En elektronisk signatur kan t.ex. oavsiktligt skapas och skickas iväg genom en enkel knapptryckning. Varningsfunktionen uppfylls inte med en knapptryckning. Det krävs att undertecknaren upplyses på ett sätt som frambringar en mer aktiv handling. Användandet av ett lösenord för aktivering kan delvis uppfylla funktionen. Vid köp över Internet kan exempelvis en varningstext i kombination med lösenord anses uppfylla funktionen. Varningstexten kan fungera så att undertecknaren måste intyga att han/hon har läst innehållet genom en knapptryckning (likt en disclaimer). En sådan kan lätt infogas och anpassas till olika situationer eller avtalsvillkor. Den elektroniska signaturens största brist när det gäller varningsfunktionen är dess enkelhet, men med enkla medel kan signaturen överträffa den varningsfunktion som de traditionella signaturerna har.[85]

4.2.6 Slutsats

En elektronisk signatur motsvarar i de flesta fall en traditionell signatur och i flera situationer till och med bättre den traditionella underskriftens grundläggande funktioner. Den elektroniska signaturen kan möjliggöra detta med hjälp av PKI strukturens olika delar. Till exempel kan med en CA:s

[84] Hiselius, s 66f, 75f. Lindberg, s 31, 40f. Prop. 1999/2000:117, s 15ff.
[85] Hiselius, s 31, 41. Lindberg, s 66, 75. Prop. 1999/2000:117, s16.

försorg en säker identifiering göras av undertecknaren till ett elektroniskt meddelande. Eftersom PKI systemet bygger på asymmetrisk krypterings- och hashfunktionsteknik, kan även den (kvalificerade) elektroniska signaturen med större säkerhet än den traditionella garantera innehållets äkthet. Tekniken möjliggör nämligen upptäckt vid minsta lilla avvikelse från vad som ursprungligen signerats. Vidare tillämpar vi i Sverige principen om fri bevisprövning. Det finns således inga legala hinder för att åberopa en elektronisk signatur som bevis inför rätten. Det kan emellertid trots avsaknaden av legala hinder finnas andra hinder, som t.ex. den tekniska utvecklingen. Denna försvåra tillämpningen av klara regler och principer för en stor del av de rättsliga problem som kan uppstå vid användandet av elektronisk kommunikation. Mot bakgrund av detta bör därför de tekniska rutiner som omgärdar användandet av elektroniska signaturer utformas så att bevisvärderingen underlättas. I jämförelse med den traditionella penna pappers situationen, behöver de elektroniska signaturernas utförande särskilt anpassas för att uppfylla avsluts- och varningsfunktionerna. Om de elektroniska rutinerna utformas, så att varningsfunktionen uppfylls, är den elektroniska signaturen säkrare och mer effektiv än den traditionella. Med effektiv menas inte bara att den möjliggör snabbare kommunikation. Utan även att en elektronisk signatur avser hela dokumentets innehåll, medan en traditionell underskrift endast avser innehållet på samma sida som underskriften. Sammantaget anser jag att den elektroniska signaturen bättre uppfyller den traditionella underskriftens bakomliggande funktioner.

4.3 Pappersdokument – elektroniska dokument

När det uppställs krav på underskrift eller liknade avses vanligtvis en underskrift på ett dokument. Är det då ett pappersdokument som åsyftas eller kan även ett elektroniskt dokument användas? Frågan har ett nära samband med diskussionen angående signaturen och dess funktioner. På motsvarande sätt som ovan, kan därför det traditionella dokumentets funktioner vara vägledande för det elektroniska dokumentets rättsverkan. Som inledningsvis noteras reglerar varken direktivet eller den svenska lagen de elektroniska dokumentens rättsliga effekt. Direktivet nämner endast att den kvalificerade elektroniska signaturen inte får nekas rättslig verkan enbart p.g.a. dess elektroniska form. Till skillnad från direktivet och den svenska lagen reglerar den amerikanska Uniform Electronic Transaction Act (UETA) även det elektroniska dokumentets rättsliga verkan:

”In a proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form” [86]

Begrepp såsom dokument, urkund, faktura, skriftlig handling o.s.v. behöver nödvändigtvis inte innefatta just ett pappersark som bärare av informationen. Papper såväl som penna, skrivare eller annan anordning kan ses som verktyg med vars hjälp en vis information fixeras.[87] Frågan om

[86] UETA , Sec. 13. Hultmark, 1999, s 151.
[87] Hiselius, s 38.

vilken typ av dokument som en viss bestämmelse avser varierar. Exempelvis är det vid köp av fast egendom ett krav på att köpehandlingen ska vara skriftlig.[88] För att avgöra om ett krav på skriftligt dokument kan uppfyllas på elektronisk väg, måste den aktuella bestämmelsens bakomliggande syfte undersökas. Det är därför viktigt att dokumentets primära funktioner analyseras. Resultatet från en sådan analys är vägledande för om den aktuella situationen eller bestämmelsen kan uppfyllas på elektronisk väg.

Likt signaturen anses pappersdokumentet fylla en rad viktiga funktioner:[89]

1. Informationsfunktion
2. Handläggningsfunktion
3. Upplysningsfunktion
4. Bevisfunktion
5. Symbolfunktion
6. Spridningsfunktion
7. Fixeringsfunktion

Med hjälp av ovanstående funktioner ska den inledande frågan om ett elektroniskt dokument kan motsvara ett traditionellt pappersdokument försöka besvaras. Nedan ska varje funktion analyseras var för sig, för att se om funktionen kan uppfyllas på elektronisk väg. Resultatet från analysen kommer avslutningsvis att utmynna i en sammanfattande slutsats.

4.3.1 Informationsfunktionen

Pappersdokumentets främsta funktion är att distribuera information i form av text. Informationen kan lätt lagras och transporters eftersom den presenteras i papprets varaktiga form.

Informationsfunktionen kan med lätthet också uppfyllas på elektronisk väg. Informationen kan distribueras via Internet och göras läsbar via en skärm eller efter utskrift. Lagring kan även med enkelhet göras elektroniskt. Den enda tänkbara begränsningen är att det krävs särskild utrustning för att den elektroniska informationen ska bli läsbar, såsom PC, skrivare osv. [90]

4.3.2 Handläggningsfunktionen

För att hanteringen av dokumenten ska bli enkel och effektiv har en funktion som underlättar detta ansetts viktig. Bland de företag eller myndigheter som hanterar en stor mängd inkommande dokument har interna rutinerna skapats utifrån rutiner med pappersdokumentet. Med andra ord har

[88] Jordabalken (JB) 4:1
[89] Hiselius, s 30-32, 38-46. Linberg, s 7-13, 19-21.
[90] Hiselius s 30, 44. Lindberg s 11.

papprets funktion varit att underlätta hanteringen av inkommande information.

De senaste åren har emellertid pappersdokumenten i allt större utsträckning ersatts av elektroniska dokument. Den elektroniska behandlingen av inkommande information anser jag vara både bättre och effektivare.

4.3.3 Upplysningsfunktionen

Denna funktion kan sägas inrymma två moment. För det första fungerar pappersdokumentet som en upplysningskälla för tredje man. Funktionens andra moment rör parterna, eftersom informationen i form av text blir tydliggjord för parterna. Dokumentet är därför inte bara bärare av information, utan parterna uppmärksammas även genom dokumentets existens om de sakförhållanden som detta föranleder.

Handläggningsfunktionen kan även uppfyllas med hjälp av ett elektroniskt dokument. Det första momentet att dokumentet ska fungera som en upplysningskälla för tredje man, kan med lätthet infrias på elektronisk väg. Det räcker med att den information som lagrats eller skickats elektroniskt ska kunna återskapas i läsbar form. Om parterna före avslutet tvingas signerar dokumentet med en elektronisk signatur, medför detta även att de uppmärksammas på de rättsliga konsekvenser som handlingen innebär. Därmed uppfylls även funktionens andra moment.

4.3.4 Bevisfunktionen

Ett pappersdokument kan i en eventuell tvist åberopas som skriftlig bevisning. Signaturen fyller här en viktig funktion och ett dokument utan signatur har därför ett svagt bevisvärde.[91]

Likt resonemanget ovan angående signaturer har säkerheten i det elektroniska signaturerna en avgörande betydelse för bevisfunktionens uppfyllande. Som jag ovan framhåller uppfyller PKI systemet motsvarande eller till och med högre bevissäkerhet och bevisvärde än det traditionella pappersdokumentet och dess underskrift. Som tidigare förklarats utgår den svenska rätten från principen om fri bevisprövning. Domstolen är inte heller skyldig att bedöma bevisningens värde utifrån några förutbestämda regler. Rättens ”egna” inställning till vilket värde som den elektroniska signaturen och dokumentet får, är därför ytterst avgörande för bevisfunktionen och bevisvärdets styrka.

4.3.5 Symbolfunktionen

Pappersdokumentet har en speciell funktion avseende vissa värdepapper. Löpande skuldebrev, checkar och växlar osv., fungerar inte bara som bärare

[91] Hiselius, s 30-32.

av information eller som bevismedel, utan även som bärare av en rättighet. Innehav och traditionen är avgörande för vem som är berättigad att erhålla viss prestation eller för att avgöra sakrättsliga problem. Symbolfunktionen är därför starkt knuten till rättsföljden av besittning och tradition.

Det är tveksamt om denna funktion kan uppfyllas på elektronisk väg. Ett problem med elektroniska dokument som inte förkommer vid brukande av pappersdokument är att avsändaren även efter avsändandet i princip har ”besittning” över dokumentet. Möjligen skulle ett system med registrering av information kunna lösa ovanstående problem. Om den elektroniska informationen registrerats till förmån för mottagaren eller tredje man, kan avsändaren inte i ordets bemärkelse anses ”besitta” dokumentet. Registreringen bör då utformas med en tidsangivelse, så att rätt innehavare från och med registreringen kan utläsas. Vid en eventuell tvist kan det sedan konstateras vem som rättmätigt förfogar över dokumentet.[92]

4.3.6 Spridningsfunktionen

Med denna funktion avses informationsbärarens förmåga att snabbt och säkert kunna sprida informationen. Pappersdokumentet uppfyller endast svagt denna funktion. Pappret i sig uppfyller inte funktionen utan behöver hjälp genom postgång. Postgången kan ifrågasättas, då den anses som långsam och inte alltid helt tillförlitlig, vilket budfirmornas expansion är ett bevis för. För att sprida informationen via papper måste antingen ett original eller en kopia av pappret skickas iväg. Detta är ett osäkerhetsmoment, då varken ett original eller en kopia är tillfredsställande att skicka iväg. [93]

De elektroniska dokumenten har här betydligt bättre förutsättningar för spridning än de traditionella pappersdokumenten. Utifrån PKI strukturen kan elektroniska dokument snabbt och säkert spridas till en eller flera mottagare. Ytterligare en fördel (dock inte symbolfunktionen) med dessa dokument är att avsändaren behåller sitt original, samtidigt som mottagaren får ett original.

4.3.7 Fixeringsfunktionen

Här avses informationsbärarens uppgift att hålla informationen intakt och oförändrad. Eventuella förändringar måste gå att upptäcka eller ska framgå vid en enkel kontroll. Papperskopior anses idag inte speciellt pålitliga och kräver vanligtvis vidimering. Pappersoriginal anses inte heller helt säkra eftersom dagens teknik relativt enkelt möjliggör mycket bra förfalskningar.

Med utgångspunkt i PKI strukturen och den asymmetriska kryptotekniken, så uppfylls fixeringsfunktionen betydligt bättre elektroniskt. Som jag ovan

[92] Hultmark, 1998, s 67. Andersen, Grundlæggende aftaleret, 1997, s 169. Vad det gäller tradition och möjligheten att tradera elektroniska dokument råder osäkerhet.
[93] Hiselius, s 30.

har beskrivit upptäcks minsta lilla ändring eller manipulations försök i de elektroniska dokument som signerats med en kvalificerad elektronisk signatur.[94]

4.3.8 Slutsats

Vare sig det är ett pappersdokument eller ett elektroniskt dokument, är det förmedling av information i form av läsbar text som är det primära syftet. Information som förmedlas med traditionellt papper kan på motsvarande sätt framföras elektronisk. Det elektroniska dokumentet har även visat sig på flera punkter överträffa pappret. Till exempelvis är det elektroniska dokumentet bättre och effektivare att handlägga. Det är vidare viktigt att dokumentet kan fungera som bevis i en eventuell tvist. Dokumentets funktion som bevis skapas främst genom signaturen. Säkerheten är mycket hög vid användandet av signaturer som baseras på asymmetrisk kryptoteknik, därför anser jag att det elektroniska dokumentet i flera fall överträffar papprets bevisvärde. Vidare är det elektroniska dokumentets spridningspotential både säkrare och effektivare än papprets postgång. Detta förutsätter emellertid att mottagaren har tillgång till ett medium för att läsa det elektroniska dokumentet. I dagens samhälle har de flesta en dator eller tillgång till en, därför är utgör inte tillgängligheten någon begränsning för de elektroniska dokumenten.

Vad det gäller den viktiga egenskapen att dokumentet ska hålla informationen intakt och oförändrad är ett elektroniskt dokument som signerats med en elektronisk signatur överlägset pappersdokumentet på kort sikt. På längre sikt har pappret en fördel då det inte går att garantera äktheten i en elektronisk signatur i mer än en begränsad tidsrymd. Så fort som de oknäckbara nyckellängderna vi använder idag går att knäcka, är den elektronsiska signaturen värdelös. En lösning på problemet kan vara att en CA garanterar dokumentets ursprung, äkthet osv. En sådan ”säker lagring” av dokumentet, bör fungera som ett mer långsiktigt alternativ.

I en elektronisk miljö finns endast original, då alla ”kopior” är identiska med originalet. Med PKI systemet som bas kan därför förmedlandet av de elektroniska ”originalen” ske säkert, medan en papperskopia för att erhålla någon pålitlighet måste vidimeras. Inte ens det vidimerade pappersdokument får enligt min mening samma säkerhet som ett elektroniskt dokument som signerats med en kvalificerad elektronisk signatur. Dock uppstår i vissa situationer problem med de elektroniska dokumenten, då de endast existerar i identisk form. Den symbolfunktion som pappersdokumentet har kan svårligen uppnås på elektronisk väg. Problemet ligger i det att avsändaren även efter avsändandet fortfarande har kvar ett identiskt exemplar av det som skickats iväg. Med andra ord skapar den elektroniska teknikens exakthet och effektivitet problem vid uppfyllande av symbolfunktionen.

[94] Ibid. s 31, 46.

Sammanfattningsvis kan konstateras att det traditionella pappersdokumentets funktioner gott och väl kan uppfyllas på elektronisk väg, med viss reservation för symbolfunktionen, som troligtvis kan uppfyllas med hjälp av registrering.

5 Regleringar och alternativa synsätt

5.1 Inledning

Under följande avsnitt ska alternativa synsätt samt befintliga och föreslagna regleringar angående elektroniska signaturer behandlas. Tanken är att klargöra vilka alternativa regleringar och principer som en domstol kan använda sig av när inte nationella lagregler eller principer är direkt tillämpbara. Bl.a. kommer direktivförslaget om elektronisk handel att behandlas.

5.2 UNCITRAL

5.2.1 Bakgrund

FN:s generalförsamlig skapade 1966 United Nations Commission on International Trade Law (UNCITRAL), vars syfte var och är att harmonisera den internationella handelsrätten. UNCITRAL och dess regelverk har haft betydelse för flera nya lagar beträffande elektronisk handel och elektroniska signaturer. 1996 grundades UNCITRAL Model Law on Electronic Commerce (modellagen) vars syfte är att förenkla användandet av modern kommunikations teknik, med eller utan Internet som bas. Genom att skapa standarder som rättsliga värden enkelt kan utvärderas ifrån, eftersträvar lagen att spela en viktig roll i att öka användandet av ”papperslös” kommunikation. UNCITRAL:s modellag bygger på principen om funktionell ekvivalens. Lagen är en s.k. ”soft law”, då den är utformad som en ”riktig” lag, men saknar lagens karakteristiska tvångselement. Enligt modellagen kan formkrav, såsom ”skriftligt” i vissa fall uppfyllas på elektronisk väg. Likaså kan krav på ”handling” eller ”dokument” även omfatta elektroniskt överförd information.[95]

5.2.2 Funktionell ekvivalens

Vid tillämpning av principen om funktionell ekvivalens måste först det bakomliggande syftet med bestämmelsen analyseras, för att sedan avgöra om syftet kan uppfyllas på elektronisk väg. Principen utgår till skillnad från den strikta bokstavstolkningen från ändamålet bakom regleringen och bedömer om den aktuella regeln likväl kan infrias på elektronisk väg.[96]

[95] Andersen, 1997, s 72. http://www.uncitral.org
[96] Hultmark, 1998, s 21f. Hultmark, 1999, s 130-131.

Modellagen har fungerat som inspirationskälla för direktivet, vilket tydligt framgår av lagens art 5; *”Information shall not be denied legal effect, validity or enforce- ability solely on the grounds that it is in form of a data message”*.[97] Motsvarande innebörd går att finna i direktivets art 5.2. Huvudregeln i UNICTRAL:s modellag slår alltså fast att ett elektroniskt meddelande inte ska nekas rättslig verkan endast p.g.a. att det framförts i elektronisk form.

Det finns exempel från svensk rättspraxis där rätten har använt sig av en metod som påminner om principen om funktionell ekvivalens. I fallet NJA 1981:853 utgick rätten från syftet bakom den aktuella regeln. I fallet hade en intern, istället för sitt verkliga namn signerat en överklagan (besvärsinlaga) med ”prisoner 1006”. Enligt RB:s dåvarande lydelse skulle en besvärsinlaga vara egenhändigt undertecknad av den klagande eller dennes ombud. Emellertid godtog HD i fallet det något speciella ”undertecknandet”, med motiveringen att syftet med bestämmelsen var att göra det möjligt för rätten att konstatera att överklagan var undertecknad av rätt person. HD konstaterade visserligen att identifieringen försvårades när inte rätt namn angivits, men ”om det av andra omständigheter framgår vem som undertecknat inlagan, får kravet på egenhändigt undertecknade anses uppfyllt”.[98]

När lagen uppställer krav på ”skriftlighet” och inte specificerar vilket medium som den ”skriftliga” informationen ska ”bäras av” uppstår osäkerhet. Visserligen är det allmänt känt att ”skriftligt” kan vara text skriven med en penna på ett papper, men kan det även innefatta andra varianter.[99] Vid kontraktstvister gällande bestämmelser i kontraktet avgörs dessa vanligtvis genom att rätten försöker avgöra parternas gemensamma partsvilja. Parterna avsikt vid kontraktets ingående är således avgörande.[100]

På motsvarande sätt kan avsikten med en aktuell regel som föreskriver ”skriftlighet”, avgöras utifrån principen om funktionell ekvivalens. En regel i ett kontrakt att kommunikationen mellan parterna ska ske skriftligt, bör tolkas utifrån regeln bakomliggande syfte. Vilket kan vara att möjliggöra en tillförlitlig kommunikation mellan parterna. Hur kommunikation sker är inte avgörande. Den kan ske antingen via ett pappers- eller ett elektroniskt dokument. Avgörande för regelns uppfyllande är därför om kontakten mellan parterna skett tillförlitligt.

När en lag föreskriver att information ska vara skriftlig kan enligt modellagens art 6(1) kravet likväl uppfyllas på elektronisk väg”…..*if the*

---

[97] 1999/93/EG, art 5.
[98] NJA 1981:853
[99] **Skrift**: systematiskt sätt att återge språkligt innehåll med grafiska tecken, bildskrift, bokstavsskrift, kilskrift, ljudskrift, runskrift, maskinskrift, neonskrift, handskrift, underskrift, utskrift, guldskrift, inskrift osv. **Skriftlig**: som uttrycks i skriven form (mots. muntlig). Allén Sture, Svensk Ordbok, 1988.
[100] Bernitz Ulf, Standardavtalsrätt, 1993, s 43.

information contained therein in accessible so as to be usable for subsequent reference." Ett elektronisk meddelande bör enligt art 6(1) uppfylla eventuella krav på "skriftlighet", så länge som mottagaren kan ta emot informationen i läsbar form.

Modellagens art 7 föreskriver att när en lagstiftning kräver en "underskrift", ska kravet likväl kunna uppfyllas på elektronisk väg, om den elektroniska underskriften kan säkra undertecknarens identitet. Undertecknaren ska även ha godkänt informationen som är kopplad till signaturen. Med godkännande innebär att undertecknaren har haft möjlighet att tänka efter, och att underskriften inneburit en "varning" för denne (se varningsfunktionen ovan kap 4.2.5).[101]

Art 7 underlättar tolkningen av elektroniska signaturer och klargör deras legala verkan. Men den lämnar över ett stort ansvar till rätten för att avgöra om kraven kan uppfylldas på elektronisk väg.[102] Detta leder i sin tur till att det ställs höga krav på rättens ledamöter. Rätten måste ha vetskap om den aktuella tekniken, samt känna till dess olika varianter och funktioner. Denna problematik belyser även modellagens övriga regler, eftersom dessa till stor del förlitar sig på rättens uppfattning vid varje nytt fall.

Regelverket har flera fördelar, bl.a. att den är teknikneutral vilket ökar reglernas "livslängd" och flexibilitet. De regler och bestämmelser som inte är strikt knutna till dagens teknik är ju enklare att applicera på nya företeelser. När det gäller informationstekniken är det allmänt känt att förändringshastigheten är hög. Med en teknik som ständigt förändras och finner "nya vägar", utsätts befintliga regler för tillämpnings problem. Genom att utforma regler likt modellagens, skapas goda möjligheter för dagens regler att förbli intakta. Med teknikneutrala regler kan lagstiftaren undvika att nya och ändrade regler ständigt måste införas.

5.3 E-handelsdirektivet

I följande avsnitt ska e-handelsdirektivet och de konsekvenser som detta få på den svenska rätten behandlas. I analysen behandlas även formkrav och tolkning samt en föreslagen lagändring i konsumentkreditlagen (KkredL). Förslaget är intressant för de elektroniska signaturernas acceptans och tillämpning.

Europarådets och rådets direktiv om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (e-handelsdirektivet), avser att förbättra den rättsliga infrastrukturen. En förbättrad infrastruktur medför att den interna europeiska handeln kan fungera mer friktionsfritt. Vilket i sin tur leder till en positiv

[101] Hultmark, 1999, s 133-137, 142f.
[102] Boss Amelia H, Electronic commerce and the symbiotic relationship between international and domestic law reform, 1998, s 1969f.

ekonomisk tillväxt som anses öka den europeiska industrins konkurrenskraft.

Enligt e-handelsdirektivets art 9.1 *”… skall varje medlemsstat se till att deras rättssystem tillåter att avtal ingås på elektronisk väg. Medlemsstaterna skall särskilt se till att de rättsliga krav som är tillämpliga på avtalsprocessen varken skapar hinder för användningen av avtal på elektronisk väg eller medför att sådana avtal frånkänns rättslig verkan och giltighet på grund av att de kommit till stånd på elektronisk väg.”*

Artikeln föreskriver att formkrav som hindrar avtal från att ingås på elektronisk väg ska upphävas i den nationella lagstiftningen, med vissa undantag. Därför ska de medlemsstater som har lagstiftning som innehåller särskilda formkrav ändra dessa, så att de inte hämmar användningen av t.ex. elektronsikt förmedlade avtal. E-handelsdirektivet hindrar emellertid inte enskilda medlemsstater från möjligheten att ställa upp generella eller särskilda krav för avtal som ingås på elektronisk väg. Särskilt när det gäller kvalificerade elektroniska signaturer.[103] De krav som här åsyftats kan t.ex. var krav på speciella certifikatutfärdare osv. Medlemsstaterna får också behålla vissa krav som hindrar avtal från att ingås på elektronisk väg, såsom avtal om fast egendom med undantag för hyresavtal. Vidare får undantag från art 9.1 även föreskrivas för avtal rörande familjerättsliga eller successionsrättsliga bestämmelser.[104]

Effekten av e-handelsdirektivet är som tidigare nämnt liten på svensk lagstiftning, då den svenska civilrätten innehåller få lagregler som kräver att avtal ska ingås i pappersform med egenhändiga underskrifter.[105] Som ovan diskuterats kan krav på skriftlighet i flera samanhang också innefatta användandet av elektroniska medel. I vissa fall avser krav på skriftlighet allt som inte sker muntligt, medan i andra fall begreppet skriftligt uteslutande avser papper och penna.[106] Innebörden av begreppet bör därför tolkas i varje fall för sig. När det krävs att en handling ska vara ”undertecknad” råder det olika åsikter. Lagstiftaren förefaller ha den åsikten att när en handling ska vara ”undertecknad”, så innefattas inte elektroniska rutiner.[107] Hultmark är av en annan uppfattning och anser att syftet med formkravet ska analyseras för att avgöra om regelns bakomliggande syfte likväl kan uppfyllas på elektronisk väg.[108]

I vissa fall kräver alltså lagstiftningen att avtal ska ingås skriftligen med en egenhändig underskrift. Ett exempel är 9 § KkredL, där ett avtal om kredit

[103] Ingressen till Direktiv 2000/31/EG, Europaparlamentets och rådets direktiv om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på de inre marknaden (e-handelsdirektivet), p 34, 35.
[104] Ibid. art 9.2.
[105] Ds 2001:13, s 37f.
[106] Prop. 1999/2000:84, Lag om konsumentskydd vid distansavtal och hemförsäljningsavtal, s 41.
[107] SOU, 1996:40, s 93ff. Prop. 1999/2000:117, s 16. Ds 2001:13, s 107.
[108] Hultmark, 1998, s 21, 65f. UNCITRAL:s modellag, art 5-7.

måste ingås skriftligen och undertecknas av konsumenten för att villkor som är till nackdel för konsumenten ska gälla.[109]

För att harmonisera med e- handelsdirektivet har därför den svenska lagstiftaren lagt fram ett ändringsförslag avseende 9 § i KkredL. En ändring av KkredL anses nödvändig trots att det endast är de villkor som är till nackdel för konsumenten som omfattas av formkravet. Artikel 9 i e-handelsdirektivet omfatta nämligen även villkor som är till konsumentens nackdel. Den föreslagna lydelsen innebär alltjämt att avtalet skall ingås skriftligen, med ändringen att:

”Avtalet skall … undertecknas av konsumenten eller signeras av denne med en kvalificerad elektronisk signatur” (min understrykning).

Paragrafen innehåller två formkrav, nämligen ”skriftligt” och ”undertecknas”. Undertecknandet kan ske med en kvalificerad elektronisk signatur, medan kravet på skriftlighet inte behöver en kvalificerad signatur för att uppfyllas. Kravet på ”skriftligt” bör därför kunna uppfyllas genom t.ex. ett vanligt avtal som ingås över Internet. Förslaget har dessutom kvar kravet att konsumenten ska få en kopia av avtalet. Med kopia avses inte en kopia som skapats på elektronisk väg utan en traditionell papperskopia.[110]

Förslaget anger att undertecknande kan ske med en kvalificerad elektronisk signatur. Innebära detta att ”endast” en kvalificerad elektronisk signatur kan uppfylla KkredL:s krav på undertecknande? Då lagstiftaren valt att specifikt ange denna typ av signatur, torde inte en icke kvalificerad (enkel) elektronisk signatur innefattas av paragrafen ordalydelse. Situationen hade emellertid varit annorlunda om paragrafen utformats, så att avtalet skall ”undertecknas av konsumenten eller signeras av denne med en för ändamålet säker elektronisk signatur”. En sådan utformning hade till skillnad från det aktuella förslaget öppnat upp för andra signaturer än de kvalificerade, eftersom en ”enkel” elektronisk signatur i flera fall också kan ge en tillfredsställande säkerhet.

Vidare innebär ”valet” av kvalificerade signaturerna att endast s.k. öppna system, avses vid skapande av elektroniska signaturen vid ingående av konsumentkreditavtal. För att skapa en kvalificerad elektronisk signatur måste kraven i LKS uppfyllas. LSK omfattar endast öppna system och därför faller signaturer som skapas i ett slutet system automatiskt utanför LKS och därmed även KkredL. Bankerna på den svenska marknaden har uteslutande använt sig av slutna system, vilket medför att de banker som i fortsättningen vill ingå kreditavtal med sina kunder över Internet, måste anpassa sina system så att de blir öppna, och därmed omfattas av LKS.

[109] Förslag till lag om ändring i konsumentkreditlagen (1992:820).
[110] Ds 2001:13, s 17, 108f, 176.

5.4 Slutsats

I avsnittet har ett antal regler och principer diskuterats som domstolarna har att utgå ifrån när de ska avgöra kommunikationsteknikens rättsliga effekter. Principen om funktionell ekvivalens som kommer i uttryck i UNCITRAL:s modellag är ett exempel på en princip som en domstol kan tänkas tillämpa. Modellagen har nämligen fungerat som förebild för ett flertal nationella och internationella lagstiftningar.

För att avgöra vilka regler eller principer som domstolarna har att tillgå, är även äldre praxis en ändamålsenlig metod för vägledning. NJA 1981:853 utgör ett bra exempel på när en svensk domstol har tittat på regelns syfte istället för dess ordalydelse. Fallet visar också att fastställande av kommunikationsteknikens tillämplighet, inte alltid går att finna i modern praxis eller doktrin. Vägledning bör därför med fördel även sökas i äldre praxis, som är lämplig att tillämpa på den moderna tekniken. Med UNCITRAL:s modellag som förebild är det viktigt för framtidens lagstiftare att skapa rättsregler som är teknikneutrala. Med en sådan utformning kan reglerna förbli intakt trots att kommunikationstekniken ständigt förändras. Dessutom är det ur rättssäkerhetssynpunkt bra om lagstiftningen är någorlunda konstant. E-handelsdirektivet är ett bra exempel på en modern lagstiftning som ser till teknikens utveckling. Här har modellagens inverkan varit tydlig. Direktivet föreskriver nämligen att nationella formkrav som hindrar avtal från att ingås på elektronisk väg ska upphävas eller ändras, med några få undantag. Effekten av e-handelsdirektivet på den svenska lagstiftningen blir emellertid begränsad, då den svenska lagen innehåller få regler som uppställer krav på ”egenhändig underskrift” osv.

E-handelsdirektivet för inte bara med sig att medlemsstaterna tvingas ta bort vissa nationella formkrav utan även ett budskap som verifierar informationsteknikens betydelsefulla rättsfunktion i dagens samhälle. Förhoppningsvis kan därför e-handelsdirektivet bidra till att minska den osäkerhet som råder i medlemsstaternas lagstiftningar, angående de nationella rättsreglernas tillämplighet på informationssamhällets tjänster.

Del ??

6 Fallstudie på Anotopennan

6.1 Inledning

I nedanstående kapitel ska en praktisk studie av företaget Anoto och dess digitala penna (A-pennan) genomföras. Studien har sin utgångspunkt i två fall (fall ? och fall ??). Dessa har direkt anknytning till Anoto produkten och den teknik som denna innefattar. I varje fall kommer ett antal avtalsrättsliga problem som jag anser viktiga för A-pennans framtida användning att analyseras. Tanken är att analysen ska ge svar på de frågor som uppställts för fallen, och därmed minska den rättsliga osäkerhet som finns angående den aktuella tekniken. Kapitlet avslutas med en analys där de traditionella bevisen ställs mot de elektroniska bevisen. Författaren vill med anledning av ämnets komplexitet och osäkra rättsläge starkt understryka att resultatet av studien mer ska ses som kvalificerade antaganden än som precisa fakta. Det material som har använts är främst IT-rättslig doktrin samt traditionell avtalsrättslig doktrin.

6.2 Företagsbeskrivning

6.2.1 Allmänt

Anoto AB grundades i Lund i slutet av 1999 som dotterbolag till C-Technologies AB, noterat på Stockholms Fondbörs O-lista (Attract 40). C-Technologies AB är ett ungt svenskt IT-företag med spetskompetens inom områdena digital kamerateknik, bildbehandling och digitala pennor. Företagets huvudprodukt är läspennan C-Pen, som erhållit flera internationella utmärkelser för bästa IT-produkt. Anoto har en hög expansionstakt och har idag drygt ett hundratal anställda med kontor i Lund, Stockholm, Boston, Tokyo och HongKong. Ericsson är minoritetsägare (30 %) i Anoto och har representation i styrelsen. Anoto tekniken är en kombination av en intelligent penna, ett egenutvecklat mönster, avancerad bildbehandling, Bluetooth-kommunikation och en informationsinfrastruktur. Handskrivna anteckningar lagras, grafiska e-postmeddelanden skickas och elektroniska beställningar görs med hjälp av endast papper och penna. Kommunikation sker med vem som helst som har en mobiltelefon, handdator eller annan PDA (Personal Digital Assistant). Det behövs dock ett speciellt, digitalt papper. Hemligheten ligger i ett mycket svagt mönster, som tryckts på pappret, därför kan det digitala papperet vara vilket vanligt papper som helst. Idén är immateriellt skyddad, vilket även omfattar pennan och flera av dess funktioner och former. Anotos vision är att skapa en global

de facto standard för pappersbaserad kommunikation genom att föra in penna och papper i den digitala världen. Med hjälp av trådlös kommunikation ska information tas direkt från papper genom att överföra handskriven information med vardaglig elektronisk kommunikation från person till person och person till dator. Anoto ska dessutom skapa en infrastruktur för att säkerställa att information med ursprung från A-pennan kommer till rätt mottagare.[111]

6.2.2 Teknisk beskrivning

Här följer en mer ingående tekniks beskrivning av A-pennan och det speciella Anotomönstret (A-mönstret).

Att använda en A-penna skiljer sig inte från att använda en vanlig penna. Pennan både liknar, känns och skriver som en vanlig penna. Det speciella A-mönstret (se fig.2 nedan) utgör basen för A-pennans applikationer. Anoto pappret (där det unika Anotomönstret är tryckt) är ett helt vanligt papper, med ett tryckt mönster. A-mönstret består av små prickar, som är utspridda med ca 0.3 mm mellanrum och bildar tillsammans ett unikt mönster. Detta kan tryckas på vilket vanligt papper som helst eller annat material som tillåter en upplösning på 1000 dpi. Pappret kan även ha vilken form eller design som helst. I A-mönstret kan vissa delar fördefinieras, och kan då direkt uppfattas av pennan (i kombination med serverns behandling). Exempel på information som en mönsterbit kan fördefinieras med är Lagra, Skicka, Att Göra, Adress, osv. Pennan (se fig.3 nedan) består huvudsakligen av tre delar, den digitala kameran, en mikroprocessor och en Bluetooth sändare[112]. Penna innehåller även en vanlig bläckpatron, batteri samt en minnesenhet. Precis vid pennans spets finns kamerans optik och en infraröd LED (Light Emitting Diode). Det infraröda ljuset absorberas av prickarna i A-mönstret, vilket gör mönstret synligt för kameran. Det infraröda ljuset gör att kameran kan läsa mönstret, även om pennan används i ett mörkt rum. Den digitala kameran tar ca 100 foton per sekund av A-mönstret. Mikroprocessorn beräknar sedan i realtid koordinaten, som ger en exakt position i det totala A-mönstret. Dess totala teoretiska storlek motsvarar nämligen Asiens och Europas landyta sammantaget. Under skrivprocessen beräknar även mikroprocessorn, utifrån kamerans foton en mängd andra viktiga data, vilka samlas och lagras. All information som lagrats tidsstämplas med en exakt tidpunkt. Slutligen sänds informationen via Bluetooth teknik (se fig.4 nedan), till en dator där en exakt kopia av den handskrivna informationen skapas. Informationen kan även sändas via en mobiltelefon, PC eller en PDA till Anoto servern. I pennan sker endast en minimal bearbetning av informationen. Den huvudsakliga bearbetningen sker med hjälp av en kraftfull mjukvara i servern. Efter det att servern behandlat informationen sänds aktuell information vidare till avsedd destination.

[111] Se http://www.anoto.com
[112] Möjliggör sladdlös överföring av information

Fig.2

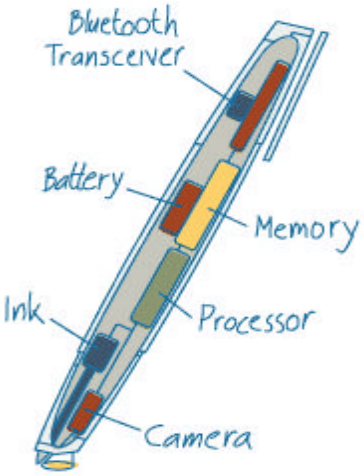


Fig.3

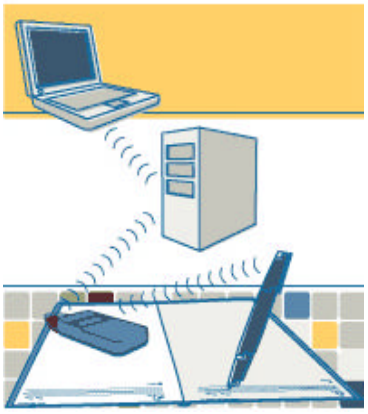


Fig.4

6.3 Fall ?– Hela dokumentet skrivet för hand

6.3.1 Inledning

Under följande avsnitt kommer två avtalssituationer där A-pennan används att behandlas. Typfallen rör huvudsakligen avtalsrättsliga problem som utgår ifrån olika varianter för avtalsbindande kommunikation. De frågor som uppstår kommer i anslutning till varje fall att försöka besvaras.

I det här fallet skriver avsändaren hela dokumentet för hand på ett från början tomt A-mönstrat papper (se fig.2 ovan). Ett exempel på en sådan situation är om Herr x skriver ett brev på ett Anotopapper vilket han signerar elektroniska för att sedan skicka till Fru y. A-pennan fungerar här dels som en vanlig penna där texten fysiskt knyts till pappret och dels digitalt via pennas kamera och processor osv. Vid användandet av en A-penna i dessa situationer skapas därför två original, ett analogt och ett elektroniskt. Vanligtvis behåller avsändaren det fysiska originalet, och mottagaren får det elektroniska originalet sänt till sig. Den elektroniska signaturen som följer med det elektroniska dokumentet signerar inte själva texten utan endast det hashvärde/kondensat som skapats ur texten (se kap 2.1.4). Som tidigare beskrivits skapas en elektronisk signatur genom att hashvärdet krypteras med avsändarens privata nyckel.

Ur bevissynpunkt är det viktigt att i efterhand kunna visa, vem det var som skrev dokumentet, när dokumentet skrevs och vad som signerats. För att påvisa vem som skrev och signerat dokumentet finns det två vägar att gå. Den första är att med hjälp av grafologi tyda den traditionella namnunderskriften på Anotopappret, en annan väg är att konstatera att endast innehavaren av den privata nyckeln kan ha signerat det elektroniska dokumentet. Vem som helst med tillgång till den privata nyckeln kan

signera ett dokument och därmed utge sig att vara den privata nyckelns registrerade innehavare. För att förhindra detta ska aktiveringen av den privata nyckeln skyddas, med exempelvis en PIN-kod. Med A-pennan kommer i framtiden kreditkortens betalningar samt en mängd andra transaktioner sannolikt att kunna utföras, en analogi med utgångspunkt i kreditkortets aktsamhetskrav är därför tänkbar. Vid konstaterande av vad som signeras, skiljer sig också tillvägagångssättet mellan det fysiska respektive det elektroniska dokumentet. Det fysiska dokumentets innehåll bestämmes genom en fysisk granskning av dokumentet, t.ex. för att kontrollera så att inget förvanskats. Medan det elektroniska dokumentets innehåll framgår och kontrolleras automatiskt vid mottagandet (se kap 2.2.4).

Vidare kan tidpunkten när dokumentet skrevs endast konstateras om dokumentet skickas direkt efter det att avsändaren skrivit klar. Denna sker nämligen när dokumentet skickas iväg. Tidsstämpling har som ovan beskrivits en viktig funktion vid bevisvärdering (se kap 3.4.1).

Ovanstående leder vidare in i avsnittets centrala frågeställningar, vilka utgår från två avtalssituationer (avsändare till mottagare):

1. A skriver xy när han avser att skriva xx.
2. A skriver xx och avser att skriva xx, men vid den elektroniska överföringen från analogt till digitalt förvanskas innehållet till xy.

Därmed uppstår frågorna vilket innehåll som är gällande mellan parterna, samt vem som ansvarar för de skador som eventuellt uppkommer?

Kan dessa situationer lösas med hjälp av avtalsrättsliga regler och principer? Eller mer korrekt, är avtalslagen tillämplig på elektroniska avtal? Av 1 § AvtL framgår att lagen inte uppställer några formkrav för ingående av avtal. Den svenska avtalsrätten utgår ifrån, att då det förekommer en viljeförklaring, är det i princip utan betydelse hur denna utförs. Följaktligen är elektroniska avtal giltiga och lika bindande som t.ex. skriftliga avtal.[113] Det subjektiva viljerekvisitet är således grunden för eventuell avtalsrättslig bundenhet. Det kan framstå som självklart att bundenhet inte ska uppstå, när någon av kontrahenterna inte vill eller avsett att bli bunden. Men som nedan kommer att framgå är det inte någon självklarhet. En fråga som skapat diskussion är om det subjektiva viljerekvisitet kan uppfyllas med hjälp av en dator.[114] När väl datorn ”tagit över” sker ju den fortsatta dispositionen automatiskt. Ett elektroniskt meddelande ingår ofta i en komplicerad process som parterna inte har full kontroll över, såsom kryptering, lagring, konvertering osv. Det har inom doktrinen framförts flera olika teorier för avtalsrättlig bundenhet vid elektronisk kommunikation. Det har bl.a.

[113] Janson Ingemar, Den elektroniska marknadsplatsen, Avtals-, köp- och bevisrättsliga aspekter, 1997, s 38f. Hultmark, 1998, s 23.
[114] SOU 1996:40, s 121f, 129ff. Lindberg, Westman, s 56. Janson, s 43ff. Hultmark, 1998, s 27.

framförts att istället för att diskutera om hypotetiska eller fingerade viljeförklaringar där en klar subjektiv vilja saknas, ska bundenhet uppkomma som ett resultat av flera yttre omständigheter. Dessa yttre omständigheter leder i kombination fram till avsedd åtgärd, och avtalsbundenhet är därför motiverad. Det är här frågan om situationer där de praktiska behoven tvingar fram avtalsbindningar, trots att inte någon viljeförklaring i strikt mening existerar. En annan teori är att bundenhet uppkommer utifrån partens hypotetiska vilja om att datorn ska utföra handlingarna på ett visst sätt. Detta förutsätter att det elektroniska meddelandet har sin utgångspunkt i en viljeförklaring. Till exempel när en person har programmerat en dator att agera på ett vist sätt, anses detta indirekt vara uttryck för dennes vilja.[115]

Hultmark framför en något annorlunda tanke som bygger på att anlägga en fullmaktsfunktion som baseras på informationssystemet skilda delar. Informationssystemet ses som en ”teknisk fullmäktig”. Syftet med fullmaktskonstruktionen är att huvudmannen, brukaren av IT – systemet, därmed skulle befrias från ansvar när hans system ofrivilligt, avger felaktig information som mottagaren fäst tilltro till. Denna teori konstateras dock av författaren som onödigt komplicerad. Teorin är dessutom inte särskilt realistisk eftersom ett IT system inte är något sättssubjekt som kan uppbära rättigheter eller skyldigheter.[116]

6.3.2 Avtalssituation 1

6.3.2.1 Problemområde

Avtalssituation 1 kan tillämpas, om en person som använder en A-penna avser att skriva 10 enheter, men felaktigt råkar skriva 100 enheter. Här uppstår ett problem, är avsändaren bunden vid sin felskrivning eller ska endast det som avsändaren avsåg att skriva (10 enheter) gälla? Felet uppstår uteslutande p.g.a. den mänskliga faktorn. Praktiskt uppstår ett problem, om mottagaren redan före eventuellt påpekande från avsändaren förlitat sig på meddelandet och vidtagit åtgärder. Här aktualiseras 32 § 1st AvtL om förklaringsmisstag. Regeln baseras på tillitsteorin, som innebär att den tillit som förklaringen givit upphov till hos mottagaren ska vara avtalsgrundande. Avsändarens verkliga vilja är därför inte avgörande, om mottagaren har goda grunder för att tro att innehållet är ett uttryck för avsändarens vilja. Tillitsteorin konstruerades för att skapa skydd åt affärslivet och därmed öka omsättningsintresset. I 32 § 1st AvtL stadgas att avsändaren av en viljeförklaring som på grund av felskrivning eller annat misstag å hans sida fått annat innehåll än åsyftat, inte är bunden av viljeförklaringens innehåll om mottagaren insåg eller bort inse misstaget. Paragrafen är avsedd att tolkas e contrario (motsatsvis). När mottagaren är i god tro och inte insåg eller bort inse förklaringsmisstaget, blir avsändaren bunden vid innehållet. Följaktligen blir avsändaren inte bunden vid sin viljeförklaring, om

[115] SOU 1996:40, s 121f, 129ff. Lindberg, Westman, s 56. Janson, s 43ff.
[116] Hultmark, 1998, s 27.

mottagaren är i ond tro angående innehållet.[117] Paragrafen omfattar inte bara felskrivningar, även felsägningar och felräkningar bedöms som förklaringsmisstag. Misstag enligt paragrafens 1st omfattar även situationer då en rättshandlande visserligen avgivit avsett innehåll, men misstagit sig angående dess innebörd, s.k. *error in motivis*.[118] Avsändaren kan exempelvis ha givit ett meddelande innehållet xx och trott att de innebar aa, då det i själva verket innebar yy. Han/hon kan t.ex. ha misstagit sig om betydelsen av någon säregen fackterm.

Vid avgörande av rättsföljden måste hänsyn tas till samtliga omständigheter som har haft betydelse för den verkliga respektive uppfattade innebörden av innehållet. Rätten har alltså att utgå ifrån det ”objektiva innehållet”, dvs. vad mottagaren med fog läst in i viljeförklaringen. Rätten ska utgå från den innebörd som mottagarens (subjektiva) goda tro lägger i avsändarens viljeförklaring, och inte vad avsändaren avsett. Vid ett rättsligt avgörande kommer dock inte vilken god tro som helst att accepteras. Rätten måste anse att god tro rimligen kunde ha förelegat. Här kan två rättsfall där Högsta domstolen (HD) tillämpade 32 § 1st AvtL, förtydliga rekvisitet ”insåg eller bort inse”, alltså i vilka fall som ond respektive god tro har ansetts föreligga.[119]

I NJA 1986:495 fick två makar ett avtalsförslag av kommunen angående höjning av tomträttsavgälderna, sänt till sig för undertecknande. Men makarna ansåg att den förslagna höjningen var för hög, och tog bort det föreslagna beloppet och skrev in ett ”eget” belopp, som var hälften så stort. Intill det egna beloppet skrev de inom parantes ”eget förslag”, och skickade det till kommunen för handläggning. Kommunen undertecknade handlingen utan granskning. Frågan för rätten var om kommunen var bunden vid sitt misstag. HD tillämpade AvtL 32 § 1st och frågade sig om makarna kunde vara i god tro angående kommunens undertecknande. Kommunen ansågs inte bunden vid det undertecknade beloppet, eftersom makarna bort inse att kommunen inte helt utan vidare kunde gå med på en halvering av avgiften, som tidigare fastställts genom ett kommunfullmäktige beslut.

I NJA 1991:3 hade en elleverantör under flera år fakturerat en kund en för låg avgift, eftersom kundens elmätare endast kunde ange femsiffriga tal. Avgörande blev om kunden hade insett eller bort inse att elräkningarna var felaktiga. HD ansåg inte att någon undersökningsplikt åvilade kunden som därför med fog hade trott att betalningarna fungerade som slutlig reglering av mellanhavandena. I fallet ansågs inte kravet för ond tro vara uppfyllt, då kravet på insikt sattes tämligen högt av HD.

Rättsföljden resultera inte bara i giltighet eller ogiltighet enligt 32 § 1st AvtL. Paragrafen formulerar nämligen till skillnad från de övriga ogiltighetsreglerna i AvtL rättshandlingen som ”icke bunden vid

[117] Grönfors Gurt, Avtalslagen, 1995, s 198f. Einersen Eivind, Elektronisk aftale- & bevisret, 1992, s 32f.
[118] Grönfors, s 198.
[119] Adlercreutz Axel, Avtalsrätt ?, 2000, s 257ff.

viljeförklaringen", när mottagaren är i ond tro. Övriga ogiltighetsregler i AvtL formulerar rättsföljden, som "icke gällande", vid ond tro hos mottagaren. Formuleringen i 32 § 1st AvtL innebär därför inte automatiskt ogiltighet när mottagaren är i ond tro, utan innehållet kan av rätten omtydas till det från början avsedda (10 enheter).[120] Bevisbördan ligger på avsändaren som för ogiltighet eller omtydning måste visa på bristande överensstämmelse mellan viljeförklaringens innehåll och vad denne verkligen avsett, och att mottagaren insett eller bort inse detta.[121]

En lösning som föreslagits istället för bundenhet, är ett ersättningsansvar för avsändaren för den skada som mottagaren lidit. En sådan lösning motverkar att avsändaren till varje pris måste hänga kvar vid sin felskrivning. Grönfors anser att ett skadestånd till det negativa kontraktsintresset är befogat. Ersättning intill det negativa kontraktsintresset, innebär att den förfördelade ska försättas i samma situation som gällde före den felaktiga kommunikationen.[122] Mottagarens intresse skyddas därmed till den grad hans tillit till meddelandet orsakat honom skada. I vissa situationer kan emellertid ersättning till det negativa kontraktsintresset vara otillräckligt. Mottagaren kan ju ha avstått från att göra andra lukrativa affärer osv. Men sådana förluster är oftast svåra att föra bevisning om. Därför anser Hultmark likt Grönfors att en rimlig medelväg om bundenhet inträffat, är ett ersättningsansvar till det negativa kontraktsintresset.[123]

6.3.3.2 Slutsats

Ovanstående resonemang leder fram till följande slutsats avseende situation 1 ovan. När någon med en A-penna felaktigt råkar skriva 100 enheter och egentligen avsett att skriva 10 enheter, är utgångsläget att konstatera om mottagaren, insett eller bort inse misstaget. Avsändaren måste dock visa att innehållet och hans vilja inte harmoniserar, för att ett insiktsresonemang överhuvudtaget ska aktualiseras. Har parterna haft kontakt tidigare eller är det första gången de gör affärer med varandra? Samtliga omständigheter är viktiga för att konstatera vad mottparten med fog bör ha insett. 32 § 1st AvtL är som ovan konstaterats utformad för att skydda den godtroende mottagaren. Om situationen är sådan att mottagaren bort inse felskrivningen är det upp till rätten att utifrån de aktuella omständigheterna avgöra rättsföljden. Rättsföljden kan om mottagaren var i ond tro, endera bli ogiltighet eller att viljeförklaringens ursprungliga avsikt ska gälla (10 enheter). Huvudregeln är emellertid att avsändaren är bunden vid sin felskrivning när mottagaren är i god tro (100 enheter). Om rätten anser att bundenhet blir för långtgående, är ersättningsskyldighet enligt ovan också en möjlig lösning.

[120] Grönfors, s199.
[121] Einersen, s 113f. Adlercreutz, 2000, s 259.
[122] Martinger Sven, Norstedts Juridiska Ordbok, Juridik från A till Ö. 1989.
[123] Grönfors, 198f, Hultmark, 1998, s 32f.

6.3.3 Avtalssituation 2

6.3.3.1 Problemområde

Till skillnad från ovanstående situationen så rör det sig här inte om någon mänsklig felskrivning, utan om fel som uppstår i den digitala överföringen. Det kan tänkas att en användare med A-pennan skriver 10 enheter, men vid den elektroniska överföringen förvanskas innehållet till 100 enheter. Vilket innehåll gäller mellan parterna, och vem står risken för de skador som eventuellt uppkommer? Intressant är också var förvanskningen uppstår:

- I pennan eller vid överföringen från pennan?
- Går inte att fastsälla, (”någonstans i cyberspace”)
- I mottagarens system?

Först ska undersökas om AvtL överhuvudtaget är tillämplig på dessa situationer. Den regel som framkallat en omfattande diskussion inom doktrinen är 32 § 2st AvtL som reglerar s.k. befordringsfel. Enligt 32 § 2st AvtL är en viljeförklaring som befordrats genom telegram eller framföres muntligen genom bud, och innehållet till följd av fel vid telegraferingen eller oriktigt återgivande genom budet blivit förvanskad, avsändaren trots att mottagaren var i god tro inte bunden till det felaktiga innehållet. Avsändaren måste dock meddela mottagaren inom skälig tid om förvanskningen. Underlåter avsändaren detta och mottagare var i god tro gäller viljeförklaringen sådan som den framkommit. I motsats till paragrafens 1st som skyddar mottagaren, så skyddar paragrafens 2st avsändaren. Grönfors anser att regeln är ”överraskande”, eftersom tillitsprincipen här frångås trots att lagstiftaren uttalat en strävan efter att i omsättningens intresse skydda godtroende mottagare. Vad det gäller regelns tillämplighet på meddelanden som skickats elektroniskt, anser föregående att en analogi som jämställer elektronisk post med telegrafering eller bud, helt saknar juridisk grund. Paragrafen anses inte tillämplig eftersom parterna vid elektronisk överföring kommer i ”direkt kontakt” med varandra, vilket de inte gör när en telegrafist eller ett bud kommer i mellan.[124]

Enligt Grönfors ska därför något förvånande befordringsfel som sker vid elektronisk överföring följa paragrafens 1st, som innebär att avsändaren blir bunden vid ett felaktigt innehåll om mottagaren är i god tro. Men enligt SOU 1996:40 och min bestämda uppfattning är 32 § 1st AvtL inte tillämplig i dessa situationer, då 1st inte kan tillämpas när ett elektroniskt meddelande som vid avsändandet var korrekt, först vid överföringen förvanskats.[125]

[124] Grönfors, s 200f.
[125] SOU 1996:40, s133f. Grönfors, s 202.

Alla är emellertid inte övertygade om att AvtL inte är tillämplig på elektronisk överföring. Det har bl.a. framförts kritik mot Grönfors resonemang om ”direkt kontakt”. Einersen menar att parterna vid elektronisk överföring oftast inte har någon sådan direktkontakt. Vidare anser denne inte att skillnaden är så stor mellan telegrafering och elektronisk kommunikation att en analogi ska uteslutas. Einersen tycker att det är:

”kunstigt at sondre mellen situationerna, hvor fejlene opstår ved kommunikation med en tredjepart (telegrafisten eller budet)[126] *eller ved kommunikation med medkontrahenten selv. Det relevanta bør være, at fejlen opstår under kommunikationen, og at den følgelig ikke skyldes afsenderen”.*[127]

Resonemanget är tilltalande, men fortfarande kvarstår ett tungt vägande skäl mot en tillämpning av 2st och det är tillitsteorins företräde framför viljeteorin. Diskussionen är emellertid inte helt relevant eftersom AvtL 32 § 2st fortfarande är utformad likt viljeteorin och frågan endast är om elektronisk kommunikation omfattas av 2st eller inte. Däremot kan följden om elektronisk kommunikation omfattas av regeln, bli att lagstiftarens eftersträvade omsättningsintresse får en negativ utveckling.

Istället för att tillämpa 32 § 2st AvtL har det framförts, att en omformulering av 40 § i samma lag bör göras. I paragrafen frångås vissa typer av meddelanden huvudregeln och går istället på mottagarens risk. När det föreskrivits en skyldighet att skicka ett meddelande i mottagarens intresse och om detta har avsänts på ett ändamålsenligt sätt, står mottagaren risken för meddelandet. Ett exempel på ett meddelande som sker i mottagarens intresse är en upplysning om att en accept kommit fram för sent. Paragrafen omfattar meddelanden befordrade med post eller ”eljest på ändamålsenligt sätt”. Det senare innebära att paragrafens allmänna principer även kan omfatta elektroniska meddelanden. I enlighet med ovanstående resonemang föreslås i SOU 1996:40 en ändring av 40 § AvtL. Förslaget har inspirerats av 82 § köplagen (KöpL), som även omfattar förvanskning av meddelanden. I SOU 1996:40 förordas därför ett tillägg till 40 § AvtL, som innebär att paragrafen får motsvarande utformning som 82 § KöpL och därmed även omfatta förvanskningar. Den föreslagna paragrafen ska tolkas e contrario. Resultatet blir att avsändaren bär risken för de meddelanden som inte omfattas av paragrafen, enligt principen i 32 § 1st AvtL.[128]

Mot bakgrund av ovanstående diskussion, anser jag att ett innehåll som förvanskats vid en elektronisk överföring, inte ska omfattas av AvtL nuvarande lydelse. Eftersom det råder osäkerhet i svensk rätt om tillämpliga regler eller principer, finns det anledning att beakta internationella lösningar.[129]

---

[126] Min text i parentesen.
[127] Einersen, s 71-72.
[128] SOU 1996:40, 134. Adlercreutz, 2000, s 263. Hultmark, 1998, s 56f.
[129] Hultmark, 1998, s 58.

En för situationen intressant regel är art 13 i UNCITRAL:s modellag. Den omfattar situationer, då elektroniska meddelanden förvanskats vid elektronisk överföringen, s.k. befordringsfel. Artikeln presumerar att den som väljer att utnyttja ett programmerat system för att skicka elektroniska meddelanden, ska bära risken för att meddelandena förvanskas under överföringen. Dock svarar inte avsändaren för felaktiga meddelanden som orsakats av något annat än programmeringen, t.ex. ett hackerangrepp. Avsändaren svara alltså enligt UNCITRAL art 13 (5) för eventuella förvanskningar i meddelandet när mottagaren är i god tro:

"… the addressee is entitled to regard the data message as received as being what the originator intended, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received."

Regeln bygger på en tanke som påminner om den svenska tillitsteorin, som bekant kommer till uttryck i 32 § 1st AvtL. Mottagarens subjektiva rekvisit i art 13 har också en motsvarande utformning i 32 § 1st AvtL, eftersom god tro anses föreligga om mottagaren inte insåg eller bort inse felaktigheten. Art 13 reglerar emellertid inte avtalsbundenhet. Följden blir istället att avsändaren blir ersättningsskyldig för de åtgärder som mottagaren vidtagit med hänsyn till det förvanskade meddelandet (se resonemang ovan angående ersättningsskyldighet för det negativa kontraktsintresset). [130]

Problemet med befordringsfel kan möjligtvis bedömas ur fler aspekter. I vissa situationer kan det nämligen vara intressant att avgör var i själva överföringen felet uppstått. Om det är möjligt att konstatera att felet inträffat i mottagarens system, och denne haft möjlighet att motverka felet, ska då avsändaren likväl stå risken för de fel som kan uppstå? Mottagaren kanske inte har uppgraderat sitt system enligt vedertagen standard. Om detta kan anses vara en avgörande och grundläggande åtgärd, och mottagaren bort inse de följder som kan uppstå vid en utebliven uppgradering. Torde en ansvarsövergång på mottagaren vara ändamålsenlig. Med tanke på den svårighet och den osäkerhet som detta kan medföra i rättstillämpningen, ska endast klara fall föranleda en rättslig avvikelse från modellagens presumtion. Vad det gäller fel som uppstår i A-pennan, kan dessa aldrig ske på mottagarens risk. Avsändaren presumeras här, svara för eventuella fel som föranlett en godtroende medkontrahent att handla. Mottagaren har ju i dessa situationer ingen möjlighet att avvärja eller förutse felet. Vanligast är nog att felen uppstår i ”cyberspace” (inte går att härleda till något speciellt led i överföringen) och att ovanstående alternativa lösningar inte blir användbara. När felet uppstår i ”cyberspace” bör därför modellagens presumtion tillämpas.

En viktig fråga är om någon annan än avsändaren och mottagaren kan bli ansvarig för eventuell befordringsfel? Med utgångspunkt i LKS som

[130] Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996), p 83ff.

föreskriver ett ansvar för de CA som utfärdar certifikat kan en bestämd inställning hos lagstiftaren skådas. Syftet med LKS är att skapa en tillförlitlighet i användandet av elektroniska signaturer. Bl.a. agerar certifikatutfärdarna som garanter för de certifikat som de utfärdat. Lagstiftningen har med de elektroniska signaturerna velat skapa en bas för en ökad tillit till elektroniska transaktioner över Internet. En följdfråga som mot bakgrund av detta är relevant, är om inte tillverkare av utrustning för framställande av elektroniska signaturer, ska ansvara för fel som dessa produkter eller program förorsakar? De skador som kan tänkas uppkomma vid användningen av dessa är främst förmögenhetsskador. Användare och tillverkaren kommer troligtvis även att står i ett utomobligatoriskt förhållande till varandra. För att en sådan s.k. ren förmögenhetsskada ska ersättas enligt svensk skadeståndsrätt krävs att skadan vållats genom brott.[131] Det finns emellertid exempel i praxis där undantag från huvudregeln i 2:4 SkL har skett.[132] I NJA 1987:692 hade en värderingsmannen lämnat felaktiga och vilseledande uppgifter beträffande ett faktiskt förhållande (värderingsintyg för fast egendom). Enligt HD var detta ett klart fall av oaktsamhet, då det inte vore speciellt svårt för värderingsmannen att verkligen verifiera uppgifternas riktighet. Oavsett vem som är uppdragsgivare måste det enligt HD stå klart att annan än uppdragsgivaren kan tänkas förlita sig på ett sådant intyg. Den som med fog satt sin tillit till ett värderingsintyg ska inte behöva stå för skada orsakad av intygsgivarens oaktsamhet. Övervägande skäl talade därför enligt HD för att värderingsmannen, i avsaknad av ansvarsförbehåll, ansvar för lämnade uppgifter även gentemot tredje man. Värderingsmannen dömdes att ersätta tredje man.[133] Diskussionen framstår kanske som något djärv, men syftar endast till att belysa tänkbara lösningar. Ett alternativ vore att tillverkarna svarade för de överföringsfel som deras produkter orsakat. Tillverkarna har större möjlighet att förutse antalet fel som kan uppkomma på x antal sålda produkter, än vad en vanlig användare har möjlighet till. Tillverkaren kan i sin tur försäkra sig mot eventuella ersättningsanspråk. De försäkringspremier som tillverkarna drar på sig, kan de sedan kompenserar genom prishöjningar. Detta leder till att användarna i slutändan betalar för säkerheten i systemet. En sådan lösning är tilltalande eftersom varje enskild användare slipper försäkra sig mot eventuella befordringsfel. Resultatet blir att en ”generell försäkring” kommer att gälla för de befordringsfel som orsakats av produkter, vars tillverkare försäkrat sig mot ersättningsskyldighet.

6.3.3.2 Slutsats

Avtalssituation 2 bör ge följande resultat. Först kan konstateras att AvtL inte är direkt tillämplig på situationer då en viljeförklaring förvanskats under elektronisk överföring. En domstol som ska behandla dessa situationer måste därför finna andra lösningar. En utblick efter internationella lösningar

[131] 2:4 skadeståndslagen (SkL)
[132] Linberg, Westman, s 80f.
[133] NJA 1987:692

anser jag vara lämplig. Rätten bör undersöka om det finns några internationella bestämmelser eller principer som kan vara vägledande för det aktuella fallet. UNCITRAL:s modellag reglerar i art 13 befordringsfel som orsakas vid elektronisk överföring. Enligt art 13 sker överföringen av elektroniska meddelanden på avsändarens risk, vilket innebär att en godtroende mottagare skyddas. Regeln bör inte var svår för en svensk domstol att tillämpa, eftersom den överrensstämmer med den avtalsrättliga huvudregeln att en godtroende medkontrahent ska skyddas. Följden blir att den som använder en A-penna, står risken för de fel som kan uppstå vid överföringen, om mottagaren är i god tro avseende innehållets riktighet. Likt avtalssituation 1 ovan, bör även ersättning intill det negativa kontraktsintresset i vissa fall kunna utdömas istället för bundenhet.

6.4 Fall ??– Delar av dokumentet innehåller förtryckt text

6.4.1 Inledning

Följande fall skiljer sig från de ovanstående, eftersom de aktuella dokumenten innehåller både förtryckt (analog och digital) text, samt möjlighet att skriva text med A-pennan (se fig.5 nedan).

Det är viktigt att förstå hur dessa dokument tekniskt är uppbyggda. Något förenklat kan det förklaras som att det speciella A-mönstret trycks på ett papper. Delar av mönstret har bestämts motsvara ett specifikt innehåll t.ex. en särskild avtalssort. Detta medför att ett vanligt papper som försetts med ett fördefinierat A-mönster även kan innehålla en vanlig tryckt text. Den vanliga texten (synlig text) trycks alltså på samma papper som det mönster till vilket den digitala texten är knuten. Delar av pappret kan därtill vara avsedda för fritext med en A-penna. Resultatet blir att ett vanligt papper t.ex. ett köpeavtal kan ha ett osynligt digitalt mönster och ett analogt mönster som synlig text, samt en text som skrivits för hand med en A-penna som både är analogt och digitalt. Dessa dokument signeras genom att en unik mönsterbit signeras. Mönsterbiten ska representera det dokument som vederbörande vill signera. När underskriften sker på den speciella mönsterbiten som därmed signeras digitalt, signeras även dokumentet (t.ex. ett köpeavtal) till vilket mönsterbiten är associerad.[134] Det analoga och det digitala mönstret måste ha exakt samma innehåll. Om dessa inte har exakt samma innehåll, kommer avsändaren inte att veta vad han signerat.

Ovanstående leder vidare in i avsnittets centrala frågeställningar, vilka utgår från två avtalssituationer (avsändare till mottagare):

1. A tror sig signera ett avtal (inte framtaget av någon av parterna) med innehållet x (synligt för A), men signerar digitalt xx (inte synligt för A).

[134] Anoto dokument, Se not 29.

2. A tror sig signerar ett avtal (distribuerat och framtaget av ett företaget som beställningsunderlag) med innehållet x (synligt för A), men signerar digitalt innehållet xx (inte synligt för A)

I avtalssituationerna används en A-penna och ett A-mönstrat papper. Vilket innehåll gäller mellan parterna, och vem står risken för de skador som eventuellt uppkommer?

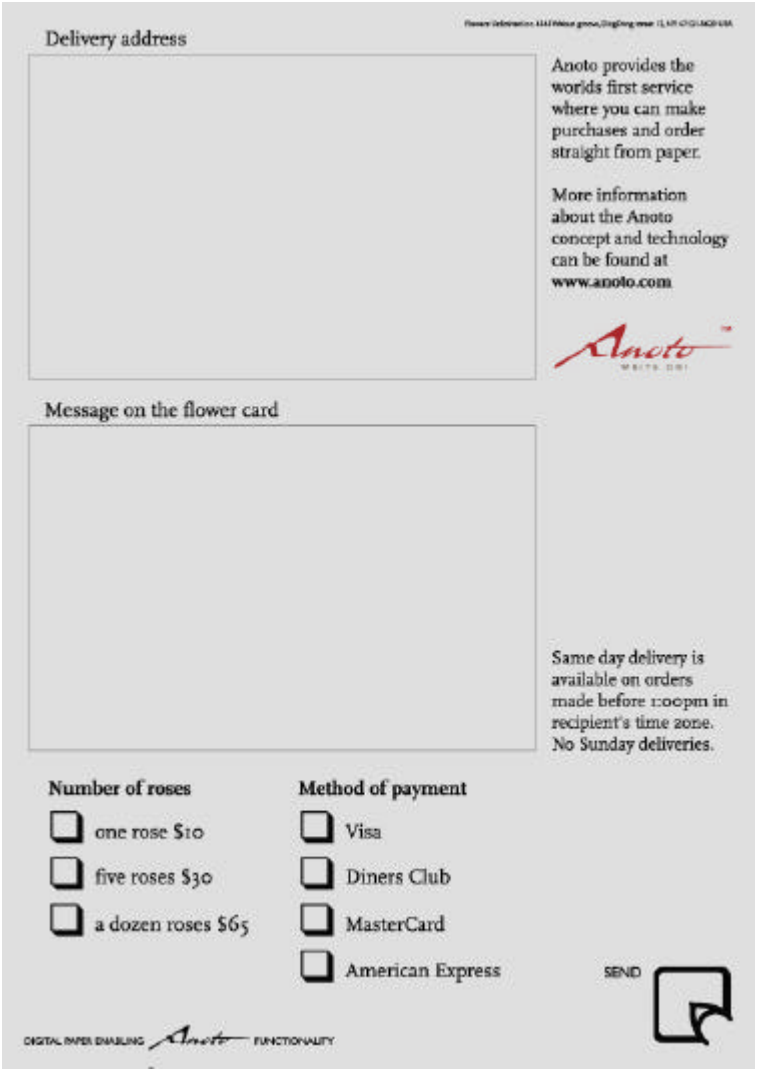


Fig.5

6.4.2 Avtalssituation 1

6.4.2.1 Problemområde

En praktisk situation kan vara följande: herr x avser att skriva under ett hyresavtal med en uppsägningsfrist på tre månader. Av hyresavtalet som herr x skriver under med sin A-penna framgår det tydligt att uppsägningsfristen är tre månader. Men i det digitala mönstret (osynligt för

herr x) som är det innehåll som mottagaren får synliggjort för sig, är uppsägningsfristen endast en månad. Felet som därmed har uppstått har inte uppkommit under överföringen, utan har orsakats genom att den speciella mönsterbiten associerat till fel dokument och innehåll.

Här uppstår flera tydliga problem. Är herr x bunden vid ett innehåll som han varken hade vetskap om, eller hade för avsikt att binda sig vid? Eller ska en mottagaren som vidtagit dispositioner utifrån ett innehåll som han mottagit i god tro inte gälla? Är det skillnad om det analoga och digitala har vitt skilda innehåll och innebörd eller om de rör samma område, men med olika innehåll. Till exempel är innehållet i exemplet ovan olika, men rör samma område, hyresavtal. Men om herr x tror sig skriva under ett hyresavtal, men skriver digitalt under ett avtal där han förbinder sig att köpa den aktuella fastigheten! Kan verkligen en avsändare bli bundet vid ett innehåll som är så främmande från vad den tryckta texten innehåller?

Trots olikheten mellan fall ? ovan och fall ??, kan tekniken för att lösa de rättsliga problem som kan uppstå, ha stora likheter. För att lösa ovanstående situation bör först ”felet” rättsligt definieras. Kan de fel som uppstår då den speciella mönsterbiten inte överrensstämmer med den synliga texten, definieras som förklaringsmisstag eller som befordringsfel? Förklaringsmisstag kan aldrig komma på tal, eftersom avsändaren inte har gjort något fel. Situationen skulle möjligen definieras som felskrivning enligt 32 § 1st AvtL om avsändaren skrivit under fel mönsterbit, och avsåg att skriva under en annan mönsterbit (som representerar avsett innehåll). Detta är dock inte speciellt realistiskt eftersom vederbörande rimligtvis bör kontrollera den synliga texten och dokumentet före undertecknandet. Kan situationen istället definieras som befordringsfel? Mot bakgrund av vad befordringsfel innebär bör den aktuella situationen inte omfattas av begreppet. Felet ska ju uppstå under befordringen eller överföringen. De fel som uppkommer då mönsterbiten associerat till fel innehåll uppstår inte under någon överföring, utan existerar redan före avsändandet. En feldefinition av en mönsterbit sker i ett tidigare stadium, troligtvis vid skapandet av de speciella A-mönstrade dokumenten.

En regel som möjligtvis kan fungera som vägledning är än en gång modellagens art 13, som behandlades ovan under fall ? avtalssituation 2. Enligt art 13 ska som ovan beskrivits, den som använder sig av ett programmerat system, själv stå risken för de fel som kan uppstå. De fel som uppstår kan ju ha orsakats genom fel i programmeringen osv. Enligt artikeln bär alltså avsändaren risken för de fel som uppstår när mottagaren är i god tro. Frågan är om den aktuella situationen omfattas av artikeln när felet på mönsterbiten har uppstått vid skapandet av Anoto dokumentet och inte vid överföringen? Med tanke på syftet med art 13 torde en tillämpning av regeln på en situation med feldefinierad mönsterbit, vara möjlig. Modellagen förespråkar som bekant funktionell ekvivalens, vilket innebär att ändamålet med en aktuell regel ska vara vägledande för dess tillämplighet. För artikelns tillämpning bör det inte enbart fokuseras på den specifika situation eller på vilket sätt som felet uppstått. Avgörande ska vara om ändamålet

med regeln uppfylls eller inte i den aktuella situationen. Min uppfattning är att art 13 kan tillämpas på ett fall med en feldefinierad mönsterbit. Som tidigare nämnt överensstämmer art 13 med den svenska tillitsprincipen, vilket torde förstärka teorin.

Resultatet blir likt ovan att avsändaren svarar för eventuella fel, om mottagaren var i god tro angående innehållet. Emellertid lär de situationer då en avsändare blir bunden vid ett icke avsett innehåll, i praktiken vara ovanliga. Som tidigare omtalat, ska mottagaren vara i god tro för att avsändaren ska bli bunden. Detta innebär att mottagaren varken ska ha insett eller bort inse felet. De fel som uppkommer vid en feldefinierad mönsterbit behöver ju inte vara av samma slag eller ens i närheten av vad avsändaren trott sig skicka iväg. I de flesta avtalssituationer har avtalsparterna någon typ av kontakt med varandra före avtalsingåendet. När en avsändare t.ex. tror sig sända ett avtal angående en hyresrätt, men i själva verket skickar ett helt annat kontrakt, bör mottagaren vanligtvis inse att något inte står rätt till. En medkontrahent bör därför ytterst sällan anses vara i god tro beträffande ett meddelande som är helt främmande för avsändaren.

Ett resultat där avsändaren får stå för risken för eventuella fel, utan hänsyn till vederbörandes möjlighet till kontroll eller upptäckt av felet, är inte bra. En idé vore att med teknikens hjälp försöka införa funktioner som ökar parternas aktivitetsgrad vid avsändande och mottagande. Om parterna ges fler moment där meddelandets riktighet kan kontrolleras, ökar automatiskt underlaget för bedömning av respektive parts insikt, avsikt osv. Med fler parametrar kan domstolen göra en mer rättvis och korrekt bedömning. Ett system baserat på bekräftelse är ett alternativ. Ett sådant system skulle kunna baseras på interaktivitet med en mobiltelefon, PC eller liknande. Till exempel kan avsändaren får en bekräftelse sänd till sig, som verifierar att det elektroniska innehållet överensstämmer med det fysiska. Om avsändaren konstaterar att bekräftelsen stämmer ska det analoga och det elektroniska innehållet vara identiskt. För att ett system med bekräftelse verkligen ska fylla sin funktion bör även mottagarens aktivitet innefattas i systemet. Med en aktivitetsplikt på mottagaren får rekvisitet ”insåg eller bort inse” en modifierad innebörd, eftersom ansvarsfördelningen i flera fall kan förändras och risken för felaktigt innehåll flyttas över på mottagaren. En mottagare skulle därför inte kunna utföra någon handling med avseende på mottaget meddelande och åberopa god tro, förrän aktivitetsplikten är utförd. Aktivitetsplikten får inte vara för betungande, då den moderna kommunikationsteknikens fördel just är dess enkelhet.

6.4.2.2 Slutsats

Först kan konstateras att ovanstående fall är något mer komplicerat än de övriga som analyserats.

Resultatet för avtalssituation 1 skiljer sig inte nämnvärt från fall ? och avtalssituation 2 ovan. Vid användande av A-pennan i kombination med ett ”fördefinierat” A-papper kan fel uppstå. Felen uppstår när de fördefinierade

mönsterbitarna inte motsvarar det för avsändaren synliga innehållet. På aktuell situation är varken 32 § 1st AvtL om förklaringsmisstag eller paragrafens 2st om befordringsfel tillämpbara. Däremot bör mot bakgrund av principen om funktionell ekvivalens UNCITRAL:s art 13 kunna tillämpas. Som tidigare nämnts blir resultatet av denna regel, att avsändaren står för eventuella fel i meddelandet som godtroende mottagare förlitat sig på. Men beroende på felets avvikelse från vad avsändaren trott sig signera, bör kraven på mottagarens insikt variera. Ett meddelande som till innehåll och syfte skiljer sig markant från vad parterna före avslutet diskuterat, bör endast i undantagsfall leda till bundenhet för avsändaren. En teknisk uppbyggnad med någon form av bekräftelse eller aktivitetsplikt för medkontrahenterna är eftersträvansvärd. Ett sådant system är speciellt motiverat, eftersom avsändaren inte har någon möjlighet att avvärja eller upptäcka fel, när en mönsterbit är feldefinierad.

Oavsett om ett system med bekräftelse eller aktivitetsplikt används, ska den primära ansvarsfördelningen utgå ifrån tillitsprincipen och modellagens art 13. Huvudregeln är därför att avsändaren står risken enligt tillitsprincipen. Ersättning till den förlitande parten kan också bli aktuellt som alternativ till bundenhet.

6.4.3 Avtalssituation 2

6.4.3.1 Problemområde

I de fall ett företag erbjuder sina kunder att använda det speciella A-pappret för kontakt med företaget (se fig. 6 nedan), är situationen annorlunda. Seriösa företag kommer troligtvis, automatiskt svara för de fel som deras dokument orsakar. Affärskommunikation av det här slaget kommer företrädesvis att uppstå mellan näringsidkare och konsument. I de fall företaget inte tar sitt ansvar, bör ett rättsligt avgörande likväl utfalla till konsumentens fördel. En näringsidkare bör rimligtvis ansvara, för de fel som deras eget ”orderpapper” har orsakat. Här kan avtalsrättens anbud och accept modell användas för att belysa situationen. Kan företagets orderpapper ses som ett anbud, som konsumenten sedan kan välja att acceptera? Om konsumenten väljer att acceptera anbudet, blir konsumenten bunden vid anbudets innehåll. Samtidigt blir företaget bundet vid avgivet anbud (det synliga innehållet och inget annat). Men kan verkligen företagets orderpapper ses som ett anbud? Antagligen inte, eftersom en förutsättning för att ett erbjudande ska vara bindande som anbud är att mottagarekretsen är tämligen bestämd. Om företagets orderpapper skickas ut (massutskick) eller görs tillgängligt (t.ex. i olika restauranger) för en stor och obestämd grupp av kunder kan orderpappret inte anses utgöra ett bindande anbud. Orderpappret kan däremot ses en uppfordran till att avge anbud, ett s.k. utbud. Med utbud betecknas erbjudanden som tekniskt inte är anbud och därför inte bindande för avgivaren. Utbuden karakteriseras av att de är mindre precisa erbjudanden i form av annonser, skyltning, massutskick

osv.[135] Trots att utbudet inte är direkt bindande för avgivaren, spelar det en viktig roll som tolkningsdata för att avgöra vad parterna, avsett respektive trott sig ingå. Allt som kan antas ha påverkat parterna är viktigt vid fastställande av ansvarsfördelning

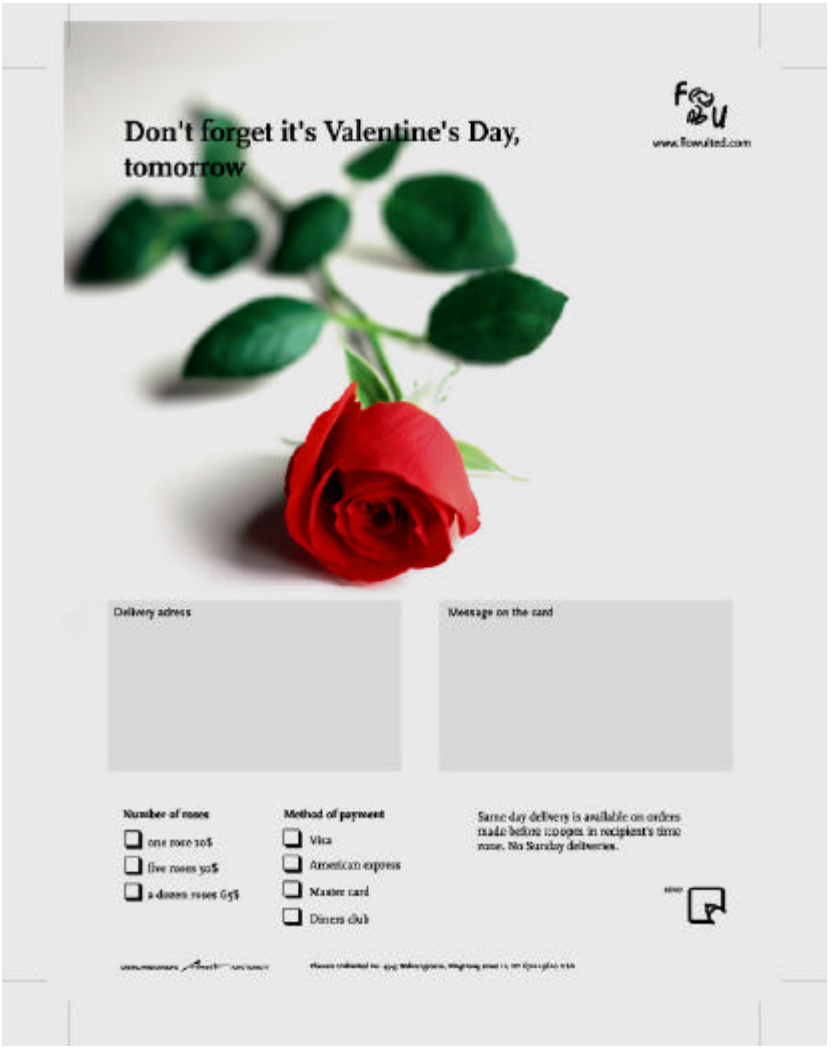


Fig.6

Svensk rätt tenderar att skydda den svagare parten i ett avtalsförhållande och har för avsikt att lägga risken på den part som har störts möjlighet att förebygga eventuella komplikationer. Ett praktiskt exempel (se fig. 6 ovan) är, om en konsument beställer en ros för leverans, och företaget levererar och fakturerar kunden för tre rosor. Företaget har dock fått in en order på tre rosor. Kunden har inte orsakat felet, utan felet har uppstått till följd av en feldefinierad mönsterbit. Mot bakgrund av det ovan anförda och att konsumenten i exemplet har betydligt sämre förutsättningar än företaget att motverka felet. Anser jag att risken för sådana fel bör läggas på företaget och inte på konsumenten. Om konsumenten sedan visa (om sparat

[135] Adlercreutz, 2000, s 52f, 66f.

originalet) att rutan för en ros har markerats på det fysiska originalet, kan vederbörande snabbt och enkelt bevisa sin oskuld.[136]

6.4.3.2 Slutsats

Avtalssituation 2 skiljer sig från ovanstående avtalssituation i den bemärkelsen att A-pappret här används av ett företag som ”orderpapper”. Bolaget erbjuder sina kunder att använda orderpappret för beställning av de produkter och tjänster som företaget saluför. Den här typen av avtal uppkommer i första hand mellan näringsidkare och konsumenter. Med tanke på näringsidkarens starka ställning och möjlighet att motverka uppkomsten av fel, är det inte rimligt att avsändaren (konsumenten) står risken för en i näringsidkarens orderpapper, feldefinierad mönsterbit. Resultatet bör därför bli att mottagaren (näringsidkaren) står risken för de fel som uppkommer i det ”egna” A-pappret. En sådan slutsats är ändamålsenligt och stärks av att lagstiftaren tenderar att skydda den svagare parten i berörda avtalsförhållanden.

6.5 Fysiskt bevis – Elektroniskt bevis

6.5.1 Problemområde

En viktig fråga i sammanhanget är, hur en domstol ska bedöma en situation då ena parten åberopar ett analogt original som bevis samtidigt som motparten åberopar ett elektroniskt original som bevis? Genom art 9 i e-handelsdirektivet och art 5 i direktivet angående elektroniska signaturer framgår tydligt att medlemsstaterna ska agera för att ett bevis som är elektroniska inte ska bedömas annorlunda enbart för att de är i elektronisk form. I svensk rätt har som tidigare omtalats rätten en skyldighet att värdera allt bevismaterial som framförts inför rätten. Därtill har UNCITRAL:s modellag art 9 (2) följande lydelse:

“information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity was maintained, to the manner in which its originator was identified, and to any other relevant factor.”

Artikeln föreskriver att information som presenteras i elektronisk form ska ges samma bevisvärde som traditionellt bevis. Vid fastställande av den elektroniska informationens bevisstyrka, ska bl.a. tekniska faktorer som säkerhet, integritet vara vägledande.

[136] Hellner Jan, Kommersiell avtalsrätt, 1993, s 91ff. Adlercreutz, 2000, s 182f. Adlercreutz Axel, Avtalsrätt ??, 1996, s 60f. Hultmark Christina, Ramberg Jan, Avtalsrätten en introduktion, 1999, s 92.

I en tvist måste en domstol pröva de framlagda bevisens styrka, oavsett om bevisen presenteras i fysisk eller elektroniks form. Bevisvärderingen måste skiljas från bevisstyrkan. Den bevisstyrka som krävs för att en omständighet ska anses bevisad beror på flera faktorer. När det gäller de elektroniska bevisen utgör bl.a. säkerhetsaspekter en tungt vägande omständighet för bevisvärdet. För avgörande av de elektroniska bevisens styrka måste rätten först avgöra deras tillförlitlighet. De kvalificerade elektroniska signaturerna anses erbjuda en mycket hög tillförlitlighet, till följd av deras höga säkerhet. Signaturerna och den säkerhetsstruktur som karakteriserar dessa avgör det värde som rätten slutligen kommer att ge den information som signerats elektronsikt.

Oavsett om de elektroniska bevisen har fått ett ”rättsligt värde”, finns det ingen garanti för att domstolarna kommer att ge dem samma värde som de traditionella pappersbevisen. Med andra ord finns det inget som hindrar domstolarna att i realiteten ge de elektroniska bevisen ett ”lägre” bevisvärde. En möjlig förklaring för en sådan risk är som tidigare berörts, den snabba IT utvecklingen. Det krävs nämligen ett stort kunnande om den moderna kommunikationstekniken för att förstå de mycket invecklade situationer som kan uppstå. En sådan kunskap och inblick kräver ständigt en kunskapsmässig ”uppdatering”. För att inte bli ”frånkörda” är det därför viktigt för dagen verksamma jurister och domare att de verkligen förstå de speciella aspekter som råder vid avtalsslutande på elektronisk väg. En bra teknisk kännedom ökar även den verksamma juristens förmåga att skapa och konstruera avtalsvillkor, som på ett ändamålsenligt sätt utnyttjar den moderna teknikens juridiska fördelar.[137]

6.5.2 Slutsats

Vad det gäller relationen fysiskt respektive elektroniskt bevis, ska en domstol inte värdera ett elektroniskt bevis annorlunda enbart för att det är i elektronisk form. De elektroniska och fysiska bevisen ska inför rätten vara berättigade till samma utgångsläge. Vilket bevisvärde som rätten ger framförda bevis, ska fastställas med hänsyn till omständigheterna i det aktuella fallet. Det finns således inget legalt stöd för att värdera elektroniska bevis, på annat sätt än traditionella bevis. Rätten ska bl.a. enligt RB 35:1 avgöra vad som är bevisat efter en prövning av allt som förekommit i målet. Viktig att observera angående denna princip är att domstolen inte är skyldig att bedöma bevisningens värde utifrån några förutbestämda kvantitativa regler. Det är rättens ”egen” inställning som ytterst avgör, de elektroniska bevisens värde. Det enda hotet mot de elektroniska bevisen är därför blott domstolens ”egna” inställning.

[137] Hultmark, 1999, s 152f. Andersen Mads Bryde, Electronic Commerse: A Challange to private Law?, 1998, s 27-32.

7 Avslutande sammanfattning

Under följande avsnitt görs en sammanfattning av arbetet. Nedanstående framställning är inte uttömmande, därför hänvisas läsaren till arbetets respektive delar för en mer riktig och allomfattande redogörelse. Sammanfattningens syfte är att ge läsaren en ”feedback” på läst arbete.

Uppsatsen består av två delar. Syftet med arbetets första del är att undersöka vilken rättsverkan som elektroniska signaturer och dokument har vid användande av modern kommunikationsteknik. Arbetets andra del utgörs av en fallstudie på Anoto AB:s elektroniska penna. Syftet är här att, utifrån ett antal fiktiva avtalssituationer, redovisa sannolika lösningar samt ge förslag på hur tekniken praktiskt kan anpassas till gällande rätt.

Handeln över Internet har ännu inte fått det genomslag som marknaden räknat med. En förklaring kan vara att säkerheten är otillräcklig. En lösning på problemet, kan finnas i en speciell teknik som möjliggör skapande av s.k. elektroniska signaturer.

De elektroniska signaturerna baseras på asymmetrisk krypteringsteknik. I kombination med ett öppet nyckelsystem (Public Key Infrastructure), kan signaturerna bl.a. garantera ett dokuments äkthet och säkra avsändarens identitet. Det öppna nyckelsystemet innehåller primärt tre parter, avsändare, mottagare och certifikatutfärdare. Varje elektronisk signatur skapas och verifieras utifrån ett unikt (elektroniskt) nyckelpar, bestående av en publik- och en privat nyckel. Avsändaren använder den privata nyckeln för att elektroniskt signera dokumentet. Mottagaren använder den publika nyckeln för att verifiera avsändarens signerade dokument. Den publika nyckeln görs allmänt tillgänglig och nyckelns koppling till den privata nyckeln garanteras av en certifikatutfärdare.

Den 1 januari i år trädde Lagen om kvalificerade elektroniska signaturer m.m. i kraft. Lagen är implementerad från EG direktivet (1999/93/EG). Den svenska lagen reglerar huvudsakligen utfärdande av s.k. kvalificerade elektroniska certifikat. Lagen syftar till att skapa en säker standard för elektroniska signaturer. De signaturer som uppfyller lagens krav, betecknas som kvalificerade. En kvalificerad elektronisk signatur ska, om det i svensk lag eller annan författning ställs krav på egenhändig underskrift eller motsvarande, anses uppfylla kraven om det är tillåtet att uppfylla kraven på elektronisk väg. Vad är det då som avgör, om en elektronisk signatur uppfyller sådana krav? För att bevara dessa frågor analyseras i kapitel 4 den traditionella underskriftens grundläggande funktioner. Även det elektroniska dokumentet analyseras: eftersom en signatur alltid förekommer tillsammans med någon sorts informationsbärare. Resultatet av analysen visar att signaturens och dokumentets primära funktioner i de flesta situationer bättre och säkrare uppfylls på elektronisk väg.

I arbetets första del, kapitel 5 diskuteras, alternativa principer och regler som en svensk domstol kan använda, när nationella regler och principer inte är direkt tillämpbara på de elektroniska signaturernas rättsliga effekt. Här behandlas United Nations Commission on International Trade Law (UNCITRAL) och principen om funktionell ekvivalens. Principen och regelverket har haft stor påverkan på flera nya lagar och regleringar. Vid tillämpning av principen om funktionell ekvivalens är regleringens bakomliggande ändamål avgörande för om en bestämmelse likväl kan infrias på elektronisk väg. Även en tillämpning av äldre praxis är en ändamålsenlig metod för vägledning. NJA 1981:853 utgör ett bra exempel på hur en svensk domstol har studerat regelns syfte istället för dess ordalydelse. Fallet visar också att fastställande av kommunikationsteknikens tillämplighet, inte alltid går att finna i modern praxis eller doktrin. Vägledning bör därför med fördel sökas även i äldre praxis. E-handelsdirektivet diskuteras också och då framförallt artikel 9. Denna artikel föreskriver att medlemsstaters lagstiftning, vars formkrav hämmar avtal från att ingås på elektronisk väg, ska upphävas eller ändras. Direktivet har emellertid endast en marginell påverkan på den svenska rätten, då denna endast inrymmer ett fåtal regler som strider mot direktivet.

I arbetets andra del görs en rättslig analys av Anotopennan. Arbetet första del fungerar här som en uppbyggnad. A-pennan är en anordning som kan skapa elektroniska signaturer och den tekniska redogörelsen för de elektroniska signaturerna är således viktig för fallstudien. Även analyserna i kapitel 4 och 5 och resultatet av dessa är av stor vikt för arbetets andra del, eftersom avsnitten behandlar kommunikationsteknikens rättsliga status.

Med en A-penna och ett speciellt A-mönstrat papper kan, med hjälp av trådlös kommunikation, information tas direkt från papper genom att överföra handskriven information med elektronisk kommunikation från person till person och från person till dator. Studien mynnar ut i två fall (fall ? och fall ??) och under varje fall analyseras två fiktiva avtalssituationer (avtalssituation 1 och 2).

Fall ?

Avsändaren skriver hela dokumentet för hand på ett från början tomt A-mönstrat papper. Under avtalssituation 1 behandlas situationen, då en avsändare med en A-penna avser att skriva x men skriver xy, ett s.k. förklaringsmisstag. Huvudregeln är att avsändaren är bunden vid sin felskrivning när mottagaren är i god tro enligt 32§ 1st AvtL. Samtliga omständigheter är viktiga för att konstatera vad mottparten med fog bör ha insett. Om rätten anser att bundenhet blir för långtgående, är ersättningsskyldighet intill det negativa kontraktsintresset också en möjlig lösning. När mottagaren är i ond tro, kan rättsföljden endera bli ogiltighet eller att viljeförklaringens egentliga avsikt ska gälla (x).

Avtalssituation 2 behandlar till skillnad från ovanstående, inte en mänsklig felskrivning, utan fel som uppstår i den digitala överföringen. Det kan tänkas att en användare skriver x, men vid den elektroniska överföringen

förvanskas innehållet till y. Här konstaterar författaren att regeln i 32 § 2st AvtL om befordringsfel inte är tillämplig. När det inte finns några regler eller principer som är direkt tillämpliga i svensk rätt, bör domstolen tillämpa internationella regler och principer. En för situationen intressant regel är art 13 i UNCITRAL:s modellag. Enligt art 13 sker överföringen av elektroniska meddelanden på avsändarens risk. Regeln bör av en domstol anses som ändamålsenlig, då den överensstämmer med den avtalsrättliga huvudregeln att en godtroende medkontrahent ska skyddas. Följden blir att den som använder en A-penna, står risken för de fel som kan uppstå vid överföringen, om mottagaren är i god tro.

Fall ??
Delar av dokumentet innehåller förtryckt text. Följande fall skiljer sig från de ovanstående, eftersom de aktuella dokumenten innehåller både förtryckt (analog och digital) text, samt möjlighet att skriva text med A-pennan. Under avtalssituation 1 kan en praktisk situation vara den att avsändaren tror sig skriva under ett avtal (inte framtaget av någon av parterna) med innehållet x, men p.g.a. att det digitala mönstret och den tryckta texten inte överensstämmer, signerar denne elektroniskt innehållet xx. På aktuell situation är varken 32 § 1st AvtL om förklaringsmisstag eller paragrafens 2st om befordringsfel tillämpbara. Däremot bör mot bakgrund av principen om funktionell ekvivalens UNCITRAL:s art 13 kunna tillämpas. Resultatet enligt art 13 blir att avsändaren står risken enligt tillitsprincipen. Ersättning till den förlitande parten kan också bli aktuellt, som alternativ till bundenhet. Författaren föreslår med tanke på de mycket ogynnsamma effekter som kan drabba avsändaren, en teknisk lösning med bekräftelse som kan ändra den ”fasta” ansvarsfördelningen mellan parterna.

Avtalssituation 2 utgår ifrån samma problem som avtalssituation 1 ovan, med den skillnaden att avsändaren skriver under ett A-papper som är distribuerat och framtaget av ett företag för försäljning av varor. Näringsidkaren har här en större möjlighet att motverka och förebygga uppkomsten av fel. Risken för eventuella fel i näringsidkarens digitala ”orderpapper”, bör således inte drabba avsändaren. Slutsatsen blir att mottagaren (näringsidkaren) står risken för de fel som eventuellt uppkommer i det ”egna” A-papperet. En sådan slutsats är ändamålsenlig och stärks av att lagstiftaren tenderar att skydda den svagare parten i berörda avtalsförhållanden.

Avslutningsvis behandlas i arbetet, de fysiska och de elektroniska bevisens rättsliga värde. Utifrån nationella och internationella regler konstateras, att de elektroniska och fysiska bevisen inför rätten ska vara berättigade till samma utgångsläge. Det finns nämligen inget legalt stöd för att värdera elektroniska bevis, på annat sätt än traditionella bevis. Slutsatsen blir att det är rättens ”egen” inställning som ytterst bestämmer, de elektroniska bevisens värde.

Litteraturförteckning

Offentligt tryck Sverige:

SOU 1996:40	Elektronisk dokumenthantering
Ds 1998:14	Digitala signaturer en teknisk och juridisk översikt
Ds 1999:73	Elektroniska signaturer
Ds 2001:13	E-handelsdirektivet – Genomförande av direktivet 2000/31/EG om vissa rättsliga aspekter på informationssamhällets tjänster
Skr. 1998/99:116	Regeringens skrivelse om kryptografi.
Prop. 1999/2000:89	Lag om konsumentskydd vid distansavtal och hemförsäljningsavtal.
Prop. 1999/2000:117	Lag om elektroniska signaturer, m m.
Statskontoret 1997:18	Svenska delen av Internet, Struktur, säkerhet och regler (rapport). Stockholm 1997.
Statskontoret 2000:40	Elektroniska signaturer och elektronisk identifiering för myndigheters e-tjänster (rapport), Stockholm 2000.
SFS 1992:1119	Lag (1992:1119) om teknisk kontroll

Förslag till lag om ändring i konsumentkreditlagen (1992:820)

Offentligt tryck Europa:

Direktivet 1999/93/EG	Europaparlamentets och rådets direktiv om ett gemenskapsramverk för elektroniska signaturer.
KOM (1997) 157 slutlig.	Meddelande från Kommissionen till Rådet, Europaparlamentet, Ekonomiska och Sociala kommittén och Regionkommittén. ”Ett europeiskt initiativ inom elektronisk handel”
KOM(1998) 297 slutlig.	Förslag till europaparlamentet och rådets direktiv om en gemensam ram för elektroniska signaturer

EESSI	Final Report of the EESSI Expert Team 1999-07-20.
UNCITRAL	Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)

Litteratur:

Adlercreutz Axel	Avtalsrätt ?, 11 uppl. Juristförlaget i Lund, Lund 2000.
Adlercreutz Axel	Avtalsrätt ??, 4 Uppl. Juristförlaget i Lund, Lund 1996.
Allén Sture	Svensk Ordbok, 2 Uppl. Språkdata vid Göteborgs Universitet, Esselte Studium AB, Norstedts Tryckeri, Stockholm 1988.
Andersen Mads Bryde	Electronic Commerse: A Challange to private Law? Roma 1998
Andersen Mads Bryde	Grundlæggende aftaleret, 1 Uppl. Christian Ejler´s Forlag, København 1997.
Aversten David	Digitala signaturer och ansvarsproblem, Institutet för rättsinformatik Stockholms universitet, IRI-Serien 1998:2.
Baum Michael Ford Warwick	Secure Electronic Commerce. Building the Infrastructure for Digital Signatures and Encryption, 2 Uppl. New Jersey 2000.
Bernitz Ulf	Standardavtalsrätt, 6 Uppl. Marknadsrättsförlaget AB, Stockholm 1993.
Edwards Lilian Waelde Charlotte	Law & the Internet regulating cyber-space, Northwestern University Press, Illinois 1997.
Einersen Eivind	Elektronisk aftale- & bevisret, Jurist-og Økonomforbundet Forlag, Charlottenlund 1992.
Grönfors Kurt	Avtalslagen, 3 uppl. Norstedts Förlag AB, Lund 1995.
Hellner Jan	Kommersiell avtalsrätt, 4 Uppl. Stiftelsen Juristförlaget vid Stockholms universitet, Stockholm 1993.

Hellner Jan Johansson Svante	Skadeståndsrätt, 6 Uppl. Norstedts Juridik AB, Göteborg 2000.
Hiselius Patrik	Elektroniska avtalsslut med signatur (EDI och smartkort), Institutet för rättsinformatik Stockholms universitet, IRI-rapport 1989:2.
Hultmark Christina	Elektronisk handel och avtalsrätt, 1 Uppl. Norstedts Juridik AB, Stockholm 1998.
Hultmark Christina Ramberg Jan	Avtalsrätten en introduktion, 1 Uppl. Norstedts Juridik AB, Stockholm 1999.
Janson Ingemar	Den elektroniska marknadsplatsen, Avtals-, köp- och bevisrättsliga aspekter, Institutet för rättsinformatik Stockholms universitet, IRI-rapport 1997:1
Lehrberg Bert	Moderna Betalningsformer, 2 Uppl. Norstedts Juridik AB, Stockholm 1999.
Lindberg Agne	Elektroniska originaldokument och elektroniska signatur, rättsliga konsekvenser av papperslös dokumenthantering. Institutet för rättsinformatik Stockholms universitet, IRI-rapport 1997:7
Lindberg Agne Westman Daniel	Praktisk IT-rätt, 2 Uppl. Norstedts Juridik, Stockholm 1999.
Lloyd Ian	Legal Barriers to Electronic Contracts: Formal Requirements and Digital Signatures cyberspace, Edwards Lilian, Waelde Charlotte, Law & the Internet regulating cyber-space, Northwestern University Press, Illinois 1997.
Martinger Sven	Norstedts Juridiska Ordbok, Juridik från A till Ö. 2 UppL. Norstedts Förlag, Stockholm 1989
Winberg Gustav	Elektroniska betalningssystem på Internet, Om teknisk säkerhet och juridisk osäkerhet, Institutet för rättsinformatik Stockholms universitet, IRI-rapport 1997:3.

Artiklar:

Affärsvärlden	2000-09-27

Boss Amelia H — Electronic commerce and the symbiotic relationship between international and domestic law reform, Tulane law review 1998:1931.

Hultmark — European and U.S. perspective on electronic documents and electronic signatures, Tulane European & Civil Law Forum, Volume 14, 1999.

Övrigt:

Telefonintervju med Bo Bergner på PTS, 2000-10-18.

Telefonintervju med Gunnar Lindström på SWEDAC, 2001-03-16.

Anoto dokument — Dokumentet är utarbetat av Per Furberg på uppdrag av Anoto AB. Dokumentet innehåller sekretessbelagt information, som författaren tagit del av i förtroende.

http://www.anoto.com

http://www.etsi.org

http://www.ict.etsi.org/eessi/EESSI-homepage.htm

http://www.uncitral.org

http://www.swedac.org

Rättsfallsförteckning

NJA 1981:853

NJA 1986:495

NJA 1987:692

NJA 1991:3